Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021)
IEEE Xplore Part Number: CFP21OAB-ART; ISBN: 978-1-7281-9537-7

2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) | 978-1-7281-9537-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICAIS50930.2021.9395964

A NOVEL PRIVACY PRESERVING BIOMETRIC AUTHENTICATION SCHEME USING POLYNOMIAL TIME KEY ALGORITHM IN CLOUD COMPUTING

Dr.Praveen Tumuluru
Assistant Professor
Department of CSE
Koneru Lakshmaiah Education Foundation,
Vaddeswaram AP, INDIA
praveenluru@gmail.com

Dr.Lakshmi Ramani Burra
Assistant Professor
Department of CSE
PVP Siddhartha Institute of technology,
Kanuru, Vijayawada, AP,INDIA,
ramanimythili@gmail.com

Dr.Durga BhavaniDasari
Assistant Professor
Department of CSE
Koneru Lakshmaiah Education Foundation
Vaddeswaram AP, INDIA
bhavani.dd@kluniversity.in

Mr. CH.M.H. Saibaba
Assistant. Professor
Department of CSE.
Koneru Lakshmaiah Education Foundation
Vaddeswaram AP, INDIA
saibaba.ch77@gmail.com

Ms. B.Revathi
Assistant. Professor
Department of CSE.
Koneru Lakshmaiah Education Foundation
Vaddeswaram AP, INDIA
6revathi@gmail.com.

Mr. B.Venkateswarlu
Assistant Professor.
Department of CSE
Koneru Lakshmaiah Education Foundation.
Vaddeswaram, AP, INDIA
bvenki289@gmail.com

Abstract: In recent years the biometric identification has become more popular. With the quick advancement of distributed computing information base proprietors are endeavoring to redistribute the huge volume of biometric information and ID assignment to the cloud to kill the costly stockpiling and calculation costs. In this paper it proposes a Novel Privacy Preserving Biometric verification Scheme utilizing Polynomial Time Key Algorithm in Cloud Computing[1][4]. The algorithm increases the authenticity at time when users access the data. The main objective is to increase the security for user with the polynomial time key which generates the six random keys. At first, one private key generates the one time password by using the present time, date, year, alphabet and numerical letter. Then, the Polynomial time key algorithm will generate the remaining keys [2][7].

Key words: Cloud Computing, Biometric identification, polynomial time key algorithm.

I. INTRODUCTION

Biometric identification is a significant method that allows of determining the identity of an individual based on its essential qualities like facial features, Iris pattern, and Finger print verification. Among all these essential qualities the finger print is unique since the probability of two individuals does not have the same finger print and durable since it does not change over a period of time[3] [5].

Recently, huge numbers of the specialists have proposed diverse security saving unique mark check frameworks which utilize an unbalanced homomorphic encryption calculation to encode the unique finger impression information with the goal that solitary key proprietors can get to their fingerprints[6][9]. In spite of the fact that the frameworks guarantee for protection safeguarding confirmation, however the computational expense of the encryption calculation is huge. In this way, they are not

versatile as the expanding number of customers.

A number of privacy-preserving biometric verification solutions are proposed[8][10]. But, most of them are mainly focus on preserving the privacy but neglects the performance, like the schemes depends on homomorphic encryption and careless exchange in for unique mark and face confirmation separately[11][14]. With the proficiency issues of neighborhood frameworks, these plans are not effective when the size of the information base is huge System model.

The proposed strategy has three items as customer, worker and cloud which are appeared in Fig.1. The customer encodes and enlists the people unique mark [12]. For check or distinguishing proof, the customer scrambles and communicates a most recent inspected unique mark to the cloud [13].

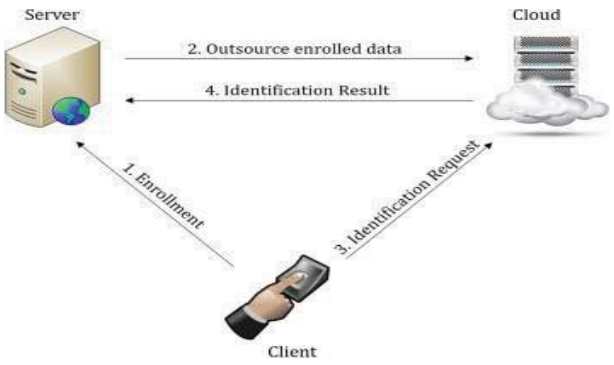


Fig.1: The proposed System model

The method adopts a matching system known as filter bank based fingerprint which uses for other verification of biometric schemes [15][17]. By utilizing the Finger code which is a chain of M free component codes gives high exactness by estimating the Euclidean separation between the fingerprints.

Risk model

The invader exists outside the system and seeks the data which send by the clients. The goal is to accomplish the crude information of customers, for example, unique mark and sidestep the check cycle and access the information worker. Thus, it is noteworthy that the biometric information is to be shielded from trespassers [16][18].

Distinguish the cloud as special and credible substance which performs exact in numerous cases. Also, there ought to be a presumption that the cloud with an external foe to reestablish the unique mark information of a customer to accomplish the unlawful advantages. Likewise, the information worker is additionally to be extraordinary about the unique mark data [19][20]. An information worker offering support to a customer doesn't basically demonstrate that permitted to get to the customers fingerprint data.

Scheme goal

The scheme objective is a triple. In the first, in enlistment and distinguishing proof the Fingerprint data ought not be unveiled any items containing the worker and cloud [27][28]. Second, the proposed framework ought to have the option to build security through the produced key [21][22]. At long last, the confirmation about calculation and correspondence ought to be viable.

II PROPOSED SYSTEM

In this work, it proposes an effective privacy preserving authentication scheme by using polynomial time key algorithm, which generates six random keys based on the

attributes that is date and time of upload of data [23][25][26]. From those six keys, the one main key generates for accessing the data and can declare the security for data.

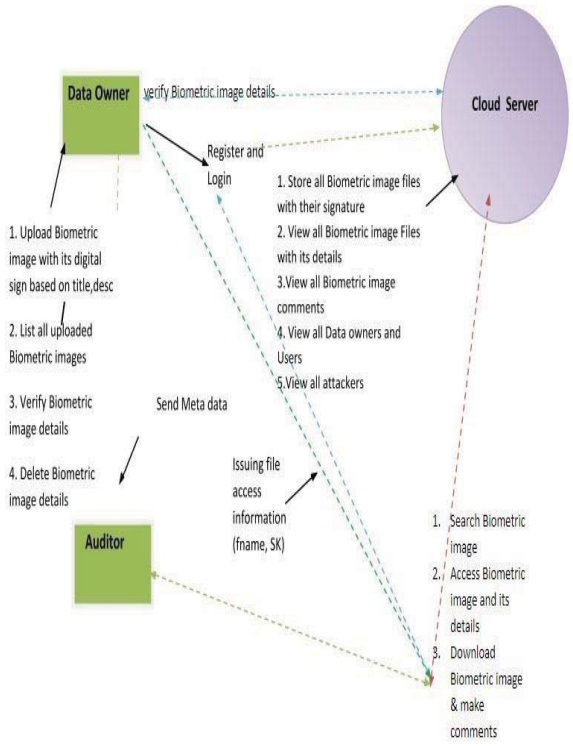


Fig.2: The proposed architecture

Architecture:

The proposed architecture is shown in the figure 2

The architecture contains the following components:

1) Data owner
2) Auditor
3) Cloud server

These are the main basic components that are required to fulfill the goal.

1) **Data Owner**: Data Owner uploads biometric image and list all uploaded biometric images, verifies biometric image details and also deletes unauthorized biometric images.

2) **Cloud Server**: Cloud server stores the biometric images with digital signatures. Allows a space for algorithm to generate keys and communicate with users and data owners [24].

3) **Auditor:** Auditor creates meta data to validate biometric images that are uploaded by the data owner. Send keys to users and also grant permission to users and also maintains records of data owner and user details.

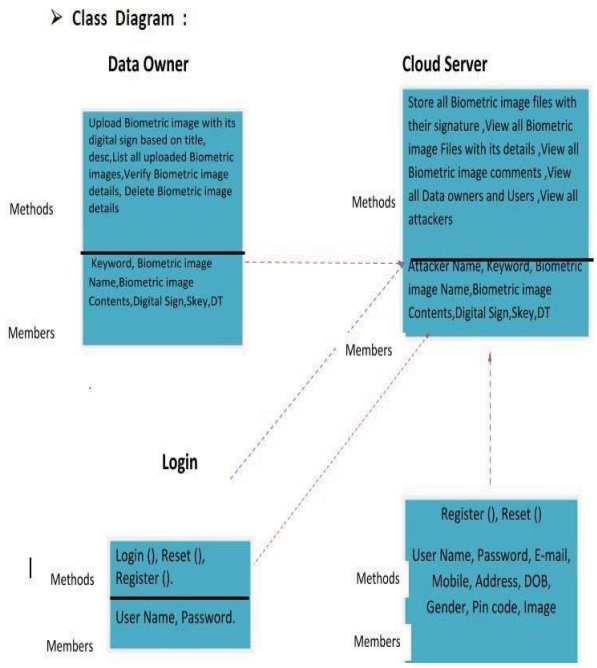


Fig.3: Class diagram between the components

III RESULTS AND DISCUSSION

Performance Analysis:

To assess the exhibition of the proposed conspire, actualized a cloud-based protection saving fingerprint confirmation framework.. To construct the hands-on biometric verification scheme, used two databases with different sizes.

Results and Discussion

The results of the proposed system is shown in the following figures

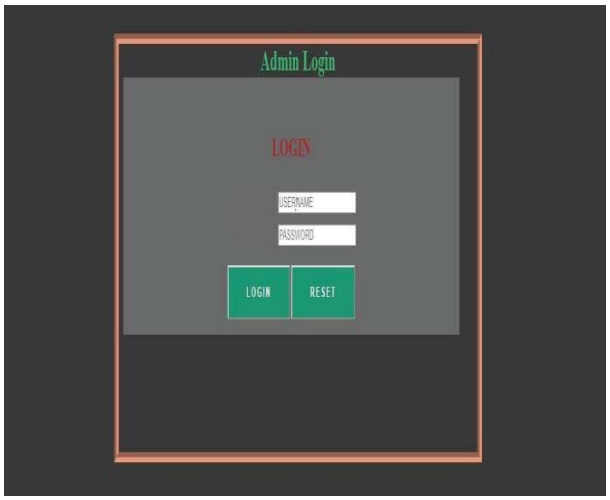


Fig. 4: Admin login

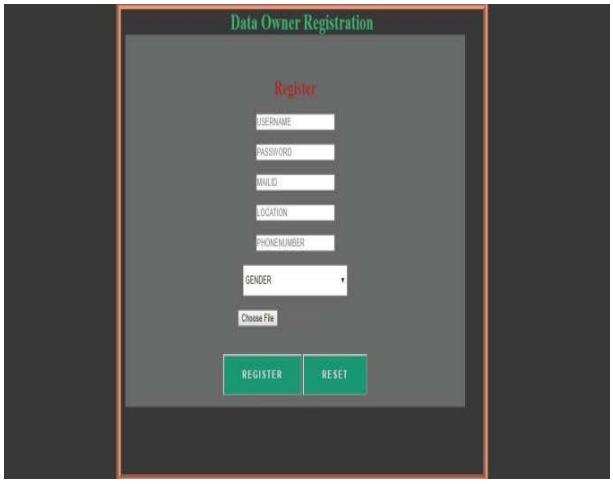
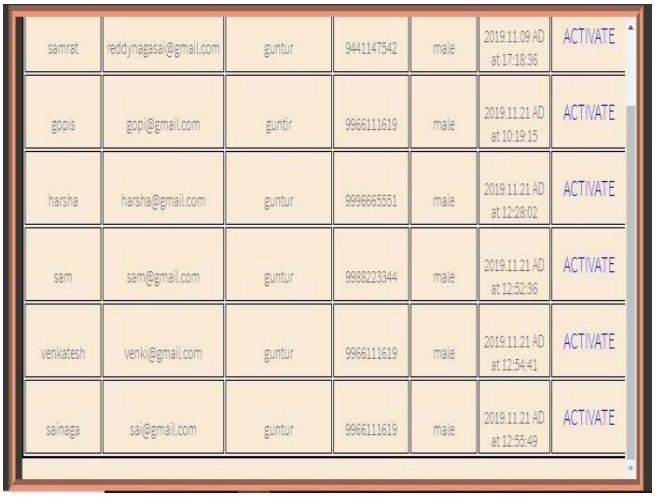


Fig. 5 Data owner Registration

The Fig. 4 shows the admin log in page to access the system. The Fig. 5 demonstrates the Data owner Registration where at the owner will register by uploading biometric and all other details



samrat	reddynagasai@gmail.com	guntur	9441147542	male	2019.11.09 AD at 17:18:36	ACTIVATE
gopis	gopi@gmail.com	guntir	9966111619	male	2019.11.21 AD at 10:19:15	ACTIVATE
harsha	harsha@gmail.com	guntur	9996665551	male	2019.11.21 AD at 12:28:02	ACTIVATE
sam	sam@gmail.com	guntur	9988223344	male	2019.11.21 AD at 12:52:36	ACTIVATE
venkatesh	venki@gmail.com	guntur	9966111619	male	2019.11.21 AD at 12:54:41	ACTIVATE
sainaga	sai@gmail.com	guntur	9966111619	male	2019.11.21 AD at 12:55:49	ACTIVATE

Fig. 6: Stored Details

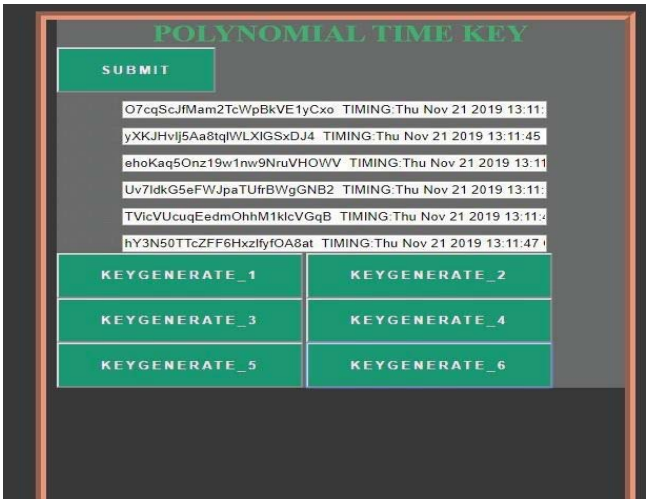


Fig. 7: Generation of key

In Fig. 7 it shows the generation of six keys which is mentioned in the system. From these six keys one main key is generated.

IV CONCLUSION

In this work, projected a Novel Privacy Preserving Biometric Authentication Scheme using Polynomial Time Key Algorithm in Cloud Computing. The algorithm increases the authenticity at time when users access the data. The main objective is to increase the security for user with the polynomial time key which generates the six random keys. To recognize the efficiency and secure requirements, designed a novel encryption algorithm and authentication. This method is a useful method to securely safe the data from the invaders and an effective method of encrypting the data for the better safety of the user and put the data in a cloud for all dangerous attacks.

REFERENCES:

[1] S.Wong, et al, A privacy preserving biometric matching protocol fir iris-codes Verification, FTRA International Conference on Mobile, Ubiquitous, & Intelligent Computing, IEEE_2012.

[2] K.Sai, et al, 'A smart industrial pollution monitoring system using Iot', International Journal of Innovative Technology & Exploring Engg_2019.

[3] Sushma , et al 'Cardiac disease prediction using naÃve bayes machine learning algorithms', International_Journal of Engg & Advanced Technology_2019.

[4] Shaik.S., et al 'A novel framework for investigation of cloud attacks', International Journal of Advanced Science & Technology_ 2019.

[5] Ravindra K. et al, 'An efficient cloud storage management optimal with deduplication', International Journal of Innovative Technology and Exploring Engineering_2019.

[6] Dasari et al,'A framework for multipurpose cloud based data entre network security',International Journal of Applied Engg Research_2017.

[7] L.S.S.Reddy., 'Distributed based serial regression multiple imputation for high dimensional multivariate data, in multicore environment of cloud', International Journal of Ambient Computing & Intelligence_2019.

[8] Praveen Tumuluru et al. "OpenCV Algorithms for facial recognition", International Journal of Innovative Technology & Exploring Engg June_2019.

[9] P., Bharadwaj et al "Implementing robots in defense through motion capture with mixed reality", International Journal of Engg and Technology.

[10] Romadhani et al , Face Authentication by fitting a morph able model using Linear shape and texture error Functions .In Europe Conference on Computer Vision Springer , Berlin ,Heidelberg_2002.

[11] Zhu,H., et al. " Efficient and Privacy - Preserving Online Fingerprint authentication Scheme over Outsourced Data". IEEE Transactions on Cloud Computing.

[12] Pan,S., Yan,S.and Zhu ,W.T.,2016,July. Security Analysis on Privacy preserving clone aided biometric authentication schemas .In Australasian Conference on Information Security & Privacy .Springer, Cham.

[13] Praveen Tumuluru, and Dr. Bhramaramba Ravi, "Chronological Grasshopper Optimization Algorithm-based Gene Selection and Cancer Classification",

Journal of Advanced research in Dynamical and Control Systems, vol.10, no.3, 2018.

[14] Praveen Tumuluru, and Dr. Bhramaramba Ravi, "GOA-based DBN: Grasshopper Optimization Algorithm-based Deep Belief Neural Networks for Cancer Classification", International Journal of Applied Engineering Research, vol. 12, no. 24, pp. 14218-14231, 2017.

[15] U. Alon, N. Barkai, et al, " Broad patterns of gene expression revealed by clustering of tumor and normal colon tissues probed by oligonucleotide arrays", vol. 96, no.12, pp.6745-6750, June 8, 1999.

[16] Praveen T, et al. "Shortest path Enhancement using improved Bellman Ford Algorithm in PPI "Journal of Engineering and Applied Sciences", Medwell Journals, 2017.

[17] Praveen Tumuluru, et al, " A Survey on Identification of Protein Complexes in Protein-Protein Interaction Data: Methods and Evaluation", in SpringerBriefs in Applied Sciences and Technology 2015.

[18] Rajakumar, R; Amudhavel, J; Dhavachelvan, P; Vengattaraman, T, "GWO-LPWSN: Grey Wolf Optimization Algorithm for Node Localization Problem in Wireless Sensor Networks", Journal Of Computer Networks And Communications, 2017, DOI: 10.1155/2017/7348141

[19] Amudhavel, Jet al, "Directed Bee Colony Optimization Algorithm to Solve the Nurse Rostering Problem", Computational Intelligence And Neuroscience 2017, DOI:10.1155/2017/6563498.

[20] Mannepalli, K, et al "A novel Adaptive Fractional Deep Belief Networks for speaker emotion recognition" Alexandria Engineering Journal 2017 DOI10.1016/j.aej.2016.09.002.

[21] Srinivasu N, et al. "Multilevel classification of security threats in cloud computing" International Journal of Engineering and Technology(UAE) (2018)

[22] Tumuluru, P., Lakshmi, et al, "A Review of Machine Learning Techniques for Breast Cancer Diagnosis in Medical Applications "Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019.

[3] Narasinga Rao, M.R, & Venkateswarlu, S, 2018, " A proposal for observing conceived ladies having high risk of premature using WHSN", International journal of Engineering and Technology(UAE), vol.7, no 2, pp. 53-56.

[24] Chintala, R.R., et al, 2018, " Review on the security issues in human sensor networks for healthcare applications", International journal of Engineering and Technology(UAE), vol.7, no 2, 32 special issue pp. 269-274.

[25] Potharaju, S.P, & Sreedevi, M, 2017, " A novel M-cluster of feature selection approach based on symmetrical uncertainty for increasing classification accuracy of medical databases", Journal of Engineering Science and Technology Review, vol.10, no.6, pp.154- 162.

[26] Shaik, R & Ahamad, S.S, 2017, " Key management schemes of wireless sensor networks a survey", Fornteiras, vol 6, no, 2, pp, 526-537.