An Effective and Protection Biometric Proof Plan in Cloud computing

Mr. D. Surendra[1] Ms. G. Padma[2]
Assistant Professor[1], PG Scholar[2],
ASCET,Dept of MCA,Gudur. [12]

ABSTRACT:

Cloud computing provides a new paradigm of computing. It offers a scalable, manageable and huge pool of resources that can be accessed by users from anywhere anytime. It also ensures the integrity of data stored on the cloud. But ensuring the confidentiality and integrity of sensitive information is still a big challenge. To overcome this challenge, a hybrid two-phase security system for preserving the privacy of data on the cloud has been proposed. The hybrid approach combines feature extraction and encryption techniques to enhance the security of accessing data from the cloud. At first, the minutiae point has been extracted from the biometric fingerprint, locally collected from the state university in Northern India. The private key has been finalized by generating an elliptic curve using the minutiae point for achieving better encryption of fingerprint. The effectiveness of the approach has been tested in terms of similarity score, False Matching Ratio (FMR), False Non Matching Ratio (FNMR) and recognition accuracy, when applied on the local fingerprint database. The evidence of the outcomes suggests that the proposed technique ensures relatively improved security and privacy of data in the cloud system as compared to some recent state-of-art methods.

1. INTRODUCTION

Biometrics identification is one of the most popular methods used nowadays for identifying the authenticity of an individual. All methods of biometric identification such as face recognition, iris, etc. have their own uniqueness, such as two persons cannot have same fingerprint, and persistence. As biometric features usually do not change over time and age, so biometric-based recognition systems are being focused day by day for identification and security of data on the cloud. These biometric systems perform user authentication by verifying an individual's characteristics. For this, it is required to maintain the database of biometric features of all individuals. Whenever any user wants to access data or resources, first, the process of verification starts. In the verification process, a user's biometric features are matched with the stored template in the database using any matching technique.

All biometric methods are generally categorized into two categories 1) Physical, 2) Behavioral [4]. Physical biometric methods are a fingerprint, palm print, iris

identification, retinal scanning, face recognition, etc. while the behavioral biometric methods are DNA matching, voice recognition, signature, handwriting, etc. [4]. All type of biometric characteristics is unique and measurable for identification and verification of an individual [5]. There are various advantages of using biometric authentication as compared to conventional techniques of verification like cryptography. Some of the advantages of using biometric authentication are as listed below:

Biometric methods give the category of authentication called as something you have. A person need not remember or carry identification separately like smart card, password, etc

(2) Techniques are diminutive chances of stealing.

(3) Techniques are cost effective and accurate. Techniques are easy, user-friendly, and secure.

Nowadays, many of the smart devices like phones, laptops,

doors, etc. are using an authentication mechanism based on biometric techniques instead of a simple password or swap cards or token system [4]. There are very fewer chances to break the system unlike other traditional methods because every individual has unique biometric features and patterns [5] Due to all the above reasons, biometric authentication systems are reliable and suitable for cloud access also. The biometric data of all the users who access the cloud can be stored and verified at the time of cloud utilization. The safety of data, especially sensitive data like biometric data or other data and managing privacy preservation are the biggest challenge in the cloud computing systems [2]. The popularity of cloud computing has forced researchers and developers to handle this issue very carefully. This can be achieved by the encryption of data available on the cloud, importantly biometric data, which will provide better security and privacy protection [6]. In this paper, a novel biometric-based system using a fingerprint detection technique has been proposed for better privacy preservation and security in cloud systems. Biometric image templates are encrypted using the elliptic curve with the digital signature encryption algorithm. For providing better security and privacy on the cloud system the paillier algorithm has been used. The main advantage of using the paillier algorithm is its Homomorphic encryption properties [7]. The road map of this paper is presented as follows. Section 2 discusses the related work done in the past by various researchers. Section 3 presents the proposed work. Section 4 describes the results generated from experiments and at last section 5 draws the conclusion of the work.

2. LITERATURE REVIEW

A lot of research has been done in the past to make secure cloud computing systems using various techniques. In most of the time, researchers have used the traditional cryptography techniques for providing security and privacy of data in the cloud. The main hassles with these techniques were in handling of security keys and data. For example, if the passwords are used for authentication of users then he may have a problem of remembrance. Especially if a user has several types of accounts then setting many passwords and remembering all these passwords is a hard task. Some other situations may arise like, if a user puts the same password for all his accounts, then it will provide a possibility of hacking all accounts. If the password is hacked or if the user saves the password in some file, then all accounts will be hacked if that file is hacked. To avoiding the situation of remembrance of password, smart cards can be used but, which have to be carried by the user all the time. If anytime it is Lost or stolen, then it may push users to some critical situations that can be considered as a major drawback of using smart cards. The above stated problems can be solved up to a great extent with biometric authentication due to its most important property i.e. "something that you have".

Literature reveals that Bhattasali et al, [8] surveyed various biometric techniques in their work. Authors claimed that remote accessing of any type of data using biometric systems is more challenging in comparison to access from a local place. In these situations, it is unavoidable to prevent unauthorized access. Biometric authentication systems are more efficient in comparison to the traditional system of authentications. Naveed et al, [9] analyzed the various biometric authentication techniques in the cloud computing environment and explores how these techniques could help in reducing security threats. The privacy reserving cloud-based system with biometric identification has been proposed by Haghighat et al, [10]. Authors have used k-d tree approach to create encrypted queries for preserving data secure. In the year 2016, Hahn et al, [11] proposed an effective privacy preserving fingerprint identification scheme for cloud computing systems with a homomorphic encryption scheme. The authors tested the proposed scheme on the Amazon EC2 cloud. In the year 2018, Bala et al, [12] presented a biometric-based homomorphic encryption algorithm for data transmission in cloud systems. The proposed scheme was able to handle phishing and shoulder surfing attacks in the cloud environment. In a study done by Pan et al, [13] authors said that biometric identification provides lots of convenience to users of cloud computing systems but simultaneously increases privacy concerns also. In this study, researchers have studied various attacks and also validated them in a cloud environment. Kumar et al. [14], proposed a security scheme using face recognition biometric identification approach in their proposed scheme on the cloud computing environment. As the main focus of the proposed work is on cloud security and privacy, so literature survey of security-

oriented research papers has been continued. Lee et al. [15], analyzed the benefits of fingerprint identification in comparison to other biometric forms. The author has also discussed various case studies of companies in the UK, to justify his work and proved that the fingerprint identification system is comparatively better than other biometric systems. Zhang et al. [16] proposed a new privacy-preserving scheme based on biometric identification which ensures lightweight database computations. They have designed a biometric data encryption algorithm and introduces perturb terms in biometric data. The biggest challenge in cloud systems is to provide an efficient solution for security that gives access to resources and data which are outsourced to the cloud. To overcome this issue, Kumari et al. [17], devised a biometric authentication system for the multi-cloud server. They have used the bio-hashing technique for better accuracy of pattern matching. Al et al. [18], addressed security issues of mobile cloud computing by presenting an effective model to solve the identification problem in the mobile cloud using fingerprints. They have combined fingerprints with a password to make the system much strong. Shakil et al. [19], proposed the biometric authentication system for the health care database by introducing a signature-based system. with the help of a back-propagation network. Encouraged by the stated techniques, one hybrid approach in combination with the biometric and encryption technique has been proposed to preserve better security as well as privacy in the cloud system.

3. PROPOSED SYSTEM

Two steps will be used in the proposed system for providing

secure access- 1. Enrollment of fingerprint, and 2. Verification of Fingerprints. In the proposed system, fingerprint biometric-based identification of individual users will be used. The main reasons for considering fingerprint as biometric for identification are the advantages it offers in comparison to other biometrics. For example, no two fingerprints are the same, it does not change with age, small storage is required in comparison to other biometrics, devices are comparatively cheap, easy to use, and require low maintenance cost [14-17]. The block diagram of the proposed system is shown in Figure. 1.

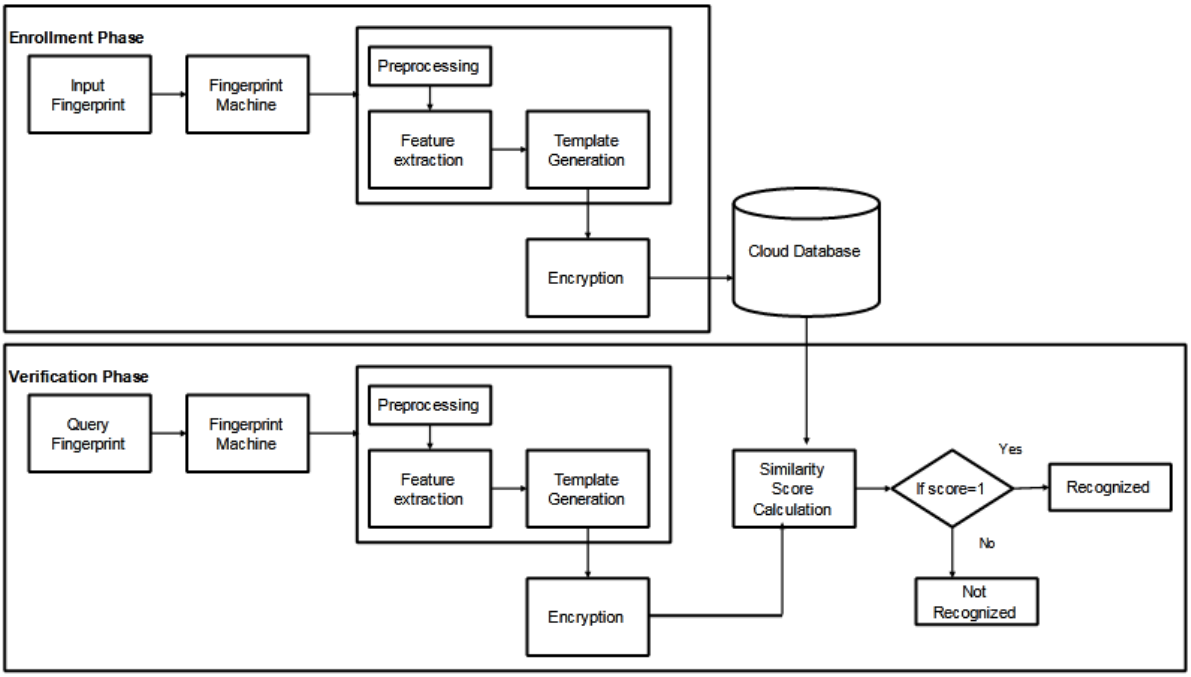

Figure1.Proposedsystemblockdiagram

ENROLLMENT PHASE

In the enrollment phase, shown in Figure. 2, an individual user fingerprint is enrolled and stored in the database by fingerprint detection machine. After the storage of an individual's image, its quality is checked and if the quality level is appropriate then feature extraction is done. The proposed system uses the minutiae point algorithm [20] for feature extraction. Minutiae points are very important and widely used features of the fingerprint detection technique. These are used for matching an appropriate fingerprint with stored templates of fingerprints in the database. Minutiae points are used to distinguish one fingerprint image from others. A fingerprint image with good quality can have 25 to 85 minutiae points [21]. These minutiae points are individualities in the finger ridge patterns of an individual. In this, the two most widely used features are ridge ending and ridge bifurcation. Ridge ending is the sudden end point of the ridge while ridge bifurcation is the point where two or more branches are generated from the single ridge shown in Figure.

ENCRYPTION OF FINGERPRINT

This is the second step in the proposed system for adding more security for individual user identification. In this Elliptic curve encryption with a digital signature algorithm is applied for encryption of fingerprint templates. It is public key cryptography, which is based on the algebraic structure of elliptic curve over finite fields.

VERIFICATION PHASE

After enrollment of all the fingerprint of authorized users, verification will be done each time a user wishes to access cloud data. The verification process is shown in Figure. 9 Verification process is done by extracting minutiae points of a user, who wants to access the cloud system. After the extraction of the features, the matching score also called a similarity score is calculated for the query image with each template existent in the database. This similarity score describes the level of similarity between two fingerprints.

PERFORMANCE EVALUATION AND COMPARISON

The minutiae point algorithm is used for matching the fingerprint and finding the similarity score for the individual users. For generating image template original image is converted into masked, thin and then minutiae-points image generated Figure. 11 shows the masked, thinned and minutiae-point generated images along with four sample input images chosen from the database. Figure. 12 displays the similarity score after matching the minutia points of query and two template images taken from the cloud database. Three verification metrics namely, False Matching Ratio (FMR), False Non Matching Ratio (FNMR), and Recognition Rate (RR) have been determined. FMR determines a probability at which any system incorrectly predicts the unauthorized biometric entity as a correct entity, while FNMR is the probability at which any system predicts the right entity as wrong.

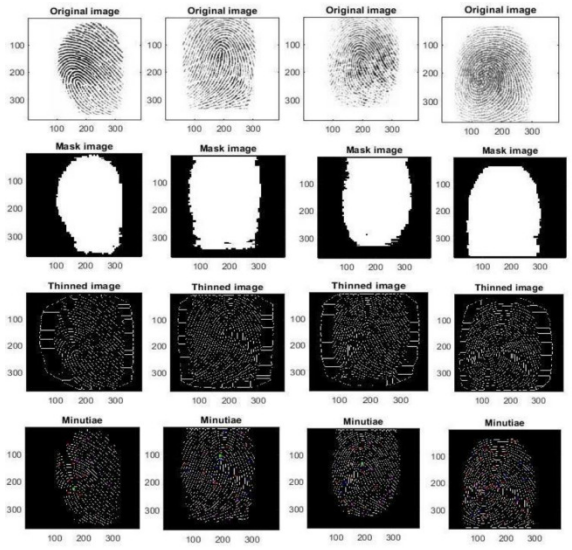

Figure . Mask, thinned and minutiae points for the four original input images

4. CONCLUSION

In this paper, a secure and privacy-preserving cloud system has been proposed, which is based on a hybrid biometric recognition system and elliptic curve cryptography. The system identifies cloud users according to their encrypted fingerprint templates stored in the encrypted domain. For feature extraction, a minutiae point detection algorithm is used which uses two features ridge ending and ridge bifurcations. The query image can be recognized according to the proposed algorithm which generates a similarity score in terms of FMR and FNMR which lies between 0 to 1. To improvise the recognition accuracy by reducing the noise PCA approach has been applied to the proposed system. After experimental evaluation of the proposed scheme, it has been found that the system recognition accuracy is approximately 97% which is quite better

than state-of-art recent approaches. The main shortcoming of the system is the storage requirement. As the system goes in real time, the database size requirement gets increased significantly because of the large size of images in comparison to traditional authentication data

5.REFERENCES

[1] Fiandrotti, A., Mattelliano, M., Baccaglini, E., Vergori, P. (2018). CDVSec: Privacy-preserving biometrical userauthentication in the cloud with CDVS descriptors.Pattern Recognition Letters, 113: 67-74. https://doi.org/10.1016/j.patrec.2017.03.024

[2] Jain, A.K., Ross, A.A., Nandakumar, K. (2011). Introduction to biometrics. Springer Science & Business Media. https://doi.org/10.1007/978-0-387-77326-1

[3] Ratnam, S., Gupta, M., Singh, D.A.S. Thirunavukkarasu, K. (2016). A survey on biometric security technologies from cloud computing perspective. International Journalof Scientific and Technology Research, 4(8): 22–24.

[4] Jain, A.K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., Wayman, J.L. (2004, August). Biometrics: A grand challenge. Proceedings of the 17th International Conference on Pattern Recognition, Cambridge, UK, pp. 935-942. https://doi.org/10.1109/ICPR.2004.1334413

[5] Jain, A.K., Ross, A., Pankanti, S. (2006). Biometrics: A tool for information security. IEEE transactions on Information Forensics and Security, 1(2): 125-143. https://doi.org/10.1109/TIFS.2006.873653

[6] Jain, P., Rane, D., Patidar, S. (2011). A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment. In 2011 World Congress on Informationand Communication Technologies, IEEE, Mumbai, India,pp. 456-461. https://doi.org/10.1109/WICT.2011.6141288

[7] Gupta, B., Agrawal, D.P., Yamaguchi, S. (2016). Handbook of Research on Modern CryptographicSolutions for Computer and Cyber Security. IGI Global. https://doi.org/10.4018/978-1-5225-0105-3

[8] Bhattasali, T., Saeed, K., Chaki, N., Chaki, R. (2015). A survey of security and privacy issues for biometrics