Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 10083 - 10091

Research Article

An Integrated Manet Approach For Biometric Authentication System: Applications And Comparative Analysis Of Deep Learning Techniques

V. Azhaharasan[1], P. Prabhusundhar[2], M. Ramalingam[3]

Abstract

Security is a major concern for providing trusted communications in mobile ad hoc networks (MANETs) in a potentially hostile environment. This concern is mainly due to the peer-to-peer (P2P) architecture in MANETs, system resource constraints, shared wireless medium, and highly dynamic network topology. Authentication is a common prevention-based approach used in MANETs to reduce intrusions. Biometrics provides some possible solutions to authentication used in MANETs since it has the direct connection with user identity and needs little user interruption.The biometric data can't be recreated or hacked, so it makes the distinctive verification more strong.Unimodal biometrics has to face several challenges such as noise in sensed data, intra-class variations, inter-class similarities. Security problems could be resolved by adopting multimodal biometric systems. Multimodal biometric system presents a more reliable authentication method due to the combination of statistically independent biometric traits.In this article, different varieties of bio-metric approaches and the deep learning methods are compared where effective algorithm is identified by the comparison.

Keywords: Biometrics, Authentication, Hacking, Iris, Retina, deep learning, MANET, and pattern matching.

1. INTRODUCTION

MANETs consist of mobile platforms, known as nodes, interconnected by radio links or multihop communication paths. An important characteristic of such networks is the absence of a fixed infrastructure, such as mobile switching centres, base stations, access points, and other centralized machinery seen in traditional wireless (and wired) networks [1]. The network topology may constantly change due to the movement of nodes in and out of or within the network. Packet forwarding, routing, and other network operations are not the task of specialized devices, but rather are carried out by the individual nodes themselves. Typically in traditional networks, when traffic is detected, the minimum actions of the IDSs are to log the event and/or alert related personnel, but human interaction is the most time consuming element in an attack response cycle. ETs) [2].

Biometrics comes from the words bio meaning Life and woman meaning Measurement. It is in this manner the unmistakable evidence/affirmation by use of assessment of somebody of sort

[1] Asst. Professors of CS, Gobi Arts & Science College (Autonomous), Gobi, Tamil Nadu
[2] Asst. Professors of CS, Gobi Arts & Science College (Autonomous), Gobi, Tamil Nadu
[3] Asst. Professor of CS, Gobi Arts & Science College (Autonomous), Gobi, Tamil Nadu

characteristics of the customer [3]. So the pattern of endorsement of customer to sign in to the record or acquiring permission to singular data, etc by using the novel ascribes of customer for instance finger impression check, facial imaging, signature, voice affirmation, is the Biometric Identification. Affirmation of Identity happens when the customer is enrolled or customer's data is as of now chose the system programming. For the present circumstance the customers input data being dealt with is differentiated and the as of late dealt with data, if the data for instance the physiological or lead brand name matches with as of now chose brand name, by then the customer is affirmed and allowed to acquire induction to or sign in. If customer isn't enrolled, and is choosing startlingly, by then the brand name data is dealt with and saved in the item for any further access [4, 5]. This system gives better steady quality then the standard PIN or some other Identity or chronicle based structure as:

- The person needs not to carry any identity card or remember any passwords or login-ids.
- The person in regard needs to be present at the point of time and place, the system is one to one interface, so more secure.
- Biometric authentication can be classified into two classes of identification schemes:
- Behavioral characteristics
- Physiological characteristic

Multimodal biometrics are deployed to work with intrusion detection systems (IDSs) to alleviate the shortcomings of unimodal biometric systems. Since each device in the network has measurement and estimation errors, more than one device needs to be chosen, and observations can be fused to increase observation accuracy using Dempster-Shafer theory for data fusion. The system decides whether or not user authentication (or IDS input) is required, and which biosensors (or IDSs) should be chosen depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and each IDS [6].

This paper is concerned with the study and analysis of biometric-based security for mobile ad hoc network to progress the security in order to decrease the network attacks and leakage of information. With the propagation of inexpensive, smaller and more powerful mobile devices, mobile ad hoc networks (MANETs) have become one of the wildest growing areas of research and it becomes a popular research subject due to their self-configuration and self-maintenance capabilities. Wireless nodes can initiate a dynamic network without a static infrastructure. This type of network is very useful in tactical operations where there is no communication setup. However, security is a major concern for providing reliable communications in a potentially hostile situation. This new type of self-organizing network combines wireless communication with a high degree node mobility. Unlike, conventional wired networks mobile ad hoc networks don’t have fixed structure (base stations, centralized management points and the like) [7].

The remainder of the paper is organized as follows: different forms of biometric authentication system is discussed in Section 2, challenges and advantages in the biometric authentication system is detailed in Section 3, MANET based biometric system is given in Section 4, comparative analysis of deep learning approach is discussed in Section 5 and the article is concluded in Section 6.

2. BIOMETRIC AUTHENTICATION SYSTEM

Different forms of biometric authentication system is discussed in this section and depends on the need these are incorporated into the real time system [8, 9].

- Fingerprints Identification: It is most seasoned Biometric trademark utilized. In this innovation the computerized imaging of fingerprints is done. It checks the erosion edge skin impression of the human fingers. The sensor detects the extraordinary bends, bifurcations of the skin of fingers. Same occurs in palm examining.

- Eye Scanning: There are two strategies for eye acknowledgment:

  Retina scanning: The client needs to glance in a gadget that performs laser-checking of his retina. The gadget investigates the design of veins of the client. The veins design of anindividual is special. It represents a trouble as client needs to fix a point till the laser is examining his eye.

  Iris Scanning: Unlike the Retinal scanning the person needs not to be close to the device. In this, the imaging is done by a camera. The iris patterns are obtained through a video- based imaging system. The image so acquires is analyzed by the device. The image contains 266 different spots, these spots are based on the characteristics of iris, i.e. furrows and rings. The iris is stable throughout the life. No timely updating of image is required.

- Face Recognition:In face acknowledgment, a decent goal straightforward camera or a web camera is utilized. Facial acknowledgment in obvious light gets highlights from the focal bit of face picture. These qualities don't change over the long run. Shallow highlights, for example, outward appearances, hairs are kept away from. The portrayal is contrasted and existing data set, which whenever coordinated, the client is verified.

- Handprint Imaging: In this technique, the image of a client's hand is being examined. Qualities like distance between fingers, length of fingers, and length of hand are extricated and saved with the assistance of computerized signal preparing calculations. The formats are created. The qualities are with these formats for confirmation. Hand math is filtered generally by optical scanners.

- Palm print Recognition:Highlights like particulars, edges, standard lines, wrinkles, direction, and vein math are extricated for acknowledgment. For various people, vein math is particular. For validation, hand is put on the screen, infrared light is utilized for examining of the veins. It catches picture of hand, an example of veins is removed, which is the brilliant and dull example. The more obscure example is framed because of retaining of infrared light by veins of hand. A format of this natural example is saved in the gadget. This picture is changed over into computerized picture by transducer for coordinating and correlation reason.

- DNA Analysis: This Method of check is generally utilized in criminal cases. DNA of the client as blood, tissue, hair, nails is gathered for affirming. DNA examining requires some investment. DNA additionally is interesting trademark however a hair or nail can be taken.

- Voice Verification: In voice verification, user is asked to speak a phrase or a secret code. His vocal characteristics are measured i.e. both physiological (shape and size of vocal cords) and behavioral (pitch of voice) characteristics. The verification process is different from voice identification process. In verification sample of speaking style pattern is saved and is compared with the same person's speech but identification is rather many to one or one too many process. The verification system is been trained for a particular speaker's voice verification.

- Signature scanning: It is the dynamic assessment of the shape, size of imprint, making speed, time taken for stamping, pressure applied by customer's hand on the screen while checking, etc, anyway imprint may be copied at this point the properties while stamping may not be

- Keystroke: It is basically the way of pressing the key. The measurable traits are the time for which key is pressed, releasing time, sound made while pressing and releasing. The categorization of bio-metric authentication system is given in Figure 1.

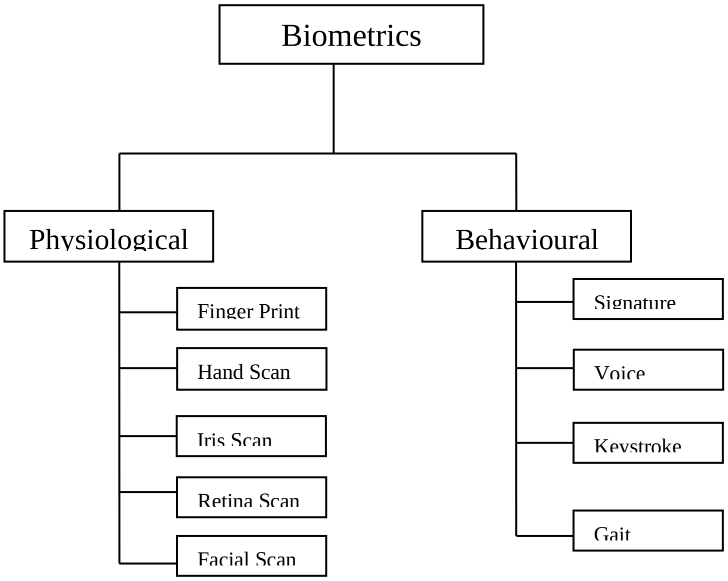


Figure 1. Categorization of Biometric authentication system

3. ADVANTAGES AND DISADVANTAGES OF BIOMETRIC AUTHENTICATION SYSTEM

In this section, the advantages and disadvantages faced in the bio-metric authentication system and its applications are discussed [10].

Advantages of bio-metric authentication system

- No recalling of passwords or login ID's is required.

- Better substitute of saving time and assets.

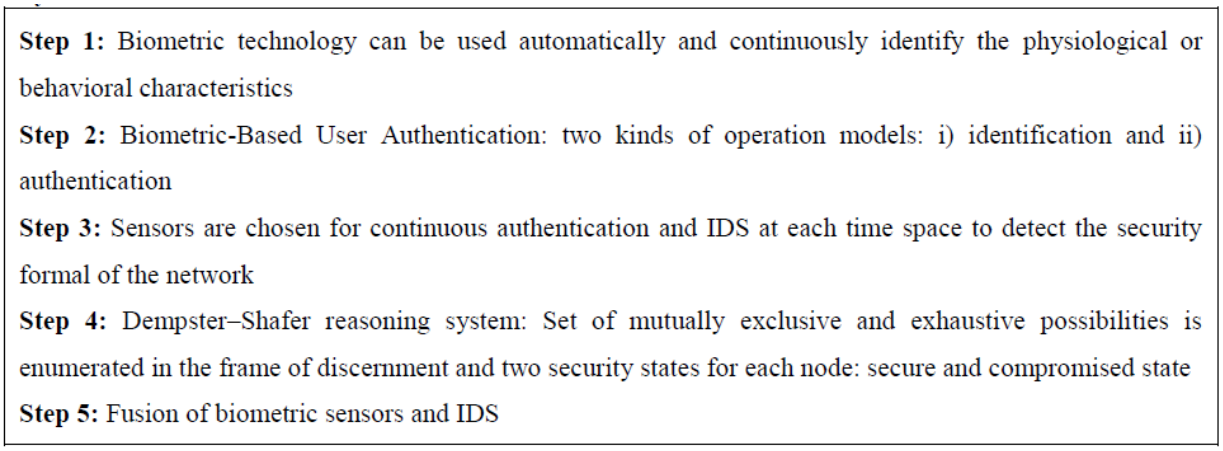
- Only Legitimate client can gain admittance to the individual information or records.
- Elimination of need of conveying approved reports.

Disadvantages of bio-metric authentication system

- Some of these strategies are impediment for genuinely tested individuals.
- Changing of measure of light going into eye because of understudy constriction may prompt framework indicating mistake.
- DNA investigation requires significant investment, retina filtering requires costly gadget.
- Some qualities of face or palm may change with time and age.

3. MANET FOR BIOMETRIC

The architectural model express MANET node as routers with hosts committed. This denotes that, connectivity is via a classic IP link from the point of view of the hosts, and the applications running on these hosts. Hosts, and its applications, are not visible to the specific characteristics of the MANET interfaces and are linked to the MANET via a router, which has one or more MANET interfaces. The prefix P can be allotted to the classic IP link(s) when the MANET router is delegated, and hosts can be assigned addresses from within this prefix, and configured with this prefix. The MANET for Biometric is given in Algorithm 1.



Step 1: Biometric technology can be used automatically and continuously identify the physiological or behavioral characteristics

Step 2: Biometric-Based User Authentication: two kinds of operation models: i) identification and ii) authentication

Step 3: Sensors are chosen for continuous authentication and IDS at each time space to detect the security formal of the network

Step 4: Dempster–Shafer reasoning system: Set of mutually exclusive and exhaustive possibilities is enumerated in the frame of discernment and two security states for each node: secure and compromised state

Step 5: Fusion of biometric sensors and IDS

3.1.Multimodal Biometric Systems

In order to overcome the disadvantages of uni-modal biometrics, biometrics to be ultra-secure and to provide more-than-average accuracy, more than one form of biometrics is required and hence, the need arises for the use of multimodal biometrics. Instead of using a single biometrics, a combination of different biometric can be used for recognizing a human being. Multimodal biometric can be composed in three different fusion methodologies, such as fusion at the feature level, match score level and decision level. As fourth level, a new fusion technique is can be utilized, which fuses the security services provided by the system by adding more biometric modalities the security level increases.

3.2.Biometric-Based Continuous Authentication and IDS in MANETs

Biometrics is a technique commonly known as the automatic identification or verification of an individual by his or her physiological or behavioral characteristics. Biometrics provides some possible solutions to authentication used in MANETs, since it has direct connection with user identity, can be continuously monitored, and needs little user interruption. Each biometric technology has its own strengths and weaknesses. For example, iris pattern is more accurate than voice identification, but getting a good image of the iris is difficult. Signature is a widely accepted authentication method, but it still remains a question if it could acquire the same level accuracy as the other biometric technologies. Currently, there is no best biometric modality since it depends on the environment applied.

Unimodal biometrics has to face several challenges such as noisein sensed data, intra-class variations, inter-class similarities. Some of these problems could be resolved by adopting multimodal biometric systems. Multimodal biometric systems present more reliable authentication methods due to the combination of statistically independent biometric traits. This system can exploit the benefits of one biometric and mitigate the shortcomings of another biometric. The increasing use of multimodal biometrics has led to the investigation of different modes of system operation: serial mode, parallel mode, and hierarchical mode. In serial mode of operation, one output of a biosensor will be used at one time. In the parallel mode of operation, multimodal biometric traits have to be used simultaneously. The hierarchical mode of operation is suitable for the system using a large number of biometric traits.This paper will consider the serial mode of operation since the continuous authentication is necessary for MANETs[6].

4. COMPARATIVE ANALYSIS OF RESULT

In this section,different biometric based approaches are compared and the compared existing approaches are Multimodal DNN [11],Multimodal CNN [12],ANN with PSO [13],Hybrid Optimization [14], and ANN with SO [15]. The performance of the deep learning and optimization technique is investigated in terms of FAR, FRR and Accuracy.

False Acceptance Rate (FAR): The term FAR is the estimation of probability where the incorrect acceptance of security system based on biometric against the attempt used for accessing the system by illegitimate user. The FAR is determined as the ratio of the count of false acceptance divided by the count of identification attempts. The FAR is equated as follows,

$$FAR = \frac{count\ of\ false\ acceptance}{count\ of\ discovery\ attempt}$$

The value of FAR and FRR acquired for the approaches Multimodal DNN [11],Multimodal CNN [12],ANN with PSO [13],Hybrid Optimization [14], and ANN with SO [15] are given in Table 1 and illustrated in Figure 2.

Table 1. Comparison of FAR and FRR

Algorithm	False Acceptance Rate	False Rejection Rate
Multimodal DNN	0.02	1.3

Multimodal CNN	1.3	1.7
ANN with PSO	0.9	1.1
Hybrid Optimization	0.02	0.05
ANN with SO	0.3	0.7

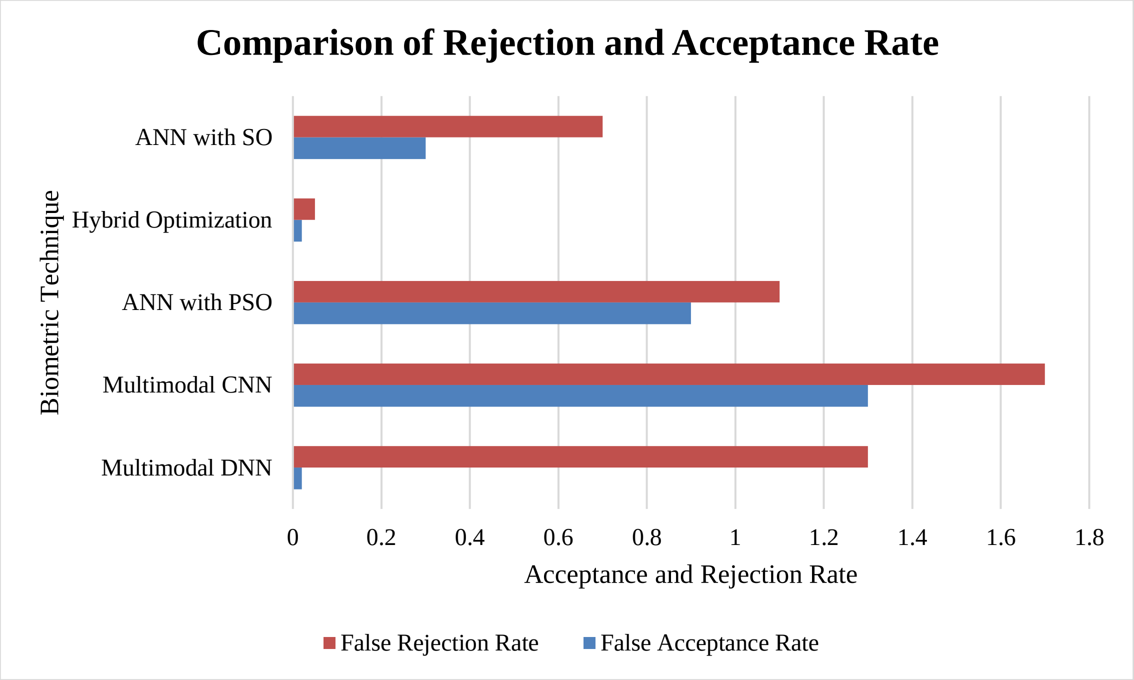


Figure 2. Comparison of Performance

From the observation of FAR and FRR in Figure 2, the hybrid optimization acquired minimum rate when compared to other techniques.

False Rejection Rate (FRR): The term FRR is the estimation of probability where the incorrect rejection of security system based on biometric against the attempt used for accessing the system by illegitimate user. The FRR is determined as the ratio of the count of false rejections divided by the count of identification attempts. The FRR is equated as follows,

$$FRR = \frac{count\ of\ false\ rejections}{count\ of\ discovery\ attempt}$$

Accuracy: Accuracy indicates the closeness of the value determined from the classified biometric signals and it is the illustration of systematic errors or statistical bias. Accuracy is the near value of calculated true positive and true negative values from the investigated signal classes. The acquired accuracy values are given in Table 2 and Figure 3. The accuracy is estimated as,

$$Accuracy = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative}$$

Table 2. Comparison of Accuracy

Algorithm	Accuracy in %
Multimodal DNN	97.6
Multimodal CNN	98.66
ANN with PSO	85
Hybrid Optimization	99
ANN with SO	91

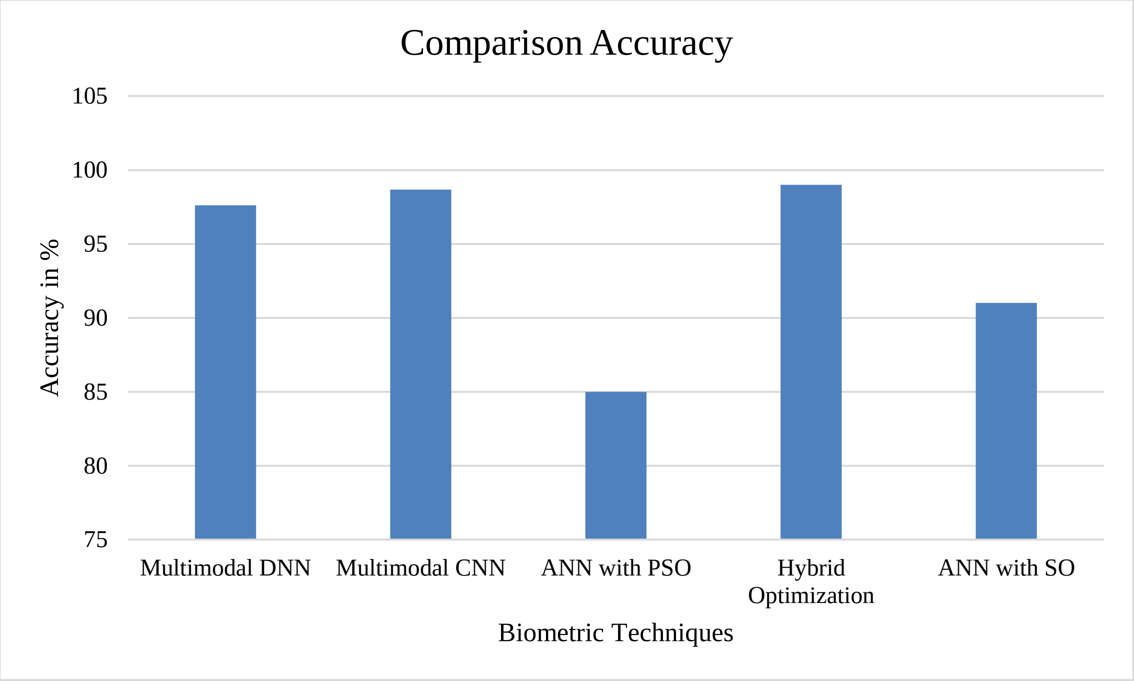


Figure 3. Comparison of Accuracy

From Figure 3, it is identified that the performance of Hybrid optimization technique is effective and it achieved 99% accuracy for the classification when compared to other optimization techniques.

5. CONCLUSION

The biometric framework may discover applications in participation framework, security frameworks, and distinguishing proof purposes and may discover much more applications in the future time. The predominant frameworks would be worked upon and changed for mistake free secure framework. The exactness levels should be expanded for productive security framework. Legitimate choice of method must be considered by the prerequisite.The MANET security systems have been studied and classified into prevention-based approaches such as authentication and detection-based approaches such intrusion detection.From the comparison of different deep learning and neural network, hybrid optimization technique achieved better accuracy and also outperforms other existing techniques. Logical work is being completed for future applications and progress in the biometrics.

REFERENCE

1. Liu, J., Yu, F. R., Lung, C. H., & Tang, H. (2009). Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks. *IEEE transactions on wireless communications*, *8*(2), 806-815.
2. Richard Yu, F., Tang, H., Leung, V. C., Liu, J., & Lung, C. H. (2008). Biometric-based user authentication in mobile ad hoc networks. *Security and Communication networks*, *1*(1), 5-16.
3. Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., &López-Gutiérrez, R. M. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications*, *42*(21), 8198-8211.
4. Malathi, R. (2016). An integrated approach of physical biometric authentication system. *Procedia Computer Science*, *85*, 820-826.
5. Hemalatha, S. (2020, February). A systematic review on Fingerprint based Biometric Authentication System. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)* (pp. 1-4). IEEE.
6. Kaur, N. (2018, December). A Review of Biometric based Authentication for MANET. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 575-579). IEEE.
7. Liu, J., Yu, F. R., Lung, C. H., & Tang, H. (2009). Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks. *IEEE transactions on wireless communications*, *8*(2), 806-815.
8. Rui, Z., & Yan, Z. (2018). A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE access*, *7*, 5994-6009.
9. Kumar, K., &Farik, M. (2016). A review of multimodal biometric authentication systems. *Int. J. Sci. Technol. Res*, *5*(12), 5-9.
10. Alsaadi, I. M. (2015). Physiological biometric authentication systems, advantages, disadvantages and future development: A review. *International Journal of Scientific & Technology Research*, *4*(12), 285-289.
11. Sengar, S. S., Hariharan, U., &Rajkumar, K. (2020, March). Multimodal Biometric Authentication System using Deep Learning Method. In *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 309-312). IEEE.
12. Hammad, M., Liu, Y., & Wang, K. (2018). Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. *IEEE Access*, *7*, 26527-26542.
13. Evangelin, L. N., & Fred, A. L. (2017). Biometric authentication of physical characteristics recognition using artificial neural network with PSO algorithm. *International Journal of Computer Applications in Technology*, *56*(3), 219-229.
14. Sujatha, E., & Nil, A. C. (2018). Multimodal biometric authentication algorithm at score level fusion using hybrid optimization. *Wireless Communication Technology*, *2*(1), 1-12.
15. PRIYAN, S. V. (2018). BIOMETRIC AUTHENTICATION USING HYBRID ARTIFICIAL NEURAL NETWORK WITH SWARM BASED OPTIMIZATION. *substance*, *4*, 5.