RESEARCH ARTICLE OPEN ACCESS

Online Transaction using Behavioral Biometrics

Mrs. Deepashree Mehendale*, Mrs. Vidya Bankar**, Mrs. Reshma Masurekar***, Mrs. Harsha Patil****, Mrs. Sujata Patil*****
**(Department of Computer Science, SPPU University, Pune*
*** (Department of Computer Science, SPPU University, Pune*
**** (Department of Computer Science, SPPU University, Pune*
***** (Department of Computer Science, SPPU University, Pune*
****** (Department of Computer Science, SPPU University, Pune*

ABSTRACT
In today’s digital era we all focus on getting everything in just a click, so day by day we see that there is increase in the Online transactions. Online transaction has become a need of the hour. But while doing so all the users are worried about the security of the same. Trust is the main issue while working with such type of online transaction. We can increase the trust of our customers by always giving them up to date, efficient and reliable service. Authentication is one of the crucial factor in security. Authentication can become strong if it has more layers of security. Adding more layers of security will make the authentication strong. This paper focuses on doing the Authentication not only at the beginning but it focuses on Continuous Authentication which can be implemented using Behavioral Biometrics. Behavioral Biometrics depends on how a person acts which cannot be copied in anyway. It focuses on Behavioral factors Keystroke Dynamics, mouse scroll with some additional factors like IP address, geo-location of the user which cannot be copied by the attackers. The related studies show that for secure authentication Biometrics is best way. In this paper we propose a workflow model where we combine password, OTP, Physical biometric i.e.:- face recognition with Behavioral Biometric making the Authentication system more strong. This model will work as a Multifactor Authentication and will help in attracting more and more users to use the online transaction in a seamless way.

Keywords - Behavioral Biometrics, Password, Physical Biometrics, Online transaction, OTP

Date of Submission: 13-02-2021 Date of Acceptance: 27-02-2021

I. INTRODUCTION

The security of a system includes many components like authentication and authorization. Authentication is considered as a basic principle of security. It confirms whether an individual is what he states to be. Traditional authentication techniques can only provide proof of possession and knowledge, therefore they are insufficient for identification of an individual and these techniques are related to something that the individual has and something that the individual remembers. Something that one has can be identity card, a smart card or a token which may be stolen, shared and forged. Something that an individual remembers is a password or a PIN which may lead to problems because individuals mostly use uncomplicated and easy way to remember passwords or PINs which can easily be guessed by others. To make the knowledge-based authentication systems strong, many password policies are defined. Many individuals are following these policies, but as these passwords are likely to be forgotten, they are often written down in places which are not at all safe. Two-factor authentication technology which combines possession and knowledge based techniques increases the level of security up to some extent, but using this technology only card and the PIN are authenticated and not the actual individual, which results to unsolved authentication problem. In the absence of an actual individual someone else having the card and knowing the PIN can provide his identity. Solution to this problem is biometrics which is one of the improved forms of authentication and it depends on actual individual’s presence and biological features.

Biometrics is the technology of biological measurements and analyzing of physical and behavioral characteristics of human which can be used for authentication or identification of an individual while granting access to device, data, system, service or to any other resource. This is digital identification of an individual through distinguishable, unique and specific biological characteristics. This one is comparatively very fast and reliable method of authentication.

For unique identification of an individual two categories of identifiers are considered it can be either physical or behavioral. Out of which physical biometrics comes under static approach of identification and behavioral biometrics belongs to dynamic approach of identification. For authentication purpose we have traditional methods like passwords but biometrics is faster, easier, secure and accurate method for it. But organizations which are using this as a method of authentication need to take care about security of data which is collected for authentication purpose. There are many biometric identifiers out of which fingerprints, hand geometry, face recognition, vein, retina or iris pattern recognition belong to physical measurements and voice recognition, signature dynamics, keystroke dynamics, mouse scrolling methods belong to behavioral measurements. Physical measurements remain stable throughout the life of an individual in contrast to behavioral measurement. Using both of them one can have much more accuracy of authentication. Because of accuracy and low prices of required resources like sensors, camera and software it is easy to install biometric systems. Biometric technology relies on statistical algorithms, hence so many applications are now a day using it for authentication along with other technologies likes smart card for more reliability.

II. RELATED STUDY

The work related on “Use of Biometrics in Mobile Banking Security: Case Study of Croatian Banks”[1] reveals the massive use of mobile devices in financial transaction. From the study, author finds the impact of biometric in banking environment. He further states that more biometric features in banking sector would be used to solve various social, ethical and technological aspects and to provide better security. The research paper on “Mobile Biometrics in Financial Services: A Five Factor Framework” [2] is based on a longitudinal study of users’ attitudes towards the impact of biometric authentication for digital payment and an opinion survey of a intended group of financial services professionals. The study findings are two-fold. From the study, users (>90%) trust biometrics are more secure and convenient than passwords, and that users are ready to accept biometrics instead of current password-based authentication system. As well as he stresses the use of finger print and face recognition for physical biometrics. Nevertheless, the industry survey try to fill the gaps in experience and importance on various features of deploying biometric systems: only 36% of respondents are friendly with biometrics, compared to 88% of them that would be involved in their deployment. These gaps prohibit adoption of biometrics, as they prevent effective communication. Some of the reasons for the gaps include inexperience and background (user or fraud prevention-oriented). These gaps cause a slowdown in deployment of biometric systems, as confirmed by our survey. The study on “Authentication of Smartphone Users Using Behavioural Biometrics”[3] highlights the potential risks that can arises when smart phones are stolen. Author discussed the concept of continuous authentication, and analyses current approaches and behavioural biometrics methodology such as handwaving, keystroke, touch screen behaviours, gait, signatures, voice and behavioural profiling, associated datasets and evaluation approaches. Continuous authentication method is applicable to improve security and privacy in promising areas for use of social or transactional application and touch screen behaviour in smartphone. The research paper on Biometric-A Fraud Reduction Technology in E-payment and its impact on Inclusive Growth of India“ [4] highlights the use of biometric technology to reduce financial frauds. Author suggests that biometric is useful for inclusive growth of India, to fight against corruption and bust fake workers, etc. He deeply believes that biometric is one of the securest technologies for identification and authentication for society.

The study on “A Survey on Behavioral Biometric Authentication on Smartphones”[5]states that smartphones’ sensors and accessories are used to extract behavioral attributes such as touch dynamics, keystroke dynamics and gait recognition to verify or identify users implicitly and continuously on smartphones. Active authentication system has 2 characteristics- Continuity, transparency. It consist of Data acquisition module, Feature extraction module, Feature templates, Matching and decision-making module, Mode of operations such as verification mode and identification mode, Performance metrics, Common Behavioral Biometric Traits. He also described a review of commonly used behavioral biometric traits like Gesture based authentication Keystroke dynamics, Behavioral profiling Behavioral Profiling, gait recognition are considered to design an active authentication systems on smartphones. The research on “On keystrokes as Continuous User Biometric Authentication”[6] focuses on biometric trait - keystroke dynamics. He states that in desktop platform, keystroke dynamics is used for continuous user biometric authentication. Biometric Authentication has three main phases as enrollment phase, verification phase and identification phase. The proposed Continuous User Biometric Authentication (CUBA) System takes unlimited free text input from keyboard. Unsupervised One-class Support Vector Machine is used for continuous authentication where it classifies the authenticated user's input from all the other inputs. From that data, author extracted dwell time and flight time which helps to create a user profile. Author expressed the result that shows the system is capable of detecting intruder actions. The research on "A comparative study on the application of biometric technologies for authentication in online banking" [7] deals with assessment of biometric authenticators and suggests that fingerprint and face recognition are more suitable for biometric authentication. The study further recommends the use of these biometric technologies for Online Banking purpose.

Biometric Authentication

Biometric authentication system captures individual's characteristics and keeps them inside a database. Later on at the time of verification new record or input is again captured and it is compared with existing database. If match found, then only an individual get authenticated for further processing.

In the recent years awareness and acceptance regarding this technology have been increased, as millions of Smartphone users are already using biometric authentication to unlock their Smartphone either with fingerprint or face. For many other purposes also now a day this technology is used some of them are:

i. To unlock computers or other devices automatically after authentication of user.
ii. To control entry in restricted area only to trusted system administrators.
iii. To extract appropriate information from support line of help desk system after recognizing employee's voice.
iv. To protect sensitive documents.

Behavioral Biometrics

Today's world is technology oriented where we need to perform most of the transactions online more specifically banking transactions. Major issue faced in such transactions is identity fraud. To ensure security against online fraud and cybercrime, passwords are the traditional method where as physical biometrics is a static method but to help better there is a new technology, behavioral biometric authentication, which is not only helpful in security but also useful in access or fraud prevention. Most of the industries use behavioral biometrics for payments, online banking, e-commerce etc.

Behavioral biometrics first came into exist in 1860s. People started to notice that each telegraph operator sent signals in a particular way, so they authenticate by the way they sent their messages. Today, the method is much more advanced, analyzing is done differently but the basic idea remains same. Advanced technologies are used in behavioral biometric for better security and accuracy.

Behavioral biometric is one of the authentication techniques based on behavioral characteristic of an individual, which identifies user by their unique patterns exhibited while they are using devices such as Smartphone, mouse, keyboard etc. This technique includes signature and keystroke dynamics, typing style, gait analysis, speech patterns, mouse use characteristics and cognitive biometrics.

Password and physical biometrics authentication technology focuses on user's knowledge and user's access permission, on the other hand behavioral biometrics is more advanced cyber security technology which authenticate users by focusing on, user's action and its way of performing them. Many more fraud cases found in traditional biometrics which highlights weaknesses of them, the major one is it usually authenticate user at the point of login. Solution to this security problem is behavioral biometrics which is using concepts of Artificial Intelligence. While doing online transactions it helps to perform authentication of user. This technology works in background of a session which can be web or mobile and observe many parameters of users, including the way users holds the device, the force they use when they type, and how they scroll or toggle between fields which provide continuous authentication of user throughout the online transaction and not just at the beginning. Since each user's interactions with a device are distinctive, behavioral biometrics can differentiate between the activities of an authentic user and the activities of an attacker or hacker.

Benefits of Behavioral Biometrics

Behavioral characteristics or features of an individual is not at all useful for attackers as they cannot be reused, duplicated or stolen, where as physical biometrics data which is present inside a database is vulnerable to attackers, it is very risky if it gets compromised anyhow by attackers. Cyber criminals are testing the integrity of authentication technology all the time hence risky biometric authentication technology may be vulnerable, so we need an alternative solution, behavioral biometrics is emerging as a more secure alternative noticed by many industries and becomes a form of cyber security in this digital world.

i. Accuracy

Behavioral biometric is a unique way of identifying an individual. Since there are many data points collected we can use any combination of them to identify an individual which will give us accurate and precise identification.

ii. Convenience

Here registration and authentication method is passive, which avoid an unpleasant user experience. Without disturbing the user experience it examines the behavioral characteristics of a user.

iii. Efficiency

Behavioral characteristics are extremely difficult for humans to differentiate and practically impossible to replicate when multiple characteristics are examined concurrently.

iv. Flexibility and Specificity

As per the need we can find an option specific analysis of required behavioral biometric features which can be used further easily. Depending on device used for online transaction, specific movements of an individual are tracked and used for identification purpose.

v. Improved Security

During entire online transaction behavioral biometric authentication works at background, this helps to protect internal frauds powerfully than other authentication mechanism. Physical biometrics like a fingerprint or a facial scan is easy to spoof. Each individual is having its unique way of handling Smartphone, keyboard or mouse which cannot be spoofed by hackers, which prevent identity theft and minimizes risk of online fraud hence improves security.

vi. Fast and Inexpensive Deployment

It offers easy-to-use API, which allows developers to integrate this authentication technology very quickly and easily into an existing hardware thus no need to use costly additional hardware devices, deployment cost is also low.

Online Banking without behavioral biometrics

In today's digital world mostly all financial organizations have developed online banking functionality as an easy and convenient way to manage customer's money. These changes in banking sector take away bank users from traditional banking and attract towards online banking. Online banking has developed and succeeds over the years, but is now facing key challenges due to the online banking frauds like phishing, data compromises, and other attacks. Increase in these attacks has caused a decrease in the use of online banking. Because of which customers trust in the ability of financial organizations functionality has been affected negatively. Customers are always having fear in their mind regarding safety of their money and they are expecting a permanent solution from the banks.

So now to attract the customers towards online banking, it is a tough challenge in front of financial organizations. It becomes mandatory for them to take necessary actions against these online frauds to ensure security, where authentication technology plays a vital role.

Traditional method used for user authentication and access control in online banking is password mechanism, which is not strong enough if it is the only authentication method and has found several cyber attack cases all around.

Problems in Password

Online banking has made our life easier but has also increased some amount of risks using the same. Even though the online banking sites and mobile apps are designed to be more secure and banks are constantly using higher security protocols but still online transactions can be hacked. The hackers may make use of some or the other software to guess the password which the user uses. If the passwords are weak then it may be more vulnerable to attacks. Passwords are the key to unlock our digital or online transactions.

Flaws in Password:-

i. Passwords kept are generally simple.
ii. Passwords are not complicated as the user can remember simple words.
iii. Passwords used are not generally unique for all websites.
iv. Passwords are not changed often.
v. It is very difficult to keep different passwords for accessing different resources or services.
vi. Hackers can get clue of Password through the used security questions and answers.
vii. To create unbreakable password user need to follow password policies, but password following such structure are difficult to remember.
viii. It is just a one factor authentication process.
ix. They are static in nature.
x. Password maintenance is a very big concern for system administration which includes creating, resetting, or changing user passwords.

Features of Behavioral Biometrics

Behavioral biometrics is better than other authentication system, as ones credentials can be compromised but behavior cannot be copied or replicated. The key to working of behavioral biometrics is machine learning process, which have the ability to automatically learn for themselves and improve data. A user's behavioral patterns, such as the way one holds their Smartphone, moves their mouse, or swipes their finger on a screen, are measured and recorded using sensors. Advanced software algorithms then analyze the collected data to create a profile for the user. This profile is then used to continuously check against a user who is in an online banking session. The true user will almost always match their profile, while it would be impossible for an attacker to mimic their victim's behavior. Behavioral biometrics is used for continuous authentication, risk-based authentication, insider threat detection, and fraud detection and prevention.

For Online banking transaction Behavioral Biometric can be considered as an added security layer which has the following highlighted features:-

i. Continuous Authentication

As contrast to the current Online Banking process the behavioral biometric authentication focuses on continuous authentication till the user is logged onto the website and doing the transaction. Contrastly the password Authentication which is used is done at the starting of the transaction and once the password and one time password is entered correctly the user is a considered to be a valid user and is allowed to do all types of transaction. But as we know both static password and the OTP can be compromised so it will be a better solution if a continuous process of authentication runs while using the system, this will protect the system from being hacked while actual transfer or any other important transaction is going on. As it is continuous authentication the customers are also satisfied with this type of authentication and this will surely help to improve more and more customers attract using the same.

ii. Risk Based Authentication

As behavioral biometrics authentication collects all sorts of behavioral qualities such as typing speed along with some supported features like device type, IP address and geo location. The user's historical behavioral factors, such as the typical timing of user access, patterns, etc. get stored which enable the risk of fraud in online transaction. The factors reduce the risk of an intruder who is willing to intrude in between the transaction. As the behavioral characteristics of a person cannot be copied or duplicated, even if anyone who will be trying to do so will be caught, as the pattern of his behavior will not match the pattern of a valid user. Reducing risks while using Online Transaction will also attract more customers.

iii. Fraud Detection and Prevention

Behavioral biometrics also increases the chance of fraud detection and prevention. As the user profile is recorded in the database it will allow to detect intruder if pattern does not match by using pattern matching algorithm. Fraud detection also becomes easy by using this technique as database has a huge collection of historical data. This historical data will be useful to detect the patterns or actions of an unauthorized/illegitimate user.

Behavioral Biometrics for Authentication in Online Banking

While using Online Banking procedure, the customer uses his password which he has to remember, but we know that studies have already proven that password a 1-factor authentication is highly vulnerable. Multi-factor authentication is based on more than one authentication factor. The most famous amongst the multi-factor authentication is the combination of static password which the user knows and a One Time Password generated. However the OTP which is generated is sent on the user's mobile device by SMS service or it can be also sent through the email. For doing the further transaction the user has to enter the OTP which he has received on to the banks website for completing the transaction. This technique is also not proven as one of the reliable technique. The study done reveals that there are cases of illegal tracking of one-time codes sent through SMS and then using them for fraud money transfers. SMS-based authentication has been compromised through mobile malware. Therefore 2-factor authentication on its own is also not good enough as a security tool, so there is a need to include more layers of security tools like behavioral biometrics.

Phases of Behavioral Biometrics Authentication Process

i. Enrollment Phase

The first step for authentication in the process is creation/enrollment of a registration profile where we will require to do data collection. For this step we will have to collect the different types of behavioral data from user like the keystroke dynamics which include the rate at which the user presses or releases the key. We can collect data from user by allowing him to enter username and password and all the information related with the profiling can be then captured here in this process. By collecting all the needed data a reference template can be created for the same.

ii. Authentication Phase

All the collected data should be stored in data base. This database will be used further for matching the behavioral characteristics while the user logs into the system. For matching the users behavioral characteristic with the database we can use a matching algorithm which will have correct accept ratio. ie:- The algorithm should be able to produce correct result so that the valid user should be authenticated and invalid should be restricted from entry into the system.

iii. FAR and FRR ratio

We can make use of a particular threshold value so as to select the False Accept Ratio and False Reject Ratio. FAR is calculated as a fraction of negative scores exceeding the threshold value and FRR is calculated as a fraction of positive scores falling below the threshold value. In this phase the chosen algorithm will calculate the FAR and FRR ratio by comparing the actual keystroke dynamic features with the stored historical data.

iv. Verification phase

At last, the process of verification yields two types of action: accepted or rejected user access. It will be decided by the calculated threshold value ie:- FAR and FRR ratio whether the user is legitimate or not.

Proposed Model

In digital era it is necessary that we focus all our transaction to be switched from Offline to Online. Online Transactions have greater efficiency and is also easier to use. All users of banks are attracted towards the same but are worried about the security of the transaction. If customer gets satisfied with the Authentication system and feels that it is very flexible and efficient to use the number of customers which will get attracted towards the system will increase day by day.

We propose a model which has several layers of security. Not any one scheme i.e.:- 1 factor or 2 factor authentication is fully reliable. We can combine all the advantages of different authentication types like what you know i.e.:- Password, what you have i.e.:- Token or One Time Password, what you are i.e.:- Physical Biometrics and what you do which focuses on Behavioral Characteristics. This combination will work as a Multifactor Authentication and will make the Authentication strong. This Authentication will not only work at entry level but go on working continuously till the transaction ends.

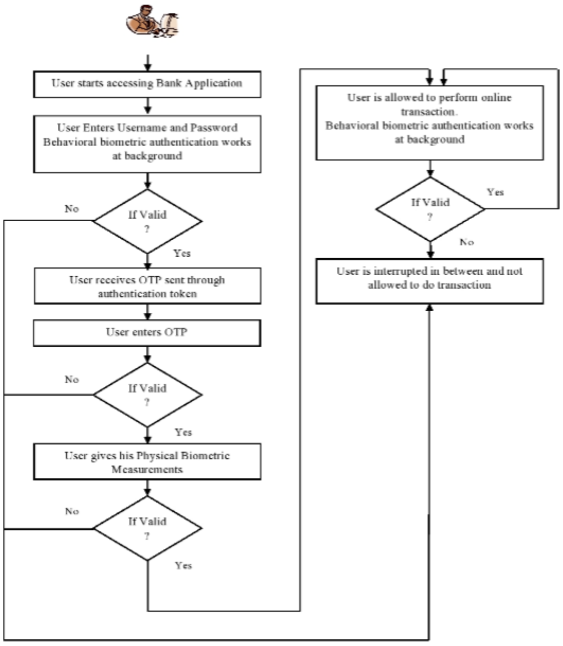
User starts accessing Bank Application
User Enters Username and Password
Behavioral biometric authentication works at background
If Valid ?
No
Yes
User receives OTP sent through authentication token
User enters OTP
If Valid ?
No
Yes
User gives his Physical Biometric Measurements
If Valid ?
No
Yes
User is allowed to perform online transaction.
Behavioral biometric authentication works at background
If Valid ?
Yes
No
User is interrupted in between and not allowed to do transaction

Fig.1: Workflow diagram for Proposed Model

The steps for Proposed Model are as follows

Step 1

The user/customer starts accessing/using the Mobile/Desktop Bank Application.

Step 2

User is first asked to enter his User name and Password. This Password will work as the first factor of Authentication which should be correctly entered.

Step 3

While making entry of User Name and password the model can keep track of user's action of how he uses the keystroke dynamics for making entry.

Step 4

After correct password entry user will get an OTP (One Time Password) which will be sent through Authentication token mechanism. This OTP will work as a second factor Authentication and it will work as what user has.

Step 5

After correct entry of OTP the user will now have to give his Physical Biometric Authentication, Which will act as a third layer/ third factor authentication scheme this scheme will work as what you are? The user will get authenticated through Face recognition.

Step 6

After the successful authentication of user physical trait he will get access to do the online transaction, while doing this the behavioral characteristics can be used. Here Keystroke dynamics, Mouse scrolling along with the extra geo location, IP address will also be checked. If all these factors match then the user will be allowed to do the transaction till the end otherwise the user is interrupted in between and not allowed to do the transaction.

Step 7

If all the behavioral characteristics match then the Online Transaction will become successful.

III. FIGURES AND TABLES

IV. CONCLUSION

Behavioral Biometrics is having more capability of efficiently implementing the Authentication system. The system Provides continuous and transparent authentication. Due to its highlighted features like continuous Authentication, risk Based Authentication and fraud detection and prevention it is more suitable in deploying it with the Online Banking transactions. As Online Banking Transactions are more Vulnerable to attacks the security of this area has become of utmost importance. Only Passwords or 2 factor authentication is not sufficient for the same. If more layers of security are added the system will become stronger and efficient. Behavioral Biometrics is dynamic form of authentication, and if deployed in current Online Banking system it will not rule out the use of password but it can act as an extra security layer for Authentication and thus protecting our sensitive and important data. Even though the procedure mentioned in above model will take some more time as compared to the traditional authentication it will be satisfied and reliable model. The future scope of applying Behavioral Biometrics is also vast it can be used not only for banking but can be also added to Online Shopping or any online delivery systems involving payments. With the massive use of AI, it is now possible to monitor behavioral anomalies and prevent security threats with much more precision. The use of behavioral biometrics will surely attract more users doing transaction Online as it will be one of the secure and reliable methods.

REFERENCES

Journal Papers:

[1]. Ammar Acdic - Use of Biometrics in Mobile Banking Security: Case Study of Croatian Banks *International Journal of Computer Science and Network Security, VOL.19 No.10,* October 2019

[2]. Giulio Lovisotto, Raghav Malik, Ivo Sluganovic, Marc Roeschlin, Paul Trueman, Ivan Martinovic - *Mobile Biometrics in Financial Services: A Five Factor Framework , University of Oxford*

[3]. Abdulaziz Alzubaidi and Jugal Kalita- Authentication of Smartphone Users Using Behavioral Biometrics 11 No 2019

[4]. Swatantra kumar, Sanjay Baijal, Arjumand Bano– Biometric-A Fraud Reduction Technology in E-payment and its impact on Inclusive Growth of India, *International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 3 Issue II, ISSN: 2321-9653,* February 2015

[5]. Ahmed Mahfouz, Tarek M. Mahmouda, Ahmed Sharaf Eldin - A Survey on Behavioral Biometric Authentication on Smartphones, *Journal of Information Security and Applications.DOI:0.1016/j.jisa.2017.10.00212* October 2017

[6]. Suhail Javed Quraishi, Sarabjeet Singh Bedi - On keystrokes as Continuous User Biometric Authentication, *International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6,* August 2019

[7]. Silvia Parusheva - A comparative study on the application of biometric technologies for authentication in online banking, *Egyptian Computer Science Journal Vol. 39 No. 4 ISSN-1110-2586* September 2015

[8]. http://www.m2sys.com/blog/financial-services/biometric-banking- technology-can-secure-transactions/

[9]. https://www.entersekt.com/news/blog/the-rise-of-biometrics-in-banking

[10]. https://www.scnsoft.com/blog/how-biometric-authentication-can-increase-mobile-banking-security

[11]. https://www.bankobserver-wavestone.com/towards-biometric-banking/

[12]. https://thenextweb.com/syndication/2019/10/02/the-case-against-traditional-passwords-and-how-biometrics-can-better-secure-us/

[13]. https://www.alliedmarketresearch.com/behavioral-biometrics-market

[14]. https://www.privateinternetaccess.com/blog/behavioral-biometrics-websites-and-apps-are-learning-from-how-you-type-hold-your-phone-and-use-your-mouse/

[15]. Behavioral Biometrics-IBIA

[16]. https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html