CENTRAL INTELLIGENT BIOMETRIC AUTHENTICATION BASED ON VOICE RECOGNITION AND FUZZY LOGIC

DR. ALIA KARIM ABDUL-HASSAN[1] AND IMAN HASSOON HADI[2]
[1] Asst. Prof. in The University Of Technology, Computer Sciences Dept.-Iraq
[2] PHD Student in The University Of Technology, Computer Sciences Dept.-Iraq
E-Mail: [1]110018@Uotechnology.edu.iq, [2]iman.h.1439@gmail.com

ABSTRACT

Reliable identity management must be built with an accurate user identity recognition method. This recognition usually is the core of the authentication method which is the essential part of any identity management system. The authentication must carefully be designed, especially when it is used among different service providers. The authentication is a user identity verifying and protecting mechanism. It consists of three main components, user identity attributes, the verification method, and the log-in mechanism. The log-in component has great impact on authentication, when the user needs to be authenticated to be given access to several service providers. In addition, the verification of the claimed user attributes, involve the decisive role in the authentication because it will produce the final decision of the identity proving process, so it is important to be accurate and intelligent as much as possible. In this paper, a central intelligent biometric authentication approach is proposed; this authentication is based on the Mel-frequency Cepstral coefficients (MFCC) voice attributes, fuzzy classifier, and client-server model as log-in mechanism. The proposed fuzzy classifier depends on the fuzzy set inner product and a predefined threshold. This classifier is designed as an intelligent identity verification method. The experiments show 95.45% accuracy in offline user authentication using ELSDSR dataset.

Keywords*: Central Authentication, Voice, Fuzzy Logic, MFCC*

1. INTRODUCTION

Authentication is an essential process in any information security system. Traditionally, authentication methods are classified according to the following five concepts:
1. Something the user knows: a password, a passphrase, a PIN code, 2. Something the user owns: a USB token, a phone, a smartcard, 3. Something that qualifies the user: a fingerprint, DNA fragment, voice pattern, hand geometry, 4. Something the user can do: a signature, a gesture, 5. "Somewhere the user is: a current location/position, a current time information.."[1].

These concepts show that the authentication utilizes critical information and attributes that belong to the user, so the protection of this information is one of the most important issues related to the design and implementation of authentication architecture. In addition, this issue becomes larger when a user wants to login more than one service provider server, because he has to go through the process of authentication repeatedly. This becomes impractical when the number of service providers increases, especially if the user has to remember separate usernames and passwords for each service provider. To overcome this problem, centralized authentication architecture could be used. In this architecture every time a user needs to be authenticated, he does it against a central server. This also means that all the accounts are stored in the same place, so there is no redundancy [2].

One common model that uses central authentication is where the service provider (SP) server runs on non-trustworthy machines outside the control of the client. In this case, the SP servers must be considered untrusted and the clients and authentication servers should protect themselves and restrict the access given to clients. Under these environments, the client-server model has a natural advantage because only the central authentication servers need to be trusted [3].

In addition, the identity recognition is the core of any authentication architecture, so it must be accurate enough to discriminate between users. The intelligent recognition is the promised method to enhance the biometric authentication decision. This is achieved by using a proposed fuzzy classifier as an intelligent method to recognize the similarity between training and testing utterances to assign the required threshold. Added to that, the fuzzy classifier discriminates between the claimed user voice utterance and the authenticated user utterance even if two utterances were too close in some features.

In this paper, the Central Biometric Authentication (CBA) mechanism is proposed as a broker between clients and service provider servers using a proposed fuzzy classifier. The central biometric authentication could protect the user identity attributes and facilitate the interaction between him and service providers.

2. RELATED WORK

Many types of central authentication architecture were proposed during the last decade. Each of these researches has advantages and disadvantages. It could not be possible to find a research that used the combined voice attributes with an intelligent fuzzy recognition method.

[Chun-Ta Li et al., 2010] proposed a biometric-based remote user authentication scheme, using one-way hash function, biometrics verification and smart card. They implement three phases: registration phase, login phase and authentication phase. Even the proposed authentication system was secured by hashing technique, but it needs high computation time because it is designed for various authentication-crypto systems [4].

[S. Christianet et al., 2011] specify a list of evaluation criteria for biometric Authentication-as-a-Service (BioAaaS) systems from a data protection perspective, including elements specific to both biometrics and SaaS. They apply these criteria on a prototypical implementation of a software-as-a-service (SaaS)-compliant biometric authentication service based on keystroke dynamics for enterprise deployment. They used an implementation of a fixed text method during identity verification mode. They propose an Identity provider (IdP) to be responsible with alternative authentication controls like voice authentication. Although, this implementation takes into consideration data protection aspects, but it was limited to the public cloud platform, so it may lead to risks exhibition due to open accessibility [5].

[Z. Liang et al., 2012] established a unified identity authentication system and a unified rights management system by the adoption of the agent and broker model as the basis for single sign-on model for cross-domain web application. They proposed the reverse proxy to enhance the response time twice as fast as the one out of use proxy. But this enhancement could not be obtained with a small number of concurrent users [6].

[S. Kaman et al. ,2013] proposed an authentication system using voice recognition to authenticate remote-users based on the combination of two of the following authentication factors: something the user knows (e.g., password) and something the user is (user voice). The proposed system presented a predefined sequence of steps the user should follow to register and verify his identity, with the message digest of fixed size called the voice code (VC). They used a simple comparison method to recognize the authenticated user [7] .

All of the above related work proposed a central authentication approach to protect

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

user credentials and enhance response time using various techniques like (a secret pass code, reverse proxy, hashing function, etc.). But none of them uses an intelligent method to recognize the authentication method. So this paper proposes the central intelligent authentication method based on MFCC voice attributes and fuzzy classifier.

3. METHODOLOGY

This section presents the essential characteristics of methods and techniques that are basic in this paper for voice recognition, MFCC features extraction, voice features matching using inner product of fuzzy vectors, and central authentication architecture.

3.1 Voice Biometric Recognition

Voice biometric recognition system has a main task to recognize a person from a spoken phrase, usually called Automatic speaker recognition. Speaker recognition (SR) contains two methodologies; first Speaker identification (SI) and second speaker verification (SV). SI determines the identity of the unknown speaker depending on his/her utterance properties [8]. The general structure of speaker recognition is shown in figure 1, the first phase is speaker identification and the second phase is the verification using a classifier to verify the identity of speaker based on his voice attributes. Regardless of the type of voice attributes, the main phases of voice authentication methods are: (a) *The registration phase:* where the user's feature vectors are extracted and registered as a digital feature vector and stored in a database. In addition, an acceptance threshold is computed. The recognition process depends on this threshold, being above or equal, for which the utterance is accepted as the target speaker. *(b) The log in phase*: the user inputs his credentials and his voice signal using a specific input device (microphone to capture his voice signal. (c) *The verification phase*: in this phase , the user voice is extracted from the input signal and matched with stored feature vectors of the authenticated users data base. Based on a predefined threshold, the system decides whether that user is authenticated or not [5].

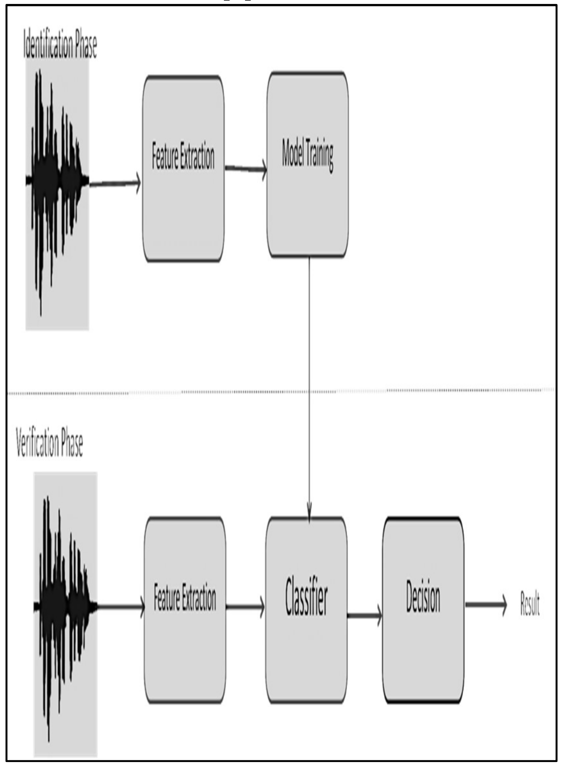

Figure 1. Voice Recognition System Diagram

An individual's voice is difficult to forge because the vibration of an individual's vocal chords and the physical components that produce the human voice are as unique as fingerprints. Biometric authentication captures the unique voice features during the registration phase, associated with an individual's voice to create his voiceprint which is called speaker model. The voiceprint is a secure attribute for authenticating an individual's identity, which is better than the other type of authentication like (PIN, smart card, etc.) that could be stolen or forged [9].

The voice recognition is a method can be used for proving the identity of the claimed user during the authentication. Voice recognition has two approaches: text-dependent or text-independent. Text dependent recognition compels users to speak specific phrase, such as a password or personal identification number, to be recognized from other speakers. While in text independent approach, the user could use any phrase to be recognized by the system.

3.2 VOICE FEATURE EXTRACTION

The most popular short-term acoustic features are the Mel-frequency Cepstral coefficients (MFCCs); these features are better from prosodic. The latter features suffer from many disadvantages, such as the difficulty of identifying the part of the signal that contains important information and determining an appropriate model of calculation as well as what is the amount of robust and efficiency when combined with the other characteristics [10]. These features are extracted from short voice frames of duration within 20–25 milliseconds [11]. This extraction process mimics the human hearing system. The following steps are used to compute MFCCs coefficients [12] :

1. Segment the signal into small frames.

2. For each frame, compute the periodogram estimate of the power spectrum. This is done by taking the Discrete Fourier transform using the equation (1) :

$$S_i(k) = \sum_{n=1}^{N} \left(s_{i(n)} L(n) e^{-j2\pi kn/N} \right) 1 \le k \le K \ldots\ldots \ (1)$$

Where *L(n)* refers to the *N* sample long analysis hamming window, and *K* represents the length of the DFT. The periodogram-based power spectral is obtained by using equation (2):

$$P_i(k) = \frac{1}{N} |S_i(k)|^2 \ldots\ldots(2)$$

3. Apply the Mel filterbank to the power spectra ,then the sum of the energy in each filter. The Mel scale approach distinguishes frequency of a tone to its actual measured frequency. Using this scale makes MFCC features much more mostly to what humans hear.

The equation for obtaining Mel scale from frequency is:

$$M(f) = 1125 \ln\left(1 + \frac{f}{700}\right) \ldots\ldots\ldots..(3)$$

To go back to frequency, the following equation is used:

$$M^{-1}(m) = 700\left(\exp\left(\frac{m}{1125}\right) - 1\right) \ldots\ldots\ldots (4)$$

4. Compute the Mel-spaced filterbank. This is (20-40) usually 26 is used as standard triangular filters that will be implemented to the periodogram power spectral estimate obtained from step 2. Each vector is close to zeros, but is non-zero for a specific section of the spectrum. To calculate filterbank energies, multiply filterbank with the power spectrum, and then sum up the coefficients. When this is implemented, then 26 numbers are obtained that give an indication of how much energy is in each filterbank.

5. Compute the logarithm of all filterbank energies. This leaves us with 26 log filterbank energies.

6. Compute the DCT of log filterbank energies to give 26 cepstral coefficients.

7. Keep DCT coefficients 1-13, and discard the rest.

3.3 Voice Feature Matching Using Fuzzy Vectors:

Fuzzy set theory is based on the approximate rather than crisp logic. The fuzzy truth represents the degree of approximation in sets, which is different from the likelihood of a condition, since these sets are based on vague definition, not randomness [13]. The two samples of the speaker's voice (training sample and test sample), sometimes have very close values, so fuzzification of these feature vectors can enhance the recognition performance.

The goal of the recognition process is to find which element in feature vector A and feature vector B matches most. To solve this problem, the inner product of fuzzy vectors is used. The inner product is the most important operation on fuzzy vectors, which is used in pattern recognition.

There are certain features and operations implemented using fuzzy sets which could be used as fuzzy pattern recognition methods. To explain these methods, let *a* be a fuzzy vector, a=(a1,a2,…,a3) , and $0 \le a_i \le 1$ for $i = 1,2,\ldots,n$.

In the traditional pattern recognition method, it is interesting in comparing a data sample to a set of pre-defined

Journal of Theoretical and Applied Information Technology
31st August 2019. Vol.97. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

patterns. As an example, if there is a collection of *m* patterns, each is represented by a fuzzy set, *Ai*, where *i =1, 2, …, m*, and a sample pattern *B*, all defined on most close domain. A traditional metric that has appeared in the literature is to compare the universe X. The question is as follows: "Which known pattern *Ai*, does data sample *Bi* data sample approach to each of the known patterns in a pairwise fashion", determine "the approaching degree value" for each of these pairs comparisons, and then choose the pair with the largest approaching degree value as the one deciding the pattern recognition process. The known pattern that is involved in the maximum approaching degree value is then the pattern of the data sample most closely look alike in a maximal sense. This concept has been defined as the *maximum approaching degree* [14].

To clarify this concept, let us define *a* and *b,* as fuzzy vectors of length *n*, then the fuzzy inner product is as in equation (1):

$$\wedge_{i=1}^{n}(ai \wedge bi)\ldots\ldots \quad (5)$$

Depending on maximum approaching degree concept, mentioned above, if two fuzzy vectors are similar, a=b, the inner product reaches a maximum value compared with other samples. This norm, the inner product, can be used simultaneously in any pattern recognition studies (like voice recognition) because they measure closeness or similarity.

Let X= [-∞,∞], a one-dimensional universe on the real line, A and B are two fuzzy sets having normal Gaussian membership, which are defined mathematically by the equations:

$$\mu A(x) = \exp[-(x-a)^{\wedge}2/\sigma_a^2] \ldots\ldots (6)$$

$$\mu B(x) = \exp[-(x-b)^{\wedge}2/\sigma_b^2] \ldots\ldots (7)$$

Where σ is the standard deviation, and *a*, *b* arethe mean of A and B.

These operations are very useful when used in a metric of similarity between two vectors. The inner product of two fuzzy vectors shown in figure 2 [14], are computed using Gaussian membership function as in the following equations (9) :

$$= \exp[-(a-b)^{\wedge}2/(\sigma a+\sigma b)^{\wedge}2\,]$$

$$= \mu A(x0) = \mu B(x0) \qquad \ldots\ldots\ldots(8)$$

$$\textit{inner product}\ (A,B) = \frac{1}{2}\left\{\exp\left[\frac{-(a-b)^2}{(\sigma_a+\sigma_b)^2}\right]+1\right\}\ldots\ldots(9)$$

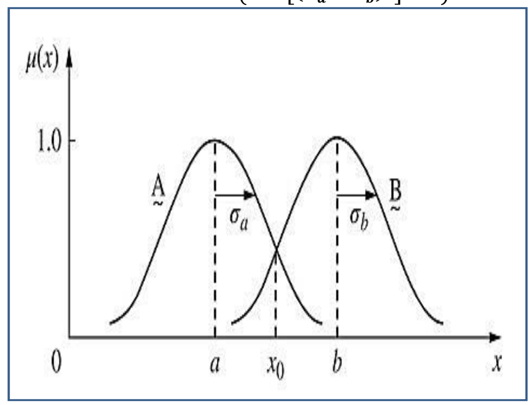

Figure 2. The fuzzy inner product of A, and B

To explain these concepts, the following example shows patterns which can all be represented by Gaussian membership functions, *Ai*, where *i* =1,2,…,6 where parameters a_i and σ_{ai} define the shape of each membership function. Table 1 provides information for the six regions. The unknown pattern, represented by a fuzzy set *B*, with the following characteristics [11]: *b=41,* $\sigma_b = 10$ is *to determine the maximum approaching degree from the calculation results using the equation (9) which represents the inner product between B and Ai,*

Table 1. Parameters for Gaussian membership function for patterns (A1 to A6)

	A1	***A2***	***A3***	***A4***	***A5***	***A6***
a_i	5	20	35	49	71	92
σ_{ai}	3	10	13	26	18	4

Where i=1,..., 6,

(B,A1)=0.5 , (B,A2)=0.67 , (B,A3) =0.97 , (B,A4)= 0.98 , (B,A5)=0.65 , (B,A6)=0.5

As a result, B is similar to A4, because the inner product value between B and A4 has the maximum value 0.98.

The utilization of such approach in voice-based authentication could be done by comparing each test voice sample with each of the voice samples in train data in pairwise order, to find the approaching degree value for each pair, and then select the pair with the maximum approaching value as the threshold.

3.4 Central Authentication Model:

The central authentication model consists of a central authentication server (CAS), which is an identity provider, used to authenticate the users. Service provider offers many resources for users, such as Web servers, media servers, databases, etc. Service providers usually have their local user authentication databases with the local accounts that have meaning for the specific service provider, and not dedicated accounts for each Web user. The service provider organization trusts the identity provider organization to authenticate users [15].

This model depends on distribution of functions between two processes: Sever and Client. A client is any process that request services from the server process, which represents the log-in process used by user. A server is the process that executes a specific task to implement service requested by the client process [16].

4. THE PROPOSED CENTRAL BIOMETRIC AUTHENTICATION:

The methodologies of the proposed system include three main components, the first is the central biometric authentication architecture. The second is the authentication protocol that is governed the authentication process by pre-defined steps. The last is the intelligent authentication algorithm (IVA) which is the core of the proposed central biometric authentication.

4.1 The proposed Central Biometric Authentication Architecture:

The proposed CBA depends on the identity-based authentication concept, and this identity is represented by the user voice. But every authentication process does not rely on the users' attributes only because the architecture of CBA system plays a major role in the performance of the authentication.

In the central biometric authentication, a claimed speaker requests permission from CAS to access list of SPs as shown in figure (3).

The main task of CAS is to verify if this identity of that user is authenticated and included in the database that stores voiceprints of the authenticated users. This is done by comparing his voice sample with a set of samples of registered authenticated users and deciding if the claimed speaker is what he claimed [11].

The proposed CBA architecture consists of the following main components:

1- The Central Authentication server: this server is an Identity provider which is a system that creates, maintains, and manages biometric identity information for users and provides authentication information to predefined service providers (applications). It is a trusted server that can be relied by users and SP servers when users and servers are establishing a communication that must be authenticated [17].

This server protects the voice attributes of the users and never passed this information to the service providers.

2- The client: This is reference to the machine that the users will use it to send their requests to the CAS.

3- Service providers: They are group of servers that present services to the clients, these servers have a database of user accounts and specific field related to the authentication status of each client, which is fed by CAS.

4.2 Central Authentication Protocol

The central authentication protocol is designed to govern the authentication process between the user and the other main components in the central authentication system. The authentication protocol main steps are as follows:

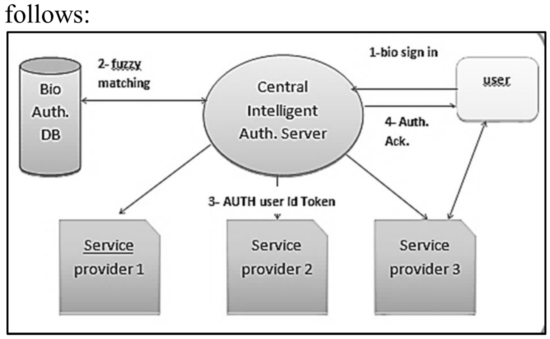

Figure 3. the Proposed CBA architecture

1- The claimed user logs in the system by sending the sample of his voice with a request to the CAS to get permission to access a specific service provider(s) .
2- The CAS receives the feature vector of the claimed user with the identifier(s) of the required service provider.
3- The CAS implement the intelligent voice recognition process by the fuzzy matching between the received features vector and the features stored in the registration database.
4- The CAS send the result of step 3 to the user, if that user is authenticated, then the acknowledgement token representing user identifier is sent to the required SP at the same time,
5- The SP receives the identifier and turns on the authentication flag to ON-status for that authenticated user.
6- The authenticated user can access the SP and he must sign out after the session ends.
7- The sign-out process consists of the following (delete the wave file of user, and turn off the authentication flag in the SP database).

4.3 The Intelligent Authentication Algorithm

The proposed algorithm *Intelligent Voice Authentication (IVA)* for the user verification includes the main steps to show how to identify the identity of the user for verification purpose, using MFCC feature vectors and matching process by the using inner product of fuzzy vectors (see equation 8) with Gaussian membership function.

The input of algorithm (IVA) is the MFCC feature vector of claimed user, which includes 13 coefficients, and the database that stores the MFCC features of authenticated users that are extracted during the registration phase as mentioned in sections 3.1 and 3.3 . Each authenticated user has 7 MFCC feature vectors as training data and each vector holds 13 coefficients. The last input is the authentication decision threshold (TH) that is obtained from training (registration) phase also.

The output of the algorithm is the intelligent authentication decision either "Rejected" or "Authenticated" with the identity of authenticated user.

Algorithm* (IVA)** ***Input *:the claimed user voice signal, the authenticated users voice signals training data set, and decision threshold (TH).* ***Output****: the authentication decision, identity*
Step1: *compute the MFCC features of the claimed user, MFCC1(T1,13)// T1 represent length of voice signal and 13 is number of MFCC coefficients* ***Step2:*** *Repeat for each user voice signal (speaker2) in data set of authenticated user* ***Step3:*** *Retrieve MFCC array for speaker2 from DATABASE, MFCC2(T2, 13).* ***Step4:*** *minimize MFCC1 and MFCC2, by computing mean value and standard deviation of MFCC coefficients to get user1_vector(13), user2_vector(13)* ***Step5:*** *compute fuzzy inner product between user1_vector and user2_vector* ***Step6:*** *append the fuzzy inner product value of corresponding speaker2 to recognition_test_list* ***step7:*** *Until the last MFCC feature Vector in DataBase.* ***step8:*** *Select the identity number (id) corresponding to the maximum value in recognition_test_list.* ***Step 9:*** *compare maximum inner product value with Threshold (TH),* *if maximum inner product => TH : auth_decision= "Authenticated"* *else: auth_decision= "Rejected"* ***Step 10****: Return auth_decision with the recognized user identity (id)*

5. EXPERIMENTAL RESULTS AND DISCUSSION

The main implementation was done using English Language Speech Database for Speaker Recognition (ELSDSR) which consists of 7 audio file samples for each speaker; the total number of speakers is 22 volunteers. The text language is English [18]. The voice samples are recorded into file type (.wav).

The ELSDSR data used in the proposed CBA system are divided into two parts: training data and test data. Train wave samples are labeled (the speaker identification to which this sample belongs). The ELSDSR training

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

voice features are stored in main table using MYSQL in central authentication server (CAS), which contains other demographic attributes (name ,gender, age). The test data are samples of voice belonging to authenticated speakers, which are labeled for testing the overall performance of the authentication process.
We chose two different recorded voice files for each speaker from this dataset for testing purpose. Then each file is loaded into an array (as plotted in figure 4) using LibRosa python library.
The wave file of the claimed user voice is loaded using python language library. Then the MFCC features are extracted using computations in section 3.2. The outputs of these computations as raw MFCC features without minimization are plotted in figure 5. where y-axis represents the value of MFCC coefficients that result from feature extraction , explained in section 5.1 and x-axis represents the sequence of 13 MFCC coefficients (from 1 to 13). Figure 5 shows that raw MFCC features are large data and the minimization is needed to enhance the execution time in the authentication system.

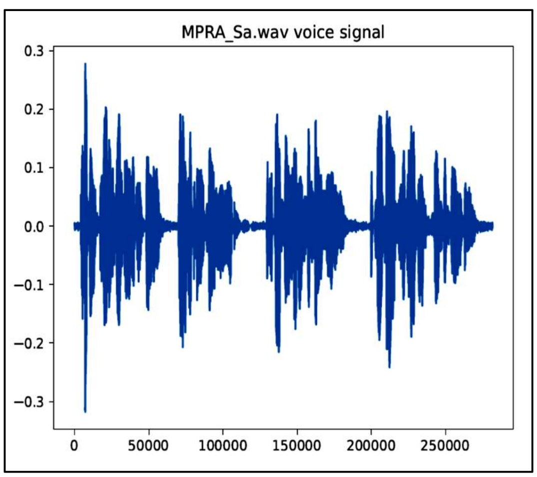

Figure 4. Voice wave signal plot

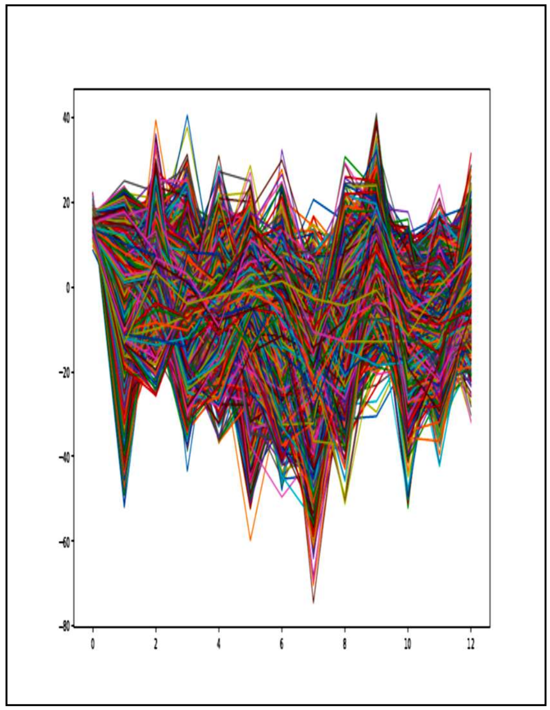
Figure 5. Raw MFCC features of one speaker

5.1 Fuzzification of Voice Features:

The MFCC features were minimized by computing the mean and standard deviation of these coefficients represented by MFCC1, MFCC2,.., MFCC13 referring to the mean of the raw MFCC features (see table 2). In addition, the standard deviation of raw MFCC features of the 22 speakers ere extracted and stored in the data base with the mean of these MFCC , see table 3 where MFCC1_s,MFCC2_s, MFCC3_s, .., MFCC13_s ,representing the standard deviation of these feature vectors. These values are used to compute the fuzzy vectors. Figures 6 and 7 shows the fuzzification of MFCC vectors where x-axis represents the sequence of MFCC coefficients and y-axis represent the fuzzy value of MFCC value result from fuzzy membership function.
These features are stored as identification features of the authenticated users. They are extracted and stored in the central data base in the central server.

Table 2. ELSDSR MEAN of MFCC Features

sp_name	MFCC1	MFCC2	MFCC3	…	MFCC11	MFCC12
FAML	16.11	-3.49	4.26	…	-9.84	-8.69
FDHH	15.13	-4.40	0.59	…	-10.91	-7.34
FEAB	15.65	-6.96	0.27	…	-4.29	-8.46
FHRO	15.60	-5.87	0.28	…	7.29	-20.57
FJAZ	16.53	-6.20	-4.50	…	-3.03	-6.79
FMEL	15.85	-4.67	-1.22	…	1.00	-16.12
FMEV	16.10	-2.69	-2.25	…	-0.13	-7.77
FSLJ	15.51	-6.36	2.62	…	-6.05	-18.94
FTEJ	15.26	-0.37	5.33	…	-1.97	-10.16
FUAN	14.94	-5.14	6.26	…	-4.97	-17.12
MASM	16.34	-1.10	-6.43	…	5.17	-0.04
MCBR	16.35	-0.46	2.32	…	-2.50	3.24
MFKC	15.75	-8.85	6.53	…	-2.20	-13.66
MKBP	16.69	-2.59	1.23	…	-1.07	-4.43
MLKH	16.48	0.40	-8.00	…	2.84	-7.39
MMLP	16.58	-0.39	-1.28	…	8.71	-2.29
MMNA	15.65	-0.89	0.79	…	4.38	-8.90
MNHP	16.04	-6.62	1.43	…	7.10	-4.40
MOEW	15.63	-6.06	2.05	…	-0.59	-0.46
MPRA	14.71	-4.61	7.05	…	-1.73	-1.09
MREM	15.81	-4.92	-3.88	…	2.95	-6.84
MTLS	15.20	-2.86	0.43	…	4.77	0.84

Table 3. ELSDSR SD of MFCC Features

sp_name	MFCC1_s	MFCC2_s	MFCC3_s	…	MFCC11_s	MFCC12_s
FAML	2.22	15.98	11.18	…	11.01	11.81
FDHH	3.91	15.75	12.75	…	11.72	10.68
FEAB	2.97	14.60	10.69	…	11.21	11.08
FHRO	3.39	16.16	13.31	…	11.60	13.60
FJAZ	2.24	15.63	13.55	…	12.29	10.81
FMEL	2.57	13.89	12.25	…	12.23	13.00
FMEV	2.49	14.49	13.67	…	11.26	11.92
FSLJ	2.27	15.20	11.23	…	10.94	13.03
FTEJ	3.40	15.79	11.21	…	10.06	11.59
FUAN	3.58	16.05	11.08	…	11.74	11.57
MASM	2.64	14.48	11.82	…	10.17	12.60
MCBR	2.00	15.29	8.95	…	12.00	11.33
MFKC	2.70	15.08	11.08	…	10.14	10.32
MKBP	2.52	13.31	11.65	…	11.81	12.76
MLKH	2.65	15.47	12.63	…	11.13	12.67
MMLP	2.54	16.35	11.48	…	13.38	11.22
MMNA	2.49	16.54	10.10	…	9.69	11.94
MNHP	3.40	15.05	10.72	…	11.72	10.75
MOEW	3.03	14.90	9.81	…	10.13	14.37
MPRA	3.83	16.19	9.12	…	10.71	13.12
MREM	3.41	14.31	12.34	…	10.35	12.30
MTLS	2.20	13.95	11.34	…	9.81	10.12

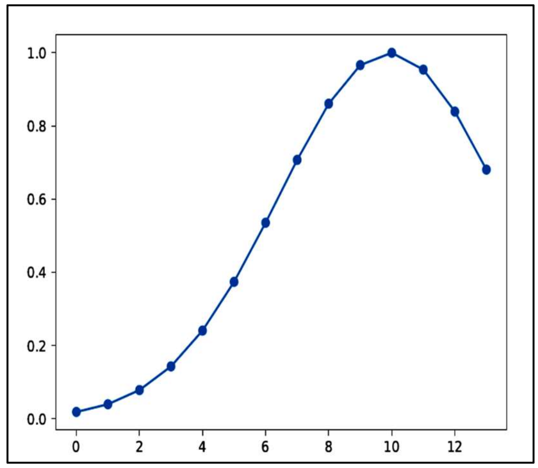

Figure 6. Fuzzification of one speaker minimized MFCC feature vector

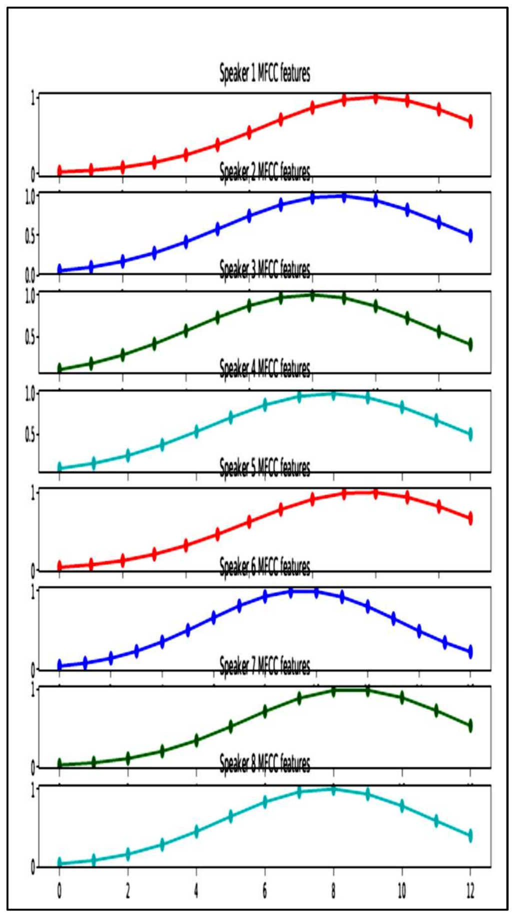

Figure 7. Fuzzy membership functions of MFCC features of 8 speakers

While the service provider sever did not store any attributes related to the user identity, instead it contains an authentication flag referring to the authenticated status that is changed when

CAS send the session token of the authenticated user.

5.2 INTELLIGENT AUTHENTICATION DECISION:

To test the proposed CBA architecture, every test wave file of all users in data set is used in log-in phase as the claimed user voice signal and the extracted feature vector is sent to CAS. Table 4 shows an example of inner product of two MFCC features vectors. Then the fuzzy matching phase (verification) is implemented for all voice files in the data set , through CAS architecture mentioned in section 4 and the result is shown in table 5. The first column represents the actual identity of the user. The second column shows the length of the voice signal used as test sample, while, the third column presents the result of recognized identity resulting from the application of IVA algorithm using equation (8), and the fourth column contains the time required to complete the authentication process for that voice file. These values are compared with the threshold (12.7) that was obtained from registration phase. The time consumed to verify each individual was on average 3.6 sec using PC with the following specifications of processor, intel® Core™ i5-3210M and 4 G RAM, using three sessions for the CAS server, the SP server , and the client.

As a result the proposed intelligent authentication method recognized the true identity of all the speakers in the data set except one speaker whose identity is (MMLP) who is recognized as (MCBR).
\

Table 4. Fuzzy Inner Product Of Two MFCC Feature Vectors

Fuzzy Inner product	***MFCC coefficients index***
0.947376966	1
0.999276404	2
0.999061719	3
0.999088437	4
0.994970621	5
0.833692251	6
0.973413075	7
0.993400486	8
0.999904435	9
0.994471516	10
0.853504696	11
0.963745783	12
0.880550211	13
12.4324566	**sum**

Table 5. the voice recognition result in CBA

ELSDSR speaker identity	Wav. File length	recognized identity	Sum of Fuzzy inner product	CBA time (sec)
FAML	938	FAML	**12.7**	**3.89**
FDHH	799	FDHH	**12.91**	**3.50**
FEAB	849	FEAB	**12.86**	**3.85**
FHRO	779	FHRO	**12.78**	**3.54**
FJAZ	819	FJAZ	**12.75**	**3.84**
FMEL	649	FMEL	**12.79**	**3.66**
FMEV	899	FMEV	**12.82**	**3.56**
FSLJ	729	FSLJ	**12.88**	**3.58**
FTEJ	869	FTEJ	**12.95**	**3.61**
FUAN	772	FUAN	**12.83**	**3.70**
MASM	749	MASM	**12.76**	**3.64**
MCBR	669	MCBR	**12.83**	**3.88**
MFKC	839	MFKC	**12.81**	**3.65**
MKBP	608	MKBP	**12.7**	**3.66**
MLKH	699	MLKH	**12.83**	**3.66**
MMLP	771	MCBR	**12.71**	**3.47**
MMNA	654	MMNA	**12.71**	**4.14**
MNHP	709	MNHP	**12.37**	**3.88**
MOEW	839	MOEW	**12.75**	**3.43**
MPRA	739	MPRA	**12.85**	**2.64**
MREM	779	MREM	**12.79**	**3.32**
MTLS	609	MTLS	**12.72**	**3.29**

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

These experiments show high accuracy in the recognition of individual identity voice signals. Central biometric authentication performance metric derived from table 5 , is as follows :

True Identity rate = $21/22 * 100$ =95.45%

False Identity rate = $1/22 * 100$ =4.54%

6. CONCLUSION

Authentication methods have been developed according to the architecture of the information system and the type of attributes related to the users, who need to be authenticated. Although these methods depend mainly on the user attributes but the authentication architecture has an impact on the protection of user attributes especially when this authentication process implemented among untrusted service providers. So the proposed central biometric authentication architecture based on voice recognition and fuzzy matching methods present an architecture and specific speaker classifier, which are implemented under client-server model. Central authentication server is designed as the broker between the user (client) and service provider servers.

The experimental results show high accuracy in user identity recognition using intelligent authentication algorithm based on fuzzy vector inner product method. Also, the execution time of the central authentication was minimized in contrast to the standalone authentication.

8. FUTURE WORK

Voice biometrics authentication is used in a number of applications and in different architectures. In future we intend to add a second factor in addition to the voice attributes. Using this two-factor authentication, we can easily identify a user in a close-set of users and by so we can verify his identity. Added to that, this work implemented as offline authentication in order to test the proposed authenticated method, we intend to implement central biometric authentication in real-time manner.

REFERENCES

[1] S. Zulkarnain ,S. Idrus, E. Cherrier, C. Rosenberger, J. Schwartzmann. "A Review on Authentication Methods", Australian Journal of Basic and Applied Sciences, vol. 7, no. 5, pp. 95–107, 2013.

[2] F. Alenius and G. Joao and U. Bauknecht, “Centralised Authentication”, Uppsala University,department of information technology, 2009.

[3] Amir, Yair, Cristina Nita-Rotaru, and Jonathan R. Stanton. "Framework for authentication and access control of client-server group communication systems", International Workshop on Networked Group Communication. Lecture Notes in Computer Science, vol 2233. SpringerSpringer, 2001.

[4] Chun-Ta Li and Min-Shiang Hwang , "An efficient biometrics-based remote user authentication scheme using smart cards", Journal of Network and computer applications ,Vol. 33, Issue 1,p. 1-5, 2010

[5] Senk Christian, and Florian Dotzler, "Biometric authentication as a service for enterprise identity management deployment: a data protection perspective." , Sixth International Conference on Availability, Reliability and Security, pp. 43-50, IEEE, 2011.

[6] Z. Liang, Y. Chen, “The Design and Implementation of Single Sign-on Based on Hybrid Architecture.”,Journal Of Networks, Vol. 7, No. 1 ,2012.

[7] S. Kaman, K. Swetha, S. Akram, and G. Varaprasad, “Remote User Authentication Using a Voice Authentication System,” Information Security Journal: A Global Perspectiv, vol. 22, no. 3, pp. 117–125, 2013.

[8] Rasha H. Ali, Mohammed Najm Abdullah And Buthainah F. Abed, “Speaker Identification And

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Localization Using Fusion Of Features And Score Level Fusion", Journal Of Theoretical And Applied Information Technology ,Vol.96. No 21, 2019.

[9] Z. Saquib, N. Salam, R. Nair, and N. Pandey, "Voiceprint Recognition Systems for Remote Authentication-A Survey," International Journal of Hybrid Information Technology , Vol. 4, No. 2, 2011.

[10] E. S. Al-Shamery And W. M. Al-Hameed, "Two Scopes Of Acoustic Signal And Fuzzy-Relief Algorithm For Improving Automatic Speake Recognition", Journal Of Theoretical And Applied Information Technology, Vol.97. No 2 ,2019.

[11] J. H.L. Hansen , T. Hasan , Speaker Recognition by Machines and Humans, IEEE Signal Processing Magazine, 2015.

[12] http://practicalcryptography.com/miscellaneous/machine-learning/guide-mel-frequency-cepstral-coefficients-mfccs/ accessed on 11:40 PM on 04/05/2019.

[13] K. R. Venugopal, K.G. Srinivasa and L.M. Patnaik, Soft Computing for Data Mining Applications, Springer, 2009.

[14] T. J. Ross, Fuzzy Logic With Engineering Applications, Fourth Edition, 2017.

[15] D. Todorov, "Mechanics of User Identification and Authentication", Auerbach Publications, 2007.

[16] C. Y. Subhash, "Introduction To Client Server Computing", New Age International, 2009.

[17] http://kb.mit.edu/confluence/display/glossary/IdP+(Identity+Provider) (accessed on 12:00 PM on 18/01/2019)

[18] L. Feng, L. K. Hansen, "A New Database For Speaker Recognition", department of Informatics and mathematical modelling, Technical University of Denmark (DTU),2005.