TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

A Novel Biometric Authentication in Cloud Computing for Secure Data Transfer

Vinoth Kumar J[1], Dr. K. Venkatachalapathy[2]
[1]Research Scholar/Dept. of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University, Chidambaram, India.
[2]Prof/Dept. of Computer and Information Science, Faculty of Science, Annamalai University, Chidambaram, India.
jaivinothkumar.mca@gmail.com[1], omsumeetha@rediffmail.com[2]

Article Info
Volume 82
Page Number: 14587 - 14600
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 28 February 2020*

Abstract:
The demand towards implementing cloud services increases every day in many business organizations, individual customers and government agencies because of its convenience. When the client data is migrated from data owners to cloud the security control is also transferred to cloud service providers. So that it is essential to define a data access limit and it will help the data owners to protect the data from unauthorized access. Traditional methods use security tokens and passwords to access the remote cloud and that may be stolen or misused. In order to enhance the security this proposed model implements bio metric authentication system in end user. It uses finger prints to ensure the data access is limited to the unauthenticated cloud service providers and other users also ensures potentially offers practical and reliable option for remote access.
Keywords:*Biometric, Cloud Computing, Security, Data Transfer*.

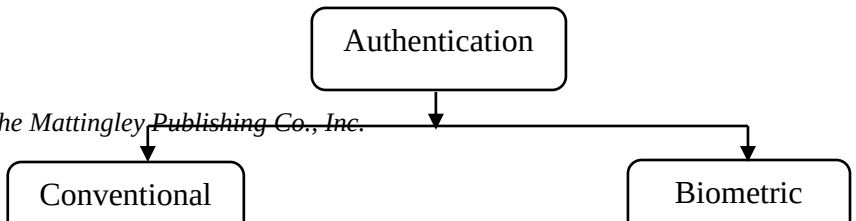
I. INTRODUCTION

Cloud computing is an emerging technology which allows multi users to request for resources through their service providers based on the demand of the environment. Proving end to end user services through internet is the key role in cloud computing which helps in modern business needs. Also, it changes the perception of people about utilization and allocation of resources as it has provision of allocating storage resources, computing power and network resources in cloud environment. So that a service-based computing model could be developed for an organization or a firm and they would pay only for their services apart from the everything like technical services, setting up of environment and maintenance of environment which improves the business value by saving the infrastructure physically. The important factor in cloud computing is integrity, availability and mainly confidentiality of the data. Since preserving the data stored over distributed database in important and the integrity refers the unauthorized data access. User authentication is essential and it reduces unauthorized data access and allows only the authorized persons as a part of cloud services can access it. Several identification methods are available like password entry, virtual one-time password entry which helps to reduce the risks in data access from unauthorized persons. One of the biggest issues in these conventional authentication systems is existence of many passwords of each user which leads them to forget the password and username some time. So that the users are used to save the passwords and usernames in some other data based and it is easy for the authorized person to gain the password information from their saved data list. Figure 1 gives an illustration about cloud computing environment for different end to end application which requires passwords for each access. If all the systems are maintained for a single firm then the user will definitely set a same password for all the access to ease their work. This gives a chance for unauthorized person to gain information from all the platforms if they cracked a single password.

January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

Fig. 1.Illustration of Multiple platformsconnected intocloud Infrastructure

Some of the users uses their simple day today terms as their passwords to remember it easily such as telephone numbers, car numbers etc and this thins can be easily guessed by the other persons so that possibility of accessing the data increases. such access to the data by unauthorized person is dictionary attack. Smart card-basedauthentication is another model which provides two factor authentications. The first authentication holds the client's information in a smart card and the second authentication in the model keeps a security password for the card which avoids the access of unauthorized access and also it doesn't need to bother about the server which holds the secret key. But the limitation is it needs a special card reader to access the data and middleware application to match the smart card and their respective models which increases the cost if the configured platforms are more in numbers. To improve this security factors in cloud computing numerous techniques are developed by researchers and the research still goes to attain the maximum secure authentication model. Figure 2 gives the classification of authentication model in cloud.



January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

Fig.2. Classification of authentication models in cloud computing

A simple and high secure authentication model from all the above is biometric based model where any of the human parts such as eyes in IRIS model, Face recognition using Image processing models are used to access the system. Since the biometric models used the human physiological traits which is differed for each one so it is easy to identify the user. But the implementation cost for such model increases more compared to conventional authentication model. So, in order to maintain secure data access with reduced cost finger print based biometric authentication models are developed. Figure 3 gives a random finger print sample and its impressions for high pressure and low pressure. Finger print based authentication gets highlighted in authentication not only because of its cost and also due to its uniqueness and Genuity. Numerous genuine applications are utilizing finger prints as their identity since the arrangements of raises and its values are stable and unique for each person. The arrangement of rims and structures are unique for each person and it remains same till their life time unless injury or everlasting event occurs. It is mechanized process which determines the uniqueness and evaluates the impression by matching the existing finger print and present.

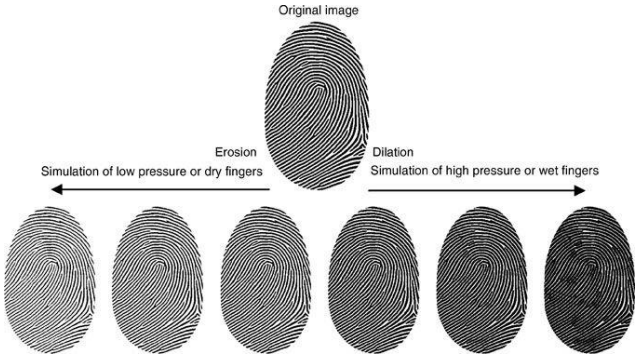


Fig.3. Finger print sample

Sometimes the wetness or dryness in the fingers may change the pattern similarly the pressure applied over the capturing device may produce inaccurate results as it couldn't validate the same

January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

which is stored in the data base. In order to sort the issue coordination calculations are essential and which precisely gives a high precision result. Three methods are available to calculate the coordination points such as particulars-based method, highlight based method and connection-based method. One of these three models are used widely in figure print based authentication applications to enhance the performance of bio metric system in all situations. In this research we initially focused on the data security and privacy with help of model which extracts the data attacks over cloud services. Then a suitable finger print based biometric authentication model is discussed with experimental procedures to authenticate with its merits and demerits in other models.

II. RELATED WORKS

Before get into the proposed model an insight about existing authentication models are reviewed and summarized in this section with its merits and demerits.The traditional method authentication models are discussed in earlier section and their demerits directly relates to data control loss, trust and multitenancy. Using token for the same is also similar failure model in authentication schemes. In case of biometric models based on the physiological and behavioural the authentication models are designed. Face recognition is used in many image processing applications as an entry authentication mechanism. A model for face recognition-based authentication without interaction is attained in literature [1] using affine transformation to achieve better security system in cloud. This eliminates the interaction between service providers and end users which in term produce issues between the user and service provider.

Similarly face recognition through a deep learning convolutional neural network [2] model to obtain the authentication results. This model has a pre trained results which is used to compare the new one. The possibility of identifying the unauthorized access may be malfunctioned if the intruder modified the trained data set. But that limitation is covered up by the researcher by introducing a multi-level authentication such as handwriting gesture recognition and one-time password generation. Overall this improves the security and also increases the implementation cost as it needs three different set up to authenticate a single data access. A unified face identification and resolution scheme in cloud computing to solve storage and power problem while face recognition is in progress. Parallel matching [3] and cloud-based framework is used to improve the efficiency and secure the data with its control by acquiring the identity of the individuals. This improves the power efficiency[4] and reduces the storage capacity [5] in the cloud environment.

Iris based model in another category in authentication modules, an Iris cloud verification model [6] to improve the authentication scheme in cloud platform is presented in the literature. It helps the users to access the service through cloud server due to its unique identification features. By comparing the acquired Iris pattern with data based and collects and matches the information[7] and then provides access to the user. So that the control of data is in user hand and the trust, multitenancy is also can be achieved these models. Iris is used as an entry level access mechanism in the research article [8]. In the second phase an encryption mechanism is used to access and similarly it has a decryption model to change the data base. The application is secure.

Data centre and its importance is well known for everyone and the limitation present in the IT industries while accessing the data centres is large. Since it is essential to secure the data centre improved iris model is developed. So, Iris based authentication model [9] to secure data centres helps the firm to secure user data and their data. In this processfor each Iris a key is used to generate in the model and that key should match while accessing the data centre. But its limitation is if the generated key is identified by the unauthorized

person then they can easily enter into data centre which may produce adverse effects. Besides all the limitation in Iris model thesetup cost is the major issue when it is implemented and maintained in a real time environment.

Finger print based biometric model is the important and simple authentication model in physiological model. Using scanned image of the finger a unique password is assigned which is stored in the data base. If the image and password match in the data base allows the user whenever the wants to access the service. Several research models are available using finger print authentication in this few better resulted modules are highlighted. Finger print model in mobile cloud computing [9] generates a secret code for biometric and it is generated based on the entropy value. This helps the person to access the data and not allows the unauthorized persons. Not only for accessing the system for accessing all the application this model is configured with finger prints which is considered as advantage. Dimension of certainty for individual check and Identification is achieved using palm print recognition for cloud environment in literature [10]. Advantage of this model present when it is implemented for a single user like mobile cloud computing but the disadvantage is data size, since it needs a large data base to store all the images of palm of users which increases the cost of storage unit if it is considered for an large organization. Figure 4 gives an illustration about security issues in cloud computing.

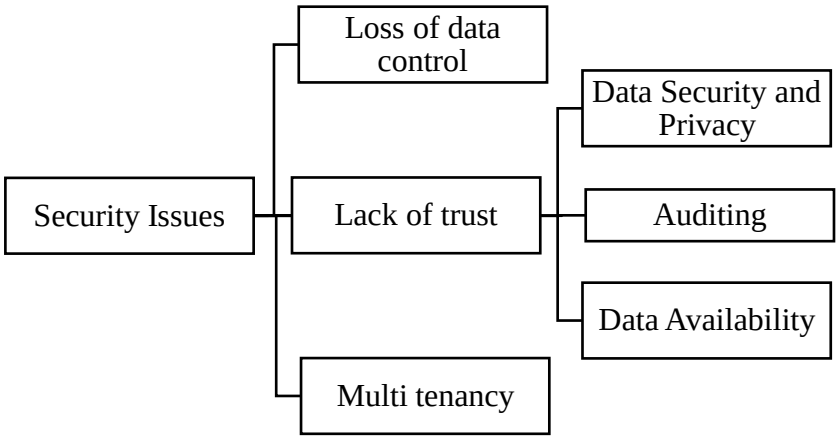


Fig. 4. Security Issues in cloud computing

Cloud auditing process used in cloud computing to obtain the trust of user to access the data from anywhere. It helps the user to retrieve the data when there is data loss or disasters happens. A periodic check is essential to analyse the changes in data over a particular time. The issues in cloud auditing is classified into two as private audit and public audit [11] which defines the verification of data by user or a third-party

application. If it is by the user then comfortable finger print based authentication model is suitable so that the user can check the process easily. In case of using third party application a secure authentication system is essential as there is a chance of data misuse. This third-party application must provide privacy to the user data and it should not learn the content of data. Because of that TPA is cost effective and also it needs professional knowledge and audit skills to perform. Considering all these issues in the cloud computing security the proposed model is developed to achieve better classification accuracy

January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

and security efficiency with minimum implementation cost.

III. PROPOSED MODEL

In order to develop a secure authentication model with public auditing protocol the proposed model is entitled with AES algorithm for generating SHA-2 hash value and RSA signature for the data model. Without introducing extra burden to user, the correctness of data, integrity and confidentiality are managed by the third-party application. These gives benefits to user, cloud server storage and TPA. Figure 5 gives an illustration of AES process in general.

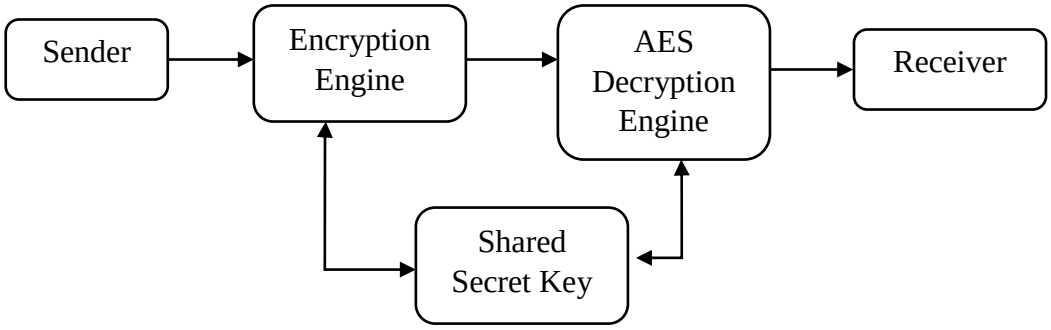
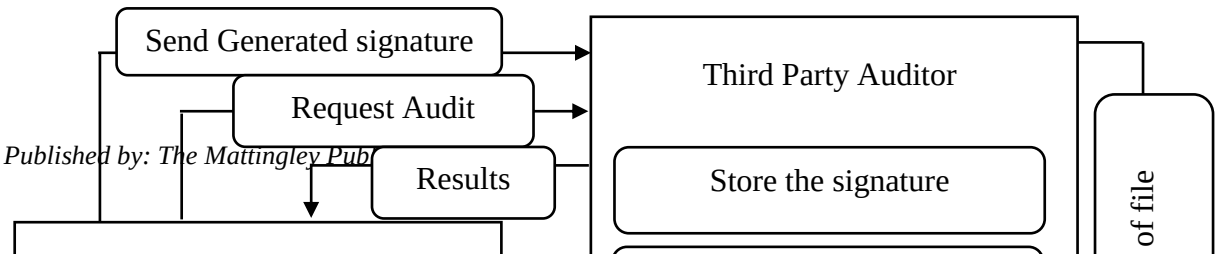


Fig.5. AES algorithm

The steps in AES is of four modules as sub bytes, shift rows, mix columns and add round key.

- In the nonlinear substitution step each byte is restored with another byte based on the value in the box so that an indirect proportion in cipher is obtained which is a matrix consists of four columns and four rows.
- Second in the shift rows each row is rotated repetitively into number of times as per the permutation each row is shifted as per the value. So that the resultant matric consists of bytes but in different order with respect to each other.
- In the mix columns step each column is changed through matrix multiplication process. Input is taken from each column and the resultant output is entirely different from the input.
- The last add round key a unique key is added to each byte so that each word in a byte is converted into multiple words of key.

The process starts with user which is responsible for splitting the data into blocks and then encrypt them using Advanced Encryption Standard (AES) algorithm. It generated SHA-2 Hash value for each block and concatenating the hashes with RSA signatures which is generated. The second process takes places in cloud server and it stores the encrypted blocks. The third process is the data auditing process which is demanded by user to TPA. Based on the request TPA retrieves the encrypted data from the server along with hash value for the blocks. TPA compared the signature generated by the user and the server and if it matched the data is intact and it was not tampered by unauthorized access. Else the data is tampered so that the integrity check is provided to the user. Figure 6 shows the architecture of proposed model.



January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

Fig. 6. Proposed model

The proposed model provides complete public auditability in hybrid cloud environment and also provides better identity. The users join themselves as a group and their information is stored in a private cloud along with the information. Biometric is used to verify whether is user is authenticated or not since the biometric is valid for some time if the user needs to modify the stored data the user needs to request cloud again for biometric image. Once the biometric is verified and it is valid then it generates the algorithm to process the data bytes. The computation cost is reduced in the proposed model by auditing the data in the private cloud and not in the user cloud. The proposed algorithm is summarized and given as below

1. To *Acquiring an ID and Fingerprint image from user.*
2. *For level 1, generate random number n = randperm (5, j) returns the row vector which contains j unique integers are selected randomly from 1 to 5 inclusive, where j = 2 (no. of divisions).*
3. *Select n(k) division from input image for k = 1: j.*
4. *Get a n(k) database image by using user ID.*
5. *Compare these two images and compute the matching score if matching score is greater than 0.8 then the user is valid person otherwise the user is not a valid person.*
6. *For level 2, repeat the step 2 to 5 where j = 3.*

IV. RESULT AND DISCUSSION

The proposed model is experimented with Images from CASIA database constituting 100 fingerprint images. A 5x5 median filter has been

initially used to filter the noise and other artefacts from the images and a 2D Ridge let transform has been applied to these images to get clear vision. Two levels of authentication process are experimented as medical data model, in the first level has two images from 20 possible combinations whereas second level has three images from 60 possible combinations.

Table 1
possible combinations for finger print

Permutation nPr = n! / (n-r)!	
Level 1	5P2=20 I (3,2)
Level 2	5P3=60 I (4,1,5)

Figure 7 shows an example of such possible combinations for a finger print. The server will select combination of images from database and at the same time it acquires a same set of combinations from user. If the acquired images will match with original images which are all stored in admin database then the user carry on their process else halt the process. User needs level 1 authentication to login their application, while transferring the prescription and medical data from one user to another user the level 2 authentications must be required. Suppose the login process fails it will give 3 more chances for make the correct authentication otherwise its halts the process.

Fig. 7.Finger print combinations

From Table1 the n denotes the size of the set from which elements are permuted and r denotes the size of each permutation. These 80 images are stored in admin database. Consider in Level 1 the server chooses a combination I (3,2) from 20 possibilities similarly Level 2 choose a combination I (4,1,5). Note that the division values never be repeated i.e. level 1 and level 2 divisions does not match. These images are in either png or tiff images due to resolution level as well as database complexity. These images are selected by randomly at the same time there is no duplications of division images.

Table 2
Image Comparison Table

January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

Image Format Type	PNG	BMP	JFG	GIF	TIF
Image					
Size	6.31 MB	14.3 MB	7.83 MB	3.54 MB	12.6 MB

Once the security level is fixed and the features are successful then authentication was successful for the user else, they are considered as imposter. Based on the terms the following parameters are calculated to define the efficiency of the system such as false acceptance rate (FAR), false rejection rate (FRR), genuine acceptance rate (GAR) and total error rate (TER). All the above metrics are expressed as percentages and denote the classification accuracy. These four metrics are accordingly defined as follows.

$$FAR\ (\%) = \frac{number\ of\ false\ acceptances}{total\ number\ of\ impostor\ tests} * 100 \quad (1)$$

$$FRR\ (\%) = \frac{number\ of\ false\ rejections}{total\ number\ of\ client\ tests} * 100 \quad (2)$$

$$GAR\ (\%) = 100 - FRR(\%) \quad (3)$$

$$TER\ (\%) = FAR\ (\%) + FRR(\%) \quad (4)$$

The overall implementation of the work is projected in figure 8 where the GUI developed for the authentication purpose is projected.

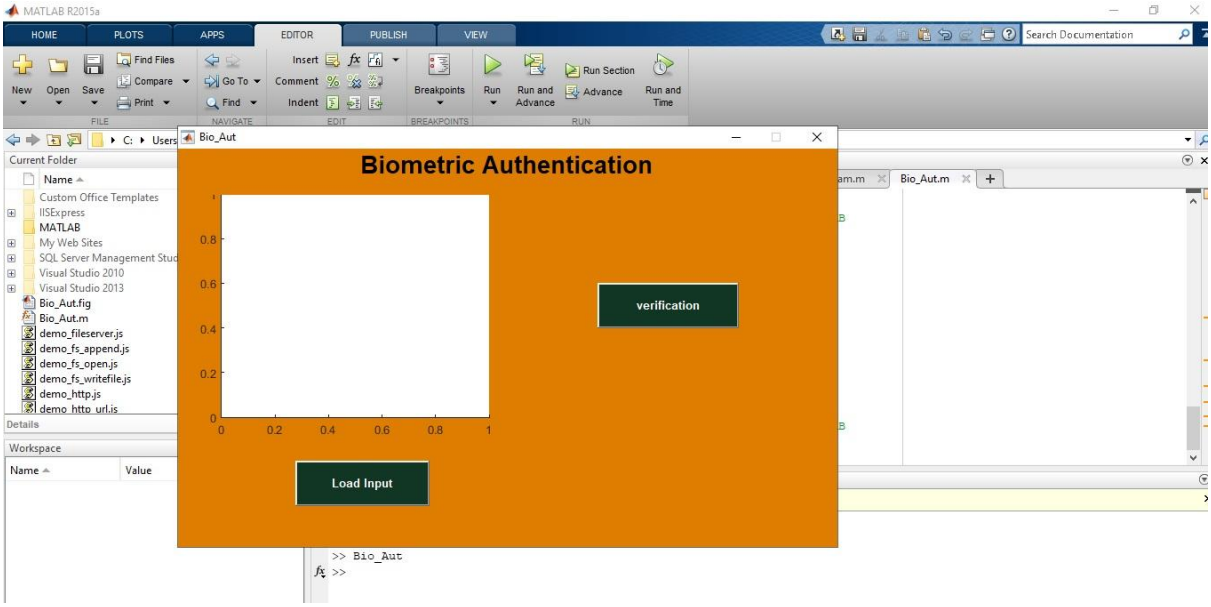


Fig. 8. Snapshot of biometric authentication module implemented in MATLAB

Figure 9depicts the matching score for the imposters and the genuine users in the

January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

experimental data set and it is observed that it efficiently detects the imposters among the entire data set which is better than conventional password based and other models.

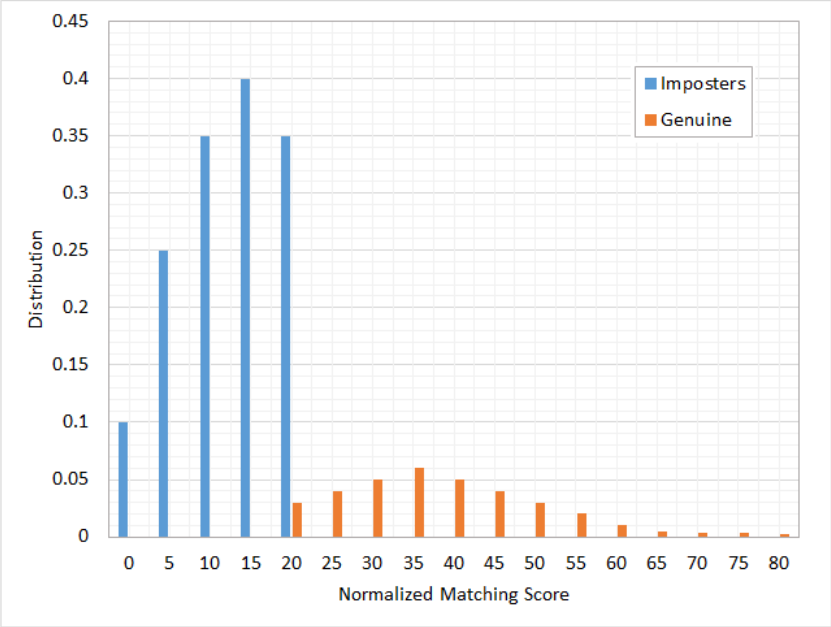


Fig.9. Normalized Distribution for Imposters and Genuine users

Figures 10 and 11 project the verification of users as genuine or impostors simulated in MATLAB.

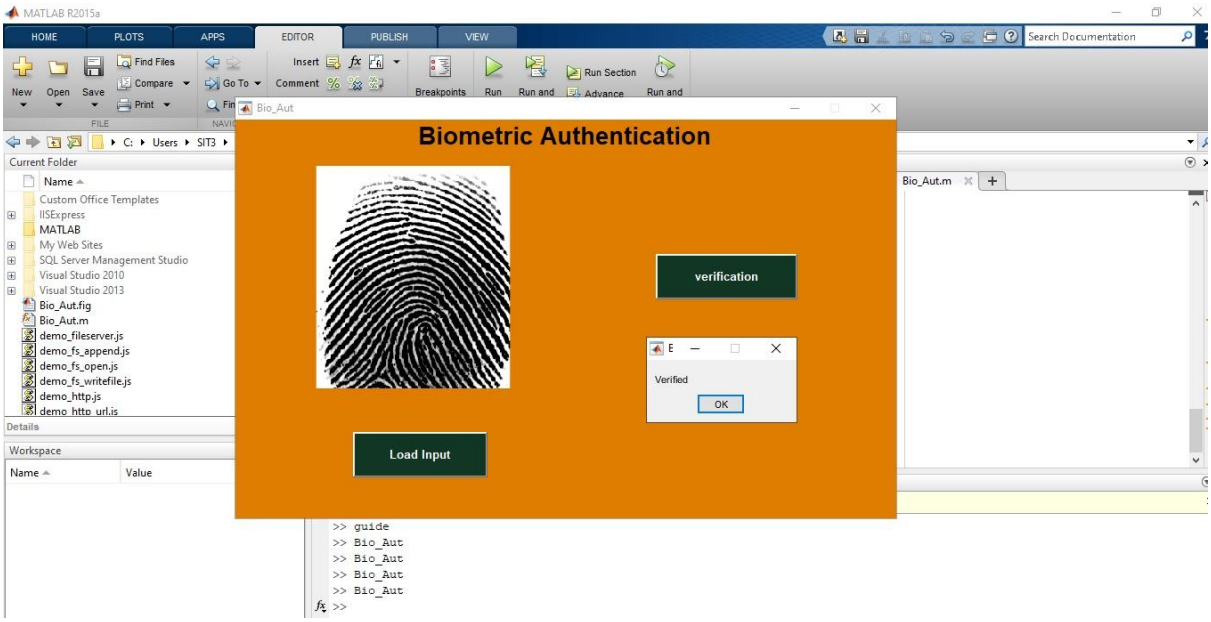


Fig.10. Biometric authentication output – case I – Genuine user

January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

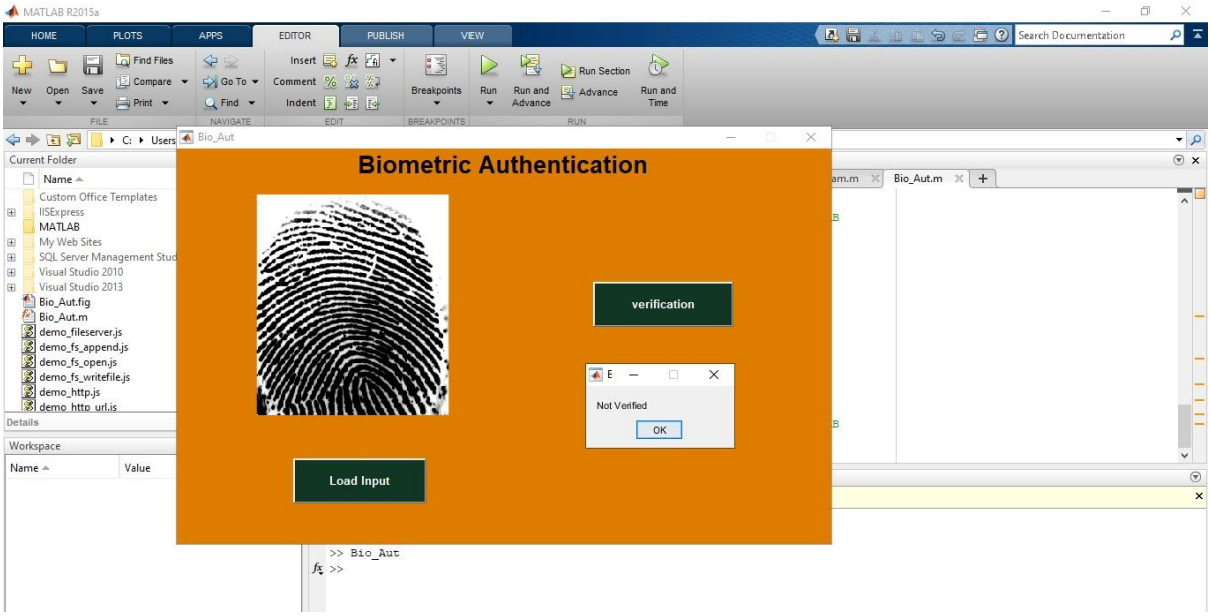


Fig.11. Biometric authentication output – case II – Impostor

The FAR and FRR analysis for the proposed model is plotted in figure 12. From this it is observed that they are proportional to each other and provides better performance for entire data range. Based on the threshold values the values are calculated and, in some places, both values are reaches nearly same that's because of the threshold and it is inevitableto choose different threshold for each calculation.

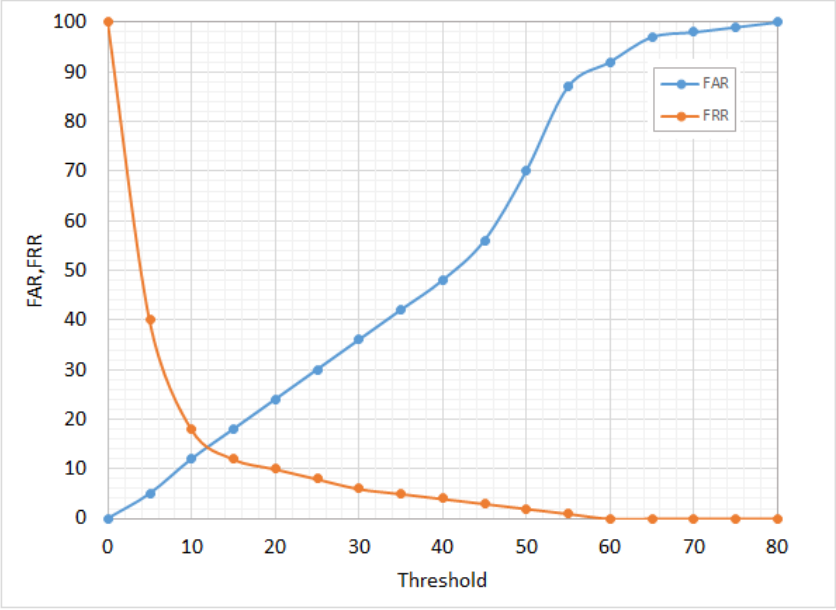


Fig.12. Plot of FAR and FRR analysis of proposed model

The computation time analysis to arrive at a decision for increasing sample size is depicted in figure 13. It could be seen from the plot that as sample size increases the proposed model converges quickly due to fast process thus resulting in an average of 100-150ns duration for authenticating compared to conventional model.

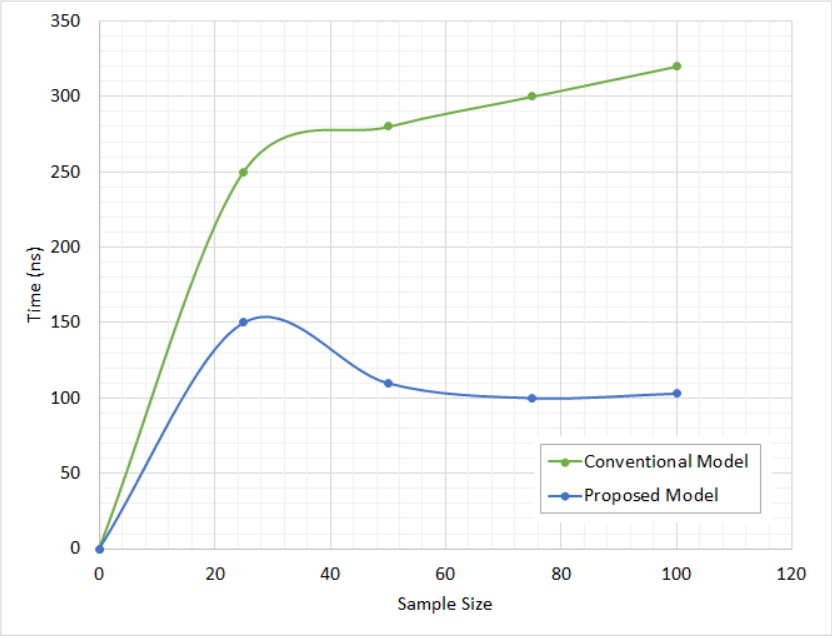


Fig.13. Computation time analysis

V. CONCLUSION

Data handling is a crucial task in every environment and in particular securing such data is essential so that unauthenticated users could not use the data. In many applications the conventional security mechanism is available and it leads to issues in case of authentication so this proposed research provides simple and efficient authentication mechanism using fingerprint model. Using advanced encryption model the authenticated data are encrypted and then send to the destination. Hash key and signature code are essential for the receiver to know the details which helps to transfer the data securely and also improves the system security. In future this model could be developed with other encryption algorithm as multi-level authentication model which improves the security of the data in cloud. The experimental analysis proves that the proposed authentication model achieves better efficiency and enhances security of the data in cloud environment than the conventional model.

VI. REFERENCES

[1] ShangweiGuo, Tao Xiang, Xiaoguo Li (2019), "Towards efficient privacy-preserving face recognition in the cloud" Signal Processing, Vol.164, pp.320-328

[2] Earl Ryan M. Aleluya, Celesamae T. Vicente (2018), "Faceture ID: face and hand gesture multi-factor authentication using deep learning" Procedia Computer Science, Vol.135, pp.147-154

[3] Pengfei Hu, Huansheng Ning, Tie Qiu, Yue Xu, Arun Kumar Sangaiah (2018), "A unified face identification and resolution scheme using cloud computing in Internet of Things" Future Generation Computer Systems, Vol.81, pp.582-592

[4] Yogesh Sharma, Bahman Javadi, Weisheng Si, Daniel Sun (2016), "Reliability and energy efficiency in cloud computing systems: Survey and taxonomy" Journal of Network and Computer Applications, Vol.74, pp. 66-85

[5] Irfan Mohiuddin, Ahmad Almogren, Mohammed Al Qurishi, Mohammad Mehedi Hassan, Giancarlo Fortino (2019), "Secure distributed adaptive bin packing algorithm for cloud storage" Future Generation Computer Systems, Vol.90, pp. 307-316

January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

[6] Kesavaraja, Sasireka, Jeyabharathi (2016), "Cloud Software as a Service with Iris Authentication" Journal of Global Research in Computer Science. Vol.1, No. 2, pp.16-22

[7] Peng Gong, Yuan Cao, BaigenCai, Kun Li (2018), "Multi-information location data fusion system of railway signal based on cloud computing" Future Generation Computer Systems, Vol.88, pp.594-598

[8] Priyadharshini, Saravanakuamr (2018),"Amalgamation of Iris Biometrics and cryptography in cloud computing for improved authentication "Journal of engineering and applied science, Vol.13, No.8, Pp. 2018-2022

[9] Bastina, Rama, (2017), "Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access", International Journal of Electrical and Computer Engineering. Vol.7. pp.408-416

[10] Sahithi,A.Anirudh, B.Swaroop, K.RuthRamya (2019), "Biometric Security for Cloud Data using Fingerprint and Palm Print" International Journal of Innovative Technology and Exploring Engineering, Vol.8, No.6S3,pp.338-343

[11] SubramaniJegadeesan, Maria Azees, PriyanMalarvizhi Kumar, GunasekaranManogaran, Ching-Hsien Hsu (2019), " An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications" Sustainable Cities and Society, Vol.49

[12] HodaJannati, Behnam Bahrak (2017), "An improved authentication protocol for distributed mobile cloud computing services" International Journal of Critical Infrastructure Protection, Vol.19, pp. 59-67

[13] MojtabaAlizadeh, SaeidAbolfazli, MazdakZamani, SabariahBaharun, Kouichi Sakurai (2016), "Authentication in mobile cloud computing: A survey" Journal of Network and Computer Applications, Vol.61, pp. 59-80

[14] Xun Yi, Zahir Tari, Feng Hao, Liqun Chen, Albert Y. Zomaya (2019), "Efficient threshold password-authenticated secret sharing protocols for cloud computing" Journal of Parallel and Distributed Computing, Vol.128, pp.57-70

[15] HoonJeong, Euiin Choi (2012), "User Authentication using Profiling in Mobile Cloud Computing" AASRI Procedia, Vol.2, pp. 262-267

[16] Marta Beltrán (2018) , "Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things" Computers & Security, Vol.77, pp.595-611

[17] Nalini Subramanian, Andrews Jeyaraj (2018), " Recent security challenges in cloud computing" Computers & Electrical Engineering, Vol.71, pp.28-42

[18] Christos Stergiou, Kostas E. Psannis, Brij B. Gupta, Yutaka Ishibashi (2018)," Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT" Sustainable Computing: Informatics and Systems, Vol.19, pp.174-184

[19] Hefei Jia, Xu Liu, Xiaoqiang Di, Hui Qi, Huamin Yang(2019), "Security Strategy for Virtual Machine Allocation in Cloud Computing" Procedia Computer Science, Vol.147, pp.140-144

[20] Nabeel Khan, Adil Al-Yasiri (2016), "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework" Procedia Computer Science, Vol.94, pp. 485-490

[21] Muhammad BaqerMollah, Md. Abul Kalam Azad, Athanasios Vasilakos (2017), "Security and privacy challenges in mobile cloud computing: Survey and way ahead" Journal of Network and Computer Applications, Vol. 84, pp. 38-54

January - February 2020
ISSN: 0193 - 4120 Page No. 14587 - 14600

[22] PV Kamala Kumari, S Akhila, Y Srinivasa Rao and B. Rama Devi. "Alternative to Artificial Preservatives." Systematic Reviews in Pharmacy 10.1 (2019), 99-102. Print. doi:10.5530/srp.2019.1.17

[23] Siddaiah, N., Roshini, T., Sai Krishna, V., Prasanth, G., Likhith, K.Performance analysis of cantilever based bio-sensor for pathogendetection(2018) International Journal of PharmaceuticalResearch,10(2),pp.107109.https://www.scopus.com/inward/record.uri?eid=2-s2.085046462145&partnerID=40&md5=6d963e53671a635c8d5a6776afa25265

[24] K. Bhavya sri (2018) a brief overview of the very rare fibrodysplasiaossificansprogressiva (stone man syndrome). Journal of Critical Reviews, 5 (1), 19-3. doi:10.22159/jcr.2018v5i1.22809

[25] Melnichuk, M., 2018. Psychosocial Adaptation of International Students: Advanced Screening. International Journal of Psychosocial Rehabilitation. Vol 22 (1) 101, 113.

[26] Daly, A., Arnavut, F., Bohorun, D., Daly, A., Arnavut, F. and Bohorun, D., The Step-Down Challenge. International Journal of Psychosocial Rehabilitation, Vol 22(1) 76, 83.

[27] Knapen, J., Myszta, A. and Moriën, Y., 2018. Augmented individual placement and support for people with serious mental illness: the results of a pilot study in Belgium. International Journal of Psychosocial Rehabilitation, Vol 22(2), pp.11-21.