AN EFFICIENT AND PRIVACY PRESERVING MULTIMODAL BIOMETRIC IDENTIFICATION IN CLOUD COMPUTING

[1]SURYA K,
[2]M. GOPIKRISHNAN

[1,2] PRATHYUSHA ENGINEERING COLLEGE
ARANVOYAL KUPPAM,
POONAMALLEE,
TIRUVALLUR ROAD,
TIRUVALLUR-602025

***Abstract* — Security from different options will give a high preservation model. There are more security schemes in terms namely biometric, face detection, eye based security and password types. Each one has unique terms, here we have used the all models together for bringing the system more secure. We named it as multimodal biometric identification. We have also taken the cloud computing platform for checking the identification before it comes to usage. Cloud has more security but it does not have more security on identification. For reducing this gape, we have used this all schemes together in a single place, it registration based verification. We have created the application for this system, in that we have to register face, fingerprint, and eye contact as well as. Only after the registration, the system will use to access the cloud platform in further, finally, we compared our system with the existing model to check the security level. We have achieved the result on the comparison.**

Keywords — ***Cloud security, Identification, registration, Administration, Database management***

I. INTRODUCTION

Biometric is the main area for allowing people for access. In this situation, more people were using this system as illegal. They are using fake identification to access. If it single type of identification like a fingerprint, etc. then they are simply printing the finger area as a duplicate to use the access as illegal. So for reducing this fraudster, we are producing the multi-level security to cloud computing region. The fraudster will do the duplicate security scheme for getting access like the original person. Many areas are struggling because of this duplication, if someone is securing the system by their face, then hackers are doing the same face cut image in front of the camera for making the system bad. Cloud computing has many possibilities and options, we can choose any one of it but come to accessing we have to choose the best identification which is providing the service we want. Now a day's number of identification does not have security platform for securing the user from the fraudster. More information will be displayed openly to the company as well as the intermediate person that is trying to hack the person as he wants. There are some attacks which are purely aiming to access the system. Which is like an agent, feedback provider and so on. Validating the attacks and setting up the application to the next level. There are some system will not be noticed by the administrator in that point of view, our proposed system will come forward to check the access and the malicious behavior, it will be like a gateway and shield. The area which was used in separation will have some rules and regulations in those cases we implemented the secure intermediate for auditing. It is very important for the people and they do not have any idea about the detection methods. Wherever peoples crowd is high, we can expect the dangers of a malicious person in any way. Understanding this situation, we have proposed the multi-level identification system for the person who is willing to access the cloud. This identification scheme will reduce the malicious person.

II. Related Work

Numerous research works are proposed by various researchers for the attendance management system. Attendance is one of the primary management systems that need to be present in all educational institutions and organizations for keeping track of the staffs and students. In [1], the author has presented an elaborate survey on various developments in fingerprint sensor technologies with respect to their strengths and weaknesses. Related issues on technology, underlying physics, Liveness detection, resolution, performance assessment, limitations, and standardization are discussed. Eczema [2], has proposed an attendance management system that made use of fingerprint authentication for tracking the attendance. The system was standalone and handheld which was not connected to any computer systems. She observed that the use of fingerprint attendance systems without connection to any computer systems performed better when compared to other systems that made use of computers for connection. A barcode based attendance system was designed by Lakshmi Sudha [3], that made use of barcodes in the identity cards instead of fingerprints for attendance. The system made use of a barcode scanner. The barcode consisted of a unique number that was registered for each and every student. A display screen was also included in the system that showed whether the student has marked his attendance or not. Tabassam Nawaz [4], developed an academic attendance system by making use of fingerprint detection. He stated that the entire process was automated while using this system. The need for maintaining files and records were eradicated as the process was entirely automated. The system made use of fingerprint sensors and LCD screens for tracking the attendance in the academic institutions. In [5], a fingerprint-based attendance system was designed that was intended to eradicate the fraudulent issues in attendance systems. Most of the people are likely to cheat by keeping attendance of someone else in their absence. As the fingerprint of each and every person is unique, the system has used the fingerprint sensor attendance system [6], [7], [8], [9], [10].

III. PROPOSED SYSTEM

We have explained our security terms step by step with diagrammatic views and also discussed our application based security

Cloud-based Application

We have created the software application for securing the cart, information of the user and so on. This scheme will act like a security application which has more options that are discussed in result evaluation, every information will be auditing by the identification before it gets to the user side. This scheme will have methods like a request with permission or analyzing the person before accepting. Some hackers will install the virus filled an application to the computer or to the network connected server that system will act as a hacker for a long time without knowing us. In these cases, our proposed system will detect the fake application and removing it completely from the system. It is the concept which is used to secure the user from unauthorized access or unauthorized user. Malicious will return every time when a user online. On that time we no need afraid of. This system of method will reduce and delete the malicious information from the hackers. There are more options were developed in this paper on comparing the previous paper. We have achieved the system development. Our system will demonstrate everything about cloud computing identification security.

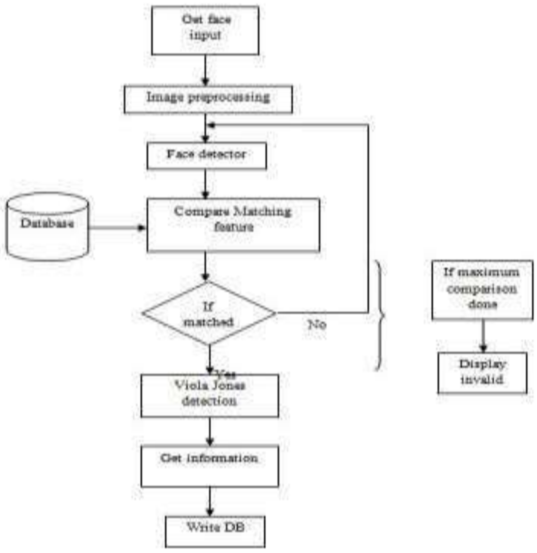


Fig. 1 Architecture Model

Our proposed system will save the identification information on the database by using the biometric device on three separations. After saving all the database, there will be a cross check for the details. Then identification is checked as per the fig. 1, if the data is matching the database then it gives access the user, if user's data is not matching the database then it will again go to image processing for registration of the identifications. This flow can be used in the future for enhancement and comparison.

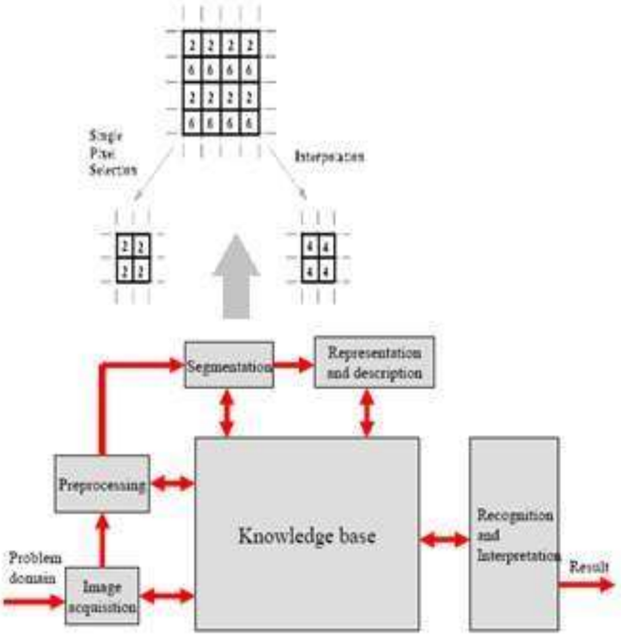


Fig. 2 Image processing

Image Processing

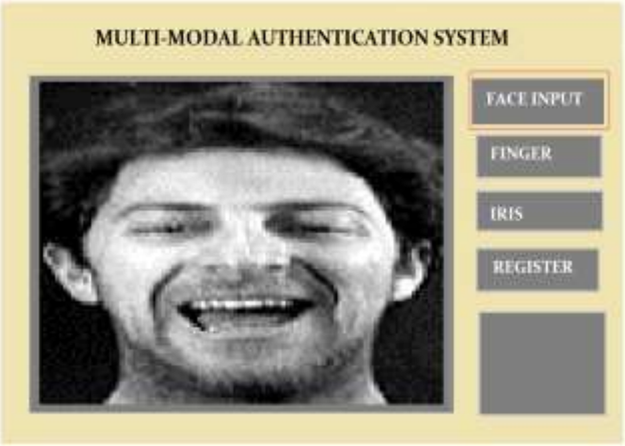
1. Segmentation and Preprocessing

Segmentation is also known as separation, here there is some table as listed in Fig.2 are separated as requested. There are some values are separated from the table and divided into two, those values are preprocessed by the segmentation. Then send it to the enhancement further. It will show the particular is from the image that we want in the face, eye or fingerprint, important is for differentiating the object in depth.

2. Converting to Gray Scale

Here we have to enhance the preprocessed data from the segmentation for seeing the neighbor values for extraction and the texturing level. The median value is important for choosing the particular area from the image and for medical images it may be implemented in software as an option. Images will be converted into grayscale for comparing the images and to save the images in the database.

IV. EXPERIMENTAL RESULTS



Security terms

These schemes are introduced in this application for registration and security. There are three types of terms has been applied.

1. Face detection

This type of detection is using the image processing concept for the establishment of the face. In later, object detection was introduced to check the saved data from the database. This option is kept in the application with the camera in front. When the camera is on the detection can be started for registration. It is also using the separate mechanism for the detection. Without any grayscale scheme, it has been implemented. The result was discussed in the evaluation.

2. Fingerprint

The fingerprint is using in the many areas for securing the system from the unauthorized person. It is unique to every person. It is the only natural security from birth. It can be used for our security. It can be read by the device and saved in the cloud database later. In these cases, we have added this option to this system for increasing the level high on comparing with the existing model.

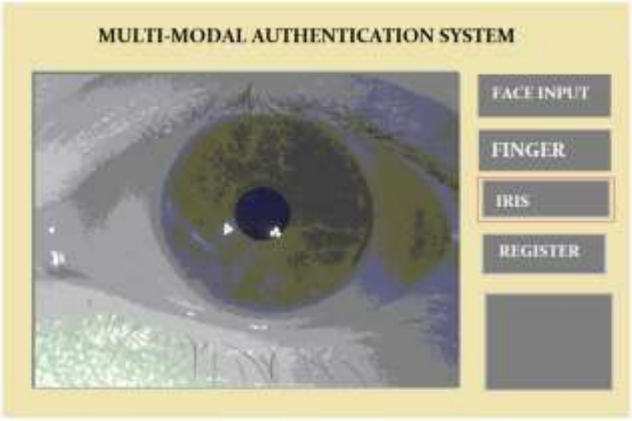


Fig. 5 IRIS Registration

3. Eye detection (IRIS)

It is the unique security signature from the birth irises of the eye will not be the same as everyone. Because it has a number of minute changes and lines available. It will also use the system to make better. This option was also fixed in our system. This can be read and converted into grayscale and then ready to save in the cloud database.

Fig. 3 Face Detection Registration

Here we have tested some images with the datasets, by clicking the face input as shown in Fig.3, we can register the face using the camera. Then it will be changing from normal to the grayscale. This the first step, once the face is recognized correctly and conversion happened, it goes to another step for reading the fingerprint.

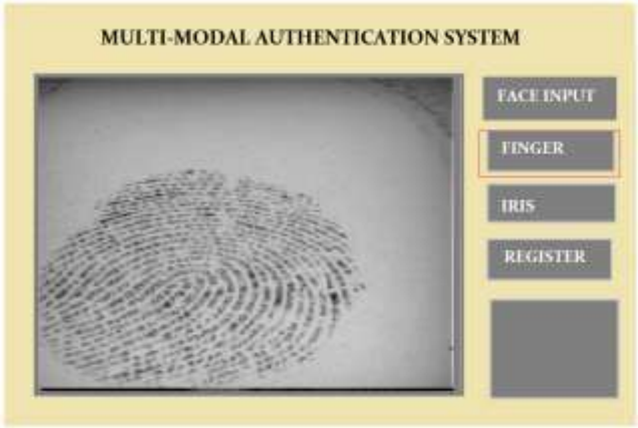


Fig. 4 Fingerprint Registration

The second step for registration is fingerprinting, by clicking the finger in fig.4, we can keep our finger in the reader, and after the reading, it will convert the image to another scale for saving the data in a cloud platform. Then it goes to read the eye for completing the registration. As seen in fig.5, the eye is ready to read the image and saved in the scale. Finally, registration is completed by clicking the register button on the screen.

In Fig. 6, we can see the comparison of the existing system and proposed system by choosing the area of security level. It has given good result and achieved the data very well. On deploying the system by checking the data in creating the cloud platform. We have achieved the analysis by checking the system and represented in the graph area. In the graph we can see the number of the proposed system is having more security level than the existing model, it was compared by seeing the level in depth and achieved well.

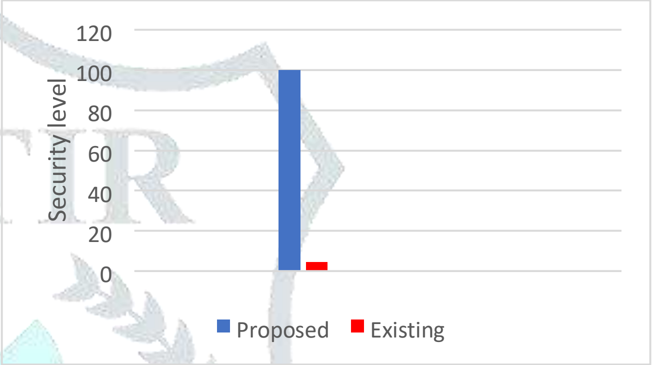


Fig. 6 Security level

V. CONCLUSION

More usage is occurring in cloud computing as same to this, there is a number of attacks are also occurring. To solve these issues and complexity, we have proposed the special scheme for protecting the area which is getting affected by a spammer in the Cloud Computing using multi-level identification scheme. The result was achieved by hybrid security with analyzing models. There are some comparison shows up well and discussed as per the details proceeded by the researchers. In future work, this method can be used in banking region for securing the user message and banking information.

REFERENCES

[1] Shahzad Memon, Mojtaba Sepasian, Wamadeva Balachandran, “Review of Fingerprint Sensing Technologies”, Brunel University, West London, United Kingdom, 2008

[2] Ezema, L. S., & UJ, C. (2015). Fingerprint Based Attendance Management System. International Journal of Science& Engineering Research, 1623.

[3] Sudha, K. L., Shinde, S., Thomas, T., & Abdugani, A. (2015). Barcode-based student attendance system. International Journal of Computer Applications, 119(2).

[4] Taxila, P. (2009). Development of academic attendance monitoring system using fingerprint identification. IJCSNS, 9(5), 164.

[5] Krishnamurthi, K., Mary, S. I., Sumalatha, B. N., & Pereira, A. (2015). Fingerprint-based attendance system. International Journal of Advanced Research in Computer and Communication Engineering, 4(3), 621-623.

[6] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, ‘‘An effective key management scheme for heterogeneous sensor networks,’’ Ad Hoc Netw., vol. 5, no. 1, pp. 24–34, 2007.

[7] X. Du and H. H. Chen, ‘‘Security in wireless sensor networks,’’ IEEE Wireless Commun. Mag., vol. 15, no. 4, pp. 60–66, Aug. 2008.

[8] X. Hei and X. Du, ‘‘Biometric-based twolevel secure access control for implantable medical devices during emergencies,’’ in Proc. IEEE INFOCOM, Apr. 2011, pp. 346–350.

[9] X. Hei, X. Du, J. Wu, and F. Hu, ‘‘Defending resource depletion attacks on implantable medical devices,’’ in Proc. IEEE GLOBECOM, Dec. 2010, pp. 1–5.

[10] M. Barni et al., ‘‘Privacy-preserving fingercode authentication,’’ in Proc. 12th ACM Workshop Multimedia Secur., 2010, pp. 231–240