RESEARCH ARTICLE OPEN ACCESS

Authenticating Data Access in IOT Healthcare Systems Based on Fingerprints

Ahmed Alghamdi*, Mahjoub Hammad**
**Department of Information Systems, Bisha University, KSA*
*** Department of of Information Systems, Bisha University, KSA*

ABSTRACT
The spread of infectious diseases such as the Corona pandemic highlighted the need to share the medical records of patients among various health institutions, so the doctor can, check the patient health record and know if the patient suffers of any chronic or allergic diseases before examination. While patients' privacy must be preserved, the researcher suggested a system for authentication of users by fingerprint, in order to verify the identity of who has access to the patients' files, based on deep conventional neural network. The proposed model was simulated using MATLAB simulator, trained using CASIA-FingerprintV5 and tested using SDUMLA-HMT. Five classifiers were implemented in addition to the proposed model for evaluation purposes Support Vector Machine, Linear Discriminant Analysis, combined learning vector quantization, Multilayer Perceptron and Restricted Boltzmann Machine. Results indicated that the proposed model outperformed the other classifiers in sensitivity with 99.02% and accuracy with 99.06 % while RBM has achieved equality with the proposed model in precision with 100% and specificity with 100%.

Keywords – Healthcare, EHR, Fingerprint, conventional neural networks

Date of Submission: 21-04-2021 Date of Acceptance: 06-05-2021

I. INTRODUCTION

healthcare systems have a vital and continuing responsibility for people`s health including individuals, families and societies everywhere. According to the World Health Organization (WHO), every healthcare system should be directed to achieve three overall goals enhancing health while taking into consideration, reducing the costs of expensive medical bills, responding well to what people expect of it, responding equally to everyone, without any discrimination [1][2].

Healthcare Information System (HIS), is an integral part of the healthcare system, connotes a system prepared to manage healthcare data. This involves systems that collect, store, manage and transmit a patient's electronic health record (EHR), operational hospital management, or a system that supportshealthcare policy decisions [3-5].

Internet of Thing (IOT) can automate patient care workflow with healthcare mobility solution and modern technologies help. IOT allows many benefits to healthcare systems including as shown in Fig 1 interoperability, peer-to-peer communication between machines, information reciprocity, and data movement that delivers healthcare service effectively [6][7].

However it is difficult to store and manage huge amount of data sent by healthcare device in short time owing to their real-time application, if the access to cloud is unavailable. Cloud of e-healthcare is the virtual resources and application processes which is considered transparent to users that are interested with standard health records and don’t need to know where data is physically stored. The cloud means that application can be accessed at any time andeverywhere through internet [8-10].

In spite of all of this, electronic healthcare systems consider critical and require many of information, many of data and computing power. Physicians need the medical history of patients. Patients move to different investigations, supposing a high rate exchange of data between departments of medical units. Therefore, Physicians need a full view of patient medical information for providing a complete and accurate treatment. Also when a patient moves from hospital to hospital, therefore he needs to have all his medical records and reports with him that is hard to be possible especially in emergency cases [11][12].

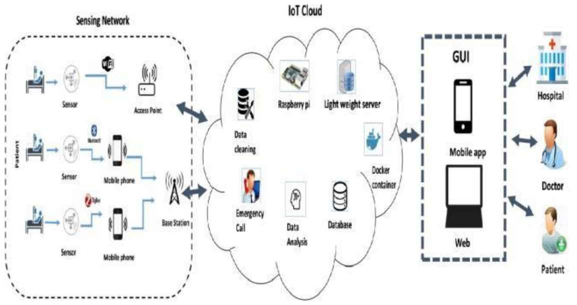


Figure 1. Healthcare information system based IOT [7]

Based on many real cases the researcher as an information technology specialties working in public hospital has faced, he noticed that sharing patients records between hospitals based on the IOT healthcare system can be a great benefit to patient to make it easier for him to receive medical care in any hospital around the kingdom without worrying about his medical records or his history which represent a main cause of different medical faults.

Based on that the researcher proposes, a user authentication system shown in Fig 2, allowing physicians to access patients records in any hospital around the Kingdom of Saudia Arabia (KSA) without breaching patient privacy using physician and patient fingerprints taking into consideration that the physician to access the file the patient should be registered in the same medical facility the physician work in.

Through the proposed model if a patient has entered any medical facility for emergency case, the physician in this facility will need to grant access to the patient EHR stored on the cloud of the IOT system. So the physician fingerprint and the patient fingerprint will be used to grant access to the physician or access will be denied. Access will denied in case of any fraudulent tried to access patient EHR or even if the physician is not working in a medical facility the patient has checked in it to keep the patient privacy.

This paper is organized in into five sections.. Section two introduces the literature review of authentication models and biometrics. Section three, introduces the proposed model in details. Section 4 presents the simulation settings and section five presents results and discussion. Finally section six outlines conclusions.

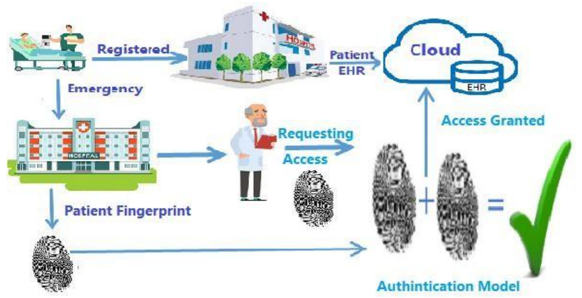


Figure 2. The proposed model architecture

II. LITRETURE REVIEW

2.1 Healthcare Information System Authentication

In this section we will introduce and discuss some of the data access control in healthcare systems based IOT studies. As Boonyarattaphan et. al., in [13] offered a cost-effective framework based on two risk adaptive authentication techniques and different encryption algorithms, for e-health authentication and data transfer. The framework consists of efficient protocol architecture for an e-health service; to deal with data of different levels of importance, and to achieve the required security requirements for e-health applications. Results indicated that the proposed model has effectively reduced computational complexity and delay in e-health communications.

Jun Zhou et. al., in [14] introduced an authorized accessible privacy model where physicians could be authorized by patients in different including levels direct authorization of physicians and indirect authorization of physicians. However the unauthorized individuals in medical consultation can also decipher the personal health information or verify patients' identities through satisfying the access tree with their own attribute sets based on a new technique of attribute-based designated verifier signature. Results indicated that the proposed scheme is resistible to different types with acceptable communication and storage overhead computational complexity.

Moosavi et. al., in [15] proposed a secure and efficient authentication and authorization IoT-based healthcare architecture based on distributed smart e-health gateways. Due to hardware limitations of medical resources sensor, it is not feasible to use traditional encryption in health care based on the Internet of things. In addition, Internet gateways focus only on current things simple tasks without dilution of authentication and licensing challenges.

The proposed architecture relies on the certificate- based DTLS handshake protocol as the effective solution to secure IP in IoT. Results indicated that the proposed architecture outperformed the state of art in security especially in denial of service attacks confrontation in addition to reducing communication overhead by 26% and communication latency from the smart gateway to the end-user by 16%.

Azaria et. al., in [16] proposed a decentralized record management system to secure electronic health records using Leveraging unique block-chain through which medical stakeholders can act as miners. The proposed system simply can provide authentication, confidentiality, and accountability to authorized stakeholders when accessing and aggregating patient sensitive information.

In the same year, Kuo-Hui Yeh in [17] offered secure crypto-primitives IoT-based healthcare system, operating through body sensor network architecture. The proposed system mainly depends on constructing two communication mechanisms for achieving confidentiality and authentication of transmission between the local processing unit and the backendbody sensor network server.

Kahani et. al., in [18] proposed an information access method based on a zero-knowledge protocol combined with two-stage keyed access control to achieve authentication in cloud-based e-Health systems. The proposed method authenticates users based on their privileges on the system through, a two-step combination of derived unrivaled key per transaction management schema and public key encryption. Results indicated that the proposed method outperforms the state of art in processing a high number of concurrent authentication requests in terms of acceptable time complexity.

Liu & Chung in [19] introduced a user authentication scheme based on smart cards and passwords and to facilitate security and privacy protection, during the physician examination of the patient. In addition, a secure cryptosystem was applied for establishing a data transmission mechanism. Results indicated that the proposed scheme outperforms the state of art in confronting impersonation, replay, and password guessing and stolen-verifier attacks.

Kumari et. al., in [20] introduced a scheme based on elliptic curve cryptography and bilinear paring to overcome users' private key leakage, user impersonation attacks, lack of authentication between trusted authority and sensor nodes, replay attack, Denial of Service attack and forgery attack. Based on the authors' claims, the results of their proposed scheme clarified its safety against well-known attacks.

2.2 Biometric Traits

Authentication based on biometrics recently became widespread in private and public security systems, consumer electronics and point-of-sale applications. Using a biometric trait as an authenticator provides many benefits as there are no passwords or tokens to retain. Many studies have been proposed to investigates and discuss the role of biometrics in authentication process as Ju et. al., in [21] introduced authentication model based numeric password and fingerprint authentication system as the user can change the password easily but not the fingerprint information, so this authentication system provides security and flexibility.

Also in [22] Kumar et al., proposed a user authentication model based fingerprint and the keystroke dynamics of the password entry. The proposed model involved three stages first to Login using Username and password; second Fingerprint and third the Keystroke. Results showed that the proposed model achieved superiority over that state of art.

In [23] Kumar et al. proposed a fingerprint-matching algorithm based on extraction of the orientation features of the Region of Interest fingerprint. Their proposed algorithm used Euclidean Distance to determine the distance between the extracted orientation features and the stored images of fingerprints.

Jain and Prasad in [24] proposed a dynamic clustering-based fingerprint-indexing scheme where Su et al. in [25] proposed a learning-based fingerprint pose estimation algorithm for indexing fingerprints into a common finger coordinate system. Anush et al.
[26] proposed an adaptive latent fingerprint segmentation method based on random decision classification.

Okokpujie et al. in [27] introduced a combined model of the fingerprint, pin and password to 0secure customers payment for purchasing staff. The results indicate that the proposed model has a zero false match and false non-match rate achieving superiority over the state of art.

Hammad & Wang in [28] proposed a convolution neural network model based ECG and fingerprint for human authentication. The Q-Gaussian multi support vector machine (QG-MSVM) was used as a classifier to improve the performance of the authentication stage. The proposed model was trained and tested using PTB and LivDet2015 databases for the fingerprint. Results indicated that the proposed model achieved superiority over the state of art in efficiency, robustness and reliability.

2.3 Healthcare System Authentication based biometrics

Recently many studies have been proposed to discuss the ability of making use of biometrics in securing and authenticating data access control in healthcare information systems especially in the cloud layer. As in [29] Kumar et. al., introduced an authentication schema based on biometrics for Naked hospital environment. The proposed schema allowed patients to get health services from smart and intelligent surroundings of hospital without using explicit gadgets while considering protecting his identity privacy. Results indicate that the proposed schema has confronted different insider attacks, replay attacks and identity privacy among others.

Kwao et.al., in [30] introduced a schema based on local minutie features and fast stereo matching algorithm. This proposed schema tries to verify a user based on matching his fingerprint with the fingerprints stored in the system database to classify him as authorized or fraudulent. Results indicated that the proposed schema achieved a compromise between time and space complexity and recognition accuracy. Hamidi in [31] proposed an IoT standard smart healthcare model based on using biometric traits to provide authentication to patient's data. The proposed model aims at providing users, ease of use of the system in addition to increasing the capacity of data.

Results indicated that the proposed model outperforms the state of art in securing data access on IoT smart healthcare systems while providing fast identity recognition of users.

Hathaliya et. al., in [32] investigated using biometrics to control patients EHR access from any location. The proposed schema confronts different security threats on accessing EHR from the repository of database. The Automated Validation of Internet Security Protocols tool is utilized for the verification of the proposed schema, results indicated that the proposed schema outperforms the state of art in reducing time and space complexity of the communication process.

Also in [33] Hathaliya et. al., introduced an information healthcare system based on mobile devices. The proposed system allowed self-authentication of patients utilizing mobile and wearable devices biometric scanners. In the nest step the patient will be re-verified by the cloud server after the mutual authentication. Results indicated that the proposed system outperforms the state of art in reducing space and time complexity of communication in addition to providing greater security to the patients.

III. PROPOSED MODEL

The proposed model identifies physician using his fingerprint and confirms patient acceptance of allowing physician to access his EHR through patient fingerprint. Figure 3 we can see that, the proposed model mainly includes two stages

1. Preprocessing stage
2. Matching stage
3. Majority check of patient and physician authentication

3.1 Preprocessing stage

Through this stage, Fingerprint images were prepared for the recognition stages through four main steps equalization, binarization, region of interest (ROI) detection and image thinning. The equalization of the fingerprint is done using histogram because of the low quality of fingerprint images and the need to enhance between ridges and valleys contrast. After the equalization fingerprint images is binarized to become black and white image in order to be able to proceed with the ROI process.

In ROI step, the fingerprint as a region of interest to extract features from is detected to finally turn images to a connected skeleton of unit width or to thin them. These four steps mainly aim to frame the variation of the features values between fingerprint images to facilitate the matching process. Fig 3 clarifies all these four preprocessing steps in details.

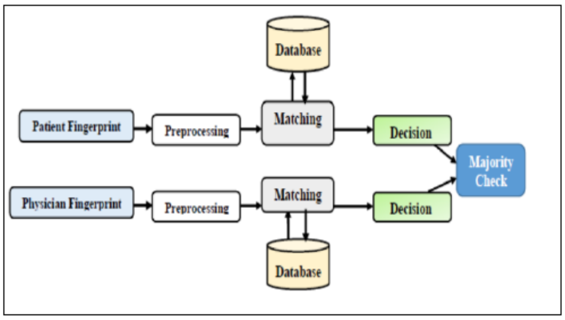


Figure 3 . The Proposed Model Stages

3.2 Matching stage

Through the matching stage the fingerprints of the patient and the physician are used to find a match for each one in the patterns stored in the medical facility dataset. Through this stage we have used the Deep Conventional Neural Network architecture (DCNN) as it is one of the most successful deep learning architectures in image analysis.

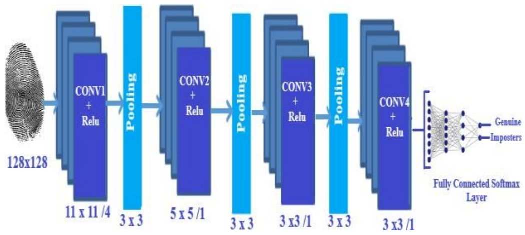
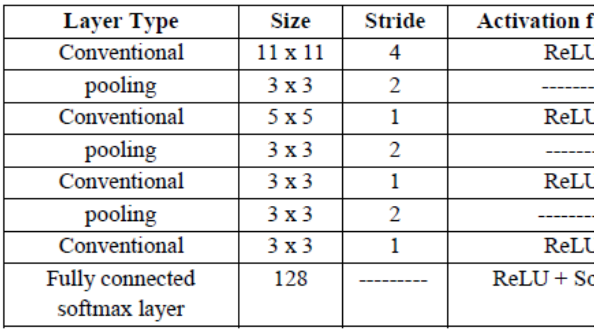


Figure 4. DCNN proposed network

Through the proposed CNN architecture the fingerprint image, goes through a series of convolutional, nonlinear, pooling and fully connected layers, to get an output. Mainly the proposed CNN architecture (shown in Fig 4) has four convolution layers, three pooling layers, and one fully connected Softmax layer. The outputs in our model are two classes genuine class and imposter class. Support vector machine (SVM) was used for training the proposed network. Table 1 clarifies the topology of the proposed CNN. The convolutional layers extract patterns found within local regions of the inputted images that are common throughout the dataset by convolving a template over the inputted image pixels and outputting this as a feature map for each filter.

Table 1. Settings of the proposed network



Layer Type	Size	Stride	Activation f
Conventional	11 x 11	4	ReLU
pooling	3 x 3	2	-------
Conventional	5 x 5	1	ReLU
pooling	3 x 3	2	-------
Conventional	3 x 3	1	ReLU
pooling	3 x 3	2	-------
Conventional	3 x 3	1	ReLU
Fully connected softmax layer	128	---------	ReLU + Sc

Rectified linear unit (ReLU) activation function is an element-wise operation used after each conventional operation for replacing negative pixel values in the feature map by zero otherwise inputs will be output directly if it is positive. ReLU is also needed for enhancing non-linearity in fingerprint images which are naturally non-linear in order to allow fast learning especially we are using a large dataset for training the CNN.

The results of the ReLU are forwarded to max-pooling layer to collect the information within a set of small local regions, to produce a smaller size pooled feature maps as the output. Finally we have a fully connected Multi-Layer Perceptron layer using Softmax activation function. The fully connected layer are responsible for classifying the high-level features of the input image resulting from the conventional and pooling layers into two classes genuine and imposter

3.3 Majority check of patient and physician authentication

This is the final stage of the proposed authentication model where the model checks if both the patient and the physician have been identified as genuine the model will grant access of EHR of the patient to the physician otherwise access will be denied.

IV. SIMULATION SETTINGS

4.1 Datasets

Through this study we have used two datasets CASIA- FingerprintV5 for training the proposed CNN and SDUMLA-HMT for testing. CASIA-FingerprintV5 has 20000 fingerprint images of 500 subjects including graduate students, workers and waiters. Eight fingers of each subject were scanned five times as gray-level BMP images with resolution 328×356 pixels.

4.2 performance Metrics

- False Acceptance Rate (FAR):
- $= \frac{\text{Number of False Accepted subjects}}{\text{number of Subjects inthe dataset}}$ (1)
- False Rejection Rate (FRR):

$= \frac{\text{Number of Falsely Relected Images}}{\text{Total number of persons out the database}}$ (2)

- Recognition Accuracy $= \frac{TP + TN}{TP + FP + FN + TN}$ (3)
- Recognition Sensitivity$= \frac{TP}{TP + FN}$ (4)
- Recognition Specificity $= \frac{TN}{FP + TN}$ (5)
- Recognition Precision $= \frac{TP}{TP + FP}$ (6)

Where TP is true positive, TN is true negative, FP is false positive and FN is false negative.

4.3 Experimental environment

Two experiments were conducted, the first experiment a survey study using SVM for evaluating the fingerprint trait against face, iris and finger veins taken from SDUMLA-HMT. The second experiment was conducted for evaluating the proposed model using fingerprint trait from CASIA-FingerprintV5 dataset for training and from SDUMLA-HMT for testing.

These two experiments were conducted using MATLAB R2019b image processing and computer vision libraries on a core I7 laptop with 16 Gigabyte RAM and one Terabyte storage capacity. Five well known classifiers were implemented for evaluating the performance of the proposed model Support Vector Machine (SVM), Linear Discriminant Analysis (LDA), combined learning vector quantization (CLVQ), Multilayer Perceptron (MLP) and Restricted Boltzmann Machine (RBM).

V. RESULTS AND DISCUSSION

Fig 5 clarifies that fingerprint has achieved the highest recognition accuracy 98.7% outperforming the other three traits iris 96.40% , finger vein 94% and finally face 93.7%. While in Fig 6 fingerprint has achieved the lowest FAR and FRR 0.07 and 0.05 respectively outperforming the other three traits iris 0.17 and 0.09 , finger vein 0.1 and 0.089 and finally face 0.4 and 0.05.

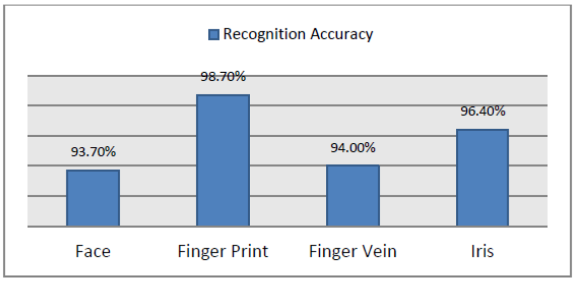


Figure 5 the recognition accuracy of the four traits

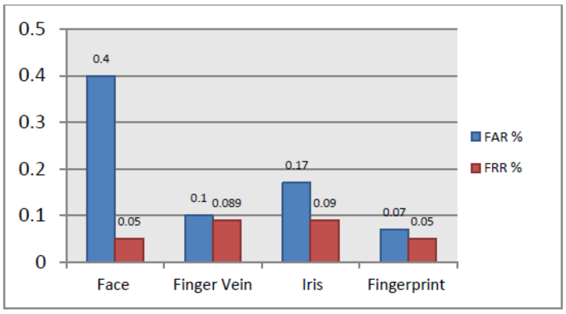


Figure 6. FAR and FRR of the four traits in the survey study

For evaluating the proposed model sensitivity, precision, specificity and accuracy of five well known classifiers SVM, LDA, CLVQ , MLP and RBM in addition to the proposed model. Fig 7 clarifies the sensitivity of the implemented classifiers confirming the superiority of the proposed model with 99.02% while the SVM has the least sensitivity 93.44%.

In Fig (8) the precision of the implemented classifiers confirmed the superiority of the proposed model and RBM with 100% precision while the MLP has the least precision 98.96%.

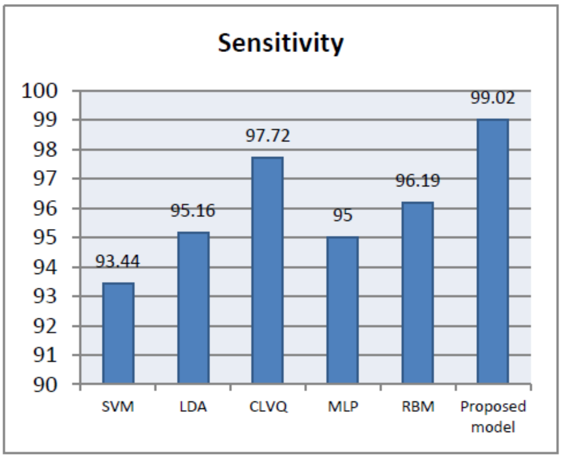


Figure 7. Sensitivity of the implemented classifiers

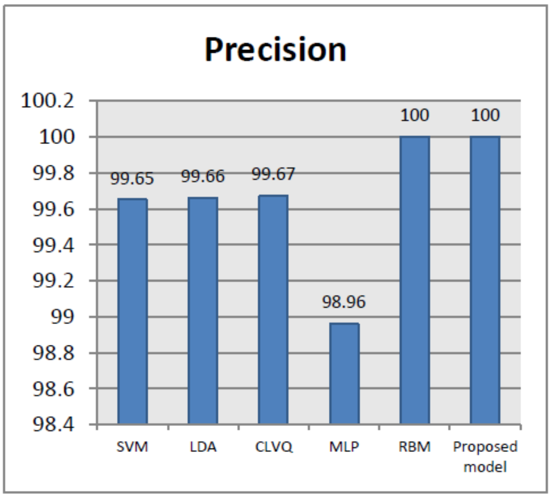


Figure 8. Precision of the implemented classifiers

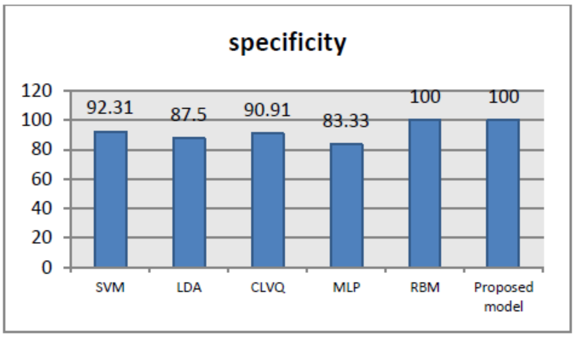


Figure 9. Specifity of the implemented classifiers

Also in Fig. 9 the specificity of the implemented classifiers confirmed the superiority of the proposed model in addition to RBM with 100% specificity while the MLP has the least specificity 83.33%.

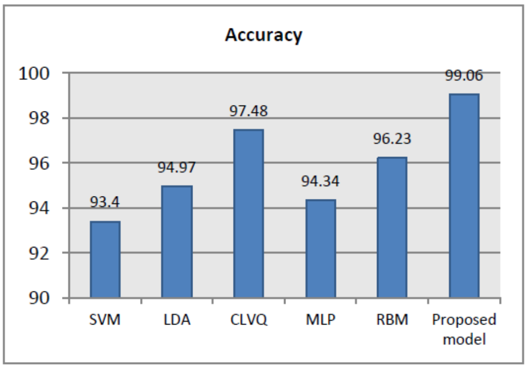


Figure 10. Accuracy of the implemented classifiers

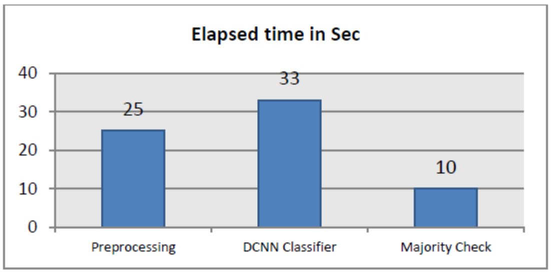


Figure 11. Elapsed time in sec for the proposed model

In Fig 10 the Accuracy of the implemented classifiers confirmed the superiority of the proposed model achieving 99.06 % Accuracy while the MLP has the least accuracy 94.34%. Finally in Fig. 11 the elapsed time through the proposed model stages are presented clarifying that the classification and matching stage consumed the highest time while the majority check stage has consumed the least time.

From all of the above we can confirm that fingerprint trait is the most suitable trait for our authentication model which has outperformed the implemented classifiers SVM, LDA, CLVQ , MLP in sensitivity, precision, specificity and accuracy while RBM has achieved equality with the proposed model in precision and specificity

VI. CONCLUSIONS

Healthcare information systems play an important role in delivering services to patients in and automated, easy and effective way. The appearance of IoT systems effectively contributed in healthcare medical information systems especially with the cloud technology that helps in providing availability to Electronic health records so a physician can easily access the patient data at any time and from any place just a simple touch on the mobile screen. In this paper we introduce and authentication model based on fingerprint biometric recognition using deep conventional neural network. The proposed model was simulated using Matlab simulator; trained using CASIA-FingerprintV5 and tested using SDUMLA-HMT. Results indicated that the proposed model outperformed the other classifiers in sensitivity with 99.02% and accuracy with 99.06 % while RBM has achieved equality with the proposed model in precision with 100% and specificity with 100%.

REFERENCES

[1]. Nolte, E., & McKee, M. (2008). Integration and chronic care: a review. *Caring for people with chronic conditions. A health system perspective*,64-91.

[2]. McGinnis, J. M., Powers, B., & Grossmann, C. (Eds.). (2011). *Digital infrastructure for the learning health system: the foundation for continuous improvement in health and health care: workshop series summary*. National Academies Press.

[3]. Acquah-Swanzy, M. (2015). *Evaluating electronic health record systems in Ghana: the case of Effia Nkwanta regional hospital* (Master's thesis, UiT Norges arktiske universitet).

[4]. Nyame-Asiamah, F. (2020). Improving the 'manager-clinician'collaboration for effective healthcare ICT and telemedicine adoption processes–a cohered emergent perspective. *Information Technology for Development*, *26*(3), 525-550.

[5]. Brugués de la Torre, A. (2016). Contributions tointeroperability, scalability and formalization ofpersonal health systems.

[6]. Tuan, M. N. D., Thanh, N. N., & Le Tuan, L. (2019). Applying a mindfulness-based reliability strategy to the Internet of Things in healthcare–A business model in the Vietnamesemarket. *Technological Forecasting and SocialChange*, *140*, 54-68.

[7]. Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2019). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*, 1-23.

[8]. Rajabion, L., Shaltooki, A. A., Taghikhah, M., Ghasemi, A., & Badfar, A. (2019). Healthcare big data processing mechanisms: the role of cloud computing. *International Journal of Information Management*, *49*, 271-289.

[9]. Zhou, J., Cao, Z., Dong, X., & Lin, X. (2015). PPDM: A privacy-preserving protocol for cloud-assisted e-healthcare systems. *IEEE Journal of Selected Topics in Signal Processing*, *9*(7), 1332-1344.

[10]. Althebyan, Q., Yaseen, Q., Jararweh, Y., & Al- Ayyoub, M. (2016). Cloud support for large scale e-healthcare systems. *Annals of telecommunications*, *71*(9), 503-515.

[11]. Nelson, J. E., Puntillo, K. A., Pronovost, P. J., Walker, A. S., McAdam, J. L., Ilaoa, D., & Penrod, J. (2010). In their own words: patients and families define high-quality palliative care in the intensive care unit. *Critical care medicine*, *38*(3), 808.

[12]. Armony, M., Israelit, S., Mandelbaum, A., Marmor, Y. N., Tseytlin, Y., & Yom-Tov, G. B. (2015). On patient flow in hospitals: A data-based queueing-science perspective. *Stochastic systems*, *5*(1), 146-194.

[13]. Boonyarattaphan, A., Bai, Y., & Chung, S. (2009, September). A security framework for e- health service authentication and e-health data transmission. In 2009 9th International Symposium on Communications and Information Technology (pp. 1213-1218). IEEE.

[14]. Zhou, J., Lin, X., Dong, X., & Cao, Z. (2014). PSMPA: Patient self-controllable and multi- level privacy-preserving cooperative authentication in distributedm-healthcare clou computing system. IEEETransactions on Parallel and Distributed Systems, 26(6), 1693-1703.

[15]. Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia ComputerScience, 52, 452-459.

[16]. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, (2016, August). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.

[17]. Yeh, K. H. (2016). A secure IoT-based healthcare system with body sensor networks. IEEE Access, 4, 10288-10299.

[18]. Kahani, N., Elgazzar, K., & Cordy, J. R. (2016, April). Authentication and access control in e- health systems in the cloud. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 13-23). IEEE.

[19]. Liu, Y., Chang, C. C., & Chang, S. C. (2017). An Efficient and Secure Smart Card Based Password Authentication Scheme. IJ NetworkSecurity, 19(1), 1-10.

[20]. Kumari, A., Yahya Abbasi, M., Kumar, V., & Khan, A. A. (2019). A secure user authentication protocol using elliptic curve cryptography. Journal of Discrete Mathematical Sciences and Cryptography, 22(4), 521-530.

[21]. Ju, S. H., Seo, H. S., Han, S. H., Ryou, J. C., & Kwak, J. (2013). A study on user authentication methodology using numeric password and fingerprint biometric information. BioMed research international, 2013.

[22]. Kumar, T. S., Suresh, A., & Karumathil, A. (2014). Improvised classification model for cloud based authentication using keystroke dynamics. In Frontier and Innovation in Future Computing and Communications (pp. 885-893).Springer, Dordrecht.

[23]. Kumar, R., Chandra, P., & Hanmandlu, M. (2016). A Robust Fingerprint Matching System Using Orientation Features. Journal of information processing systems, 12(1).

[24]. Jain, A., & Prasad, M. V. (2016). A novel fingerprint indexing scheme using dynamic clustering. Journal of Reliable Intelligent Environments, 2(3), 159-171.

[25]. Su, Y., Feng, J., & Zhou, J. (2016). Fingerprint indexing with pose constraint. Pattern Recognition, 54, 1-13.

[26]. Sankaran, A., Jain, A., Vashisth, T., Vatsa, M., & Singh, R. (2017). Adaptive latent fingerprint segmentation using feature selection and random decision forest classification. Information Fusion, 34, 1-15.

[27]. Okokpujie, K., Noma-Osaghae, E., Okesola, O., Omoruyi, O., Okereke, C., John, S., & Okokpujie, I. P. (2018, June). Fingerprint biometric authentication based point of sale terminal. In International conference on information science and applications (pp. 229-237). Springer, Singapore.

[28]. Hammad, M., & Wang, K. (2019). Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network. Computers & Security, 81, 107-122.

[29]. Kumar, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2017, May). Identity privacy preserving biometric based authentication scheme for naked healthcare environment. In 2017 IEEE international conference on communications (ICC) (pp. 1-7). IEEE.

[30]. Kwao, L., Ativi, W. X., Hayfron-Acquah, J. B., & Panford, J. K. (2019). User Authentication Model for Securing E-Health System using Fingerprint Biometrics. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 7.

[31]. Hamidi, H. (2019). An approach to develop

the smart health using Internet of Things and authentication based on biometric technology. Future generation computer systems, 91, 434-449.

[32]. Hathaliya, J. J., Tanwar, S., Tyagi, S., & Kumar, N. (2019). Securing electronics healthcare records in healthcare 4.0: a biometric-based approach. Computers & Electrical Engineering, 76, 398-410.

[33]. Hathaliya, J. J., Tanwar, S., & Evans, R. (2020). Securing electronic healthcare records: A mobile-based biometric authentication approach. Journal of Information Security and Applications, 53, 102528.

AUTHORS

Ahmed Alghamdi received his B.S. degree in Information systems from College of Computing and Information Technology, Information Systems Department, Bisha University, KSA. He is pursuing his master degree in Cyber-security. He is currently an IT specialist in Saudi Ministry of Health, Prince Mashary hospital at Bulgrashi, Albaha, KSA. His current research interests include cyber-security, IOT and biometrics.

Dr. Mahjoub Hammad is an assistant professor of Information systems at College of Computing and Information Technology, Information Systems Department, Bisha University, KSA. Dr. Mahjoub currently serves as a head of Information Systems Department in Bisha University. Dr Mahjoub has many published papers in cyber-security and information systems areas. He also serves as a reviewer in many international journals. His current research interests include cyber-security, IOT and biometrics.

Ahmed Alghamdi, et. al. “Authenticating Data Access in IOT Healthcare Systems Based on Fingerprints.” *International Journal of Engineering Research and Applications (IJERA)*, vol.11 (4), 2021, pp 35-43.