International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SKRGC Since 2012

http://www.ijcsjournal.com Volume 10, Issue 2, No 2, 2022. ISSN: 2348-6600
Reference ID: IJCS-429 PAGE NO: 2867-2874

INERNET OF EVERYTHING: A SOLUTION TO MOBILE BANKING USING VOICE RECOGNITION

[1]*Ebole Alpha Friday* [2]*.Shomope Adewale Abduirasaq.* [3] *Amusu Mary*
[1,2,3] *Department of Computer Science*
School of Technology,
Lagos State University of Science and Technology,
Ikorodu, Lagos State Nigeria.
alphaechoeb@gmail.com

Abstract— The advancement in the banking transaction systems over the years has been enormous, and the needs for identifications of customer authentication, validation, and confirmation are of utmost priority and should be dealt with judiciously. Mobile banking has emerged as one of the main divisions in the digital world of financial transactions and consists of information inquiry, notifications and alerts, applications, and payment transfers. Mobile-based application is used for connecting customer handsets with bank servers for all such services in the banking industry. The current trend of Mobile banking has gone beyond the use of Time Password (OTP) applications used by banks. The problem with current banking applications is that they send data directly to customers in plain text form compromising with security recognized as OTP in most online transactions. An online banking customer logging in to the bank's website with a username and password triggers a request to send an OTP to his or her registered mobile phone or the OTP may not be necessary after one or two transactions. There is every likely hold of Mobile phones been stealing, accessed by unauthorized persons, or hacked. Upon receipt of a text message with the OTP, the customer enters it with an additional field on the banking site's login page to complete the login process since your details are already on your phone. It could have been fine if the mobile network can act immediately but blocking of network provider involves the presentation of the National Identification Number (NIN), which is a chain reaction. The purpose of this research work is to provide a cost-effective, secure, fast Mobile banking solution combining features of cryptography as well as behavioral pattern and Interactive Voice Response for final authentication and authorization of customer identification in all forms of financial transactions.

Keywords : Mobile Banking, Online Transactions, Cryptography, OTP.

I. INTRODUCTION

The mobile banking system is recognized as daily banking operations to the customer with mobile handset and supported application software, it includes all potential to provide access or delivery of very specific and highly necessary information to the customer as given by Venugopal, H et al (2012) "Enhanced voice recognition to reduce fraudulence," it is driven by various facilities like the convenience of banking operations, greater reach to consumers and Integration of other electronic commerce services with mobile banking as stated by Mohammad Shirali-Shahreza and Hassan Shirali-Shahreza (2007).

Recently there has been a tremendous increase in the use of biometric features in recognition systems such as voice, fingerprints, face, iris, etc. The development of real-time Mobile Banking in Africa has taken another dimension and an avenue for criminals to hack customer accounts in case of misplacement of mobile devices or stealing. The criminal gains access to the details of information, such as customer bank transactions which are stored in individual handsets. The idea of mobile banking was to pave way for quick service and the safety of customers' funds in the bank account but this objective was not met due to unlawful accomplishments endangered by a conspirator. Presently, the only method for authentication is the customer entering his or her password in the device (mobile handset) in other to carry out transactions but it has some problems associated with it if the user is not the actual owner of the device such password can be entered and the unauthorized person gain access to the account and perform his illegitimate activities on the account.

A voice-dependent access control system is necessary for third-level validation and will help in verifying the authenticity of a person by the electronic assessment of the voice characteristics of the person concerned. Of late, the biometric methods used to remove the loopholes associated with the Mobile banking and for validation of legitimate person for device accessibility may include any of the following face, voice, hand shape, fingerprint, and iris. This paper discusses a voice-dependent on the Mobile transaction as a means of final level authentication and access control system which can provide correct verification of identity from an individual's voice characteristics in terms of pattern recognition stored in the database of the bank database tier (server). The preference of voice as a biometric feature is necessary because it is easily accepted by the users, can be recorded by any voice sensor, the hardware costs are reduced significantly, etc.

However, there are several challenges that need to be addressed to completely utilize the benefits of the Mobile Banking like handset compatibility, security, scalability, reliability, etc. Due to the increase in the use of mobile handsets for many electronic commerce applications, the chances of mobile hacking for financial benefits are heavily increased. Currently, most banks in Nigeria and outside are sending text SMS directly to the customer handset for basic bank services without any security and this can be accessed by any malicious person because the information is over the air and can be hijacked. There is every likelihood that Mobile data can be hacked in the network path from bank to customer mobile handset and all-inclusive in the device that can identify end-user identity in Mobile banking. Thus, there is a need for a secure and cost-effective solution that can easily be available on all types of handsets. The significant of this research work is to include voice authentication on the back end at the customer service network in the banking system as an additional security level for the protection and authorization of individual identity on Mobile banking in case of customer misplacement of their mobile phone or any form of being hacked.

Voice signal identification transforms a speech signal into features that aid in further processing. Quite a number of algorithms and techniques are used as stated by Muda, M., Begam, and I. Elamvazuthi (2010), "Voice recognition algorithms using Mel frequency cepstral coefficient (MFCC) and dynamic time warping (DTW) techniques. The ability of a system or program to receive as well as interpret dictation, or to understand and follow the matching spoken instructions stored in the database or inform of cloud storage of the Bank. In general, it is regarded as one of the convenient and safest recognition techniques. The basic block diagram for voice recognition is given in Figure 1. A big challenge of proliferating accuracy and recognition speed is faced by the real-time automatic system for speech recognition. Degradation in the performance of the speech recognition system occurs due to noise. Also, it is affected by modifying speech data due to dependence on the speaker's gender, environmental conditions, and style in which it is spoken. The accuracy of recognition depends on the method of feature extraction and training, so one of the core issues of speech recognition research is the recognition accuracy, speed, and aim.

Moreover, system performance improves in the presence of noise with the use of noise-robust feature extraction and training techniques Chavan R. C and Sable, G.S (2013) "An Implementation of Text-Dependent Speaker Independent Isolated Word Speech," International Journal of Engineering Sciencs and Research Technology

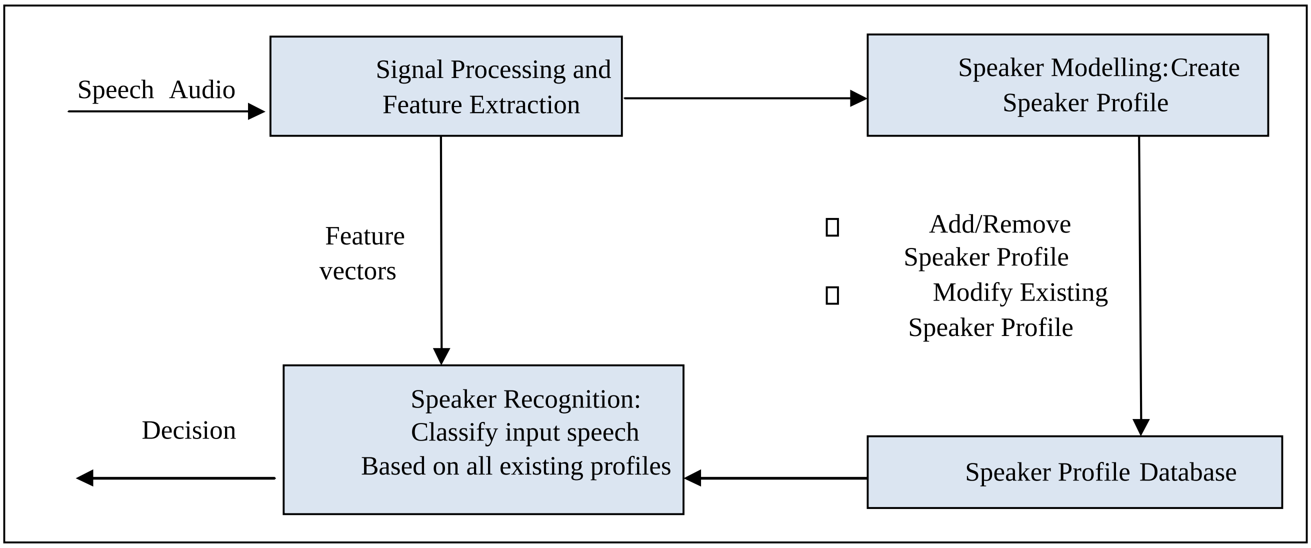

Speech Audio
Signal Processing and Feature Extraction
Speaker Modelling:Create Speaker Profile
Feature vectors
□ Add/Remove Speaker Profile
□ Modify Existing Speaker Profile
Speaker Recognition: Classify input speech Based on all existing profiles
Decision
Speaker Profile Database

Figure 1: Voice recognition System by Chavan R. C and Sable, G.S (2013)

Two-factor authentication of an individual can help voice to combine what the masses say and the way in which they say it. Other identifications such as fingerprints, handwriting, iris, retina, and face scans can also help, whilst voice identification is required as authentication that is not only secure but unique also. Voice recognition systems are economical and easily understood by users. There are some problems associated with Voice recognition such as However, it is the most popular and widely used method of password-less authentication but it suffers from some inherent limitations of human voice given such as

1. Low Signal to Noise Ratio, which can be caused because of background noises, low-quality microphones, or interference by electrical devices.
2. Difficult to recognize and individual when in a meeting, conference, etc.
3. Unable to identify words that have similar spelling and pronunciation but differ in their meaning.
4. It is difficult to identify whether the voice sample submitted for authentication is presented by some machine (recorded voice) or by the individual itself.

II. RELATED WORK

[1] Human identification of characteristics such as the face, fingerprint, iris, hand geometry, voice, Biological biometrics such as DNA, blood, hair, etc., and Behavioural biometrics such as the signature, the keystroke dynamics, and the gait recognition, etc. In the literature, biometrics-based mobile authentication is an emerging issue. Some researcher considers the following modalities as biometrics such as fingerprint, face, voice, and iris. In the recent paper Wang, S. and Liu, J. (2011) on *Biometrics on Mobile Phone*, the authors propose an overview of biometrics on mobile phones through some standard modalities (fingerprint, speaker recognition, iris recognition, gait). Most authors recognize that specific Speaker Recognition for Mobile User Authentication modality as well as Face recognition is dealt with in the paper written by Hadid, A., Heikkila, A, J., Silven, O. and M. Pietikainen, M.(2017) on Face and eye detection for person authentication in mobile phones, or as in Mohammad Shirali-Shahreza (2016), where a real-time training algorithm is developed for mobile devices. The authors propose to extract local face features using some local random bases and then incrementally train a neural network. The image processing also concerns hand biometrics on mobile as in the reference, where hand images are acquired by a mobile device without any constraint in orientation, distance to the camera, or illumination. The author of Jiehua Wang, Song Yuan, "*A Novel Security Mobile Payment System Based On Watermarked Voice Cheque*". details an iris recognition system, based on a three-step pre-processing method relying on (a) automatic segmentation for pupil region, (b) helper data extraction and pupil detection, and (c) eyelids detection, and feature matching. Some recent papers N.L. Clarke and S.M. Furnell (2007). Advanced user authentication for mobile devices. *Computers & Security*, Mohammad Shirali-Shahreza and M. Hassan Shirali-Shahreza,(2007) "*Text Steganography on* International Conference on Convergence Information Technology, and Martinez Borreguero, F. Javier and Chaparro Peláez, Julián," *Spanish (2005) Mobile Banking Services: An Adoption Study*", Proceedings of the International Conference on Mobile Business. deal with keystroke-based recognition. The first paper makes a study about user identification using keystroke dynamics-based authentication (KDA) on mobile devices, relying on 11-digit telephone numbers and text messages as well as 4-digit PINs to classify users. The second develops a more performant KDA process, with optimized enrolment and verification steps, whose principle is extended in the latter paper for touch screen-handled mobile devices, along with a pressure feature measurement. The reference [7] presents a new modality for authentication on a mobile device, namely gait recognition. The first deals with text-dependent speaker verification. It means that both the user's voice and the uttered text itself are used for the verification. The second paper proposes a new method to extract features from speech spectra called slice features. The

aforementioned references show that many biometric modalities can be used for user authentication on mobile devices. Therefore, speaker recognition seems the most natural modality choice for implementation on mobile phones. In the vast literature dealing with speaker recognition, two trends stand out: text-dependent and text-independent speaker recognition techniques. We are only interested in the second field Yekini NA et al. (2012) presented a voice-dependent access control system for ATMs. Figure 3 shows the block diagram of the discussed system. The system consists of 3 important components: a Voice sensor e.g. microphone, a speaker verification system, and an access control system for the ATM machine. A low-cost voice sensor is used to record the ATM user's voice and subsequently send it to the voice-dependent verification system to validate the authenticity of the user.

The human voice is a complex information-bearing signal, depending on physical and behavioral characteristics. The raw speech signal, uttered by any person, is extremely rich in the sense that it involves high-dimensional features. To perform efficient speaker recognition, one must reduce this complexity, while keeping sufficient information in the extracted feature vector.

2.0 Principles of Speaker Recognition

Both speaker recognition and speech recognition belong to the category of voice signal processing, but speaker recognition focuses on the identity information of the speaker, while speech recognition focuses on the text information corresponding to the voice Martinez Borreguero, F. Javier and Chaparro Peláez, Julián," *Spanish Mobile Banking Services: An Adoption Study*", Proceedings of the International Conference on Mobile Business 2005. Voiceprint can be understood as the pattern of the voice frequency spectrum obtained by the time-frequency analysis technology of the wave-form signal of the human voice. Due to the inherent differences in the physiological structure of each person, it also causes the diversity of human speech styles, which provides us with a principle basis for automatically identifying the speaker's identity information through machines.

2.1.Speaker recognition classification

According to different application scenarios, speaker recognition can be divided into two tasks: speaker verification and speaker identification. The former refers to judging whether the current speaker is a certain identity entered in the system, which is a 1:1 confirmation question; The latter means that you don't know the identity of the current speaker, and you need to find the most similar one among the N speakers that the system has entered. It is an N:1 classification problem. According to the different recognition objects, speaker recognition can be divided into three categories: text-related, text-independent, and text-prompt. The text-related speaker recognition method requires the speaker's pronunciation of keywords and key sentences as a training text, and the pronunciation is based on the same content during recognition. The text-independent speaker recognition method does not need to limit the speech content during training and recognition, and the recognition object is a free voice signal. The speaker recognition of text prompts, as the name suggests, the recognition object is the random generation of some specific text given by the system.

2.2.Speaker recognition process

Speaker recognition technology recognizes the identity of the speaker by analyzing the speaker's characteristic information contained in the voice signal, which mainly includes two stages of training and recognition: In the training phase, according to the training speech of each speaker, feature parameters are extracted to establish a speaker model; in the recognition phase, after the speech features of the speaker to be recognized are extracted, it is matched with the established speaker model for judgment. The basic principle is shown in Figure 1.

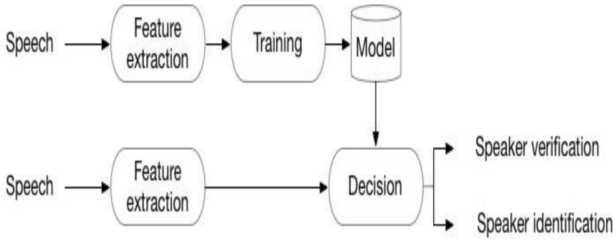


Figure 1: Basic speaker recognition system framework

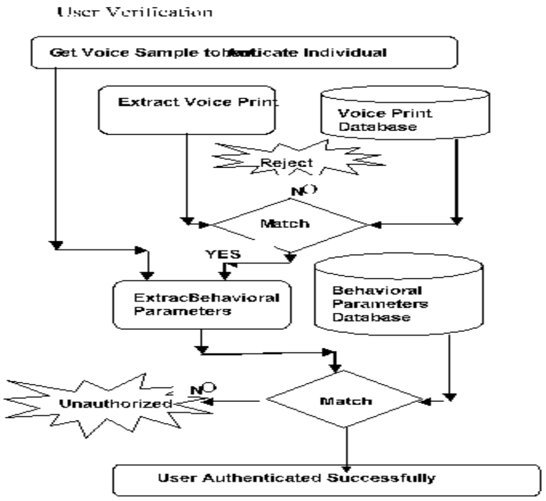
RESEARCH METHODOLOGY

PROPOSED WORK

Getting motivated by the above-discussed issues being faced in the voice authentication system, a new method is proposed below. The proposed method is a hybrid of Behavioral Identification with Voice Recognition. While registering an individual for the first time, along with taking its voice samples for extracting voice prints, the behavioral parameters also get extracted and stored in a database. This behavioral parameter can be voice message identification, to be provided by end-users for negative emotional information sympathy by the bank for reference purposes. Whenever an individual claims their identity for authentication, then it will be first verified message stored in the database in line with the saved voice print as an additional layer of security. It will be authenticated automatically only after successfully passing both stages. It can be illustrated by the following flow diagrams:

Image Upload

The voice samples of first-time users are taken in order to extract and save their voice print as well as a behavioural parameter in the databases.


User Verification
Get Voice Sample toAuthenticate Individual
Extract Voice Print
Voice Print Database
Reject
NO
Match
YES
ExtracBehavioral Parameters
Behavioral Parameters Database
Unauthorized
NO
Match
User Authenticated Successfully

The Voice samples are presented for extraction of voice prints and matched with the saved details in the database. If the match is successful, then the match of behavioural parameters is done. If the individual qualifies for both the tests, only then access is granted otherwise rejected.

Since the proposed method is verifying the individual with an additional layer, higher security is supposed to be achieved. The proposed method may be modified to counter attacks against impersonation where the speaker's voice gets recorded and presented later on impersonating the speaker. A human is not supposed to match behavioral parameters 100% each time. There comes an obvious and slight deviation. If there is a case of impersonation of the speaker by some machine then there will be a 100% match of the behavioral parameters. On the basis of this fact, the mathematical model can be prepared and simulated as well to justify the intended result.

IV. CONCLUSION

Different finance firms, as well as industries, are relying on voice recognition authentication for their security. Speech recognition can be used for disabled people who are otherwise not able to authenticate themselves using traditional techniques. In Africa, it can play a major role in moving the technology to the doorstep of a common man who is not much literate and not familiar with digital media techniques. As the current system needs to be changed for software only not specific hardware in order to deploy this technology, hence it is cost-efficient and feasible to deploy too. In the current work, its hybridization with the behavioral authentication technique is proposed as it would result in an additional layer of secure authentication and is expected to withstand impersonation attacks.

Nowadays, mobile technology has become a definite requirement for carrying out millions of transactions that happen in day-to-day life. A large number of frauds can be carried out using mobile systems, In order to overcome these problems hackers and misplacement of mobile phones, it is highly recommended that the banking sector should make the use of voice biometrics. This method when fully taken into practice will not only enhance secured and correct authentication, but will also render support in the implementation of complex banking mobile transactions in terms of performing deposits and money transfers, as this system provides enhanced security.

REFERENCES

[1] Mohammad Shirali-Shahreza and M. Hassan Shirali-Shahreza, “*Mobile banking Services in bank area*”, SICE Annual Conference 2007, Japan

[2] Martinez Borreguero, F. Javier and Chaparro Peláez, Julián,” *Spanish Mobile Banking Services: An Adoption Study*”, Proceedings of the International Conference on Mobile Business 2005.

[3] Mohammad Shirali-Shahreza*,” Improving Mobile Banking Security Using Steganography* “, International Conference On Information Technology 2016.

[4] Przemyslaw Krol, Przemysław Nowak, Bartosz Sakowicz,”*Mobile Banking Services Based On J2ME/J2EE*”, CADSM’2007.

[5] Yousuf S. AlHinai, Sherah Kurnia, and Robert B. Johnston,” *Adoption of Mobile, Commerce Services by Individuals: A Meta-Analysis of the Literature*”**,** Sixth International Conference on the Management of Mobile Business.

[6] T N T Nguyen, P Shum, and E H Chua,” *Secure end-to-end mobile payment System”.*

[7] Ashutosh Saxena, Manik Lal Das, and Anurag Gupta,” *MMPS: A Versatile Mobile-to-Mobile Payment System*”, Proceedings of the International Conference On Mobile Business 2005.

[8] Iron-Chang Lin and Yang-Bin Lin,” *An Efficient Steganography Scheme for M-Commerce”.*

[9] Mohammad Shirali-Shahreza and M. Hassan Shirali-Shahreza, ”*Text Steganography in SMS*”, 2007 International

Conference on Convergence Information Technology.

[10] Sandeep Singh Ghotra, Baldev Kumar Mandhan, Sam Shang Chun Wei, Yi Song, Chris Steketee, ”*Secure Display and Secure Transactions Using a Handset*”, Sixth International Conference on the Management of Mobile Business.

[11] Jiehua Wang, Song Yuan, “*A Novel Security Mobile Payment System Based On Watermarked Voice Cheque*”.

[12] M. Shirali-Shahreza, "*Stealth Steganography in SMS*", Proceedings of the Third IEEE and IFIP International Conference on Wireless and Optical Communications Networks 2006.

[13] Kevin Chikomo, Ming Ki Chong, Alpin Arnab, Andrew Hutchison, “*Security of Mobile Banking*”.

[14] Dilla Salama Abdul Minaam. Hatem M. Abdul Kadir, Mohily Mohamed Hadhoud*,” Evaluating the effects of Symmetric Cryptographic algorithms on Power Consumption for different data types*”, International Journal of Network Security, Volume 11, September 2010.

[15] Managing the Risk of Mobile Banking Technologies, Bankable Frontier Associates. Deshpande Neeta, Jamalpur Snehal,” *Implementation of LSB Steganography and its Evaluation for various bits*”.