A REVIEW ON AUDIO AND VIDEO BASED PERSON AUTHENTICATION USING MACHINE LEARNING

Roshni Wadhwani[1], Dr. Vishal Shrivastav [2], Dr. Akhil Pandey [3]

[1] M.Tech Scholar, Computer Science Engineering Department, Arya College of Engineering and IT, Jaipur, Rajasthan, India
[2] Professor, Computer Science Engineering Department, Arya College of Engineering and IT, Jaipur, Rajasthan, India
[3] Professor, Computer Science Engineering Department, Arya College of Engineering and IT, Jaipur, Rajasthan, India

ABSTRACT

Identity verification is a method that usually uniquely identifies a person based on a password and a personal identification number (PIN). The main problem with this authentication technology is that users are not willing to remember long-term and challenging combinations of numbers, letters and symbols that may be lost, forged, stolen or forgotten. In this article, we examined recent developments in the use of behavioral biometrics for user authentication. The application of behavioral biometric authentication basically consists of three main modules, namely data capture, function extraction and classification. The application focuses on extracting user-related behavioral characteristics and using these properties for identity verification measures. The goal is to determine the classification technology that is primarily used for data analysis in the identity verification process. Through comparison, we expect to find gaps in improving the performance of behavioral biometric authentication. In addition, we highlight a set of classification technologies that are best suited for behavioral biometric approval. This article discusses the concept of speech recognition in deep learning methods. This article will discuss speech recognition, deep learning and the introduction of deep learning methods. This article also describes models for deep learning for speech recognition. This article defines the work related to speech recognition using deep learning methods as well as the software related to Sphinx, which allows speech recognition in Java languages. The main purpose of this review is to define the use of the sphinx and solar eclipse to recognize speech. We would suggest that we have proposed a new human recognition technology using face and voice fusion that can greatly improve the recognition speed compared to a single biometric recognition used in the development of security systems. Our system uses the Viola Jones algorithm for face recognition. The proposed system uses the Local Binary Pattern (LBP) as a technique for extracting functions to calculate local functions. In our project, MFCC function (Extracting) with Mel Frequency Divergence Coefficient (technology for extraction) is used for speech recognition. The extracted function provided by the SVM classification as input can be used to identify individuals and then display the results. The new system can be used in a variety of areas, such as identity verification and other potential commercial applications.

Keyword: - *SVM, speech recognition. Feature extraction, LBP continuous authentication, behavioral biometric, machine learning, classification, clustering*

1. INTRODUCTION

Over the last ten years, the field of computer security has evolved with changes in the nature of technology. Computer security includes measures and controls. These measures and controls can ensure the achievement of information security objectives such as confidentiality, integrity and availability defined in hardware, software, firmware and information processed, stored and communicated. The benchmark model known as the CIA Triad is used to evaluate the physical, logical, and perceived security of information in an organization. The elements of the triad are considered to be the three most critical components of information security. If any of this triad has groundbreaking capabilities, it can have a serious impact on the organization. Confidentiality largely corresponds to confidentiality or confidentiality. It can prevent sensitive information from being leaked by unauthorized persons or systems. In general, it is also the most vulnerable. Cryptography through encryption algorithms is often used to ensure the confidentiality of data stored or transmitted from one computer to another. Integrity is usually described as the reliability, accuracy and consistency of data. In this case, unauthorized Microgrid users cannot modify or modify the data themselves. Cryptography plays an important role in ensuring data integrity. This is done by hashing the original data and sending the data and hash to the recipient, then performing another hashing on the received data and comparing them with the received hash to verify that they are complete. [1]

Availability is defined as the safeguards required ensuring that authorized parties can easily access relevant information when requesting relevant information. Denial of Service (DoS) attacks may well illustrate the many threats to this security check. By having the server utilize full processing power, bandwidth, and memory to process most of the requests caused by this attack, the DoS system renders the useless and unable to accommodate legitimate requests.

Last but not least, identity verification is the key to effective information security. The identity verification process verifies the identity of the user, process or device and allows only legitimate users to use resources and services in an authorized manner while rejecting all illegal resources and services. Today, user authentication has become an issue, so for online banking systems, the challenge has become more important than ever. Due to the high sensitivity of data, it is very important to protect users' accounts and protect their assets and personal information from malicious violations. Put it inside. There are many existing authentication methods. In general, they are divided into knowledge-based methods, possession-based methods and biometric-based methods. To be sure, all methods have their own uniqueness (advantages and disadvantages). However, the environment determines which approval method is best.

When talking about authentication in general, two types of well-known methods have been proposed in the literature, namely continuous authentication methods and static authentication methods. The continuous authentication method can also be considered as dynamic authentication, which confirms the user repeatedly throughout the session. The advantage of this method is that the system can continuously monitor whether unauthorized access has occurred. At the same time, the static authentication method collects data from the user and verifies the user's access rights and privileges by manipulating the data (for example when logging in). The access service remains valid until the user logs out of the session. The combination of username and password is a popular method of static authentication. Static authentication, however, has one drawback, as the method only authenticates the user at the beginning of each session. If the user is attacked and changes occur, the system does not attract attention [2].

In this article, we outline the latest developments in biometric authentication systems. However, our focus is only on behavior-based biometric approval. To evaluate the accuracy of behavioral biometric authentication, there are three common metrics: False Rejection Rate (FRR), the percentage of users who incorrectly deny access to the system; False Acceptance Rate (FAR), which is the percentage of users incorrectly authorized by the system; And equal error rate (EER), that is, the value of FRR and FAR when the system is adjusted to have equal FAR and FRR. For an authentication system to be more convenient, it must generally have the following features: accuracy, fast response, and difficulty forging [3].

Over the last ten years, the field of computer security has evolved with changes in the nature of technology. Computer security includes measures and controls. These measures and controls can ensure the achievement of information security objectives such as confidentiality, integrity and availability defined in hardware, software, firmware and information processed, stored and communicated. The benchmark model called the CIA Triad is used to evaluate the physical, logical, and perceived security of information in an organization. The elements of the triad are considered to be the three most critical components of information security. If any of this triad has groundbreaking capabilities, it can have a serious impact on the organization.

Confidentiality largely corresponds to confidentiality or confidentiality. It can prevent sensitive information from being leaked by unauthorized persons or systems. In general, it is also the most vulnerable. Cryptography through encryption algorithms is often used to ensure the confidentiality of data stored or transmitted from one computer to another.

Integrity is usually described as the reliability, accuracy and consistency of data, where the data itself cannot be altered or altered by unauthorized users [4]. Cryptography plays an important role in ensuring data integrity. This is done by hashing the original data and sending the data and hash to the recipient, then performing another hashing on the received data and comparing them with the received hash to check its integrity Sex.

Availability is defined as the security checks required to ensure that authorized parties can easily access relevant information when requested. Denial of Service (DoS) attacks may well illustrate the many threats to this security check. By having the server utilize full processing power, bandwidth, and memory to process most of the requests caused by this attack, the DoS system renders the useless and unable to accommodate legitimate requests.

Last but not least, identity verification is the key to effective information security. The authentication process verifies the identity of the user, process, or device, and allows only legitimate users to use resources and services in an authorized manner, while rejecting any illegal users

Today, user authentication has become an issue, so the challenge is more important than ever. For online banking systems, it is very important to protect user accounts and protect their assets and personal information from malicious breach due to the high sensitivity of internal data. There are many existing authentication methods. In general, they are divided into knowledge-based methods, possession-based methods and biometric-based methods. To be sure, all methods have their own uniqueness (advantages and disadvantages). However, the environment determines which approval method is best.

When talking about authentication in general, two types of well-known methods have been proposed in the literature, namely continuous authentication methods and static authentication methods. The continuous authentication method can also be considered as dynamic authentication, which confirms the user repeatedly throughout the session. The advantage of this method is that the system can continuously monitor whether unauthorized access has occurred.

At the same time, the static authentication method collects data from the user and verifies the user's access rights and privileges by manipulating the data (for example when logging in). The access service remains valid until the user logs out of the session. The combination of username and password is a popular method of static authentication. Static authentication, however, has one drawback, as the method only authenticates the user at the beginning of each session. If changes occur in the user in the event of an attack, the system does not attract attention [5].

In this article, we outline the latest developments in biometric authentication systems. However, our focus is only on behavior-based biometric approval. To evaluate the accuracy of behavioral biometric authentication [6], there are three common metrics: false bounce rate (FRR), the percentage of users who mistakenly deny access to the system; false bounce rate (FRR)). Error Acceptance Rate (FAR) is the percentage of users approved by the system by mistake; and equal error rate (EER), that is, the value of FRR and FAR when the system is adjusted to have equal FAR and FRR. To make an approval system more practical, it must generally have the following characteristics: accuracy, rapid response and difficulty in forging.

1.1 Authentication

User authentication methods: The most important key in the authentication process is the uniqueness of security measures. It can usually be classified as something that the user knows (password), something that the user has (smartcard) or something that the user has (Biometrics). Knowledge-based methods, possession-based methods and biometric-based methods are found in Figure 1.

Knowledge-based method: Knowledge-based technology is often used to protect the security of system access. Two known examples are passwords and passwords. The password is usually entered at the beginning of any communication or action, and the password may only be entered when the user uses the correct password or action. The advantage of using a conventional password is that it does not require professionals, is easy to operate, easy to use and easy to remember. Unfortunately, passwords have many problems because they are extremely vulnerable to brutal force attacks, password guessing and key logging programs. The disadvantage is that once the password is leaked, the opponent can easily use the victim's account [7].

The marble hole method can be found at the following location, which includes a password consisting of a password in the form of a random marble sequence during the authentication process. The user must drag the number to the center of the screen in the correct direction. Then it immediately reappears in its previous position. To leave traces, three graphics-based authentication methods were implemented, one of which was grid-based and two were random graphical methods.

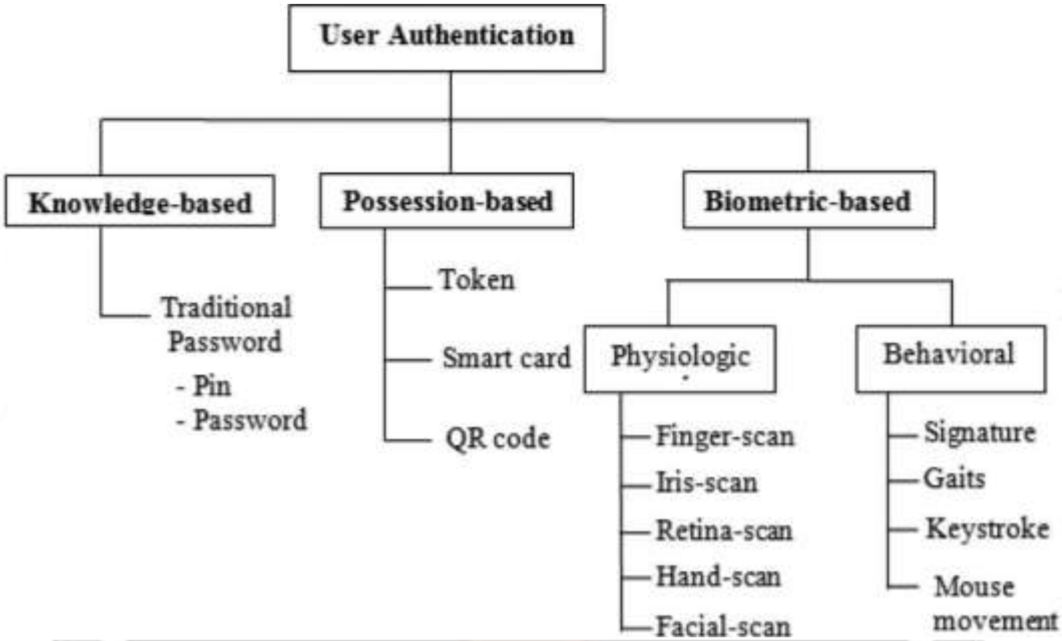

Fig -1: Taxonomy of user authentication methods

Using the matrix value of the image [8], another smartphone authentication scheme was created. This method requires pre-synchronization between the smartphone and the service server. For authentication tasks, the user must respond to the service server by entering a combination of an existing text-based password and a graphical-based password to provide better accuracy.

A location-based authentication method using a smartphone is proposed. Use static (captured during login session) and continuous (captured during session) location information. In the localization process, two different locations are used by the API. The location is verified and compared before deciding if the user is valid. The system may cause errors due to overlapping locations during the verification process. Therefore, the security of the introduced system depends on the effectiveness of location [9] Who proposed a physical proximity to use the modulated lighting of the smartphone screen to transmit PIN code to ensure security. The user enters the PIN code on the smartphone. By using a cheap custom-made receiving device, the PIN code can be transmitted via a temporary light pattern on the screen. This method is the right choice to ensure familiarity against man-in-the-middle attacks.

The hybrid graphical password method is a combination of recall and recognition schemes and provides a more secure system based on the use of graphical passwords and text passwords. In the registration phase, the user selects a username and password for text and then selects

By drawing all the information as a password stored in the database. During the authentication process, the user enters the username and text password and then draws the preset objects as expected. This solution is not suitable for users without drawing functions.

2. LITERATURE SURVEY

M.A.Anusuya et.al. A brief survey was conducted on the acceptance of automatic speech, and major topics and developments over the 60 years of research were conducted to provide technical insights and to acknowledge the fundamental advances made in this field of communication. this voice. Designing a speech recognition system requires careful attention to the following issues: defining speech categories, speech substitution, feature extraction techniques, speech classification, data, and performance evaluation. The purpose of this article is to summarize and compare some of the known methods used in different stages of the speech system, and to identify the research and application topics that are at the forefront of this exciting and challenging field. [12]

Santosh K. Gaikwad's et.al are the greatest tool of human communication. The interaction between a machine-man interface is called a machine-man interface. Voice has the potential to become an important way of communicating with computers. This article describes the key technical concepts of speech recognition, presents basic advances in speech recognition and describes the general observation technologies developed for each speech recognition process. This article helps in choosing the technology and its advantages and disadvantages. At each stage, different technologies were compared and studied. This article has finally decided on the unique direction of the use of Marathi language to develop communication system technology in human beings [13].

Shanthi, Chelpa et.al Lingam and others. The speaking voice has become a major form of human communication. The advent of digital technology has given us high-speed digital processors and allows researchers to convert voice signals into digital voice signals, which can be used in scientific research. Achieving higher grades, lower word error rates and solving the problem of inequality are the key concepts in designing an effective automatic speech recognition system. In the acceptance of speech, the exploitation of features requires special attention, as the effectiveness of the acceptance depends largely on this context. In this article, I have focused on the progress made so far in the process of exploring the speech recognition system, and described the technical visions of the automated speech recognition system. [14]

Sanjib Das et.al. Short audio interviews are the most important and appropriate tool for interpersonal communication. The interaction between a machine-man interface is called a machine-man interface. Voice has the potential to become an important way of communicating with computers. This article describes the main points of perspective, acknowledges the basic advances in speech recognition, and provides an overview of the technologies developed during each speech recognition process. This article helps in choosing the technology and its advantages and disadvantages. At each stage, different technologies were compared and studied. This article is based on a decision on the unique leadership technology of human development in different vernacular languages, and discusses the various technologies used at each stage of the process. speech appreciation, and attempts to investigate a method of designing effective speech systems. detect. The purpose of this article is to summarize and compare the various speech systems, and to identify the most recent research and application topics in this interesting and challenging field. [15]

Nidhi Desai et al. Studies show that speech is a natural form of human communication, and speech processing is one of the most encouraged areas in the field of signal processing. Speech recognition is the process of automatically recognizing the words used by a person based on the information in the signal. The Automated Speech Recognition System (ASR) takes human speech as input and reproduces phrases as products. This article presents a brief overview of automatic speech recognition and discusses key topics and improvements that have been learned over the past 60 years. These technologies provide technological hope and honor the fundamental achievements made in this field of speech communication. Defining the types of speech classification, feature extraction technology, speech classification and performance evaluation are issues that should be carefully considered when designing a speech-acceptable system. The purpose of this article is to summarize the common methods used in several stages of the speech recognition system. Guillaume. [16]

Gravier, Ashutosh Garg et.al. Studies have shown that visual and speech information from the speaker's oral region has been successfully proven to improve the noise intensity of automatic speech media, which is expected to expand its use. it in the human-sacred interface. In this article, we examine the key elements of future audiovisual language recognition and we will contribute to two main aspects: first, the design of visual feedback based on image editing. -image of the area of interest that is of interest, and the audio-visual audio. In the following topics, we discussed the combination of work and collaboration, the non-verbal model of audio-visual speech, and the new work of introducing reliable assessment on how to approach in the bimodal acceptance process. We also talked briefly about editing audiovisual speakers. We apply the algorithm through complex visual and environmental controls across small to large tasks. Our experiments show that visual models can improve the ability of automatic speech recognition in all situations and all data, but are ineffective in complex and complex environments. [17]

Li Deng and John C.et.al Pratt shows that deep learning systems have improved the accuracy of speech recognition, and in recent years there have been a variety of deep learning structures and methods available. various advantages and disadvantages. How to apply ensemble learning to different deep learning systems to achieve higher grades is the focus of this article. We developed and reported on-line and on-the-road storage methods for ensemble studies, and applied them to posterior-like cases that included convolution, recursion, and deep neural network. . The problem of convex improvement is proposed and solved, and the analytical formula of the degree training of mixed teaching can be adopted. The experimental results show that after the installation of the in-depth study software, the reliability of the phone will be improved. [18]

Li Deng, Jin Yu, et.al etc. show that deep learning has become a common technology in the recognition of industrial discourse. In this article, we provide an overview of the work of Microsoft speech analysts in this field since 2009, focusing on recent developments that provide inspiration for the core work and limitations of learning technology. deep now. We organized this overview across the features and dimensions of the model in the usual way for analyzing the talking systems. Selected experimental results, including speech recognition and related applications (such as communication and language design) were included to demonstrate and evaluate the advantages and disadvantages of the techniques described in this article. The potential for improvements to these technologies and future research guidelines are discussed. [19]

Samy Bengio and Georg Heigold et.al: Faces provide complex information, including age, gender, race, identity, personality, intentions, and emotions. In addition, the ability to speak also has a significant impact on physical appearance. All of these aspects dominate interpersonal relationships at all levels. While we can combine these complex ideas to avoid costly reasons, the presence of all of these resources makes the complex thought process more difficult. For example, when the emotion departs from a neutral emotion, the functioning of the normal emotional state decreases. Similarly, an effective acceptance system should be firmly rooted in changing your own personality structure. In the field of facial recognition, previous research has offered ways to compensate for headaches and subject inconsistencies. However, it is not known how to reduce the variability of verbal messages during verbal communication. In candid conversation, pronunciation affects the appearance of the face. The retrieval of emotion in facial expressions requires a separation of language and emotional information. By using and compensating for the content of basic vocabulary, the understanding of emotions can be improved. However, this requires transcription and phoneme information, which is not available in many types of applications. This study uses an asymmetric bilinear model to soften language and emotion (if not provided). Evaluation of the mood in the IEMOCAP data shows that this method can separate these loads directly, and improve their efficiency. This refinement is similar to a translation of a known truth. Similarly, experiments using image -based methods on the SEMAINE website also proved the effectiveness of the technology in real life. The IEMOCAP corpus is a collection of media information used to study the relationship between text and translator (5 males and 5 females). During the five stages, the film and the actor went through a series of videos and edits. Choose an environment that will make a lasting impression (e.g., airport losses and school enrollment). The conversation is divided into a series of dances, which are legally translated. Housing and boundary terms are obtained by a forced adaptation algorithm. The three observers emphasized transition using the following hashtags, which use the following hashtags: anger, happiness, sadness, shock, discomfort, frustration, fear, jealousy, neutrality, etc. [20]

Dandan Mo R et.al The hands and shoulders are widely used for biometric identification. In this work, these materials are used to create a height level. Haar port is famous for reducing port congestion. In both cases, the Haar waaret technology is used for feature extraction. This work introduces a new approach to physical physics and experimentation. Compared to conventional work, this layered appearance makes the displayed results better. The proposed algorithm optimizes the efficiency and effectiveness of each model. This is clearly seen in the simulation results. For its simplicity, ongoing research in this field (multi-modality) focuses on biometric extraction by length or category matching. However, large biometric applications still need performance improvements. Not only does it require monitoring, but it also requires more focus and time. Therefore, more specialized biometric systems should be implemented to not only achieve the required improvements, but also to reduce implementation time. The most common classes used in various biological models are vector machines (SVMs) with different values (especially Gaussian and polynomial), classes based on Gaussian complex models, ear networks and multilayer perceptrons. . Most of them can improve performance, but the results depend entirely on the available data. In the proposed work, a model for high-speed SVM students is used to evaluate the effectiveness of the proposed system. The idea behind the SVM is to use a kernel strategy to plot the vector input to a high-speed data stream, and then create a spatial map of that location to separate the series of files from each other. the last points. In general, the number of biometric technologies applied to modern systems is often equal to the number of biometric technologies studied. Using a single extraction technique to exploit the characteristics of the two participants will strengthen the design system. This research work aims to reduce false positives, false positives, and training and test links to obtain accurate information. The higher the quality of the biological samples collected from the various packaging materials, the higher the reliability of the identification. For the same biometric sample, the better the method is accepted, the higher the confidence. Therefore, this paper proposes a biometric algorithm that takes advantage of the quality of biometric samples and the reliability of recognized experts (called PSVM). First, the sample code used for markup and memory is derived from the quality of the sample and the reliability of the experts, and then the test results. XM2VTS data is used to compare the HTER, Bayes, FLD, MLP, mean and SVM of PSV. The experimental results show that the HTER of the PSVM fusion algorithm is low. [21]

3. POSSESSION-BASED METHOD

The use of traditional passwords has proven to be insecure and inconvenient as a security measure. Facts have proven that the owner-based method can eliminate the risk of attackers guessing passwords and is expected to improve data security. This method takes advantage of the user's personal belongings, such as tokens, smart cards and QR codes.

Any object or device that can be used in the authentication process is called a hardware token. They are available in various forms, such as mobile devices or easily accessible devices (smart keys and smartphones). By combining PIN and smart card, a smart card reader (smart phone that supports NFC) has been introduced [10]. The PIN code is managed as a temporary PIN code. Using a temporary PIN can reduce the chance of a hacker distinguishing between a permanent PIN.

In this system, the user identity verification is realized using the QR code identification method. In the verification phase, the user sends a request from the server; in return, the server will extract information about the user. The advantage of this method is that it is known to be faster than the certificate system.

Table 2 shows an overview of the categories based on ownership. Facts have proven that possession-based methods can eliminate the risk of an attacker easily guessing passwords from knowledge-based methods. Since a token is required during the authentication process, the disadvantage of a physical token is that an attacker can gain authorized access rights from a stolen or lost token. Therefore, ownership-based methods of user authentication can still be considered weak.

3.1 Biometric-Based Method

The use of human characteristics is the best solution compared to the user that personally knows and possesses. In other words, biometric-based method cannot be forgotten or lost

Physical biometrics: Measurements from the human body have been proposed and used to develop various physiological and biometric techniques, including finger scans, iris scans, retinal scans, hand scans, and facial scans. There is evidence that the best accuracy can be achieved using methods based on physical biological properties. Table 3 summarizes the biometrically based methods (physical biometrics) used for user authentication.

Fingerprint recognition is the most famous feature in biometric identification methods and it shows the best performance. Some methods under fingerprints are edge-based methods and rules for mining as well as image pretreatment of area segmentation techniques. The benefits of using fingerprints are ease of use and high authentication accuracy. Today, fingerprint scanners have been widely used among the users. Through the fast semi-

3D face based on vertical body restoration and the fragile watermarking technology based on chaos theory, the concept of face recognition technology provides impressive accuracy. In addition, additional security measures can be implemented by combining this technology with other user authentication methods (such as PIN). [11] Introduced Daubechie's wavelet transformation method to improve the performance of iris recognition. Iris is considered to be the most accurate feature and none of them can be repeated. However, when there are obstacles in the scan, the recognition decision may be disturbed.

Behavioral-based biometric authentication: This section aims to find good techniques for behavioral biometric authentication. Figure 2 shows different machine learning techniques, which can generally be divided into supervised (classification) and unsupervised (clustering). Monitored machine learning can be used to classify data more accurately. In the literature, researchers have used classification techniques such as K-nearest neighbor (K-NN) multi-layer perception (MLP) dynamic time distortion (DTW) (neural network decision tree algorithm normalization and exclusion method and support vector machine (SVM))) These technologies have improved system performance , and the results show that some great achievements have been made in their respective fields. At the same time, unattended machine learning can perform data reduction tasks by filtering out non-representative data. Data that cannot be grouped correctly can be considered as abnormal data. After the reduction task is completed, the classification result is expected to reach the optimal solution. The cluster algorithm can be further divided into plan partition and hierarchically based cluster algorithms.The basic purpose of implementing behavioral biometric authentication is to achieve accuracy and improve system performance. This goal led to the creation of a major classification technology for solving accuracy problems associated with biometric authentication.An Android application was developed using touch-slide biometric identification method. In this work, touch screen and training data were collected through physiological questionnaires. The measured parameters are duration, average speed, average X, average Y, average Z,Today, knowledge-based methods are often used because they are simple, economical and practical mechanisms to use and implement. However, these methods are also considered to be extremely poor forms of protection. Fraudsters can attack password-protected systems in a variety of ways. The most common type of attack is password guessing. Authentication can also use user-owned replacements, such as tokens, smart cards, and QR codes. However, these methods do not work well in the above situations. These methods are more secure than the user's PIN or password. Therefore, this ownership-based authentication method is still considered weak. To overcome the shortcomings of these identity verification methods, research for identity verification has turned to biometrically based methods because biometrics cannot be shared or denied due to uniqueness. Behavioral biostatistics is a field of research related to measurements that uniquely identifies measurable patterns in human activity. This term is the opposite of physical BIOMETRIC, which refers to inherent human traits, such as fingerprints or iris patterns. Table 6 shows user authentication methods that can be roughly divided into four categories.

4. CONCLUSIONS

This study conducted a comprehensive study of machine learning techniques in behavioral biometric authentication. In particular, we will re-evaluate papers published between 2003 and 2020. First, we introduce the concept and application of biometric approval. Second, we categorize identity verification methods and discuss in detail knowledge-based, possessive, and biometric-based methods. In the behavioral biometric approval section, we discussed two subcategories of machine learning techniques, which are supervised (classification) techniques and non-supervised (cluster technical) techniques. We examine each subcategory implemented in previous behavioral biometric approval. At the end of this article, we should be able to gain the relevant knowledge needed to improve the performance of behavioral biometric authentication.

5. REFERENCES

[1]. Kissel R. Glossary of Key Information Security Terms. Maryland: National Institute of Standards and Technology; 2013. DOI: 10.6028/NIST.IR.7298r2

[2]. Stapleton JJ. Security without Obscurity: A Guide to Confidentiality, Authentication, and Integrity. Boca Raton: CRC Press; 2014

[3]. Clarke N. Transparent User Authentication: Biometrics, RFID and Behavioural Profiling.London: Springer Science & Business Media; 2011

[4]. Ahmed AAE, Traore I. A new biometric technology based on mouse dynamics. IEEE Transactions on Dependable and Secure Computing. 2007;4(3):165-179

[5]. Bours P, Fullu CJ. A login system using mouse dynamics. In: IIH-MSP 2009-2009 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing; 2009, pp. 1072-1077

[6]. Jorgensen Z, Yu T. On mouse dynamics as a behavioral biometric for authentica-tion. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security– ASIACCS '11; 2011. pp. 476

[7]. Gorodnichy DO. Evolution and evaluation of biometric systems. In: Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009) Evolution, (Cisda); 2009

[8]. Zheng N, Paloski A, Wang, H. An efficient user verification system via mouse move-ments. In: Proceedings of the 18th ACM Conference on Computer and Communications Security; 2011. pp. 139-150

[9].Vongsingthong S, Boonkrong S. A survey on smartphone authentication. Walailak Journal of Science and Technology. 2015;12(1):1-19

[10]. Ang.R. Safavi-Naini.R, McAven.L:. Cancelable Key-based Fingerprint Templates. In C. Boyd and J. Gonzalez Nieto (Eds.), Australasian Conference on Information Security and Privacy, pp. 242-252, 2005.

[11].Anil K., Arun R., and Sharath P., "Biometrics: A Tool for Information Security," IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, pp. 125-143, 2006.

[12]. M.A.Anusuya and S.K.Katti ,Department of Computer Science and Engineering,Sri Jayachamarajendra College of Engineering, Mysore, India, (IJCSIS) International Journal of Computer Science and Inform4 ation Security,2009.

[13]. Santosh K.Gaikwad, Dr.Babasaheb Ambedkar Marathwada, Bharti W.Gawali, 2011, A Review on Speech Recognition Technique.

[14]. Shanthi Therese ,Chelpa Lingam, International Journal of Scientific Engineering and Technology , June 2013.,Review of Feature Extraction Techniques in Automatic Speech Recognition.

[15]. Speech Recognition Technique: A Review Sanjib Das Department of Computer Science, Sukanta Mahavidyalaya, (University of North Bengal), India, International Journal of Engineering Research and Applications (IJERA) MayJun 2012.

[16]. Nidhi Desai1, Prof.Kinnal Dhameliya2, Prof.Vijayendra Desai3, International Journal of Emerging Technology and Advanced Engineering , December 2013, Feature Extraction and Classification Techniques for Speech Recognition: A Review.

[17]. Audio-Visual Speech Gerasimos Potamianos, Member, IEEE, Chalapathy Neti, Member, IEEE, Guillaume Gravier,, Ashutosh Garg, Student Member, IEEE, and Andrew W. Senior, Member, IEEE 2006, Recent Advances in the Automatic Recognition.

[18]. Li Deng and John C. Platt, Microsoft Research, One Microsoft Way, Redmond, WA, USA, November 2010, Ensemble Deep Learning for Speech Recognition.

[19]. Li Deng, Jinyu Li, Jui-Ting Huang, Kaisheng Yao, Dong Yu, Frank SeideMichael L. Seltzer, Geoff Zweig, Xiaodong He, Jason Williams, Yifan Gong, and Alex Acero Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA 2009

[20]. Samy Bengio and Georg Heigold, Google Inc, Mountain View, CA, USA, feb. 2007, Word Embeddings for Speech Recognition. Rubi, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May-2015, pg. 1017-1024 © 2015, IJCSMC All Rights Reserved 1024

[21]. Dandan Mo,December 4, 2012, A survey on deep learning: one small step toward AI. 11. Aalto University publication series, Foundations and Advances in Deep Learning, Kyunghyun Cho, 2014.