Computer Systems Science & Engineering
DOI: 10.32604/csse.2022.024302
Article

Tech Science Press

A Proposed Biometric Authentication Model to Improve Cloud Systems Security

Hosam El- El-Sofany[1,2,*]

[1]King Khalid University, Abha, Kingdom of Saudi Arabia
[2]Cairo Higher Institute for Engineering, Computer Science and Management, Cairo, Egypt
*Corresponding Author: Hosam El- El-Sofany. Email: helsofany@kku.edu.sa
Received: 12 October 2021; Accepted: 16 November 2021

Abstract: Most user authentication mechanisms of cloud systems depend on the credentials approach in which a user submits his/her identity through a username and password. Unfortunately, this approach has many security problems because personal data can be stolen or recognized by hackers. This paper aims to present a cloud-based biometric authentication model (CBioAM) for improving and securing cloud services. The research study presents the *verification* and *identification* processes of the proposed cloud-based biometric authentication system (CBioAS), where the biometric samples of users are saved in database servers and the authentication process is implemented without loss of the users' information. The paper presents the performance evaluation of the proposed model in terms of three main characteristics including *accuracy*, *sensitivity*, and *specificity*. The research study introduces a novel algorithm called "Bio_Authen_as_a_Service" for implementing and evaluating the proposed model. The proposed system performs the biometric authentication process securely and preserves the privacy of user information. The experimental result was highly promising for securing cloud services using the proposed model. The experiments showed encouraging results with a performance average of 93.94%, an accuracy average of 96.15%, a sensitivity average of 87.69%, and a specificity average of 97.99%.

Keywords: Cloud computing; cloud security; biometrics technologies; biometric authentication

1 Introduction

The *biometric authentication process* refers to a security mechanism for verifying the user's identity through unique biological features such as *fingerprints*, *hands*, *face*, *retina*, *iris*, *voice*, *signature,* and *DNA* (*deoxyribonucleic acid*). Biometric data is stored in the biometric authentication systems to recognize and verify the user's identity when the user tries to access his/her account. Since this data is unique for everyone, hence biometric authentication is mostly more secure than traditional ways for authentication. Recently, biometric authentication is used increasingly in various important digital-based resources such as buildings, rooms, and computing devices. There are many types of biometric characteristics for individuals: *conventional biometrics* and *cognitive biometrics*. The first includes

physiological or behavioral characteristics. *Physiological* characteristics describe the individual physically, while *behavioral* characteristics describe the conduct. The second refers to the psychological brain state. Therefore, it depends on the measurement of brain signals directly or indirectly [1].

Recognition systems are categorized into three basic classes: (1) a *knowledge approach* that shows "what you know" like numbers, names, and passwords; (2) a *token approach* that shows "what you have" like cards and passport, and the previously mentioned approaches can be lost at any time; (3) a *biometric* that shows "who you are" like fingerprint and iris recognition. A *biometric* is a biological feature that is an alternative to traditional authentication approaches. It cannot be stolen or lost because it depends on physiological or behavioral features. Hence, researchers introduced brain signals as a biometric attribute. Brain waves are used for recognition as a type of cognitive biometric. They also have signals that can read and measure each person's status. These signals follow the body's actions, then measure the neurons' electrical activity, and finally record it through EGG (*Electroencephalogram*) [2].

Recently, cloud computing security issues are solved by combining biometric technology to a cloud computing platform that will merge the cloud computing security objectives, such as *authentication*, *privacy,* and *integrity*, with the *accuracy* of biometric systems. Consequently, biometric technology has what is needed to take care of issues identified with the present age of cloud computing technology. In any case, applying biometric technology to cloud computing security is a long process [3,4].

In this research paper, the researcher attempts to examine the previously mentioned security issues and provide dynamic scientists and designers with some vital rules concerning the best way to apply biometric technology to a cloud computing stage as a novel security benefit. The paper aims to present a CBioAM model for securing cloud computing services. The research study presents the *performance* evaluation of the proposed model in terms of three main characteristics including *accuracy*, *sensitivity*, and *specificity*, that reflect the effectiveness and reliability of the proposed system. The research study introduces a novel algorithm called "Bio_Authen_as_a_Service" using neural network concepts and MATLAB programming language for implementing the proposed model and to evaluate the accuracy and performance of the proposed approach. The proposed system performs the biometric authentication process securely and preserves the privacy of user information. Therefore, this research study is created from working in the cloud computing security and biometric application development fields.

2 Related Work

In this section, the author presents a survey of related research that reveals some recent analysis studies of biometric authentication using cloud computing concepts. Sunil et al. presented a research paper for some biometric mechanisms, their application, and their restrictions. The paper presented the motivation for biometrics adoption in current situations. This research study discussed some technical problems regarding biometric security applications [4]. Rui et al. presented some recent advances in the biometric authentication field. The authors focused on possible security risks facing the biometric system and proposed some assessment criteria for measuring the biometric authentication system's performance. The paper compared the recent research works and divided the users' authentication of biometric systems into two categories according to whether they have static or dynamic biometric features. The paper illustrated that some current automated applications face several security problems. These results opened several research directions for biometric authentication in the future [5]. Martin et al. presented a research paper on fingerprint recognition identification and classification using Euclidean distance and neural network concepts for better accuracy. The researchers used some techniques for image processing to illustrate their research study. The performance evaluation results were provided significantly for the proposed approach used especially in the fingerprint recognition system [6]. Jesus et al. presented a face recognition approach depending on LBP (*local binary pattern*). They implemented it on smartphones, where the

input image is processed using the camera of the mobile. The proposed algorithm was used for face recognition. The system implementation was tested on a smartphone, where the authors used the average of images for obtaining a template by the individual and applying Euclidean distance for classification [7]. Asadullah et al. presented a biometric authentication technique using the motion sensor-based approach of a smartphone. In this paper, the user carries out the signature by using his smartphone, and the pattern features are recognized using the accelerometer of the smartphone. The paper's results illustrated that an authorized user can be recognized by a certain level of approximate error [8]. Annies et al. proposed a biometric authentication architecture depending on iris recognition. The proposed architecture provided better accuracy and security compared with other many biometric models. The authors used a hybrid encryption algorithm for providing security to the data sent over the Internet, instead of the traditional mechanisms in which the systems use a user credential for authentication [9]. Mohamed et al. introduced a research review concerning the security mechanism of mobiles using biometric features in IoT environments. In this paper, the authors used machine learning and data mining techniques as well as unsupervised, semi-supervised, and supervised approaches. The paper also illustrated the issues and barriers of the present security mechanism model of portable IoT devices [10]. The authors presented a cloud-based concept to maintain secure authentication. The proposed cloud model provides a secured authentication approach, consisting of two main authentication processes, namely, *enrolment* and *verification*. The biometric data conversion and feature extraction are performed in the enrolment process. When the user logged into the system, the same processes were performed through the verification process. The matching process between the feature of the input data biometrics and stored records was performed through the matching module [11]. Stergiou et al. introduced a fundamental mechanism called CC (Cloud Computing) to work with Big Data systems. The presented technology refers to the processing power of data in the cloud and provides power computational and sustainable computing. In this study, the researchers proposed a new integrated system between CC and IOT, that acts as a base for manage Big Data systems. Through this contribution, the authors tried to create an architecture relying on cloud security to solve some security problems related to this integration [12]. Stergiou et al. presented a survey of IoT and cloud computing with a focus on security issues that faced these new areas. The authors compared these new concepts to illustrate their benefits for securing and transmitting Big Data. The researchers also illustrated how cloud computing and IoT technologies are integrated to improve Big Data systems [13]. Stergiou et al. proposed a secure decision system of wireless-mobile 6G network for managing big data systems on smart buildings. This new infrastructure provides the users with a secure environment for browsing the Internet and managing big data in the fog [14]. Stergiou et al. presented a research study in energy-efficient and green cloud infrastructures using CloudSim's simulator architecture. The researchers proposed an approach for performing an energy-efficient resource allocation technique for managing Big Data over a green cloud environment. The research study offered big performance results regarding the saving cost and data management under Big Data usage scenarios [15]. Stergiou et al. introduced a novel architecture based on cloud computing and the innovative paradigm of federated learning. The proposed model was developed on the resources that are presented by CSPs (cloud service providers) to be able to manage user requests faster and more effectively [16].

In this study, the researcher presents a novel model for biometric authentication to secure cloud apps. In this article, the proposed model (see Fig. 2) is considered as a more general approach compared to other approaches mentioned above which are used especially in recognition systems presented in [4–6], [7–9], [10].

3 Authentication Security in Cloud Computing

Cloud computing is a successful internet-based architecture of service-oriented computing. It is a novel paradigm for providing and organizing resources as well as providing web services to consumers. The cloud

providers use all communications via the internet as the main medium for delivering their IT resources to the organizations or individuals using a pay-as-you-use way. The cloud computing paradigm is composed of five essential components including *infrastructure, platforms*, *servers, applications*, *and clients*.

Cloud security is highly important when we plan to develop cloud systems and services. The concerns of cloud security are increasing because the customer's sensitive information is stored in a cloud provider server. Therefore, cloud security researchers address these concerns by identifying some important objectives such as *availability* (the user can use the services from any location and at any time), *authentication* (users' identity should be assured), *accountability* (all users participate easily in a data transfer between the systems, and cloud services protect them from denial of service attacks), *confidentiality* (cloud servers should secure users' data, and no unauthorized individual can access the database), and *integrity* (the cloud model ensures that the data is not changed during storage, and processing, through the cloud) [1]. The mentioned security goals need the innovation and implementation of novel security approaches and methodologies for detecting and preventing security attacks. The cloud computing model needs new and innovative solutions to secure cloud provider infrastructure and users' resources such as *data*, *information*, *applications*, and *services*. Therefore, cloud security research is a new area of motivation for researchers [3].

The user login data of the cloud-based system should be authenticated by a powerful security mechanism since most attacks occur at the login steps. Therefore, the development of a secure model to protect user authentication is essential to increase the security of the entire cloud system. In this section, the author discusses different authentication methods of cloud computing and focuses on the discussion of the *biometric authentication* techniques in the rest of the sections [1]:

1. *Username and password authentication*: In this mechanism, the user should enter the username and password to log into the system, and the system checks the input data in the cloud servers, rejects unauthorized people, and gives access only to the authorized users.
2. *Multi-factor authentication*: In this approach, the user is required to use another factor such as biometric authentication to access cloud systems.
3. *Public Key Infrastructure* (PKI): The PKI method has been adopted in the design of security protocols such as SSL and TLS (i.e., secure sockets layer and transport layer security), and the use of SET (i.e., secure electronic transaction) mainly to provide authentication. The success of PKI is based on the control of access to private keys similar to other types of encryption systems.
4. *Single sign-on* (SSO): SSO is an access control process of multiple related, yet independent, cloud systems. In this method, the user logs into the system with a single username and password to access any of the related applications or resources.
5. *Biometric authentication*: *Biometrics* refers to a unique identification that allows access to automated systems and devices through the measurement of human physical or behavioral features. Biometric is an ancient Greek word that means *bio* (i.e., life) and *metron* (i.e., measure). The advantages of biometric authentication systems include (1) *security*, in which the systems provide strong security more than traditional methods, (2) *accountability*, in which the systems can trace and discover user's activities, and (3) *scalability*, in which the system can expand by adding some resources to itself. The biometric authentication approaches are based on the recognition of the *physiological* or *behavioral* features of individuals.
    - *Physiological biometrics:* the user authentication model depends on the physical features of humans, which don't change with time. The main disadvantage of this model appears when a great number of users need to be authenticated simultaneously. This case causes some reduction

in the processing speed. The major physiological biometric authentication techniques include *hand, fingerprint*, *voice*, *face*, *retinal*, *iris*, and *DNA* recognition.

- *Behavioral biometrics*: user authentication depends on the user's behavior. Behavioral biometric authentication techniques include *keystroke* and *signatur*e recognitions.

4 Biometric Authentication Technologies

With the increase of automated systems and entrance gates for important buildings, biometric technologies are becoming the basis of most security solutions for user authentication. This appears also with the growth of transaction fraud and security infringes. Recently, the use of biometrics for user authentication becomes more convenient and accurate than other traditional techniques. This is because biometrics techniques have many characterizations as follows: (1) linking the event to a specific user (username and password may be used by someone other than the authorized user), (2) being convenient (there is no need to remember them), (3) being accurate (they provide unique authentication), and (4) being socially acceptable and inexpensive [2]. Biometrics security solutions are gaining priority and advantage in several domains in need of a strong security mechanism compared to other traditional mechanisms. As a result, the transformation for using biometrics technology offers a unique property for authentication security, in which no users can share or carry the same biometrics data [4]. The major biometric technology types, which depend on the physiological or behavioral features of individuals include *Face recognition*, which can be adopted as a biometric profile for secure authentication because every individual has a unique face [17]. The face is captured using high-capacity cameras and used as a template for matching. *Fingerprint recognition*, the matching in a fingerprint scanner is performed using minutiae (locations and directions points) and pattern matching. The recognition rate of biometric profile degrades when the finger is wet or wrinkled, therefore there are many research papers focused to solve these problems [18]. *Hand recognition*, the human hand is used as a biometric profile for authentication because its arrangement contains spatial geometry with unique dimensions for each person [19]. It is required to measure up to four fingers to authenticate an individual's information. *Iris recognition*, the iris of everyone possesses certain unique characteristics that can be used to distinguish individuals. The iris images are captured by the scanner, and the iris patterns are analyzed using various iris databases (e.g., CASIA, MMU, UPOL, and IITD), to obtain the performance rate. *Retina recognition*, this biometric type is based on the pattern of blood vessels within the retina of a human eye [20]. The characteristics generated from the blood vessel pattern are unique and can be used for the authentication process [21]. *DNA recognition*, DNA presents the most reliable personal identification because it does not change during a person's life or after his/her death. DNA recognition needs a sample, such as blood, semen, hair, or tissue, for the authentication process. *Keystroke recognition*, this technique stores keystroke data used by the user including the time, speed, and pressure, taken to type the username and password [22]. The keystroke rhythm is measured for each user and stored as a unique biometric template for future authentication. *Signature recognition*, this technology may operate in two different ways: (1) static, in which users write their signature on paper and then digitize it through an optical scanner, and the biometric system recognizes this digital signature, analyzes its shape, and stores it as a biometric template; (2) dynamic, in which users write their signature in a digitizing tablet [23]. Some dynamic systems operate on smartphones or tablets, where the user can write his signature directly on the screen using his finger, or by using a touch screen pen. *Voice recognition*, this technology focuses on identifying the speaker rather than what they are saying, where the sensor stores the voice signal and converts it into a unique digital code [24]. This code represents a unique biometric template and is used for the authentication process [25].

5 Biometric Systems

The biometric identification system contains two main modules: (1) *enrolment module,* which is responsible for registering all users' biometrics information in the biometrics database, where the system learns about all the people who will use it as biometric authentication security; (2) *identification/* verification *module*, in which the user's input is compared with all samples saved in the database, producing as output the user's identity whose features have the typical or optimal level of similarity with the registered user. For example, in fingerprint recognition, if an individual wants to gain access, he/she has to put their finger on the fingerprint scanner. The scanner will read his fingerprint, compare it with all the captured samples in the database stored during the enrolment process, and decide whether the individual is authorized to gain access or not.

The design of the biometric system used for user authentication is illustrated in Fig. 1. The general biometric system includes the following five basic modules:

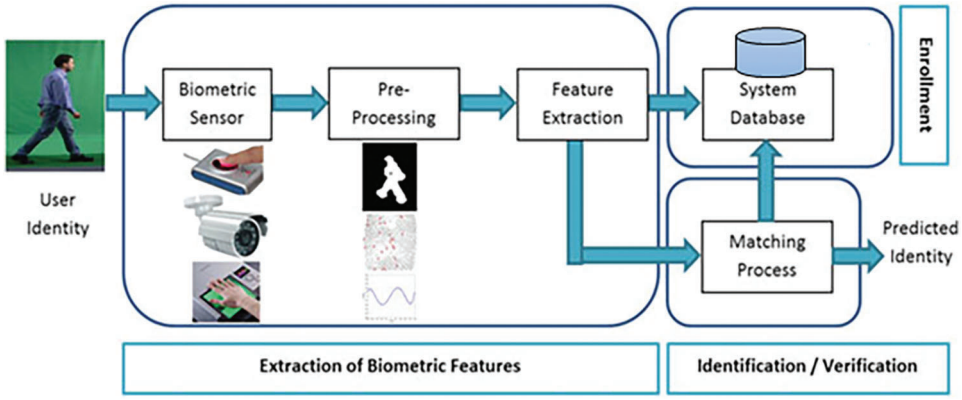

Figure 1: Design of the biometric system

1. *Sensor*: This module is used for capturing the input biometric data of the user.
2. *Pre-Processing*: This module performs the basic stage for improving the quality of the captured image by the sensor module. This module achieves three processes in the captured image including *color conversion*, *resizing*, and *normalization*.
3. *Feature Extraction*: Once the image is pre-processed, the feature extraction program is applied to produce detailed information about the image. The feature extraction module extracts only the essential information to form a new representation of the image data called *template*, and as a result, the user sample is maintained in the database. The characteristics of the image are created from three main scopes including *spatial*, *transform*, and *hybrid domain*.
4. *Matching*: In this module, the comparison between the extracted features and the stored templates is performed, determining the degree of similarity or dissimilarity between them.
5. *Decision*: In this module, the process of verifying the identity of the input user is performed and the decision is taken (*acceptance* or *rejection*) by the system based on the degree of similarity between the extracted features and the stored templates.

6 Biometric Authentication as a Cloud Security Service

The integration between biometrics and cloud computing enables organizations to use both cloud computing capabilities and biometrics technologies through the cloud environment. This new

environment includes cloud servers incorporating biometrics databases and other types of cloud computing-based tools required for biometric authentication processes. In addition to the mentioned components, the cloud service provider requires a biometric capture device (e.g., retina or fingerprint scanners). The biometrics tools hosted on a cloud-based system will support a wide range of biometrics applications and technologies.

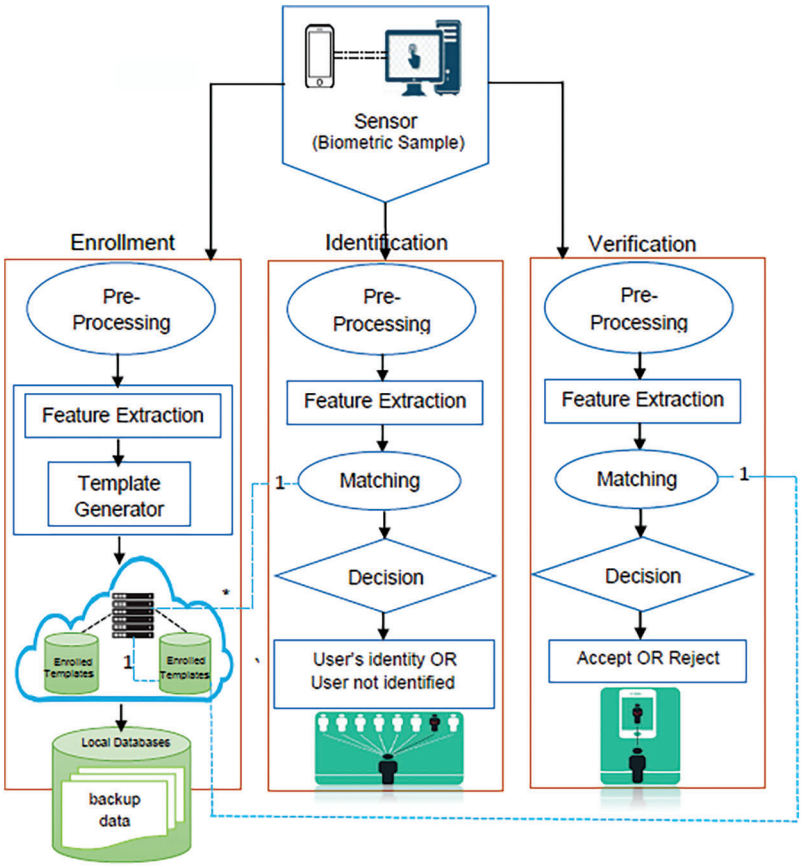

Figure 2: The proposed cloud-based biometric authentication model (CBioAM)

6.1 The Proposed Cloud-Based Model for Biometric Authentication

The *biometric app* is mainly a "pattern recognition" application that works by obtaining the basic input biometric information from the user, extracting a set of features from the inputs, and comparing these features with the templates stored in the biometric database. The proposed CBioAS is designed by extending the design of the biometric system mentioned in Section 5, as shown in Fig. 2. As mentioned, the integration between biometrics and cloud computing provides more capabilities, especially for the biometric authentication process.

In the proposed model, the biometric engine is placed in the cloud instead of a local processing unit as in traditional biometric systems. This feature increases the *accessibility* of the cloud-based biometric system and provides integration with other security applications. Also, maintaining biometric information in the cloud database servers increases system *scalability*, *reliability*, and *privacy*. As a result, the implementation of a cloud-based biometric system may gain some benefits of cloud computing characteristics such as *availability*, *reliability*, *performance*, *accessibility*, *portability*, and *manageability*.

The proposed model also provides a tool to *backup data* periodically in the *local database* server for more safety over sensitive information and local legislation of each organization.

three main processes, namely, *enrolment, identification,* and *verification* (see Fig. 2):

- The *enrolment process* is responsible for registering all users' biometrics information in the biometrics database, where the system learns about all the people who will use it as a biometric authentication security tool. During this process, the biometric sensor scans the biometric features of the user while the feature extraction program extracts the feature vector from the scanned biometric data. The feature vector is then stored as *enrolled templates* in the cloud using the template generator program.
- The *identification process*, in which the user recognition is done by searching the users' samples maintained in the database to seek the right information related to the required sample, by implementing a searching algorithm to get an individual's identity. Therefore, the proposed biometric system gets the biometric features of an individual as input and then compares these features with all possible identities stored in the database to match them and detect his/her identity. The main process outcome is the *decision* "whether the user's identity matches or does not match". Therefore, the identification module is called a 1-to-*n* matching process. Recognition systems that aim to determine if the individual is enrolled, are known as *positive-identification*, while systems that need no enrolment are called *negative-identification* systems.
- The *verification process*, in which a comparison is performed between the input biometric data of a specific user and the biometric templates stored in the cloud database server. In the proposed biometric system, this module contains the main process for biometrics system security, in which the user will claim the identity of someone already known to the system. Therefore, the verification module is called a 1-to−1 matching process. The objective of the verification mode is to do *positive recognition*, where different individuals are prevented from employing the same identity information.

To implement the *enrolment, verification,* and *identification* processes, as well as to evaluate the accuracy and performance of the proposed approach, the author implemented the "Bio_Authen_as_a_Service" algorithm using neural network concepts and MATLAB programming language.

Algorithm (Bio_Authen_as_a_Service):

```
Step 0. // enrollment process
Step 1.     for (i = 1; i <= n; i++) {          // n refers to the number of users
Step 2.         for (j = 1; j <= m; j++)        // m refers to the No. of biometric samples of each user
Step 3.         get_bio_samples(Enr(i, j)}      // to capture the biometric input data of the users
Step 4.     Cov ← covariance(Enr);              // to calculate the covariance of the inputs
Step 5.     S ← sqrt(diagonal(Cov));            // the square root of the diagonal elements in the Cov matrix
Step 6.     Cor ← Cov/square(S);                // to calculate the correlation
Step 7.     PCA ← svd(Cor);                     // performing the principal component analysis (PCA), svd
                                                   refers to singular value decomposition
Step 8.     Return PCA;
Step 9. // training process on the biometric inputs
Step 10. for (i = 1; i <= n; i++) {
Step 11.    for (j = 1; j <= m; j++)
```

(Continued)

Algorithm (continued)

Step 12.	Input(i, j) ← PCA(i, j);}	// Input(i, j) refers to the network input to be trained
Step 13.	NeuralNet ← ffnx()	// ffnx, refers to apply the feed-forward neural network function
Step 14.	NetResult ← train(NeuralNet, Input, Target)	// performing the training process on the created networkusing input and target matrices
Step 15.	Return NetResult	

6.2 Security and Privacy of the Proposed System

Generally, *security* refers to the prevention of unauthorized users to access private information and system resources, while *privacy* refers to the ability of the system to prevent the leakage of any private information to any unauthorized users. The proposed system must prevent the attackers from impersonating as authorized users and should ensure that unauthorized users don't access confidential information. Therefore, access to cloud resources is secured by both the *authentication* and *authorization* processes. The *authentication process* is used for confirming the user's identity, usually done before the authorization process, and governed by authorization protocol such as the OpenID Connect (OIDC). On other hand, the *authorization process* is used for determining what the user is allowed to access or to do, usually done after the authentication process, and governed by the authorization protocol such as OAuth 2.0 framework. The research study focuses only on the authentication concept and presented it through the proposed CBioAS system.

In the proposed system we have considered two types of attacks: Internal attacks (or insiders, e.g., employees of the organization), and External attacks (or outsiders, e.g., network/cloud attackers).

The proposed CBioAS system is secure against malicious attackers who try to access cloud apps. Without knowing confidential information and coding key, the attackers can't access the cloud services. Through the enrolment process, the CBioAS system generates and stores a biometric template f and a unique key k for each user, that is used in the verification process. In the CBioAS system, an attacker who wants to access the cloud system as an authorized user must gain access to two confidential information: (1) the authentic feature vector (f), and (2) the verification key (k). Since the verification key and the authentic feature vector corresponding to the user's biometric template are stored in the cloud server as encrypted form, then the attacker cannot be able to access the cloud system without knowing the decryption key corresponding to them. If the attacker gets the authentic feature vector of the user, he is not able to use it directly for the verification process because the encrypted verification key is not accessible. Hence, the proposed CBioAS system is secure against attackers who try to access the cloud system.

In the proposed system, all the data transmitted over the cloud network are in an encrypted form. When the attackers monitor the network processes, they cannot know any information about the authenticated users because they haven't any information about the decryption keys. Therefore, through the verification process, network attackers are not possibly gain access to the cloud system because they haven't any confidential information. Hence, the proposed CBioAS system is secure against network attackers.

On other hand, the paper considers the privacy issues on the biometric system through the protection of users' biometric templates and verification keys. The proposed system should ensure the confidentiality of all private information for users, and organizations. The proposed system stores the user's biometric template and verification key in the cloud database server in encrypted form. Therefore, the cloud service provider doesn't know anything about both the user and organization's confidential information since it hasn't any

knowledge regarding the decryption code of this information. If the decryption code of the user has been compromised, the service provider is not able to identify the authentic feature vector of the user since the biometric template has been transformed with a unique verification key in the enrolment stage. Hence, the CBioAS system protects both the verification key and the user biometric template stored separately in the cloud database server. This procedure prevents the attackers from knowing which verification key is associated with which user template in case of compromising user records. The matching process takes the verification decision through the decision module based on the similarity score (S) and the threshold value (t) (see Fig. 2). If $S < t$ then *reject* the user else the authentication process is successful and *accept* the user.

6.3 The Performance Evaluation of the Biometric Model

The proposed model shows the verification and identification process of the biometric system. The researcher uses the general term "*recognition*", where the context does not need to distinguish between both the verification and identification processes:

- The *verification process* of the proposed CBioAM is expressed mathematically as follows:

The study assumes that F_B is the input feature vector, and I is the claimed identity. The system evaluates and specifies if $(I, F_B) \in TRU_I$ or FLS_I, where TRU_I refers to a "claim is true" (i.e., a genuine or authorized user) and FLS_I refers to a "claim is false" (i.e., an impostor or unauthorized user). The system compares F_B with F_I, and the biometric templates corresponding to the user identity I, are categorized such that:

$$(I,\ F_B) \in \begin{cases} TRU_I & if\ S(F_B,\ F_I) \geq t \\ FLS_I & if\ S(F_B,\ F_I) < t \end{cases}$$

where S is the *similarity* function between feature vectors F_B and F_I, and t is a given *threshold*. The term $S(F_B, F_I)$ refers also to the *matching score* measure between F_B and F_I. Hence, every maintained identity is categorized into TRU_I or FLS_I according to the value of F_B, I, F_I, and t variables. *For example*, the biometric measurements for fingerprints of the same person taken at distinct times ($\tau = t$) are rarely similar.

- On the other hand, the *identification process* is represented mathematically as follows:

Suppose that F_B represents the *input feature vector.* Compute the identity set I_E; $E = \{1, 2, \ldots, N, N+1\}$, where $I_1, I_2, \ldots, I_N$ are the accepted identities by the system, and I_{N+1} indicates the rejected case. Therefore,

$$F_B \in \begin{cases} I_E & if\ \ Max_E\, S(F_B,\ F_{I_E}) \geq t;\ \ E = 1,\ 2,\ ..,\ N \\ I_{N+1} & otherwise \end{cases}$$

where F_{I_E} is the biometric sample for the identity I_E.

The study aims to present the evaluation of the proposed biometric system's performance, which can be evaluated and measured in different ways such as FAR, FRR, or EER (i.e., *false accept rate*, *false reject rate*, or *equal error rate*). The performance of this process depends on the feature vectors F_I and the similarity function $S(F_B, F_I)$. The accuracy of a biometric system is possibly estimated, depending on the matching scores and predetermined values. The biometric system generates two different feature sets of matching scores called *genuine* and *imposter*, which refer to *match* and *nonmatch*, respectively. The matching scores generate between a couple of patterns from the same individual and the nonmatching scores generate between a couple of patterns from different individuals. The representation of FAR, FRR, and EER that is used for evaluating the biometric system's accuracy are shown in Fig. 4.

6.4 Errors Evaluation of the Biometric Authentication System

To evaluate the errors of the proposed CBioAS, the researcher has assumed that two patterns having the same biometric features and captured from the same user *(*e.g., two fingerprints of one finger) are not exactly similar due to several reasons such as imaging status (e.g., fingers sweat), the present physiological and behavioral features of the user (e.g., fingers injury), surrounding environment and way of interacting with the scanner or sensor (e.g., fingers location). The output of the biometric system is computed by the matching score $S(F_B, F_I)$ that represents the similarity between (F_B) as input and the (F_I) as a template.

The higher score indicates that the two biometric measures drive from the same individual. The decision of acceptance or rejection is controlled by the value of threshold (t). If two biometric samples have scores $\geq t$, then they refer to *mate pairs* (i.e., for the same user); otherwise, they refer to *nonmate pairs* (i.e., for different users).

Fig. 3 illustrates the genuine and impostor distribution scores under FMR and FNMR functions, the histogram shows the genuine distribution scores (produced from pairs of samples from one person), and the impostor distribution scores (produced from different persons). The proposed CBioAS has the following two types of errors to test its verification:

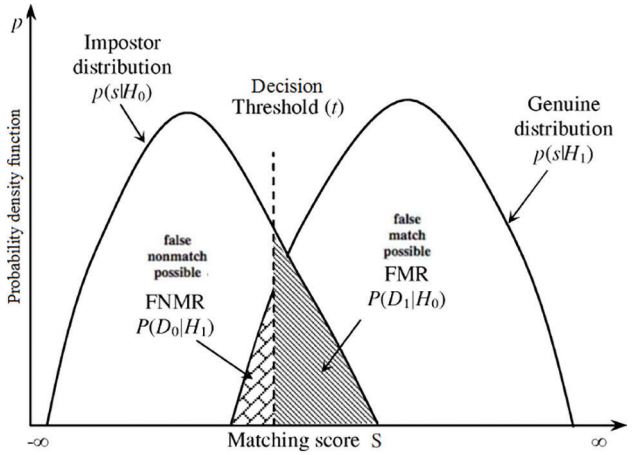

Figure 3: The genuine and impostor distribution scores under FMR and FNMR functions

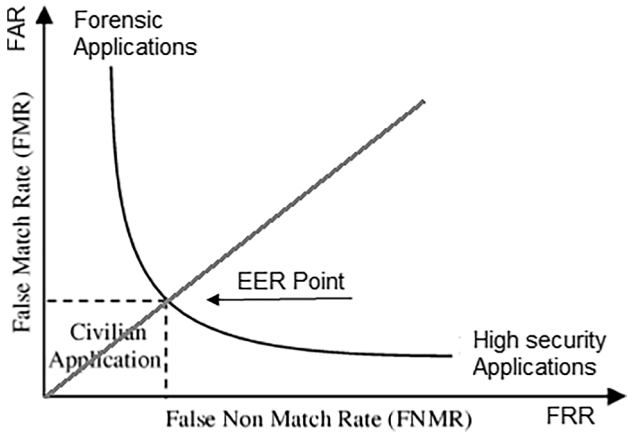

Figure 4: ROC curve for different types of biometric applications

1. FMR refers to the average of mismatched biometric signals that come from two different individuals as coming from the same individuals (i.e., FMR = FAR).
2. FNMR refers to the probability of the system's failure to determine a match between the input sample and any stored template. It equals the rate of valid inputs that are incorrectly rejected (i.e., FNMR = FRR).

The system performance at the time t is represented by a *receiver operating characteristic* (ROC) curve. A ROC histogram is drawn between FMR and (1-FNMR) or FNMR for different values of t, (see Fig. 4). The author formulates the errors in the *verification process* of the proposed biometric as follows:

Assume that F_I is the maintained biometric sample of user I, F_B is the required input of recognition. The author suggested the following hypotheses:

Hb_0: F_B doesn't get from the same individual as the sample F_I,

Hb_1: F_B gets from the same individual as the sample F_I.

The following associated decision factors are considered:

d_0: the individual who isn't required,

d_1: the person who is required.

Therefore, the decision rule can be expressed as follows:

If $S(F_B, F_I) < t$ then determines d_0;

else determine d_1;

Hb_0 means the processed signal is *noise*, and Hb_1 denotes that the processed signal is *message* and *noise*. The two hypotheses include two types of errors:

Error-Type$_1$: FMR (d_1 is determined when Hb_0 is true),

Error-Type$_2$: FNMR (d_0 is determined when Hb_1 is true).

FMR = $P(\mathrm{d}_1 \mid \mathrm{Hb}_0)$;

FNMR = $P(\mathrm{d}_0 \mid \mathrm{Hb}_1)$.

For instance, the fingerprint biometric system accuracy can be evaluated as follows:

The system collects results created from multiple patterns of the same finger (i.e., $P(S(F_B, F_I) \mid \mathrm{Hb}_1)$ and results created from several patterns of different fingers (i.e., $P(S(F_B, F_I) \mid \mathrm{Hb}_0)$. The evaluation of FMR and FNMR over *genuine* and *impostor* distributions is shown in Fig. 3.

$$\mathrm{FMR} = \int_{t}^{\infty} P(S(F_B, \ F_I)) \mid \mathrm{Hb}_0)\ ds$$

$$\mathrm{FNMR} \ = \int_{-\infty}^{t} P(S(F_B, \ F_I)) \mid \mathrm{Hb}_1)\ ds$$

The accuracy of the proposed CBioAS system can be formulated, in the *identification mode*, as follows: assume that the identification FMR and FNMR rates are represented by $\mathrm{FMR}_\mathfrak{n}$ and $\mathrm{FNMR}_\mathfrak{n}$ respectively, where $\mathfrak{n}$ refers to the *number of identities*. Therefore,

$\mathrm{FMR}_\mathfrak{n} = 1 - (1 - \mathrm{FMR})^\mathfrak{n} \cong \mathfrak{n} * \mathrm{FMR}$,

$\mathrm{FNMR}_\mathfrak{n} \cong \mathrm{FNMR}$,

If (n*FMR < 0.1) then the approximation value of (FMR_n) gives a good evaluation. The term (1-FNMR) refers to "*the hypothesis power*".

The accuracy evaluation requirements of a biometric authentication model depend mainly on the application. For instance, for the criminal identification process in some *forensic applications*, the system design focuses on the value of FNMR rather than FMR, because the investigator doesn't want to lose recognizing a criminal's identity even at the uncertainty of manually checking of many incorrect matches generated by the biometric system. In contrast to *highly secure applications*, the focus is on FMR as the most important factor, because the main objective of these applications is to deter the impostors. In the other applications such as *civilian applications*, the focus is on both FMR and FNMR values, because the performance requirements of the applications lie between them. Fig. 4 represents the ROC histogram of FMR against FNMR for different types of biometric applications.

6.5 Experimental Results and Evaluation

The researcher evaluated the effectiveness of the proposed system in terms of accuracy, sensitivity, and specificity using the following mathematical formulas:

$$Bio_{accu} = (NT_p + NT_n)/(NT_p + NT_n + NF_p + NF_n) \times 100\%$$

$$Bio_{sens} = (NT_p)/(NT_p + NF_n) \times 100\%$$

$$Bio_{spec} = (NT_n)/(NT_n + NF_p) \times 100\%$$

where NT_p is the number of *true* cases, set as biometric unauthorized packets in the experiment; NT_n is the number of *true* cases, set as normal packets; NF_p is the number of *false* cases, set as unauthorized packets; and NF_n is the number of *false* cases, set as normal packets. The researcher used the cloud-based *career guidance system* proposed in [26] as a case study with different data sizes to produce efficient experimental results of the proposed model. The cloud-based *career guidance system* uses a fingerprint recognition tool for capturing the input biometric data of the user. The system improves the quality of the captured image through three function calls: color_conversion(); resizing(); and normalization(). Once the captured image of the user is pre-processed, the feature extraction subsystem is called to produce the detailed information of the image, and as a result, the user sample is saved in the database. Once the user tries to use the system again, the function matching(); is called to compare between the user input features and the stored templates, and according to the degree of similarity, the system can take the authentication decision for the user login. The researcher used 15 random data sizes of IP packets and thresholds (K); where $K \leq NT_p$. The proposed system is implemented using various inputs such as NT_p, NT_n, NF_p, NF_n, the source IP, and the destination IP.

Tab. 1 illustrates the results of using the proposed biometric authentication model for improving users' authentication of cloud computing systems with a performance average of 93.94%, an accuracy average of 96.15% (and Std. Dev. of 0,692), as shown in Fig. 5, a sensitivity average of 87.69% (and Std. Dev. of 2,759) as shown in Fig. 6, and a specificity average of 97.99% (and Std. Dev. of 0.261) as shown in Fig. 7. As a result, the proposed model can be implemented in large-scale cloud-based systems such as a health cloud system, and smaller cloud systems like private cloud systems for small and medium-sized organizations.

Comparing the proposed model with the previous studies presented in [6–16,27] we concluded a promising result, and in our future work, we have the motivation to use a *deep learning* methodology to improve the performance and to add more features to the proposed system.

Table 1: Performance evaluation results

The impact of the cloud-based biometric authentication system								
N	K	NT_p	NT_n	NF_p	NF_n	Accuracy	Sensitivity	Specificity
1000	100	230	770	40	20	94.34%	92.00%	97.47%
2000	140	300	1700	65	40	95.01%	88.24%	97.70%
3000	180	500	2500	72	45	96.25%	91.74%	98.23%
4000	220	610	3390	82	65	96.46%	90.37%	98.12%
5000	260	730	4270	98	80	96.56%	90.12%	98.16%
6000	300	760	5240	102	93	96.85%	89.10%	98.26%
7000	340	810	6190	130	105	96.75%	88.52%	98.33%
8000	380	880	7120	127	115	97.06%	88.44%	98.41%
9000	440	930	8070	200	185	95.90%	83.41%	97.76%
10000	480	990	9010	220	205	95.92%	82.85%	97.78%
11000	520	1250	9750	235	215	96.07%	85.32%	97.84%
12000	560	1430	10750	250	225	96.25%	86.40%	97.95%
13000	600	1560	11440	265	245	96.23%	86.43%	97.90%
14000	640	1630	12370	280	255	96.32%	86.47%	97.98%
15000	680	1720	13280	310	280	96.22%	86.00%	97.94%
Performance average						**96.15%**	**87.69%**	**97.99%**

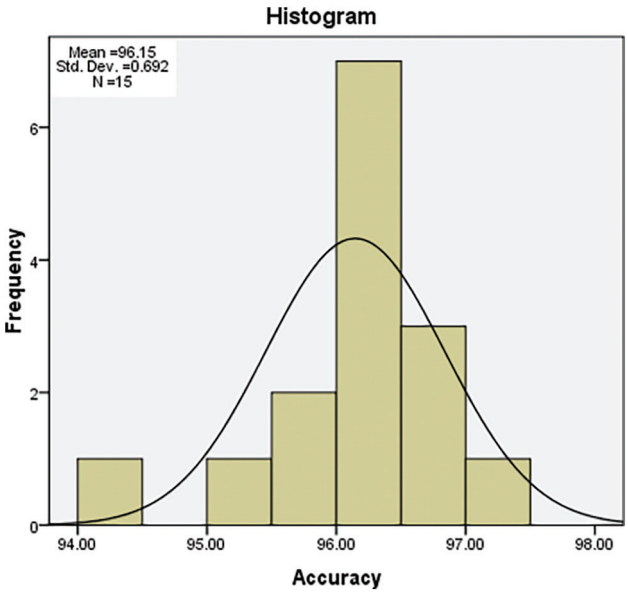

Figure 5: The performance measure of system accuracy

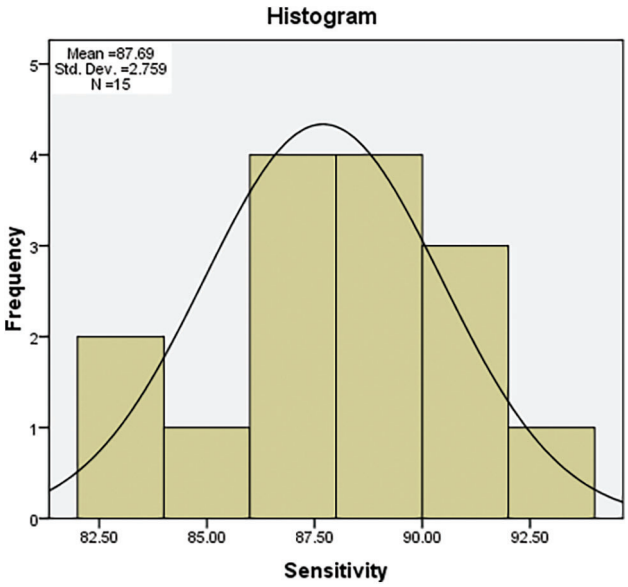

Figure 6: The performance measure of system sensitivity

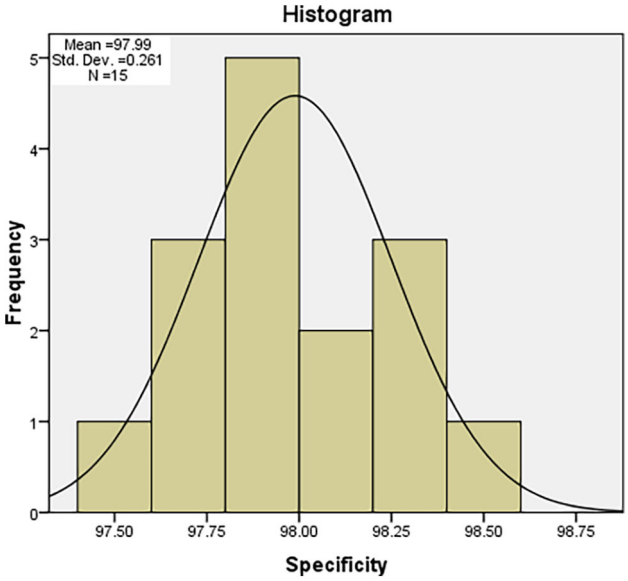

Figure 7: The performance measure of system specificity

7 Conclusion

This paper presents a cloud-based biometric authentication model to improve the authentication process for cloud computing systems. The proposed system is considered as a cloud SaaS architecture, where the biometric samples of the users are stored in cloud database servers and the authentication process is implemented without loss of any client information. In this study, the *enrolment, verification,* and *identification* processes of the proposed system were defined mathematically in terms of an input feature vector, claimed identity, and the value of similarity function between feature vectors in a predefined time. The study presented the performance evaluation of the proposed system, in different ways such as *false*

accept rate, *false reject rate*, and *equal error rate*. On other hand, the performance evaluation of the proposed system has been presented in terms of *accuracy*, *sensitivity*, and *specificity*. The study implemented the proposed system using a novel "Bio_Authen_as_a_Service" algorithm. The proposed system performs the biometric authentication process securely and preserves the privacy of user information in the cloud computing environment. The experimental result was highly promising for securing cloud services using the proposed model. The experiments showed encouraging results with a performance average of 93.94%, an accuracy average of 96.15%, a sensitivity average of 87.69%, and a specificity average of 97.99%.

Acknowledgement: The author extends his appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through General Research Project under grant number (GRP-35–40/2019).

Funding Statement: The authors received funding for this study from King Khalid University, Grant Number (GRP-35–40/2019).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Milad and S. Najafzadeh, "Authentication techniques in cloud computing: A review," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 1, pp. 95–99, 2017.

[2] C. Kalyani, "Various biometric authentication techniques: A review," *Journal of Biometrics & Biostatisticm*, vol. 8, no. 5, pp. 1–5, 2017.

[3] H. El-Sofany, "A new cybersecurity approach for protecting cloud services against DDoS attacks," *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 2, pp. 205–215, 2020.

[4] S. Sunil, C. Prashanth and B. Kori, "Comprehensive study of biometric authentication systems, challenges and future trends," *Int. J. Advanced Networking and Applications*, vol. 10, no. 4, pp. 3958–3968, 2019.

[5] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2018.

[6] K. Martin, D. Narain, J. Winston, J. Yaspy, E. Jeba *et al.,* "Authentication of biometric system using fingerprint recognition with Euclidean distance and neural network classifier," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 4, pp. 2278–3075, 2019.

[7] O. Jesus, T. Karina and S. Gabriel, "Face recognition system for smartphone based on LBP," in *Proc. of IEEE Int. Workshop on Biometrics and Forensics*, pp. 1–6, 2017.

[8] L. Asadullah, R. Waheed and A. Zulfiqar, "Biometric authentication technique using smartphone sensor," in *Proc. of the 13th Int. Bhurban Conf. on Applied Sciences and Technology (IBCAST)*, Islamabad, Pakistan, pp. 381–384, 2016.

[9] J. Annies and M. Jalaja, "Design and implementation of an IoT based secure biometric authentication system," in *Proc. of the IEEE Int. Conf. on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, Kollam, India, pp. 1–13, 2017.

[10] A. Mohamed, M. Leandros and D. Abdelouahid, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Journal of Security, and Communication Networks*, vol. 2019, pp. 1–20, 2019.

[11] C. Shekhar and S. Sasikanth "A secure and efficient biometric authentication as a service for cloud computing," in *Proc. of the 6th IBM Collaborative Academia Research Exchange Conf. (I-CARE)*, Bangalore India, pp. 1–4, 2014.

[12] C. L. Stergiou, K. E. Psannis and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Elsevier, Sustainable Computing, Informatics and Systems*, vol. 19, pp. 174–184, 2018.

[13] C. L. Stergiou, A. P. Plageras, K. E. Psannis and B. B. Gupta, "Secure machine learning scenario from big data in cloud computing via internet of things network," in *Springer Handbook of Computer Networks and Cyber Security, Principles and Paradigms, Multimedia Systems and Applications*, Springer, Cham, Springer Nature Switzerland, 1st ed., vol. 1, pp. 525–554, 2020.

[14] C. Stergiou, K. E. Psannis and B. B. Gupta, "Infemo: Flexible big data management through a federated cloud system," *ACM Transactions on Internet Technology*, vol. 19, pp. 174–184, 2020.

[15] C. L. Stergiou, K. E. Psannis and Y. Ishibashi, "Green cloud communication system for big data management," in *Proc. of the 3rd World Symp. on Communication Engineering (WSCE)*, Thessaloniki, Greece, 2020.

[16] C. L. Stergiou, K. E. Psannis and B. B. Gupta, "Iot-based big data secure management in the fog over a 6G wireless network," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5164–5171, 2021.

[17] V. Narayan, B. Kiran, R. Raghavendra, R. Gad and B. Christoph, "Band level fusion using quaternion representation for extended multi-spectral face recognition," in *Proc. of the IEEE Int. Conf. on Information Fusion*, pp. 1–16, 2017.

[18] D. Sarat, "Assessing fingerprint individuality in presence of noisy minutiae," in *Proc. of the IEEE Transactions on Information Forensics and Security*, Roma, Italy, vol. 5, no. 1, pp. 62–70, 2010.

[19] J. Kavitha and R. Joseph, "Geometric finger nail matching using fuzzy measures," *International Journal of Innovative Technology and Exploring Engineering*, vol. 4, no. 4, pp. 1–8, 2014.

[20] S. Charan, "Iris recognition using feature optimization," in *Proc. of the IEEE Int. Conf. on Applied and Theoretical Computing and Communication Technology*, Bangalore, India, pp. 726–731, 2016.

[21] P. Yan and K. Bowyer, "Biometric recognition using 3D ear shape," in *Proc. of the IEEE Transactions on Pattern Analysis and Machine Intelligence*, Toronto, Canada, vol. 29, no. 8, pp. 1297–1308, 2017.

[22] S. Mohammed, A. Syed, F. Zeeshan and A. Israr, "Advancement in DNA as source of biometric authentication," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 3, pp. 1–5, 2013.

[23] P. Baynath, K. Soyjaudah and M. Khan, "Implementation of a secure keystroke dynamics using ant colony optimization," in *Proc. of the Int. Conf. on Communications Computer Science and Information Technology*, Beijing, China, pp. 1–7, 2016.

[24] R. Manuel, F. Julian and O. Javier, "Dynamic signature verification with template protection using helper data," in *Proc. of the IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Las Vegas, NV, USA, pp. 1713–1716, 2008.

[25] S. Nilu, "A study on speech and speaker recognition technology and its challenges," in *Proc. of the National Conf. on Information Security Challenges*, Lucknow: DIT, BBAU, pp. 34–37, 2014.

[26] H. El-Sofany, "Assessment of implementing cloud-based career and educational guidance system using fuzzy logic modeling," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 3, pp. 77–84, 2020.

[27] M. Amine, E. Maglaras and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Security and Communication Networks*, vol. 2019, pp. 1–20, 2019.