Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 5): pp. 1766-1773
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.05.194

BIOMETRIC AUTHENTICATION BASED MEDICAL DATA MANAGEMENT IN CLOUD SYSTEMS

Ajina Mohamed Ameer, Research Scholar, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay, ajina1984@gmail.com
Dr. M Victor Jose, Associate Professor, Department of Computer Application,Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay, mvictorjose@gmail.com

ABSTRACT- Biometrics has proved to be an efficient solution to several of the security problems that are prominent in the modern age in most technological fields. It is the estimation of physical or behavioral features of humans utilized for distinctive recognition. Biometricsuses Digital Image Processing's pattern identification technology for recognizing the unique characteristics of humans. Fingerprint impression, facial landmarks, iris morphology, voice recognition, handwriting detection, hand geometry recognition, finger vein identification and signature recognition are the most widely applied or called biometric modalities. Biometrics is used in different areas, one of which is protection systems. We propose an intelligent biometric authentication system for data management in the cloud.A general issue is keeping biometric data safe in health facilities for patient authentication. Many experiments have shown different means of keeping biometric information, particularly biometric data from finger veins. Therefore, by implementing the above three principles of information protection and developing a robust authentication framework with high standards of reliability, privacy and security, better ways of protecting this data need to be found. Besides, biometric data is quite tough to replicate and any loss of biometric information contributes to high risks. This study uses fingerprint scanner systems to be using changed minutae algorithm to create an effective biometric identification system. Only the enclosed triangles around each minute were contrasted between the input and the stored prototype in the updated method. The suggested method gave a high degree of accuracy with an error rate equal to 0.5%.

Keywords: Biometric Authentication, Fingerprint Recognition, Cloud Authentication, Data protection, Data Encryption

I. INTRODUCTION

Today cloud computing is becoming a human's daily life activity. Many companies use the cloud to store and manage their enormous cloud server data. But for both cloud service consumers and providers, the protection of sensitive data and overcloud is becoming a problem. In old days people generally use passwords for emails and bank accounts etc. Hackers are capable of quickly cracking these passwords [3]. So, unless we have a security system to defend the data from intruders and hackers, the data is not secure. The biometric device is a mixture of sensors, extraction features and corresponding modules that implement detection algorithm. Reliable personal identification schemes are required by trustworthy and faithful programs to either confirm or ascertain the position of an object demanding their services and suitable applications. To either confirm or evaluate a person's identity, biometric identification systems should include a reliable personal identification scheme [2]. Computer device protection, safe electronic banking, cell phones, credit cards, secure access to the building, health and social services are all uses of this system. The aim of creating identification is to confirm that the services provided were retrieved only through a legitimate user and not by someone else.

Biometric technology states the automatic identification of a person depending on the physical and/or behavioral features based on even an attribute vector(s). By evaluating some feature of human anatomy or physiology (like your hand geometry or fingerprint), some profoundly ingrained ability, or other behavioral features (like your handwritten signature), but something that is a mixture of the two (like your voice), biometrics distinguish individuals [1, 12]. Biometrics enables us to confirm or regulate the individuality of a person based on who he/she is, instead of what he/she has from an ID card or what she knows, such as a password (cryptal or non-cryptal). Biometrics denotes the automated identification of a living human depends on physical and behavioral features in a much-simplified manner. Many forms of biometric systems are now on the market: face detection, identification of fingerprints, the geometry of the finger, configuration of the hand, recognition of the iris, recognition of the vein, speech and signature

[5]. For different purposes, the technique of biometric identification is favored over conventional methods requiring passwords and PIN numbers: the individual to be recognized must be physically available at the place of authentication, or the need to recall a password or hold a token or smartcard is obviated by identifier based on biometric strategies. With the exponential rise in the usage of PINs and passwords due to the technological revolution, access to sensitive/personal data needs to be limited. Biometric methods are more convenient for the user by removing PINs and passwords and can theoretically avoid illegal entry to or fraudulent need for ATMs, time tracking schemes, mobile phones, smart cards, desktop PCs, workstations, and systems of computers. It is possible to forget PINs and passwords, and token-based authentication mechanisms such as passports, driver's permits and security cards can be forgotten, stolen, or lost. For real-time recognition, different kinds of information authentication are used; the most common are focused on facial recognition and alignment of fingerprints. There are many other biometric devices, nevertheless, which use the geometry of the iris and retinal tests, voice, face, and hand. The query biometric sample is aligned during fitting with the reference materials that are saved in the system to determine the identification connected with the query. Picture sharpening and reconstruction, medical fields, directed robot vision systems, information processing systems and video processing are among the areas where image analysis is generally practiced. The discipline for observation, distinguishing the patterns in the data, and using it for more making decisions is information processing technology, which is a key application field of image processing. Biometric, referring to the assessment and statistical analysis of the distinguishing physiological and behavioral features of persons, uses the process of pattern recognition to identify and categorize persons by identifying correlation with the models contained in the database [4,11]. Along with its unique order to recognize persons, biometric technology has speedily become a way of preventing identity theft and fraud throughout the cloud setting and has thus found its position among mainstream technologies [12]. Biometric authentication is more effective in detecting duplicate addresses than conventional authentication systems that use passwords and identification documents [19,20]. While biometric systems are not inherently faultless, the scientific community is constantly making considerable efforts to recognize cloud security vulnerabilities and provide solutions to address them. Novel algorithms are emerging to secure biometric models that mitigate user security privacy issues.

As our physical techniques such as faces, fingerprints, palm veins, irises, hand geometry and voices were genuinely special, the usage of biometrics is growing every day, making them an important blockade for cybercriminals seeking to impersonate us dishonestly. They were beneficial since they are comparatively more distinctive, hidden, permanent, steady, hard to reproduce, and physically linked to us, unlike names, ID numbers, email accounts, and passwords, which also seem to be quite convenient [9]. Fingerprints were known to be the highest authentication strategy for cloud data across all biometric methods [13]. For a person, fingerprint patterns maintain the same over his or her life. The other benefits associated with fingerprints involve precision, uniqueness, cost-effectiveness and lesser storage space needed.

Instead of conventional authentication methods to exterminate identity fraud in the cloud world, a biometric technology that utilizes a person's physical or behavioral characteristics for different identification can be an effective substitution [14]. Fingerprints play an important role throughout the authentication and verification of user identification with the increasing need for smartphones in different arenas like e-health care, personal and commercial payments, and banking [10]. Since mobile devices comprise users' sensitive information, it is also very important that this information is effectively protected. Modern smartphones are using biometric authentication fingerprint scanners to meet this [15]. Biometric authentication of fingerprints is easy and rapid; nevertheless, it is susceptible to attack as hacks can store biometric data from fingerprints [16]. Consequently, in such a structure, possible leakage and security vulnerabilities pose a life-long threat to persons. A general fingerprint scheme is suggested in this study.

II. FINGERPRINT AUTHENTICATION

The most important move today to mitigate fraud and identity theft is the recognition of an individual. Therefore, by compared the actual image with both the data set regulated by various attributes, biometrics are being used to recognize a user uniquely. Biometry involves adding biological data to mathematical modeling. It is a computerized method of identifying a person and such systems comprise various stepped modules like a sensor, feature extraction, matching, and decision assembly, as depicted in Figure 1.

ID biometrics technology for fingerprint sensors is created to allow more precise and secure authentication for smartphones and mobile devices worldwide [17]. These biometric fingerprint scanner systems, such as the Fingerprint Sensors biometrics framework, yield greater degrees of security and improved authentication opportunities, paving the charge to a safer digital life without passwords and pin codes [18]. There were 4diversekinds of fingerprint scanners are optical, capacitive, ultrasonic and thermal scanners [19].

The analysis of images mostly involves the three stages: importing the input data via the capture equipment of the image; pre-processing, examining and nano-manipulating the input data; giving the output in which the picture is altered or the report generated by the analysis of the image files is evaluated.

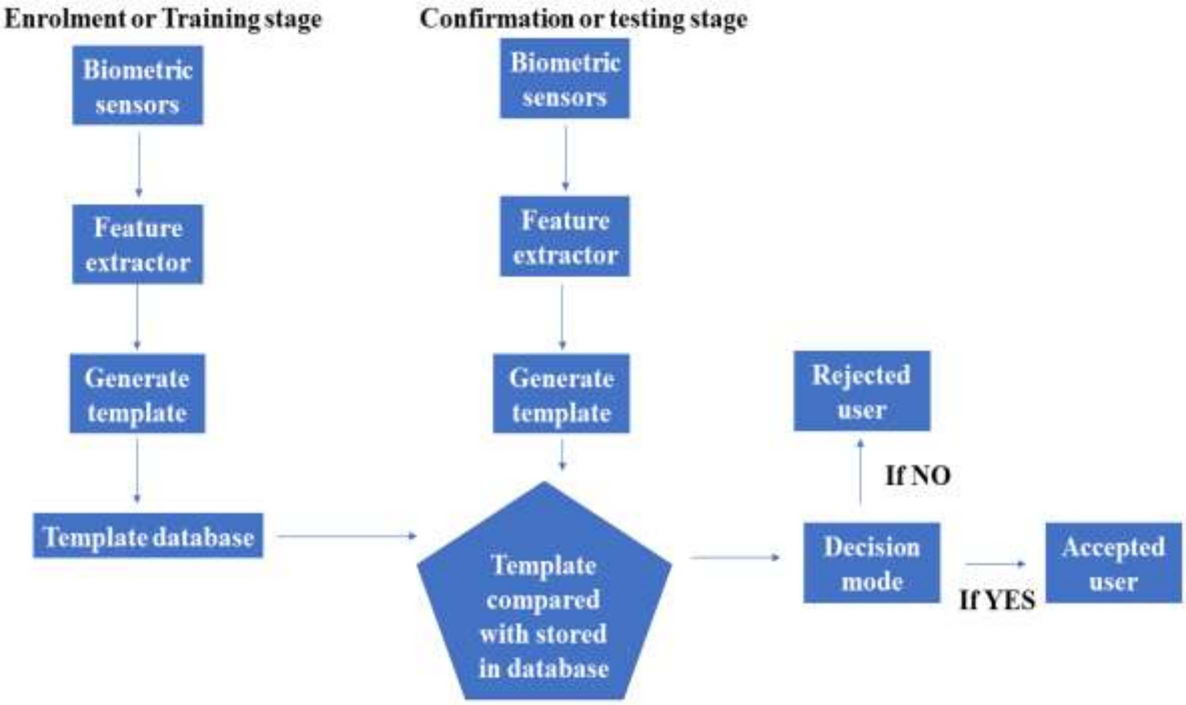

Figure 1. Biometric system design

The fingerprint in biometric and forensic science comprises of different ridge and valley patterns on the person's finger surface. A mountain, whereas the valley is the region among two adjacent ridges, is a single curved section. Consequently, the dark fingerprint regions were ridges, and valleys are recognized as white areas [20]. Most automatic fingerprint identification methods were depended on minutiae, called local ridge attributes. There are many kinds of the sequence of minutiae, like ridge ending, ridge bifurcation, ridge dot, ridge islands, lakes, spurs, bridge, and crossover, and not restricted to. Ridge ending and ridge bifurcations are by far the most generally used forms of patterns of minutiae. Based on factors like skin humidity, the pressure of a finger mostly on the sensor, scars, etc., fingerprinting mainly faces problems with deterioration. Consequently, to improve the image quality before extracting minutiae utilizing optical methodologies, it is possible to apply image processing methods. The gray-scale imaging technique attempts to explicitly extract minutiae from either a grayscale fingerprint. A correspondingvalue among 2 fingerprints is calculated by the fingerprint matching subsystem to interpret the degree of resemblance between a given fingerprint and the recorded fingerprint of an existing user. For a similar fingerprint and a lower score for diverse models, an effective matching algorithm includes a greater similarity score. The corresponding mode should be capable of dealing with interclass disparities since the user could use his fingerprint in a distinct translation, rotation, or contact area and the amount of pressure can modify. The difference of Interclass is connected to the similarities among photos of fingerprints from diverse fingers.

Minutiae are first retrieved from the fingerprint pictures and a sorting set of points on a two-dimensional plane [6] in minutiae-based matches. To determine the matching score, the following methodology would then be used. The simplified version of a Modified minutiae-based algorithm [7,8] is shown in Algorithm 1.

III. ALGORITHM 1: MODIFIED MINUTIAE-BASED ALGORITHM

```
Input: f (n1, n2): the registered finger image, д(n1, n2): thefingerpicture to be confirmed
Output: Matching score among f (n1, n2), д(n1, n2)
Pre-processing;
Arrangement;
Estimate fingerprint identical score;
```

1. The pre-process unit estimates the pairwise comparison between minutiae in these methods.
2. Transformation: This unit modifies the minutiae of the input into the adjustment set (The alignment method is estimated as per all probable joining of transformation parameter).
3. Comparison: If the values are greater than the predefined matching score, this unit calculates the matching score, the threshold, stops the matching procedure, and sends the score to an output.
3. Performance: There are two types of techniques that the fingerprint matching subsystem can end up making:

(1) False match rate (FMR): the matcher statesamatchamongpictures from two diverse fingers.
(2) False non-match rate (FNMR): the matchercannotrecognize images from asimilar finger.

FMR and FNMR are based on the functional threshold. A massive threshold score at the expenditure of higher FNMR results in a tiny FMR. In aspects of its false +ve (FPIR) and false -ve identification rate(FNIR), fingerprint identification system performance is measured. Whenever the found naturally a hit for a query fingerprint that is not registered in the system, FPIR occurs. For a query fingerprint registered in the structure, FNIR tends to occur whenever it discovers no hit or a wrong hit. Equal Error Rate is another performance metric for a matching module (EER). EER seems to be the point in which the number of false matches is equivalent to the number of false non-matches [8]. To evaluate whether an obtained fingerprint image relates to a person, the decision system contains the measured similarity score. By implementing a threshold to a corresponding score, the choice is acquired. As this price is reliant on the construction tradeoff among the threat of a false +ve and the risk of a false negative, the threshold range should be appropriately altered to the usage domain. The individual is identified if the identical score obtained from the corresponding module is greater than the mean.

Take the identification of fingerprints as an example. A consumer introduces his finger to the fingerprint sensor throughout the enrollment phase and a fingerprint picture is obtained by a sensor module. Some of the characteristics of the obtained fingerprint image are obtained and further adjusted or converted to produce template data for verification-stage comparative analysis. The fingerprint image of a question is obtained by a sensor module throughout the authentication phase. To acquire query data, the function illustrations of the query fingerprint picture go over this method as with the registration step. The query result corresponds with the template data to obtain a matching answer. Medical data and fingerprint data are processed in the cloud database and only published when the fingerprint is matched.

IV. RESULTS AND DISCUSSION

In this research, ECG signal recognition is done by performing fingerprint authentication. The input of the system is ECG signal and the output will be the result of ECG analysis. In the beginning, we will check the fingerprint authentication, if the fingerprint is belonging to the recognized person then the only system will be authorized. By using C# Application, Download the Dataset presented on the server. Here we are using Microsoft Default Cloud Server MYASP.NET. From the Cloud, we have to download the Database. We can download all the datasets in one click or we can download the dataset one by one. After download, we need to run the MATLAB, at that time the system will ask fingerprint for the authentication process, the authentication from the fingerprint database. Once the system confirmed the authorization, the ECG raw data will process. The input image is revealed in figure 2 and the input picture convert into thebinarization image is shown in Figure 3.

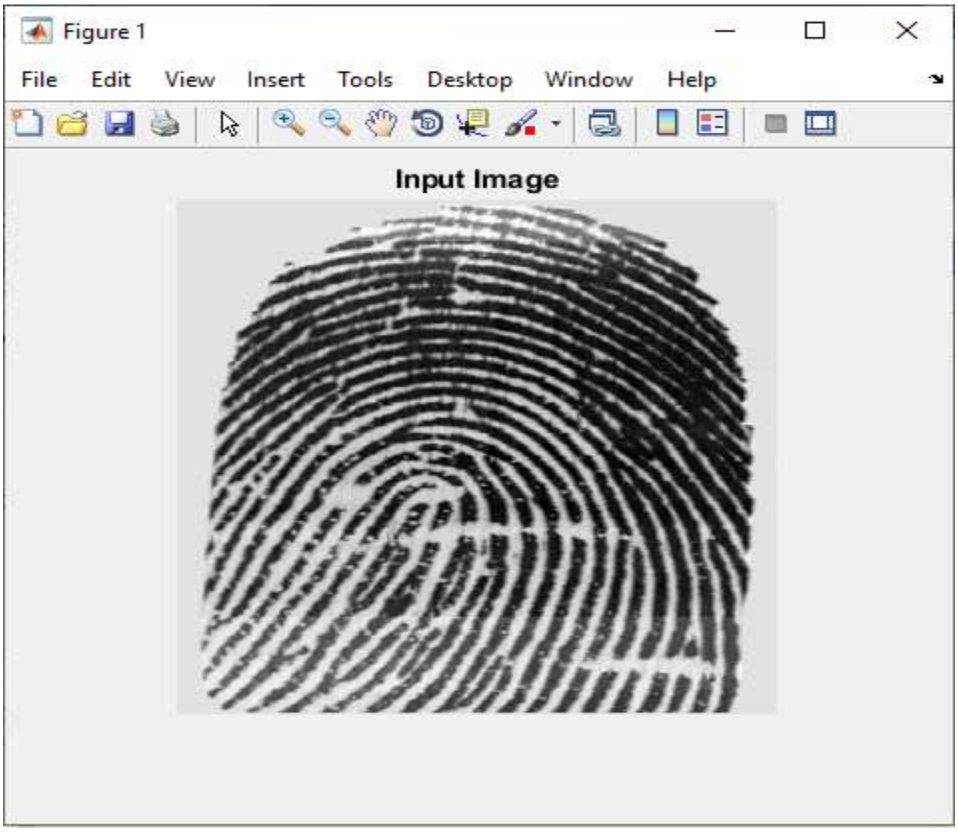

Figure 2. Input fingerprint image

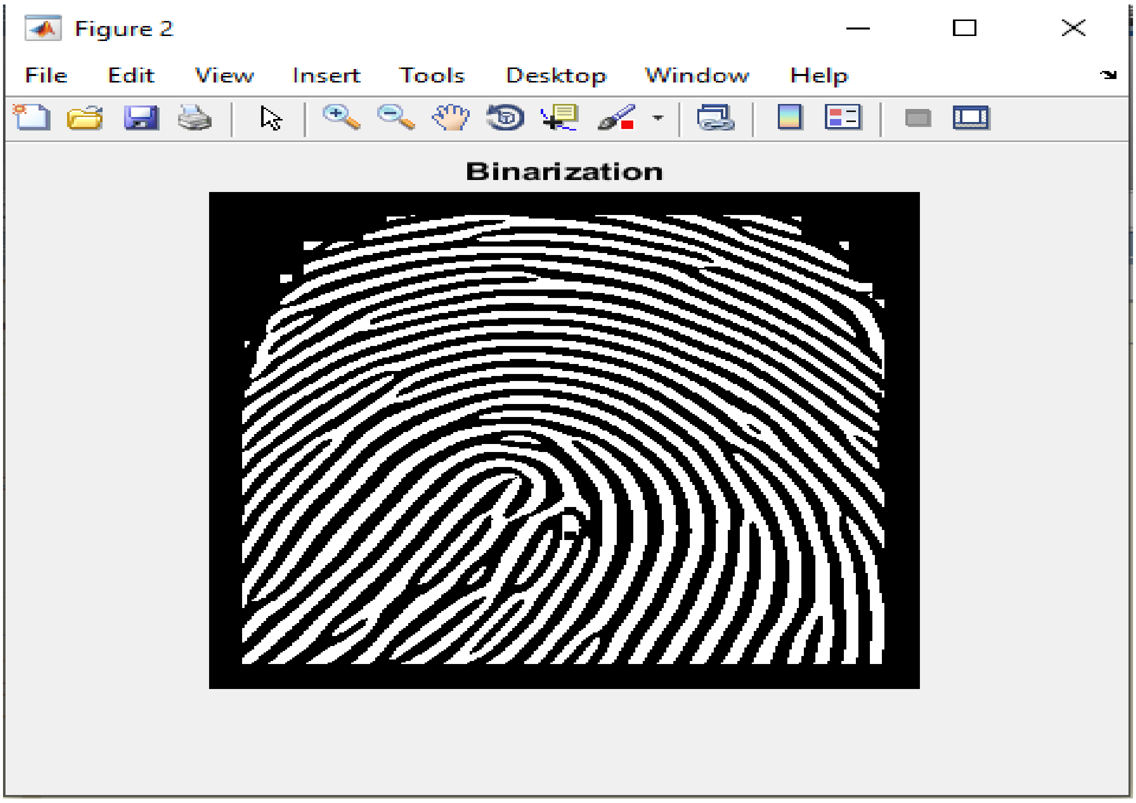

Figure 3. The input image converts into a binarization image

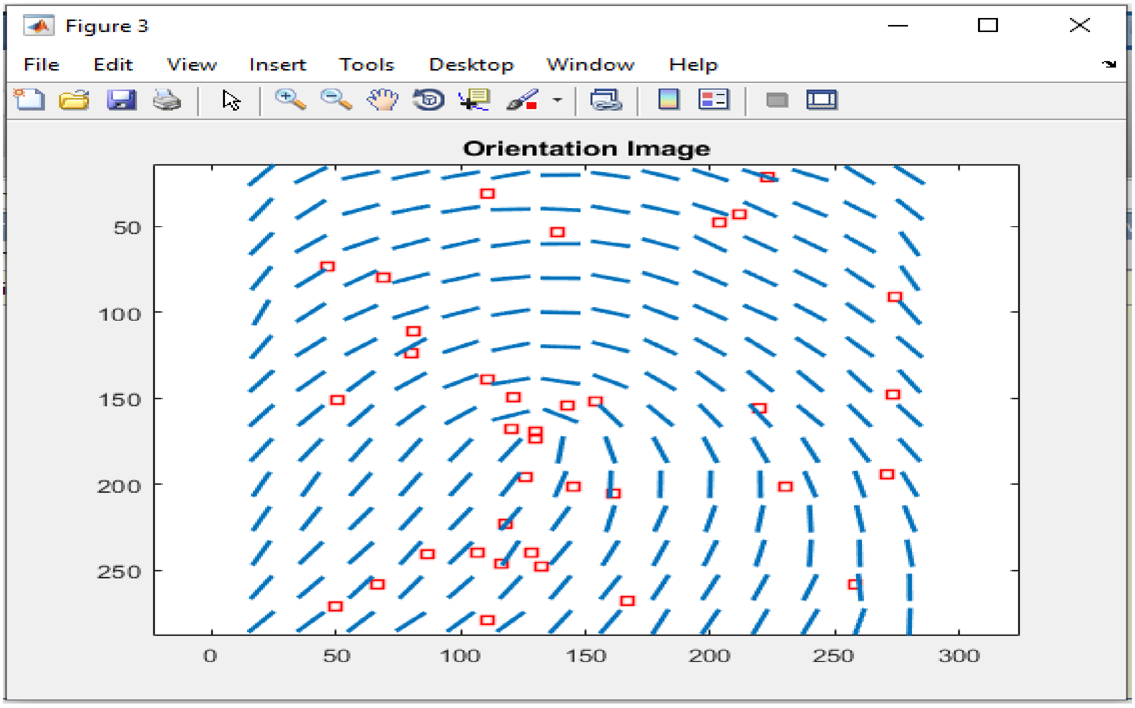

Figure 4. Orientation image with minutiae features

In the orientation image, we will have a red color mark which will be called minutiae features as in Figure 4. Minutiae features have ridges and center points. Figure 5 shows the overlayed display of fingerprint with an extracted feature of fingerprint minutiae point. From this image, we will be recognized as the person is authorized or not.

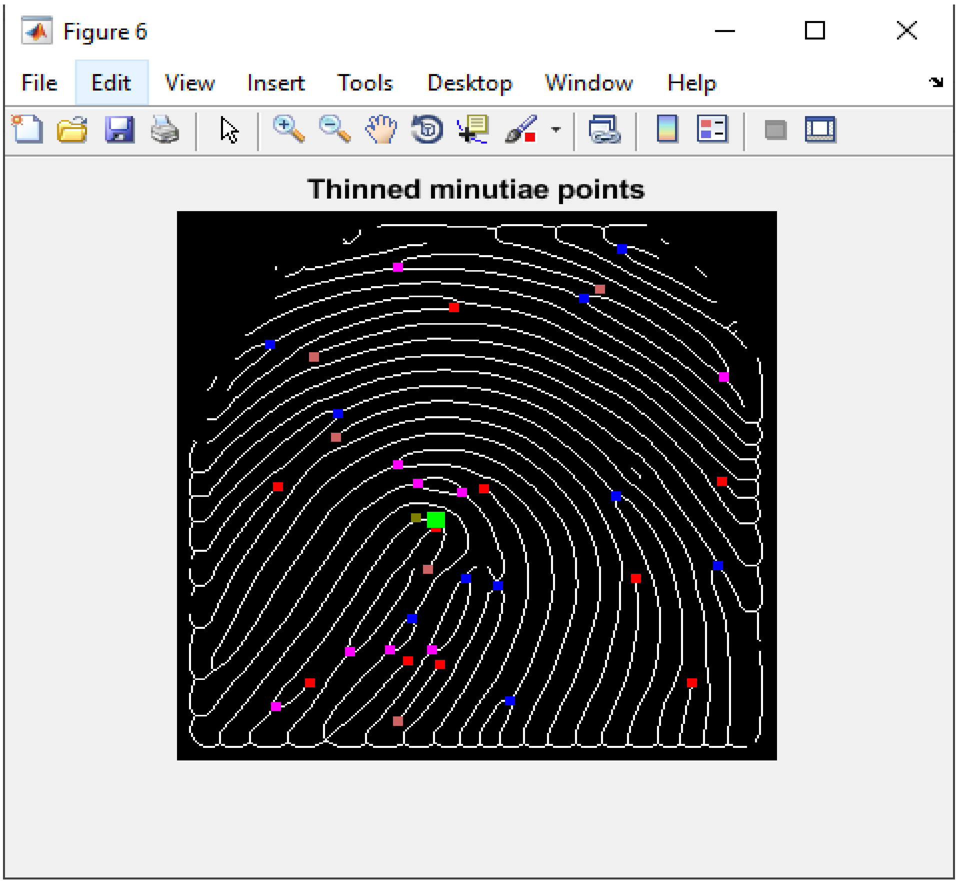

Figure 5. Thinned minutiae points.

After finishing all the algorithms then,the final result will be available on the same drive where we stored the input data (new output folder). Figure 6 shows the output data will be upload once we click the upload button on the GUI after authorization of fingerprint.

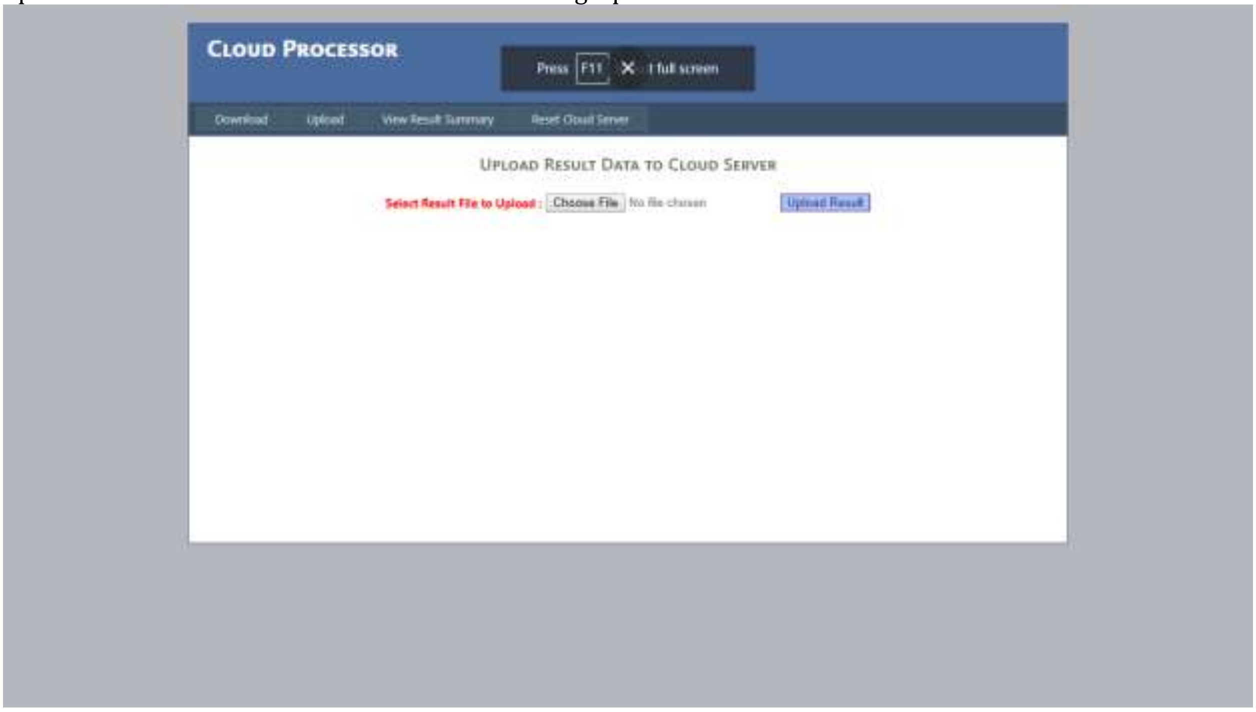

Figure 6. The processed data into the cloud server (MYASP.NET) after authentication

We proposed and applied fingerprint-based biometric authentication to extract medical data. A cryptographic key focused on fingerprints is safe. The intruder has no idea of the current user's biometrics. In the experimental outcome, it is noted that the differentiation of the fingerprint model between users opposed producing a genuine key from the impostor fingerprint prototype. The genuine recipient's fingerprint data is not retrievable as the key doesn't leak information about the minute points. Also, using any shuffling-based transformations of the template vector, the code can be transformed into some kind of revocable key. This system represents a low-cost solution, which could be affordable across medical environments.

V. CONCLUSION

To enhance cryptographic protection, cryptography and biometrics are combined. Cryptography is the main data and network security agency, while biometrics seems to be the most reliable in user authentication. The issue with cryptography is really with cryptographic identity generation. Biometric is being used to deal with the cryptography problem. In this method, we often use user fingerprints to produce a cryptographic key based on fingerprints. As it is created from the user's fingerprint, it is not necessary to recognize the key. It also means that information security is non-repudiated.Throughout the future, encryption methods must be used to secure the outcome before submitting this to the output computer to protect the fingerprint vulnerability.

REFERENCES

1) Alemu, B., Kumar, R., Sinwar, D., &Raghuwanshi, G. (2021, January). Fingerprint Based Authentication Architecture for Accessing Multiple Cloud Computing Services using Single User Credential in IOT Environments. In Journal of Physics: Conference Series (Vol. 1714, No. 1, p. 012016). IOP Publishing.
2) Andrew, A. M. (2004). HANDBOOK OF FINGERPRINT RECOGNITION, by DavideMaltoni, Dario Maio, Anil K. Jain and SalilProbhakar, Springer, New York, 2003, hardback, xii+ 348 pp., with DVD-ROM, ISBN 0-387-95431-7 (£ 46.00); Book Reviews; Book Reviews.

3) Adler, A., &Schuckers, S. A. (2015). Biometric Vulnerabilities, Overview.

4) Ross, A. A., Shah, J., & Jain, A. K. (2005, March). Toward reconstructing fingerprints from minutiae points. In Biometric Technology for Human Identification II (Vol. 5779, pp. 68-80). International Society for Optics and Photonics.

5) Bringer, J., &Despiegel, V. (2010, September). Binary feature vector fingerprint representation from minutiae vicinities. In 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS) (pp. 1-6). IEEE.

6) Maio, D., &Maltoni, D. (1997). Direct gray-scale minutiae detection in fingerprints. IEEE transactions on pattern analysis and machine intelligence, 19(1), 27-40.

7) Devi, A., Therese, M. J., &Premalatha, G. (2021, January). Cloud Computing based Intelligent Bank Locker System. In Journal of Physics: Conference Series (Vol. 1717, No. 1, p. 012020). IOP Publishing.

8) Alibeigi, E., Rizi, M. T., &Behnamfar, P. (2009, May). Pipelined minutiae extraction from fingerprint images. In 2009 Canadian Conference on Electrical and Computer Engineering (pp. 239-242). IEEE.

9) Memon, S., Manivannan, N., Noor, A., Balachadran, W., &Boulgouris, N. V. (2012). Fingerprint sensors: Liveness detection issue and hardware based solutions. Sensors & Transducers, 136(1), 35.

10) Obaidat, M. S., Traore, I., &Woungang, I. (Eds.). (2019). Biometric-based physical and cybersecurity systems. Cham: Springer International Publishing.

11) Peralta, D., García, S., Benitez, J. M., & Herrera, F. (2017). Minutiae-based fingerprint matching decomposition: methodology for big data frameworks. Information Sciences, 408, 198-212.

12) Rathore, A. S., Xu, C., Zhu, W., Daiyan, A., Wang, K., Lin, F., & Xu, W. (2021). Scanning the Voice of Your Fingerprint with Everyday Surfaces. IEEE Transactions on Mobile Computing.

13) Roy, A., Memon, N., & Ross, A. (2017). Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems. IEEE Transactions on Information Forensics and Security, 12(9), 2013-2025.

14) Mehmandoust, S., &Shahbahrami, A. (2011, June). A Comparison between Different Fingerprint Matching Techniques. In International Conference on Digital Information and Communication Technology and Its Applications (pp. 242-253). Springer, Berlin, Heidelberg.

15) Memon, S., Manivannan, N., Noor, A., Balachadran, W., &Boulgouris, N. V. (2012). Fingerprint sensors: Liveness detection issue and hardware based solutions. Sensors & Transducers, 136(1), 35.

16) Shetty, S., & Salvi, S. (2021). A Smart Biometric-Based Public Distribution System with Chatbot and Cloud Platform Support. In Sustainable Communication Networks and Application (pp. 123-132). Springer, Singapore.

17) Vinod, V. M., Murugesan, G., Mekala, V., Thokaiandal, S., Vishnudevi, M., &Siddharth, S. M. (2021, January). A Low-Cost Portable Smart Card Based Attendance System. In IOP Conference Series: Materials Science and Engineering (Vol. 1012, No. 1, p. 012046). IOP Publishing.

18) Win, K. N., Li, K., Chen, J., Viger, P. F., & Li, K. (2020). Fingerprint classification and identification algorithms for criminal investigation: A survey. Future Generation Computer Systems, 110, 758-771.

19) Ameer, A. M., & Jose, M. V. (2019). Model of Implanted Electrocardiogram (ECG) Monitoring. Journal of Critical Reviews, 7(1), 2020.

20) Ameer, A. M., & Jose, M. V. (2020). Security Issue In Implantable Medical Device: A Comprehensive Survey. Journal of Critical Reviews, 7(1), 469-473.