Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits

Dr. J. Samuel Manoharan
Professor/Dept. of ECE,
Sir Isaac Newton College of Engineering and Technology,
Papakoil, Nagapattinam – 611102,
TamilNadu, India.
drjsm1530@ieee.org

Abstract: Cloud computing models have emerged to be a key player in the field of information processing in the recent decade. Almost all the services related to data processing and storage from firms work on a cloud platform providing the requested services to the consumers at any point of time and location. Security is an essential concern in cloud models as they primarily deal with data. Since multitude of user's access cloud by way of storing confidential information in the virtual storage platform or accessing vital data from archives, security and privacy is of prime concern. This has been taken as the motivation of this research work. An effective Chaotic based Biometric authentication scheme for user interaction layer of cloud is proposed and implemented in this research paper. The proposed method uses fingerprint as the biometric trait and varies from conventional methods by utilizing a N-stage Arnold Transform to securely verify the claim of the so-called legitimate user. The experimentations have been compared with existing benchmark methods and superior performances observed in terms of detections, false detection accuracy etc.

Keywords: Cloud computing, Security, Biometric Authentication, Arnold Transform, Sensitivity, Specificity.

I. INTRODUCTION

The field of information processing and communication has evolved to be a dominating stakeholder in today's technological competition on a global scale. Most of the real time

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

technologies and applications deal with high resolution data which are mostly bulk in nature. Significant research in these fields of information technology have given birth to concepts of Big Data and Cloud Computing. Cloud computing has completely transformed the dimension of data processing and servicing to the consumers in a focused manner to reduce the sophisticated life of human beings. With active implementation of cloud concepts in most of information technology processing firms, consumers can now access seamless data on demand irrespective of geographical location and time. Advent of state-of-the-art communication standards like 4G, 5G etc. have further accelerated the user experience from cloud environments. Cloud frameworks primarily refer to a virtual provision of services on a demand basis to the consumers by appropriate and effective allocation of resources demanded by the consumers. These services are generally provided on a lease or pay-on-the-go basis, thus aiding consumers to access their required data on the move. Cloud platforms like SaaS, PaaS and IaaS aid in provision of require services to the consumers. A typical cloud network infrastructure is depicted in figure 1 shown below.

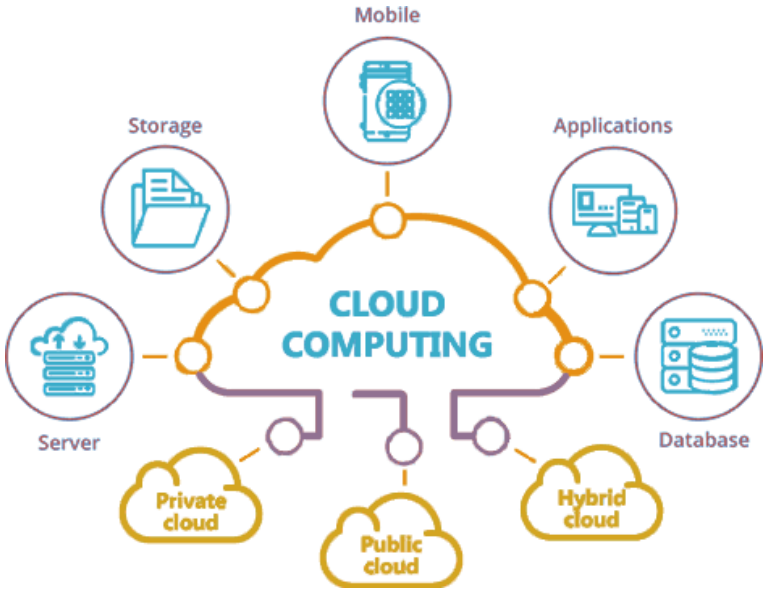

Figure 1 Illustration of Cloud Computing Schema
[Courtesy: Network Encyclopedia]

As depicted in figure 1, it could be well understood that a variety of applications are being catered to by the cloud-based services. It is also to be noted that most of the existing

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

information processing firms have migrated towards provision of cloud-based services. A typical example could be the recent cloud-based provision of Microsoft 365 for users on a rental or pay-per-use basis. The services of the recently upgraded Microsoft Office are being provided to users on a rental basis. Cloud operates in basically three layers namely the user interaction layer, middleware, and the data storage center. Since, clouds basically deal with data, the manner of clouds handling the data with utmost privacy and security is a prime issue of dictating their efficiency. With rising threats of hackers and tampering of data in recent times, a fool proof and robust system of security implementation is one of the prime issues of designing the cloud to earn the trustworthiness of the users which leads to improvement of its quality of service (QoS). In addition, it is interesting to note that, different types of threats are imminent on various layers of the cloud and hence appropriate security measures and protocols need to be put in place at various layers to develop a robust system. In this research paper, a simple yet efficient security system is proposed and implemented for the primary layer or the user interaction layer. Since, users access data or store data at this layer or through this layer, the data is being exposed to a multitude of attacks with the most predominant one being the authentication-based security threats. Biometrics form an integral form of authentication-based security systems as they are considered and known to be unique in their features. Common examples include retinal based authentication, palm print and finger vein-based biometrics and the well-known fingerprint-based authentication scheme. The latter has been chosen as the biometric trait for proposing a chaotic authentication scheme to improve the robustness of existing biometric schemes. The rest of the paper is organized by providing a brief survey of related works related to biometric security systems in section 2 followed by the proposed chaotic transform-based cloud security model in section 3. Section 4 provides the findings of the experimentations with the inferences being summarized in section 5 of the paper.

II. RELATED WORKS

Research on cloud computing security models have been on the rising trend in the past two decades. Many robust schemes have been put forward effectively for various levels and types of security in the cloud. However, since the objective of the proposed work lies in

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

authentication-based security model at user layer level of cloud, the survey of literature has also been limited to the user interaction layer pertaining to authentication-based security system.

Fingerprints have been found to be used as common biometric traits in public applications due to their ease of utility by consumers [1]. In addition to being unique, they offer a straightforward approach from a consumer perspective. In spite of biometric based methods being unique in their traits or patterns, [2] identifies certain vulnerabilities as far as security and privacy preserving features are concerned. Some of the vulnerabilities include privacy intrusion, duplication attacks, utilization of synthetic materials for lifting the fingerprints and replay attacks [2]. However, in spite of all these vulnerabilities, they are the prime candidates as far as security systems are concerned and have proved to be robust candidates towards a wide range of attacks. The literature also discusses other biometric traits like the palmprint based authentication system [3] where frequency domain transforms are rigorously applied onto them to extract critical features for template matching. Moreover, this literature also provides an essential fact that choice of transform depends on the input being taken and the target that is to be achieved. For instance, in [3], the palmprint is subjected to Contourlet transform as palmprints are characterized by circular and curved irregularities for which Contourlet transform best approximate them. In case of fingerprints characterized by ridges and valleys, Ridgelet transform is considered an ideal choice however at the cost of increasing complexity. Fusion based methods are applied to fuse the various features extracted from the input sample in frequency domain. A review and experimental proof of such fusion methods applied towards medical images have been observed in [4].

Voice based protocols and methods have also been used as authentication methods or gateways [5]. MFCC (Mel Frequency Coefficients) are considered best approximators for such applications. Fingerprint based authentication methods are being increasingly utilized in IoT based systems [6]. IoT systems have emerged to be predominant stake holder in the fields of smart computing and automation systems. IoT users at different terminals acquire data and transmit them to the control station during the process of which the data being transmitted may be vulnerable to attacks. Moreover, tampering attacks at the node points itself is a challenging issue. Biometric based systems and key generation methods best help to create a fool proof and

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

robust system. These systems also best help in mobile based IoT devices where authentication is a mandatory process to secure the device. The literature [7] provides an elaborate discussion on various state-of-the-art algorithms which help in implementing or classifying genuine or impostor users. Most of these authentication schemes work best under training methodologies where a given set of input samples are used as training data to impart knowledge to the intelligence system. Several methods are found to be effective such as LSTM, Deep Learning Convolutional Neural Networks, Random Forest, Support Vector Machines etc.

Off late, as mentioned in the previous section, most of information processing concerns have migrated their services to cloud platforms where services are rendered to users on demand. Authentication of the legitimate user from the impostor is an important criterion to hold together the overall security of the cloud framework [8]. Any lapse at any layer of cloud leads to irreversible consequences and compromise of sensitive user data. A user layer in cloud is extremely critical as it is the point where cloud services interact with the user for data transfer/access applications. Hence, security at this primary layer is quite critical. Biometric authentication schemes prove to be ideal candidates for developing a secure and robust system of primary layer cloud access [9] where efficient classification methods help to segregate legitimate from impostor users. Template matching schemes [10 -11] based on query and knowledge base have been used as prominent methods in most of biometric authentication systems in cloud. Some methods [12] have utilized two factor authentication schemes for cloud platforms. Two factor authentication schemes along with password-based schemes are found to improve the efficiency of the security system. Multimodal systems and face based biometrics are also predominantly used in literature [13 – 14]. Template protection [15] and Concept of share-based biometrics is also gaining widespread significance in recent time [16].

III. PROPOSED WORK

It is well-known that a large volume of user's work on the base layer of cloud by way of storing their valuable data or accessing their required information. During this process, it is very essential that data being stored or accessed is done by the concerned person and not by any impostor who may try to get hold of vital data or tamper them. In existing cloud models, various authentication schemes are put in place like PIN based verification, OTP based methods,

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

passwords, CAPTCHA etc. However, the former methods suffer from certain limitations wherein the user may not get access to the OTP at that instant of time or lose the PIN issued etc. Biometric methods are found to be effective in such cases and in addition, their well-known feature of uniqueness adds more flavor to their efficiency. As observed from the brief survey of literature in section II, a large volume of research is focused on biometrics which may be unimodal or multimodal. In the proposed work, a unique and novel method of double stage verification process of authentication is proposed and implemented. Three key phases of implementation are identified and elaborated below in a systematic manner. This is conceptually depicted in figure 2 shown below.

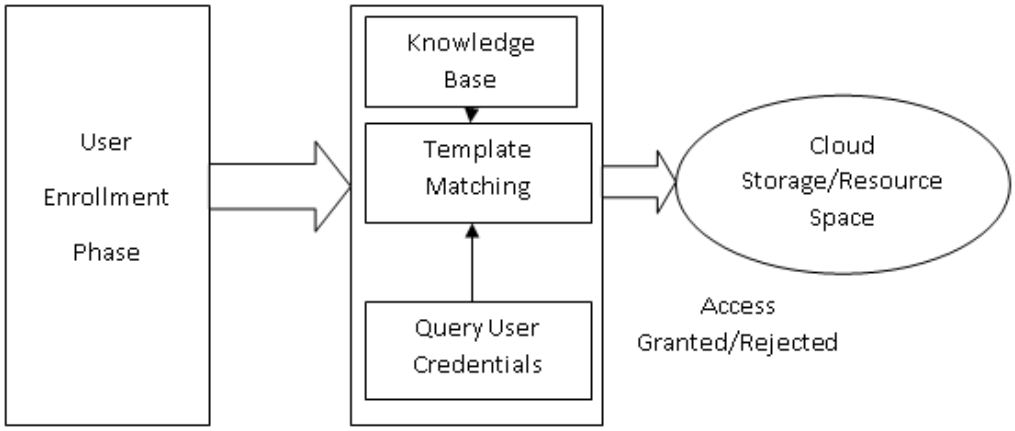

Figure 2 Proposed Template Matching based Fingerprint Authentication Scheme for Cloud

Phase I: User Enrollment

In this phase, as like any other methods, the users are supposed to register their fingerprints in the enrolment phase. The fingerprint samples of the users are collected. Five samples from any hand or combination could be taken in the proposed work. It could be either three from left hand or two from right hand or vice versa. However, in the proposed work, it is desired that the five-tuple sample be collected from a combination of both hands. This could be formulated as

$$U_{Enrol} = \{L1, L2, R1, R2, R3\} \quad (1)$$

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

As per equation (1), for a sample instance, two samples from left hand and three samples from right hand are taken in the enrollment phase. Following the user enrollment, the images are preprocess using a median filter to enhance the contrast of these images.

$$U_{input} = medfilt(U_{Enrol}) \tag{2}$$

Each of the sample collected in equation (2) is subjected to Arnold transform to scramble the corresponding input. A N-level Arnold transform is utilized for this purpose. The process could be modeled as follows

Considering the input to the Arnold transform to be L1 which generates four different features as

$$\begin{bmatrix} 4 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} \tag{3}$$

Where 4,1,1,1 is considered to four critical features generated from L1 sample, the Arnold transform in the proposed method transforms (3) as

$$\begin{bmatrix} 4 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} \rightarrow \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} \tag{4}$$

The above equation is applicable for a one level Arnold transform and satisfies the linear equation property. The Arnold transform is applied on all the remaining four samples to generate a feature vector $\overrightarrow{U_{DB}}$ which constitutes the knowledge base or the data base. These scrambled features as observed in equation (4) are normally referred to as shares.

Phase II: User Authentication and Verification

In this phase, the query or the claimant enters the credentials in the form of fingerprint trait. In the proposed work, it is sufficient to the enter any one of the samples from among the 5-tuple biometric input. Following the input to the system, the chaotic two stage Arnold transform is applied on the query biometric trait and five shares are generated. These five shares are compared with the five shares in the knowledge base. The proposed system is designed such that, only if all the five shares are matched perfectly, the user is identified as a genuine user. If any four shares match, a second opportunity or trial is offered to the claimant. On a consequent failure, the claimant is denied access and identified as an impostor. A simple flow process of this stage is depicted in figure 3 shown below.

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

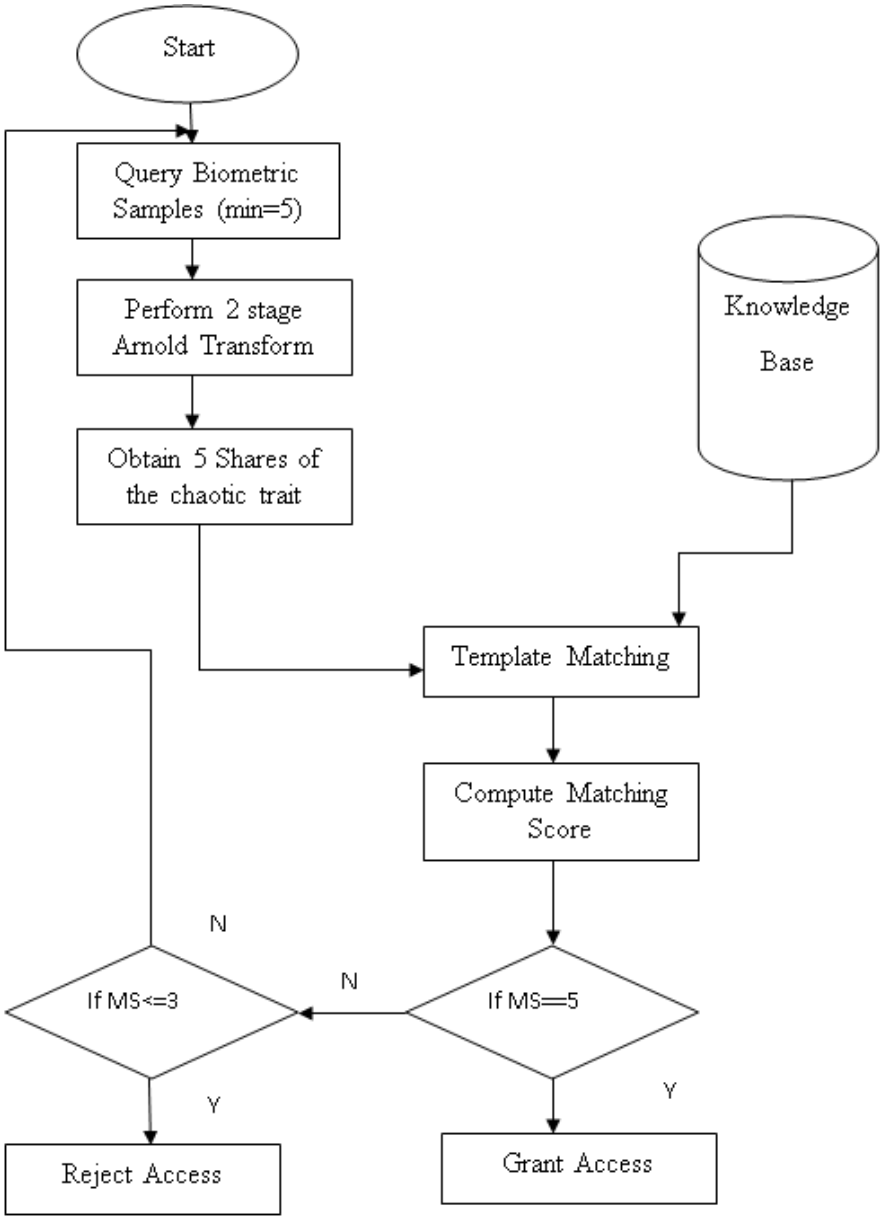

Figure 3 Proposed User Authentication and Verification Scheme – Process Flow

As observed from figure 3, the initial phase involves user data registration which involves the credentials which is the biometric trait in the proposed case. A minimum of 5 samples which are a combination from both hands are taken so as to make the target matching score as equal to 5. Variation of sample number should be reflected appropriately in the matching score. Chaotic 2 level Arnold transform is applied on the user registration data to formulate the data base grouped

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

into classes without any grouping algorithms. Following this the query data is compared using standard template matching process. A matching score of 5 grants access while any score greater than 3 – 4 is given another attempt while any score less than 3 is rejected and labeled as impostor.

Phase III: Processing and Verification Scheme

This is the base or platform for processing the query as well as enrollment data of the user. Each of the sample undergoes certain processing stages to generate a feature vector. A general scheme of the processing stage of the sample is depicted in figure 4 shown below.

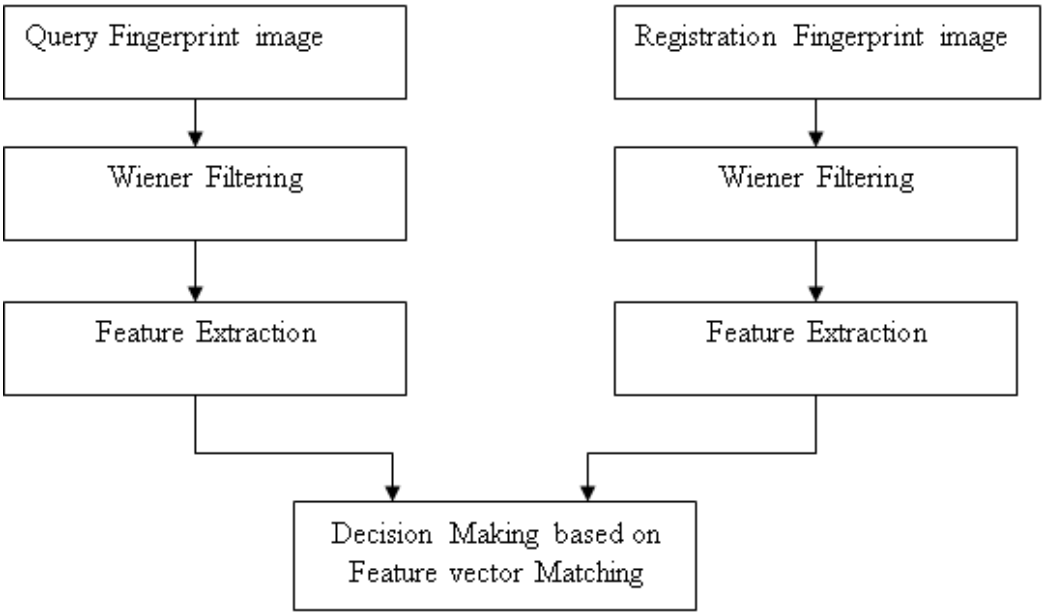

Figure 4 Biometric image processing schema in proposed work

As depicted in figure 4, all image samples are subjected to preprocessing for removal of noise through a simple yet effective Wiener filter. Following the filtering process, the minutiae point of the fingerprint from the chaotic map are extracted to form the feature vector. The parallel process is applicable for query image. Both the feature vectors are compared based on simple AND - OR rules. Based on the merits of each rule, the matching score is calculated, and the cumulative score is used for decision making of the status of the query or claimant user. A

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

vast experimentation has been carried out in this research work. The findings are presented in section IV.

IV. RESULTS AND DISCUSSION

A real time experimentation has been conducted in the proposed work. 50 users have been considered for testing the proposed methodology. A total of 250 fingerprint samples have been collected and registered in the database after the processing as depicted in figure 2. 4 Sample images are depicted in figure 4 shown below.

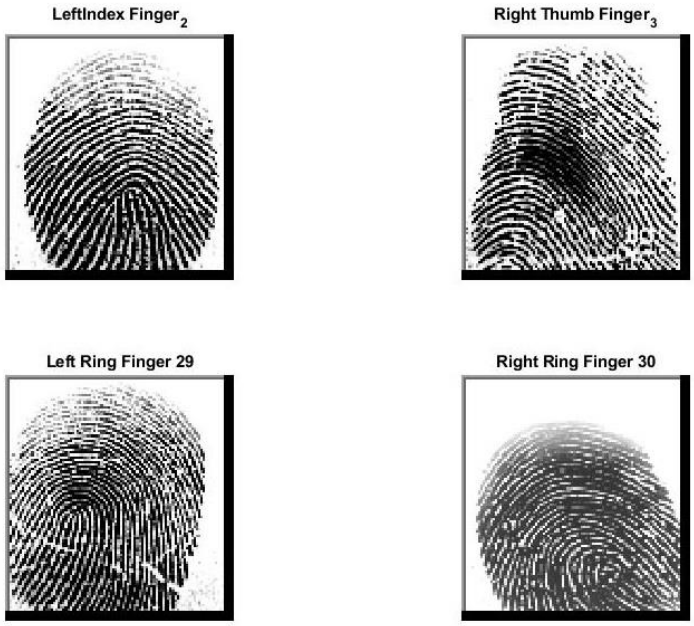

Figure 5 Biometric samples taken for investigation (Ex – 4 samples)

The above samples are taken from left index finger, right thumb finger, left ring finger and right ring finger depicting the various combinations that have been taken. Apart from these four samples, a total 246 samples have been taken for the research investigation.

The two-level Arnold transforms for SAMPLE_Left_Index_Finger_2 and SAMPLE_Right_Thumb_Finger_3 is depicted in figures 6 and 7 shown below.

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

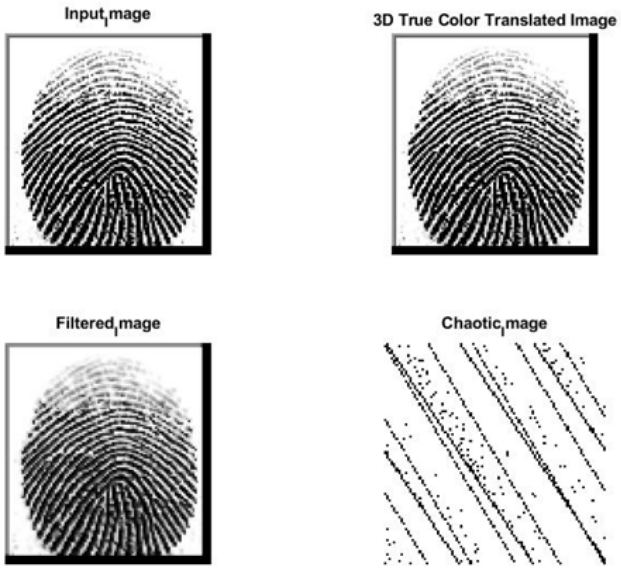

Figure 6 Two level chaotic Arnold Transform for SAMPLE_Left_Index_Finger_2

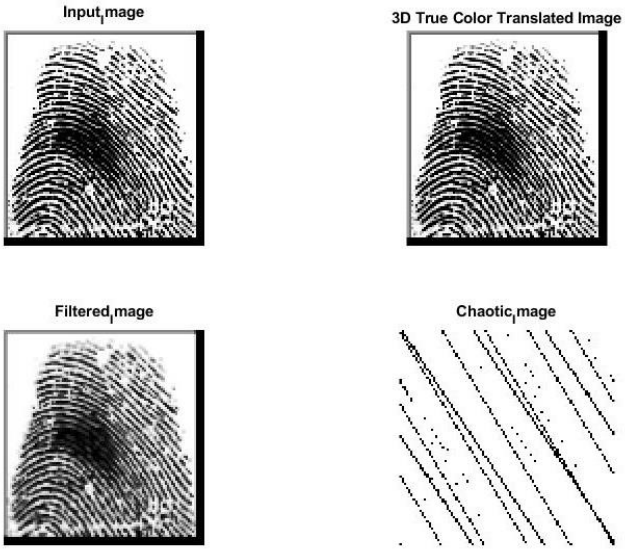

Figure 7 Two level chaotic Arnold Transform for SAMPLE_Right_Thumb_Finger_3

In all, a total of 250 such samples have been processed. Preprocessing has been done by Wiener filter owing to its efficiency at simple computational complexity. The minutiae points extracted for the feature vector in the chaotic form thus validating the security measure adopted

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

in this method. The query image is processed in same manner and the feature vectors are compared using template matching methodology using a combination of AND-OR rules thus generating the matching score. The efficiency of proposed method has been tested with various benchmark performance metrics like True Positive Rate, True Negative Rate, False Positive Rate and False Negative Rate based on which the overall accuracy has been computed. The performance has been compared against three benchmark methods to validate the superiority of proposed work. The various results observed and recorded are listed in this section. False acceptance rate (FAR) and False Rejection Rate (FRR) have been used as benchmark metrics. Table 1 lists the performances against various user scenario.

Table 1 Performance analysis of proposed biometric scheme using FAR and FRR

No. of user cases	FAR %	FRR%
10	0	5.14
20	0	6.16
30	1	7.01
40	0	7.55
50	1	9.1

Table 1 presents the FAR and FRR metrics which are critical to defining the overall efficiency of proposed biometric scheme. The data base has been varied from 10 to 50 in steps of 10 users and analysis done. It could be observed that most cases registered a FAR of 0% which is desired. In some cases, a 1% FAR is reported. This is primarily due to poor registration done by user with differing orientation angles. Table 2 presents the matching scores from 1 – 5 for varying user numbers.

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

Table 2 Performance analysis of proposed biometric scheme using matching scores

No. of user cases	Matching Score	Status
10	1	REJECTED
20	5	ALLOWED
30	3	REJECTED/RETRY
40	5	ALLOWED
50	4	RETRY

As observed in table 2, a query user claiming access to the data base or cloud primary layer with varying number of database numbers is analyzed. The Reject and retry is mostly due to improper placing of fingerprint and registration phase. Impostors are also identified. This has been tested and verified in row 1 where the query user is not in the given 10 sets of users in the knowledge causing it to be rejected with a poor matching score of 1. However, the same user is present in the second set of 11 – 20 users and is allowed access. The same user is rejected due to improper placing of fingerprint as can be seen in rows 3 and 5. The running time analysis has been presented in table 3 compared with three recent methodologies

Table 3 Performance analysis of proposed biometric scheme – Execution time (ms)

Technique	Preprocessing	Extraction	Matching	Total (ms)
Vitello *et al.* 2015	45.1	13.7	3.8	62.6
Proposed Work	40.1	14.1	2.5	56.7

As observe in the comparative analysis shown in table 3, a 9.42% improvement in computational time is observed thus justifying the simplicity in computational complexity in the proposed work.

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

V. CONCLUSION

An efficient chaotic two stage Arnold transform based biometric authentication model has been proposed and implemented for a user layer cloud model to ensure a robust performance towards illegitimate or unauthorized access or entry into cloud resources. The complexity of the proposed system is simple yet efficient enough to fend off impostor attack. Fingerprint has been taken as the biometric trait and a simple template matching technique has been applied to compare the query share with the scrambled shares in the knowledge base of the system. The performance metrics have been evaluated over several attempts and users over a customized data set to replicate a real time implementation. Superior performances have been observed over key metrics such as true positives, reduced false alarm detections and detection accuracy. Future work of this work is to extend the implemented work to a multimodal system and improvement in detection performance by utilizing the learning concepts of neural networks. A constrained two-time attempt to validate the query claim is observed to be a limiting factor but at the cost of improved security and robustness against unauthorized entry.

REFERENCES

[1] Hemalatha, S. (2020). A systematic review on Fingerprint based Biometric Authentication System. *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, Vellore, India, 2020, pp. 1-4, doi: 10.1109/ic-ETITE47903.2020.342.

[2] Zhang Rui and Zheng Yan, (2019). A survey on biometric authentication: Toward secure and privacy preserving identification. IEEE access. 7: 5994 – 6009.

[3] Prasad, S. M., Govindan, V. K. and Sathidevi, P. S. (2011). Palmprint authentication using fusion of wavelet and contourlet features. Secured Communication Networks. 4(5): 577-590.

[4] Kathiresan, N. and Samuel Manoharan J. (2015). A comparative analysis of fusion techniques based on multi resolution transforms. National Academy Science Letters. 38: 61 – 65.

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 01
Pages: 36-51
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.1.004

[5] Galka, J., Masior, M. and Salasa, M. (2014). Voice authentication embedded solution for secured access control. IEEE transactions on consumer electronics. 60(4): 653 – 661.

[6] Kanchana (2018). Fingerprint based biometric authentication in IoT for resolving security challenges. International Journal of Research and Analytical Reviews. 5(4): 1000 – 1003.

[7] Ferrag, M. A., Maglaras, L., Derhab, A. (2019). Authentication and Authorization fr Mobile IoT devices using features: Recent Advances and Future Trends. Security and Communication Networks. 2019. https://doi.org/10.1155/2019/5452870.

[8] Fan, K., Tian, Q., Wang, J., Li, H. and Yang, Y. (2017). Privacy protection-based access control scheme in cloud-based services. China Communications. 14(1): 61-71.

[9] Padma, P. and Srinivasan, S. (2016). A survey on biometric based authentication in cloud computing. *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, 2016, pp. 1-5, doi: 10.1109/INVENTIVE.2016.7823273.

[10] Chang H., Choi E. (2011) User Authentication in Cloud Computing. In: Kim T., Adeli H., Robles R.J., Balitanas M. (eds) Ubiquitous Computing and Multimedia Applications. UCMA 2011. Communications in Computer and Information Science, vol 151. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-20998-7_42.

[11] Rakhshanda Batool, Ghazal Naveed and Abdulhaq Khan. (2015). Biometric Authentication in Cloud Computing. International Journal of Computer Applications. 129 (11):6-9.

[12] Yassin, A. A., Jin, H., Ibrahim, A., Qiang, W. and Zou, D. (2012). Efficient password-based two factors authentication in cloud computing. International Journal of Security and its Applications. 6(2): 143–148.

[13] Selvwal, A., Gupta, S. K. and Surender. (2017). Low overhead Indexed Template Security Scheme for Multimodal biometrics. Journal of Intelligent and Fuzzy System. 32: 3325 – 3337.

[14] Kumar, T, Jangra, S. and Bhushan, S. (2017). Face Recognition with decision tree using SVM and SURF. International Journal of control theory and applications. 10(15): 173 – 180.

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021

[15] Jin, Z., Teoh A B J., Ong, T. S. and Tee, C. (2012). Fingerprint template protection with minutiae-based bit string for security and privacy preserving. Expert System Applications. 39(6): 6157 – 6167.

[16] Chiu, P – L., Lee, K- H. (2019). Efficient constructions for progressive visual cryptography with meaningful shares. Signal Processing. 165:233 – 249.

ISSN: 2582-4252 (online)
Submitted: 29.02.2021
Revised: 13.03.2021
Accepted: 24.03.2021
Published: 09.04.2021