VIDEO CALLING SYSTEM USING BIOMETRIC REMOTE AUTHENTICATION

G S Akhil, Chole Manjunath, V. Ashuthosh
Bachelor of Engineering, BNMIT, Bangalore, India.

ABSTRACT

Video calling is one of the widely used method of communication. The proposed system supports three tier secure video calling system. The proposed work describes about a video calling system that uses biometric authentication. In this authentication system we are using three security mechanisms, first is user id and password, second is the fingerprint scanning and third is face recognition system. For this system the user id and password is created and stored in the database, fingerprints and images are captured and also stored in database, and the entire database is on to the server where every client’s data is verified, so when two users want to participate in the video conference, they have to enter their user id, password and fingerprint and face the camera to take a live image. The three attributes of the users are verified with the ones stored in the database, if there is a positive authentication from both sides then only the video conference can take place successfully. If the authentication fails at any one side video calling will not take place.

Key words: video calling, biometric, fingerprints, images, database, authentication.


1. INTRODUCTION

In today’s corporate world, video calling is increasingly becoming popular. In oldenday’s people in the corporate world physically attended the meetings. As it was time consuming and we all know that time is very important in corporate world. As the technology in communication progressed different communication techniques were introduced. The most popular of the technique was video calling. Initially it was designed for one on one interaction. But eventually it was used for teleconferencing in corporate world. In a corporate environment, during video conferencing it is sometimes imperative to make sure you are talking to right person. Though there are many methods like PIN numbers or swipe cards but they are transferable. To avoid such malpractices this remote authentication method is proposed.

1.1. Problem Statement

The problem to be solved here is to identify or allow the authenticated persons to participate in the teleconferencing.
1.2. Objective
To design and develop a system that provides three tier security to the teleconference.

2. LITERATURE SURVEY
Software System’s invention is a major breakthrough in today’s technology and in many industries, government and critical infrastructure are depending on it. It has made most of the day-to-day life things easy. However, that poses some vulnerabilities. Of these, threats through cyber-attacks are a major and critical concern. To access the system, password is the minimum and required criteria. Notwithstanding these security enhancements, there are still attacks and even the complex passwords are not able to stop these attacks. So, negative authentication has been introduced in order to reduce the cyber-attacks.

2.1. Remote Authentication
In single-server authentication process, the ample of network services has been used by the remote user. In these servers, the user has to register his identity and has to generate a password. However, it is a monotonous process. In order to speed up the things, later a multi-server authentication scheme has been proposed. Yet it is not the optimal solution and it has some serious issues such as insecure against cryptographic attacks. In order to meet these challenges, Elliptic Curve Cryptosystems has been proposed. It is efficient and a secure multi-server authentication scheme based on biometrics. This scheme provides a strong authentication function for the user. It also provides a strong key agreement function for perfect forward secrecy. So, the proposed scheme has a strong security and difficult to decipher. Also, it has the efficiency of the computations enhanced which is more suitable for distributed multi-server network environments.

Later, a vigorous biometrics based multi-server authentication has been proposed. It is based on the key agreement scheme. However, this scheme is susceptible to offline password attack. But, later an improved scheme has arrived. This scheme has four phases such as server registration phase, user registration phase, authenticated key agreement phase, and password and biometrics update phase [7]. RADIUS - Radius Authentication Dial-In Service is a networking protocol. It has been installed in the network. It is mainly used for the remote users who actually access the network. Since RADIUS is a distributed service, it provides the consolidated management of access control for the user and protection. It also secures and husband the Local Area Network (Wlan), Virtual Private Network (Vpn) [8].

2.2. Video Conference
In video enabled conferences, there are two distinct ways. First is Point-to-Point video conferencing, where the meeting is connected between person or group to another person or group. The physical components such as microphone, camera are used to enable the meeting either in the desktops or laptops. Multi-point Video Conferencing is the second form of video conferencing where the three or more locations are connected. All the participants have a chance to see and hear each other and any content can be shared. Here the central, independent program is used to process the digital information streams of voice, video and content. The program re-sends the combined individual participant’s video and voice traffic back to the meeting participants in the form of real-time audio and video image. It does have a option of “audio only”, whenever the individual wishes to do so. Images are classified as “Active Speaker” or “Continuous Presence”. In Active Speaker mode, only the speaker who is speaking is shown on the screen at any time. Whereas in Continuous Presence, image has been divided into number of different areas by the bridge. The speaking person is shown in larger area when compared to others. It allows the interaction between the participants in the meeting.

2.3. Proposed System
Dual authentication mechanism is used in the proposed system to provide robust authentication. First process is the Fingerprint Scanning and second is the face recognition mechanism. Integrating these two
authentication mechanism it is highly impossible to fake their identity and break into the system. First, the user has to register their fingerprints and images has to be captured. Then these information is stored into the database. When the user wants to participate in the video conference, they need to go through the authentication process. First, they have to enter their fingerprint and if it successful, then the user face recognition process takes the image of the user alive i.e., in the real time. If these two process is successful to the user, then the user is eligible to participate in the video conference. This goes true for every user, and if they are successful, then only conference begins.

2.4. Advantages of the Proposed System
- Authentication of the user is entirely based on the biometric system like face and fingerprint.
- Proxy User is unlikely to login and finds it impossible.
- Misuse of resource is not possible.
- No need to remember password or id.
- Communication is entirely secure in the network.

3. BLOCK DIAGRAM

![Figure 1 Block diagram](image-url)
The above block diagram consists of three sections Client A, Web server and Client B, both the clients consists of similar hardware and software section which interact through the server simultaneously as well as parallel on various situations. The hardware components on client side include web camera, fingerprint scanner module and speaker and mic set.

3.1. Working Principle
Initially user data base will be created and stored in central server. The user data base consists of many parameters like user id, password, fingerprint and image of the user along with name and other personal details. When one party wants to have discussion with other party who is at very distant location then the initiating person will send an invite to the other person with details about the meeting.

Before actual meeting starts users will enter their credentials like fingerprint also take image using web camera. Both fingerprint and image will be authenticated using secure encrypted communication to server. After authentication successful encrypted communication path will be used for the meeting.

First the image will be taken by camera and the image is encrypted and sent to server for authentication with image stored in server. Also the fingerprint sample will captured using fingerprint scanner and sent to server after encryption. If both image and fingerprint are matched then the server will establish encrypted secure communication path between users for meeting.

4. BIOMETRICS
Biometrics refers to the distinct anatomical and behavioral characteristics of humans. Some of the anatomical features are fingerprint, face, iris etc. and an example for behavioral characteristic is speech. These features differ from person to person. Biometric authentication is used in today’s world as a form of identification and access control. The main objectives of biometrics are better security, higher efficiency and better accountability [1]. In this work two types of biometrics are used. They are:-

- Face Recognition
- Fingerprint Recognition

4.1. Face Recognition
Face recognition is based on geometric features of face. Initially the marker points (e.g. face, ears, eyes, nose etc.) were used for face recognition. But it had a drawback: the accurate measurement of the marker points was difficult and there were high chances of face being not recognized. So Eigen faces method was developed. In this work we have used Eigen faces method. In this method Eigen faces are generated using a mathematical process called principle component analysis. First the images of the face is captured at different angles and stored which acts as a sample set during comparison process. The images are always stored in matrix form. Here for sample set all the images will be stored in single set. Using principle component analysis the mean of the images is found out and stored in the database. The mean of the image is subtracted from each original images of sample set. After this the eigenvectors and eigen values of the covariance of sample set matrix are calculated and stored in the database. Each eigenvector has same dimensionality as the original image. The eigenvectors of the covariance matrix are called Eigen faces.

During face recognition process the image is captured and its eigenvectors and Eigen faces calculated. After calculating the eigenvectors and Eigen faces it is compared with those stored in the database and if it matches then face recognition is successful else face is not recognized.

The flowcharts of face detection and recognition are shown Figure 2. They both are almost similar. In face detection once the face is detected the image of the face is captured and stored in database and during face recognition the face image is captured and compared with the stored image and if they match then face is recognized.
4.2. Fingerprint Recognition

Fingerprint recognition refers to the method of identifying two similar human fingerprints. Fingerprint is also a type of biometric. Fingerprints can also be classified into three types. They are arch, whorl and loop. It is classified so on the basis of their appearance. In fingerprint recognition there are three main processes involved. They are:

- **Enrollment**: User enrollment is a process that is responsible for registering individuals in the biometric system storage. During the enrollment process, the fingerprint of a person is first captured by a fingerprint scanner which is used as sample. A feature extractor is used to generate the unique feature set of the fingerprint. A template is created for this feature set. The template is stored in the system with other information about the person such as name, gender, etc.

- **Verification**: The verification process is responsible for confirming the claim of identity of the person. During the recognition process, an identifier of the person (such as username or PIN) is provided to claim an identity; the fingerprint scanner captures the characteristic of the fingerprint and converts it to a sample, which is further processed by the feature extraction module to generate a feature set. The resulting feature set is fed to the matcher, where it is compared against the enrollment template of that person (fetched from the system storage based on the person’s identifier). The verification process produces a match/non-match decision.

![Flowcharts](image)
Identification : In the identification process, the system compares the feature set extracted from the captured fingerprint sample against the templates of all people in the system storage; the output is a candidate list that may be empty if no match is found or contain one identifier of matching enrollment templates.[6]

There are many different fingerprint scanner available in market such as optical fingerprint scanner, solid state fingerprint scanner and ultra-sound fingerprint scanner. We have made use of an optical scanner as it is low cost and effective. It works on the principle of total internal reflection.

5. IMPLEMENTATION
In order to implement the proposed system the hardware requirements are:
- Raspberry-pi 2 development board (any other similar board)
- Digital webcam
- Fingerprint scanner

The required hardware components are shown in the Figure 4. Raspberry pi is a small computer on chip. It performs all the operation that a normal computer usually does. Its main advantage is its small compact size. It is driven by a Linux operating system called as Rasp bean. It also has a powerful digital
signal processor which is why we have chosen Raspberry pi for our system. It can be programmed using python, C and C++.

![Raspberry Pi Model B+](image)

**Figure 4** Hardware Component.

R305 fingerprint scanner shown in the figure is an optical scanner. It contains a digital signal processor used for processing the fingerprints. It has a character file size of 256 bytes i.e. it can store up to 256 fingerprints. It also has a very low false acceptance rate and high false rejection rate.

Any webcam with inbuilt mic and good resolution can be used. For this system we have used a Logitech webcam as it is easy to install its drivers into a Linux system. It is used mainly for face detection and video calling.

The system architecture as shown in the figure is integration of all the hardware and software mentioned above. The raspberry pi, fingerprint scanner and webcam are installed at the clients end. When a server is created and a request for video calling is sent to client from server and if the client is a new user then the client needs to create a user id and password. Once this is done the system asks for the registration of client’s fingerprint. The fingerprint is processed, its features extracted and stored in the database. Some random images of the client’s face is captured through webcam, processed, its Eigen values calculated and stored in the database.
If the client is a registered user then the client needs to enter his/her user id and password. Once this is verified the clients fingerprint is verified with the fingerprint stored in the database. The next step involves verification of the face with the stored image in the database. If all the above three verification is successful then a browser opens and the video calling starts.

RESULTS

![System Architecture](image)

**Figure 5** System Architecture

If the client is a registered user then the client needs to enter his/her user id and password. Once this is verified the clients fingerprint is verified with the fingerprint stored in the database. The next step involves verification of the face with the stored image in the database. If all the above three verification is successful then a browser opens and the video calling starts.

**Figure 6**

**Figure 6 (a)** Refers to overall hardware view of Raspberry-Pi, Fingerprint Module and Camera.

**Figure 6 (b)** Refers to the registration of fingerprints of the two clients at the server end.
Figure 6 (c) Refers to the successful of the fingerprint and face recognition at client side-1.

Figure 6 (d) Refers to the successful of the fingerprint and face recognition at client side-2.

Figure 6 (e) Refers to the transmission of the data packets of client-1 to client-2.

Figure 6 (f) Refers to the transmission of the data packets of client-2 to client-1.
CONCLUSION
Biometric Authentication has been thriving into our day-to-day lives as they provide robust and secured authentication from the threats and malware activities. So, there are tremendous advantages from biometric signals as they are unique and distinct from person to person. Thus the integrity of the biometric signals should be implemented into the practical applications.

However, working of the internal procedure and their results in the proposed system are inscrutable to human visual system, it can resist the signal distortions and protect from the attacks. Empirical evaluation and detailed security analysis enlightens the proposed system’s execution in terms of security.

In future, the biometric data can be used in the new generation of lie detectors. It uses the artificial intelligence for support of decision making and new paradigms. Synthetic biometric signals can be used in the Cancelable Biometrics where the security is provided through the deformed biometric data. Other biometric signal like iris, voice should be examined and should be further integrated with face and fingerprint to provide rigid and high end security. They can be used in the mobile phones and personal computers which has high confidential data.

REFERENCE

