Impact of Behavioural Biometrics on Mobile Banking System

Lavanya Banga and Samaya Pillai*
Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, Maharashtra, India.
Email: samaya.pillai@sidtm.edu.in*

Abstract. The rise of online mobile banking systems has given customers a convenient and better way to interact with the bank as and when they want. Smartphones have revolutionized the world of payment. People now use mobile phones more often to make payments. But with increasing frauds and cybercrimes, customer experience and security become the major concern for any bank. In such situations, biometrics, especially behavioural biometrics, can be used. In this paper, we are going to discuss how behavioural biometrics can be widely adopted to reduce fraud. To increase the adoption of mobile payment acceptance, solutions need to be prioritized and reduce unnecessary obstacles. Customers demand mobile payments that are easy and quick. This is also used for fraud detection and prevention due to increased amounts of identity fraud attempts. Currently used methods for authentication such as passwords and email verification are quite problematic for security and user experience. This gives rise to behavioral biometrics. It is very important nowadays to authenticate the user throughout the session, and this is exactly what behavioral biometric do. Behavioral biometrics achieves this by invisibly running in the background and not interfering with the user experience. Fraud is significantly reduced by removing the setup authentication and risk-based authentication completely.

Keywords: Biometrics, Behavioural Biometrics, Online mobile banking system, fraud detection, security.

1. Introduction
Mobile banking is one of the most innovative breakthrough uses of technology in the banking sector. It enables the customer to use banking facilities anytime and anywhere they want using Smartphone or personal digital assistance(PDA). Banks are widely adopting this new system. This system has led to a 27 percent drop in branch usage and a 35 percent increase in the online banking system in the past few years. As more digitalization is coming into the picture, banks are getting more concerned about better customer experience and their security. To enhance the security of the customers, banks are adopting various strategies to make their transactions more secure. One such strategy is the increased use of biometrics for identification purposes. [1]. Biometrics is defined as the combination of technical aspects and scientific aspects which is used for authentication on the basis of biology and is majorly used in information assurance. In simple words, biometrics means the measurement of biological data. Biometrics is further divided into two types. The first type is Physical biometrics. This includes fingerprints, DNA, hand geometry, retinal scans. The other type is behavioural biometrics. This
includes speech patterns, keystrokes, signatures, gait. The main difference between biometrics and the rest of the authentication methods is biometric techniques have to absorb probabilities in the authentication process. Passwords, PINS used for authentication can be correct or incorrect, and people might forget it also sometimes. But a biometric scan will return only a probability of whether the scan matches or not. There is no question of incorrect scan or forgetting it. [2]. Figure 1 explains the Classification of Biometric Traits, Researchgate.net.

**Figure 1:** Classification of Biometric Traits, Researchgate.net.

### 1.1 Objective

The objective of this paper is to discuss what is behavioural biometrics and its impact on the mobile banking system. Behavioral biometrics studies the unique and identifiable patterns in human actions. Banking is one of the most important sectors of our Indian economy. Updated Security and authentication methods are of prime importance to be incorporated in that sector. The paper discusses some of the used cases of the technology as well as challenges related to it.

### 2. Literature Review

Nowadays, mobile has become an important and significant tool used by individuals for banking, budgeting, and shopping. With increased growth in mobile finance, mobile banking emerged to be a major contributor to the evolution of the banking system. Banks nowadays are more motivated and dedicated to integrating mobile banking systems. More than 15 billion$ has been invested by banks to implement a mobile banking system. This shift towards mobile banking systems can be linked with the technological breakthrough in mobile and telecommunication technology. Also, as the number of mobile subscribers increases globally, the market for the mobile banking system will see exponential growth. But still, people are hesitant about adopting this technology. Based on the KPMG International survey, which sampled nearly 4000 mobile service subscribers of 19 countries globally, only 19% of people were using mobile banking service of total mobile users. For instance, it is relative benefit, compatibility, trainability also complexity performance a major part in establishing customer attitude and willingness to adopt this new technology. Consumers are more inclined to practice mobile banking systems if they find mobile banking useful in their daily life. Another study in Singapore exposed that customers’ interest in adopting this technology is influenced in both positive and negative ways [5]. The positive impact is predisposed through the part of supposed practicality as well as social norms. As compared to e-banking systems, mobile banking systems have seen rapid growth. With a mobile banking system, customers can access the facility for 24 hours. In Makassar, going to a bank branch is still a common practice for people. However, with the change and evolvement of mobile technology and internet technology, financial services have also seen a rapid change. Now, most banks in Makassar have introduced mobile banking systems to decrease transaction costs and improve operations. With all these improvements still, people are hesitant to adopt this technology. The negative impact of this technology is caused by increased perceived risks. The customers’ anxiety
regarding safety matters and initial cost concerned with internet connections [3]. These were the key hindrances in the adoption of the mobile banking system. To eradicate this negative impact, it is essential to understand the factors that affect customers’ acceptance of the use of mobile banking systems. Some variables are required to be analyzed and studied to frame out strategies for adopting mobile banking systems. These variables come from a framework called the Technology Acceptance Model (TAM). [4] It was developed in 1989. This model is considered appropriate for effectively identifying the factors that have an impact on user acceptance of information technology. The model was developed based on the Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB). TAM considers two main aspects:

i) **Perceived Usefulness (Pu):** defines the usefulness of the system as seen by the user. It also signifies the user will continue to use that system until he starts perceiving the system as not useful in the future.

ii) **Perceived Ease of Use (Peou):** defines the level where a user feels that by using a particular system, they have reduced their efforts.

The Effects of external variables such as system characteristics, development process, testing, etc., are all mediated by the above-mentioned factors. Moreover, according to TAM, perceived usefulness is influenced by perceived ease of use, keeping all things constant. In simple words, the things which are user-friendly are likely to be more useful. According to many empirical tests of TAM, perceived usefulness has emerged and has a very strong determinant of usage intentions, with standardized regression coefficients being around 0.6 [5].

### 3. Proposed Method Content

Biometric authentication is used in two ways: identification and verification. Figure 2 depicts the concept of Identification Vs Verification, Slideplayer.com. Identification can be defined as the process of identifying a person by matching a current trait with the unique biometric pattern stored in the database. Whereas verification can be defined as the process that validates a person's identity by trying to match his/her biometric data with already captured biometric data templates, which are stored in a database of a system.

**Figure 2: Identification Vs Verification, Slideplayer.com**

#### 3.1 How Does Biometric Works?

The biometric sample is taken and captures features and is then processed for unique feature extraction that corresponds to a particular person. The biometric sample is then matched with the unique features saved in the database. The saved biometric sample matches, then the decision is taken that the user is authorized, and if the sample does not match, the user is then unauthorized.

#### 3.2 Why Biometrics over a traditional security system?

With the advent of machine learning and increased security risks, the need to change existing security methods arises. The major issue with existing password security methods is restrictions in maintaining
and securing them. If the passwords reach malicious hands, all personal, financial data could be at risk of exposure. Nowadays, frauds are of immense concern to any organization. To reduce this fraud issue, biometrics has been widely adopted nowadays. [6]

There are basically three ways of possible ways of proving one’s identity:

- Something which we possess: This includes a card, document, certificate, etc.
- Using something which we know: This consists of passwords, names, etc.
- Through what we are: Fingerprints, Hand, Face, the voice comes under this category

The first two ways can be easily lost or forgotten and can also be replicated. The third type cannot be replicated and is also preferred, which makes the system more protected and reduces the chances of hacking. This is called a biometric system and can be classified into First Generation and Second Generation. The first generation biometric utilizes attributes that are easily seen with the naked eyes, such as Face, fingerprints, hand geometry, etc. [7] Whereas second generation biometrics consider those characteristics which do not need much human cooperation and can run in a "transparent" and invisible manner. The most commonly used first-generation or physiological modalities used are:

**Fingerprints:** This is the longest-serving, successful, and widely accepted method for person identification. There are regular textured patterns composed of valleys and ridges on the fingerprints. These ridges are distinguished by several mark points called "minutiae". Figure 3 illustrates the Finger. The spatial distribution of these minutiae points is unique to every Finger. This collection of minutiae is used to match two fingerprints.

![Figure 3: Finger](image)

**Iris:** Is responsible for controlling the diameter, size of the pupil, and also the amount of light reaching the retina. Not only fingerprints, but iris also has complex texture patterns with numerous individual attributes like stripes, pits, etc. Figure 4 explains the IRIS. This allows for highly reliable personal identification.

![Figure 4: IRIS](image)

**Hand Geometry:** The shape of the hands can also be used to discriminate between individuals. Low-resolution hand images can be used to extract a person's identity. Figure 5 explains Hand Geometry.

![Figure 5: Hand Geometry](image)
Veins: The blood vessel pattern beneath the skin is well defined. The vascular pattern is spread throughout the body as the main function of the veins is to carry blood to all body parts. Figure 6 denotes the Veins. Hand veins are easy to acquire as they are present in hands, i.e., palm, Finger, and are also easy to obtain. Veins are usually stable for adults but with age start to shrink.

![Figure 6: Veins](image)

Face: Humans can very well identify their colleagues by their facial appearance. It acts as a natural human trait for automated biometric recognition. For facial recognition, a spatial relationship between the location of facial features such as eyes, nose, etc., is used.

![Figure 7: Face](image)

The second-generation biometric systems aim to identify the audience according to their actions and behaviours. Figure 7 denotes the Face. This kind of system is difficult to trace and will not compromise system security. A second-generation biometric system can be useful in keeping track of the legitimacy of an individual without asking them to prove their identity. The most commonly used behavioural modalities are:

Voice: Individuals are identified based on their speech pattern and voice. The human voice is generated by a combination of behavioural and physiological features. Figure 8 demonstrates the behavioural components of voice, which are made of the movement of lips, jaws, and tongue, and larynx may change due to medical conditions such as cold or cough or with age. Where, the shape of lips, mouth, and nasal cavity is responsible for the generation of psychological components of voice.

![Figure 8: Voice](image)
Signature: This is a biometric modality that is widely used for business activities. Attempts are still going on to develop a highly accurate signature recognition system is shown in Figure 9. To improve the signature recognition system, attempts have been made to develop a pressure-sensitive pen-pad.

![Signature](image)

**Figure 9: Signature**

Keystroke: Dynamics and rhythm in which an individual type on the keyboard can be captured. Figure 10 explains the systems extract many options from the user's typewriting pattern to use a single classification for user behaviour analysis, so we are able to observe unauthorized users.

![Keystore](image)

**Figure 10: Keystore**

Voice Signature Keystroke depending upon the criticality of the business applications, both first and second-generation biometrics can be used in a combined manner. This will ensure a layered structure of security and improve the effectiveness and efficiency of the system.

3.3 Advantages of Biometric System.

i) Quick and accurate identification and authentication

ii) Accountability at its best

iii) Highly efficient

iv) Convenient

v) Security and Profitability

vi) Additional capacity to accommodate growth

vii) Easy to operate and user friendly [8]

3.4 Factors to Decide Right Biometric System

Choosing the right biometric modality is the first step to ensure the success of a biometric system. Many modalities are available, such as fingerprints, hand geometry, face recognition, signatures, voice, keystroke, etc, but they can't be used in every situation. Every organization requires a different modality. The factors which are considered before deciding which modality to choose are:

**Accuracy:** It is one of the most important aspects to access while choosing a biometric system. There are several criteria such as error rate, false acceptance rate, identification rate, and also false rejection rate.

**Anti-Spoofing Capabilities:** The possibility of direct attacks has increased where intruders gain access to the system by interacting with system input devices. These types of attempts are commonly referred to as spoofing attacks. Right biometric modality must have a strong anti-spoofing capability.
Acceptability: User acceptability plays a vital role in the implementation of any biometric modality. Some biometric modalities might have some stigma associated with them and can hence create some negative impact on user perception.

Cost Effectiveness: The cost of the biometric modality is very important before its deployment. Based on the underlying technology and hardware characteristics, some biometrics modalities may be more cost-effective than others.

Hygiene: Contact-dependent biometric hardware is an important factor before making a decision to select a biometric modality. Many organizations prefer to use contactless biometric modalities for hygiene purposes. [9]

4. The Era of Behavioral Biometrics

In order to balance the act of security and to enhance the customer experience in mobile payments, behavioral biometrics has gained popularity for authentication. The evolution of machine learning and artificial intelligence and the need for replacing passwords has made behavioral biometrics a feasible choice. A new generation of software solutions is provided by behavioral biometrics for the customers. People are identified based on their unique behavior with Smartphone, keyboards etc. which can be used to confirm an individual’s identity on subsequent interactions.

4.1 What Is Behavioral Biometrics?

The measurement and recording of human behavioral patterns and use them to verify and authenticate individuals either in real-time or backdated. This biometric system focuses on how an individual conducts a specific activity rather than the activity’s outcome is shown in Figure 11. For example, the user name and password are entered correctly, but how does a user enter them: are they typing fast or slowly?

![Behavioral Biometrics](https://paymentscardsandmobile.com)

Figure 11: Behavioral Biometrics, paymentscardsandmobile.com

By 2022, the recent behavioral biometrics market is expected to grow from USD 4.03 Billion in 2015 to USD 9.33 Billion in 2022 at a CAGR of 29.3% between 2016 and 2022 is shown in Figure 12. [10] Also, Behavioral Biometrics Market by region, 2023, Marketsand Markets Analysis is shown in Figure 13.

![Recent behavioral biometrics market between 2016 and 2022](https://paymentscardsandmobile.com)

Figure 12: Recent behavioral biometrics market between 2016 and 2022
4.2 Key Driving Factors
The market’s major growth factors include a surge in online transactions and suspicious online activity around the globe and also a growing need for the multi-layered approach to security in the finance sector.

i) Market growth aspects include increased security over traditional biometrics and better compliance with AI technologies.

ii) Major applications such as identification and access control, fraud detection and protection management, risk and security management also fuel the demand for behavioral biometrics

4.3 Why Behavioral Biometrics In Banking Facility?
In this digital age, fraud is of immense concern for any organization. Cybercriminals target businesses across all sectors and try to gain access to customer’s wallets. Banks, as well as financial organizations, are between utmost required marks afterward for fakes. Most current fakers concentrate their attacks on energetic online account holders. Fakers might sensitively operate account holders by undoubted them to readily provide their login credentials. Thus, Banks also other financial organizations want to ensure the security of their online platforms and also facilitate ease of use. Many organizations opt for cost-effective and sustainable solutions that are not cybercriminals centric however the authentic account holders they objective. This is the basis of behavioral biometrics. Using this technology, banks closely monitor the everyday activity of the user and compile separate behavioral reports for every individual. Machine learning is used on this data to equate and distinguish recognized account holder traits with real-time portal activities. All these steps reduce user-interface friction. Inner working of the software is quite complex. Countless user behavior is tracked, such as typing speed, scrolling speed, etc. All this forms a reliable digital account holder profile, which machine learning uses to equate to the functions of fakers- most of them who engage either in strange account management activities. At the foundation of behavioral biometrics, the monitoring components have almost no impact on the account holders. The majority of the users have no idea that many sensors are recording their activities. This technology was launched in 2016 by The Royal Bank of Scotland. After testing the platform, they provided solutions to 18.7 million of its customers in 2018. [11]. Table 1 explains the comparison of various biometric techniques with their strengths and weakness.

4.4 Use Cases: Wells Fargo
Allows commercial clients to view bank account balance, make deposits and approve payments according to their convenience from mobile devices. Along with security features such as encryption, secondary authentication, token generation, an additional security feature of biometric eye print is also included in the solution. The users can sign in by scanning their eyes with the camera on their mobile devices. This authentication eliminates the need to remember the passwords, thus making signing in easy and secure.
4.5 Citi

In 2016, Citi deployed voice biometric authentication from NICE to recognize customers from their voice in the first few seconds of their conversation. The software used for this securely authenticates customers in real-time and also reduces service time, meanwhile improving fraud protection. This type of authentication is largely deployed in the U.S. Customers are usually routed to the appropriate agents to address their issues, but if they are calling for something else, they are directed to the right person without their identity being authenticated.

| Biometrics | Universality | Uniqueness | Permanence | Collectability | Performance | Acceptability |
|------------|--------------|------------|------------|----------------|-------------|---------------|
| face       | H            | L          | M          | H              | L           | H             |
| fingerprint| M            | H          | H          | M              | H           | M             |
| hand geometry | M       | M          | M          | H              | M           | M             |
| voice      | M            | L          | L          | M              | L           | H             |
| iris       | H            | H          | H          | M              | M           | L             |
| retinal scan| H           | H          | M          | L              | H           | L             |
| signature  | L            | L          | L          | H              | L           | H             |
| dna        | H            | H          | H          | L              | H           | L             |

4.6 Security Risks in Behavioral Biometrics

**Spoofing:** Biometrics systems can be misled sometimes by applying fake biometrics.

i) Replay Attacks: Duplicate images can be injected into the system, thus outwitting the sensors.

ii) Substitution Attacks: If a fraudster gets access to the storage, the legitimate user’s data can be overwritten.

iii) Masquerade Attacks: From a fingerprint template, a digital image is produced. This image, when submitted to the system, matches will be produced. Figure 14 explains the Bird’s eye view of the Biometric Mobile Transaction System.

![Figure 14: Bird’s eye view of Biometric Mobile Transaction System](image-url)
4.7 Other Challenges
Mobile application development is the basic component of mobile communication systems. For developing a sustainable mobile application, good amounts of hardware and software are required. With increased utilization of these components, challenges to gather them together also increase. Apart from the above-mentioned challenges that behavioral biometrics Face, there are some challenges that occur while developing mobile applications also [15].

4.8 Hardware Related Challenge
i) Cross-Platform Compatibility: It has now become imperative for mobile companies to develop applications that are compatible with various mobile devices and also perform cross-platform compatibility. This allows developers to have a proper analysis of hardware, software, and technology before implementing anything.

ii) Varying Hardware Complexity: The hardware of the mobile system keeps on changing with respect to memory, speed, graphics, processing, etc. There is a significant difference between processing speed, computational speed, etc., of mobile and desktop [14]. This is the major concern for the developers. It is challenging for the developers to maintain mobile applications as error-free.

4.9 Software Related Challenge
i) Inexperienced Resources: Style guidelines and behavior of each mobile device are two important things that need to be followed while developing mobile applications. Very few people, less than 10% participants, accepted concern for lack of knowledge with respect to this aspect.

ii) Insufficient & Uncertain Requirements: Due to this, the workload on the participant’s increases drastically as they spend a lot of time initially understanding the client's requirements.

iii) User Experience: Mobile devices and desktop devices are different from each other. Smaller display, screen layouts, etc. have a major impact in developing mobile applications. Developers have to be careful while implementing anything in both the electronic and devices to ensure an efficient user experience [12]. Figure 15 explains the Mind Map of the System.

![Figure 15: Mind Map of the System](image)

4.10 Content Analysis Performed on the Research Paper
The author performed a content analysis on the research paper using the tool lexical and sea scout. The findings are shared as follows in Table 2 [13].
Table 2: Content Analysis

| Content Analysis |
|------------------|
| **Word Count**   | 3944 |
| Character Length | 25813 |
| Letters          | 21286 |
| Sentences        | 381  |
| Syllables        | 7305 |
| Average Words/Sentence | 10.4 |
| Average Syllables/Word | 1.9 |
| Lexical Density  | 54%  |
| Lexical Diversity| 31%  |

The Keyword density can be depicted as follows in Table 3 and Table 4.

Table 3: With 3 keywords

| keyword                                | word_count | uses | density |
|----------------------------------------|------------|------|---------|
| impact behavioural biometrics         | 3          | 1    | 0       |
| behavioural biometrics mobile         | 3          | 1    | 0       |
| biometrics mobile banking              | 3          | 1    | 0       |
| mobile banking system                  | 3          | 8    | 0.2     |
| banking system [1]                     | 3          | 1    | 0       |

Table 4: With 2 keywords

| keyword                                | word_count | uses | density |
|----------------------------------------|------------|------|---------|
| impact                                 | 2          | 1    | 0       |
| behavioural biometrics                 | 2          | 6    | 0.1     |
| biometrics mobile                       | 2          | 1    | 0       |
| mobile banking                         | 2          | 23   | 0.5     |
| banking system                         | 2          | 10   | 0.2     |
| system [1]                             | 2          | 1    | 0       |
5. Conclusion
User experience is the core need of all mobile users. All companies want to enhance their customer experience to get an edge over their competitors. To make this happen is not an easy task. There has been a paradigm shift in the preference of the customers, from swiping cards for making payments to using mobile banking payments. To increase the adoption of mobile payment acceptance, solutions need to be prioritized and reduce unnecessary obstacles. Customers demand mobile payments that are easy and quick. Not only this, but they also demand a high level of fraud detection and prevention due to increased amounts of identity fraud attempts. Currently used methods for authentication such as passwords, email verification is quite problematic for both security and user experience. This gives rise to behavioral biometrics. It is very important nowadays to authenticate the user throughout the session, and this is exactly what behavioral biometric do. Behavioral biometrics achieves this by invisibly running in the background and not interfering with the user experience. Fraud is significantly reduced by removing the setup authentication and risk-based authentication completely. By doing this, users can do more during the session. The bottom line is, the future of payments is mobile. Frictionless experience is what users demand. In a world full of ever-increasing risks, continuous authentication is the only solution to reduce this, and so behavioral biometrics will grow. Many different and unique behavioral attributes can be combined as used to identify the user throughout the session.

References
[1]. N. Benari, “blog.securedtouch.com,” December 2017. [Online]. Available: https://blog.securedtouch.com/why-the-future-of-mobile-payments-lies-with-behavioral-biometrics.
[2]. K.-C. Claus May 2018. [Online]. Available: tps://www.ey.com/en_in/digital/how-biometrics-could-finally-replace-pins-and-passwords-when-we.
[3]. Y. K. D., N. P. R. Ali Abdallah Alalwan, “Factors influencing adoption of mobile banking by Jordanian bank”.
[4]. A R. Minur, “Acceptance of Mobile Banking Services in Makassar: A Technology Acceptance Model (TAM) Approach”.
[5]. V. Venkatesh, “A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies”.
[6]. June 2020. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics.
[7]. A K. Anil K Jain, “Biometrics Of Next Generation - An Overview”.
[8]. M. Ghadawala, “globalsign,” June 2019. [Online]. Available: https://www.globalsign.com/en/blog/7-benefits-security-with-biometrics.
[9]. M. Hassan. [Online]. Available: https://www.m2sys.com/blog/biometric-hardware/5-factors-consider-choosing-best-biometric-modality/.
[10]. “paygilant,” September 2018. [Online]. Available: https://paygilant.com/blog/p2p/behavioral-biometrics-and-mobile-payment-security-highs-and-lows/.
[11]. M. Chrobok, “Buguroo,” [Online]. Available: https://www.buguroo.com/en/blog/behavioral-biometrics-in-mobile-banking-applications.
[12]. X. W., S. V. C. Harleen K. Flora, “An Investigation into Mobile Application”.
[13]. “lexicool,” [Online]. Available: https://www.lexicool.com/text_analyzer.asp.
[14]. Aslam K A, Smart Reading System For Visually Impaired People, International Journal of MC Square Scientific Research, Vol. 9, No. 2 2017.
[15]. Subha K and Kushal Reddy P, Data Sharing in Cloud Computing Based On Attribute-Based Encryption System, International Journal of MC Square Scientific Research, Vol. 9, No. 2, 2017.