ASIAN JOURNAL OF INFORMATION TECHNOLOGY

MEDWELL PUBLICATIONS

Secure Authentication in Cloud Computing with Biometric Recognition

Prabu Sevugan and Tripathi Ashish Ashok
Vellore Institute of Technology, Vellore, India

Key words: Security through encrypted data, multistage biometric fingerprint-iris-face recognition, cloudserver

Corresponding Author:
Prabu Sevugan
Vellore Institute of Technology, Vellore, India

Page No.: 118-121
Volume: 19, Issue 7, 2020
ISSN: 1682-3915
Asian Journal of Information Technology

Abstract: Security of the data on the cloud is the main target for intruders to fetch protected data. Everyone wants to keep their data safe and to store at secure place. User's neither want to keep their data leaked nor to lose that's why cloud storage is the best option to go for. But, there are many talks for the leaked data of celebrity or any organization's top secret file. We can go for the authentication which will have several stages before giving of verified user and also the data which can be secured with Encryption techniques. In this study, we are going to introduce a system which can give various stages of authentication mechanism and after that data will be encrypted with Triple-DES. Main concern is given for secure authentication. So, the mechanism will work by using biometric recognition like this: Username and Password is mandatory stage, after that it will go for the respective user Cellphone number to send text message (OTP). When it is verified it will ask for the face, Iris and fingerprint image so that it can verify the same particular user who did the registration. User is authenticated and led to the storage area when they can operate their data like upload and download by encrypting and decrypting, respectively.

INTRODUCTION

The transfer of data from local to web application is massive. Daily millions of user are there to move their data on cloud so that it can available globally to themselves without worrying about loss of data on their local drive. Their also have been sharing of sensitive data through cloud services and this has been possible only through the upgrade seen in the software and their depending platform.

There are many users who wants to keep their sensitive data at a location where only they can see and also can be shared with few person. Due to increase in sharing sensitive data through cloud there is also increase in attacks on the user's account for exploiting data due to lack of more secure authentication. Users want to keep their data digitally instead of physical form. Nowadays, we can also see that users are more interested in graphical use of technology and which gives more security through hardware. To give security to user's stored data on cloud. We want to propose one setup of system which can help those users who wants to store and share their top secret information of their organization. This will help them to make their data sharable securely and speedily with others who are in different location. It is quite trending to add biometric recognition for making authentication without worrying about intruders[1]. So, this setup will have various stages of authentication: Face, Iris and Finger

print recognition. These stages will have the verification by using proper algorithm with the existing user's data for the authenticating to their data.

Literature survey

Face recognition using Facial Symmetry-Avinash Kumar Singh, G.C. Nandi: Apart from fingerprint, facial recognition is the very next option that everyone goes for. It is mostly used in Authentication for security purpose, for having interaction with Humanoid Robot and many more. The symmetry in human face is vertical and that is why that feature is used for giving facial recognition approach. Facial recognition approach also goes for verification of a user.

Face recognition: features versus templates-R. Brunelli, T. Poggio: They have used two types of algorithm for comparing the facial recognition. First is based on geometry of facial features like length and width of nose, shape of chin, etc. and the second one is based on matching done by mostly grey-level templates. By trying both algorithm, the result was somewhat apart from each other. Grey-level templates was giving perfect result in recognition compared to the other one.

Biometric authentication using mouse and eye movement data-Jamison Rose, Yudong Liu, Ahmed Awad: Here, they have shown that alone one biometric recognition less powerful compared to if we combine them and using it. Users data are collected by extracting their featured and by fusing one or more biometric approach the security will be more powerful and the results will be better. Also, the approach with fusing will be more useful when that particular device will be manufactured.

Using facial symmetry to handle pose variations in real-world 3D face recognition

Georgios Passalis Panagiotis Perakis Theoharis Theoharis Ioannis A. Kakadiaris: In this study, they are using a detector which will click the image when the pose is estimated. The facial scan will be started with the automatic detector for feature and posed detection. Everytime user will have different pose and the image will be scanned according to estimated pose. This will result in the image with proper recognition using biometric signature based on wavelet.

Is there a connection between face symmetry and face recognition?-Josh Harguess, J.K. Aggarwal: This study shows that the symmetry of the face gives more advantage for the accuracy in recognition. There's much difference in the symmetry of the face in men and women. Full face with symmetrical feature leads to more accurate results in recognition. So, half-faced sometimes play higher role in recognition compared to full face as it will not have symmetrical face for all the user.

Biometric Authentication and Data Security in Cloud Computing-G.L.Masala, P. Ruiu, A. Brunetti, O. Terzo, E. Grosso: They described how to make a cloud platform secure with biometric and data-security. Also, proposed to make a whole system which includes handling of network protocols, Biometric devices for the authentication, a separate server for authentication and VPN. Their system gives high level of protection by using data distribution and also use of biometric authentication.

Existing system: As of recent days there has been increase in number of intruders where we can see many organizations are facing leaks in their Top Secret data and user's sensitive data which are stored on cloud. Use of cloud computing also increased because of ease in availability of data and organization's profit for not maintaining data physically everywhere instead they will use the network for accessing their data. Now they will have one main concern with this is to make that account is not hacked or exploitation of data. Previously also there has been many solutions regarding the authentication done in a secure way like to use data fragmentation, distributed storage and intruder prevention through cryptography.

In our system there will multistage of authentication which can verify through proper and efficient algorithm. Also, the files which will be uploaded and their personal information will be encrypted using encryption algorithm. These many encryption algorithm and multi stage authentication containing Iris, face and finger-print recognition will led to safe and efficient authentication for cloud servers.

Advantages:

- Security mechanism for authentication in multistage
- Encrypted information and files
- Easy to create system network

Disadvantages:

- More possibility for advancement due to upgrade in technology for hardware and software
- Enhanced encryption can be used
- Advanced hardware for recognition is required
- Private network is required for utilizing protocols which are already made

MATERIALS AND METHODS

Proposed system: We will be implementing a system with multistage mechanism for authentication and securing files with encryption techniques. There will be usage of both software and hardware for completion of

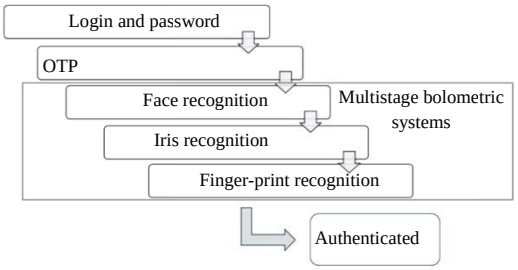

Fig. 1: Authentication flow

this system. This design of multilevel authentication will initiate from textual 4-digit number message for authentication on user's respective mobile number and with successful verification it will lead to facial, iris and finger-print recognition with GLCM algorithm. When this biometric recognition verifies the user with the data points stored on the server it will authenticate that particular user and will be redirected to their stored data on the cloud server (Fig. 1).

Though using a mobile number for the message is the most common way for authentication but then also there will be no scope of hacking done on recognition done on iris and facial as they both are done in real time and that too with the real sense camera. The deep points and feature extracted with the help of GLCM algorithm of the image taken by the camera during the recognition. This all will be happening with the client's side application. The application on the client's desktop will be responsible for authenticating and registering a user for the access of the cloud server to operate their own data.

We don't need to implement a new private network if there already exists many advanced protocols for making a virtual private network. We shall be focusing for giving access to the server more securely.

Algorithms used: Firstly, registration is done for a user where there personal details is asked like their name, cell-phone number (for sending OTP), email-ID, etc. and here also there is possibility of user's personal data getting exploited. So, we will use NOMAD for encrypting all those details before storing it on the server. If our data get exposed to the hacker then also this encryption technique will tackle them before letting them accessing to user's account details.

Secondly, after logging in the user can able to access their own storage. The files which they want to upload will be first encrypted using Triple-DES encryption algorithm and then it will be go for uploading to the Server-storage. This files will be encrypted and decrypted with specific keys and these keys will be generated by using algorithm named Blowfish.

All these algorithms are needed for encryption with some advancements. Triple-DES will be having many other variations which we can use for robust encryption. Anyhow intruder can reach to these files when they will first pass through the authentication mechanism which is more likely not that much easy[2].

Finally, there's algorithm for getting the verification of scanned images for the recognition through Biometric. GLCM is an algorithm which helps to get key features of the image after converting it to the Grey scale image from the actual RGB image[3]. The GLCM is a tabulation of how often different combinations of pixel brightness values occur in an image[3]. This will help our system to make an efficient verification technique as user don't have to worry for the lighting conditions as eventually it is going to be in grey-scale and from that we can take out the feature points from the texture which will be helpful for the comparison during the authentication.

RESULTS AND DISCUSSION

Implementation: We have implemented this system by using JAVA. As this should be interfaced with internet and it will be easy to implement. MySQL is used for storing the encrypted personal details and will have server storage connected with the server for keeping the encrypted files. It's quite different compared to MATLAB as efficiency is not that much on JAVA but made best possibility to have more similarity index. Here, today's advanced camera also play an important role as it will take more details and texture of the person's face and that will help algorithm to work at its best for quality measures. The database will be having GUI interfaced through PHP for easy usage for the admin. Algorithms will not take up that much RAM so that it can send and receive the response more efficiently as it is connected with the internet (Fig. 2).

Triple-DES Encryption is used for encrypting and decrypting whichever files are uploaded and downloaded, respectively. It is an advancement over DES encryption and it is not weaker while facing the Brute-Force attack. Files are encrypted and stored on the Storage while downloading first the file will be downloaded on the user's system and then it will be decrypted because it will take much less compared to do it on the server and also have high security risk as there may be intrusion in the network. In our system there's not only authentication which is taken care of, there has also been taken care of files which will be uploaded. This will be done on our own cloud as no other cloud services will allow us to do our security patch over their own security protocols. Response time will be less as most of the verification process will be done on the user's side[1]. If we send the image recognition algorithm on the server then first the image has to be send on the server and it will verify with the existing image, then it will give the result and this will take an immense amount of time. To reduce time the

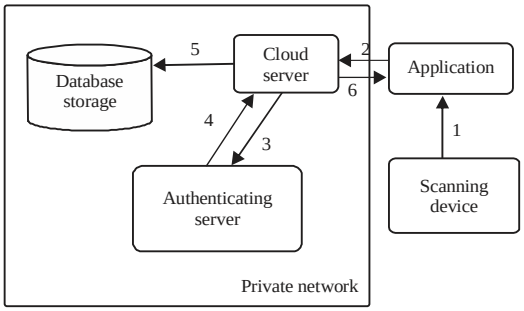

Fig. 2: System Implementation, (1) Taking image as input multistage verfication, (2) Sending data to server, (3) Request for verification, (4) Response for verification, (5) Gives access to storage with cryptorgaphy and (6) Operating data

algorithm will on the user's side application, i.e., the application has to be installed on the system before accessing the services of the cloud. This application will be responsible for the verification of the private network and the user's image capturing which is Iris, face and finger-print.

By using application and GLCM algorithm, all the image processing stages will be done on the user's side like taking out the noise from the image, converting to grey-scale, segmenting the image into pixels and digitize it so that algorithm can transform those shades of the pixel into tabulation form[3]. Those numeric digits from the table will be responsible for the similarity indexes[4]. It will give information regarding the pixel's positions which will have same grey levels. The device should also contain more storage and better RAM for all this process.

An imaging device is required for the fingerprint and Iris recognition as that same image is responsible for the verification and registration on the database. This will also be very important for the completion of a system with multistage authentication[5]. Whenever, there will be registration of user is done, first it will fetch everything like the details and image data points means grey level and then those data will be send to the server for storing, through the private network.

Biometric recognition: In our system the very first phase is to give username and password which leads to textual message on their respective mobile number for the OTP. After it is verified, it is given for the image capturing phase for the face, Iris and Finger-print. Then it will lead to the phase where actual verification of the user is done. But, before that the image processing takes place on client side. This is also an advancement as no normal user can try to attack the system. It will require a system which only those user will keep who wants their Top Secret files away from others without revealing their identity. When the algorithm executes on the image it will execute as below:

- Noise of the image is taken out for unwanted feature extraction
- Image will be converted to digitize format
- That same will be converted to grey scale
- Image will be divided in certain number of exact grids along with tagging them
- Each grid shade will be taken as the information and tabulation will be created

This information is passed on to the server for the storage and registering/verifying the user. This information will contain the texture of the image. The number of grids will be same as the number of grey-level shades. It is the way for fetching out the texture features in the form of the numeric information.

CONCLUSION

The authentication with multistage gives secure verification of user by taking face, iris and fingerprint recognition and data security using techniques in encryption. The authentication will make sure to make the access for that particular user only and that user can get storage for data. This system can be used in various fields like passport, banking, government and corporate offices, storing top secret files of the organization, etc. This system advances with the biometric authentication in various stages over the conventional method of only fingerprint. A further improvement of the system can be advance in algorithm with getting more features of the image and also the image taking device. The user side software can also be changed to the web application for making it completely server based.

REFERENCES

01. Castiglione, A., K.K.R. Choo, M. Nappi and F. Narducci, 2017. Biometrics in the cloud: Challenges and research opportunities. IEEE. Cloud Comput., 4: 12-17.
02. Verma, A., P. Guha and S. Mishra, 2016. Comparative study of different cryptographic algorithms. Intl. J. Emerging Trends Technol. Comput. Sci. IJETTCS., 5: 58-63.
03. Hall-Beyer, M., 2000. GLCM texture: A tutorial V. 3.0 March 2017. University of Calgary, Calgary, Canada. https://prism.ucalgary.ca/handle/1880/51900
04. Hamza, R.M. and T.A. Al-Assadi, 2012. Genetic algorithm to find optimal GLCM features. Master Thesis, Department of Computer Science College of Information Technology Australia, USA.
05. Masala, G.L., P. Ruiu and E. Grosso, 2018. Biometric Authentication and Data Security in Cloud Computing. In: Computer and Network Security Essentials, Daimi K. (Ed.). Springer, Berlin, Germany, ISBN: 978-3-319-58423-2, pp: 337-353.