Educational Administration: Theory and Practice
2020, 26(4) 954 – 964
ISSN: 2148-2403
https://kuey.net/

Research Article

Biometric Authentication In Digital Payments: Utilizing AI And Big Data For Real-Time Security And Efficiency

Chandrababu Kuraku[1*], Hemanth Kumar Gollangi[2], Janardhana Rao Sunkara[3]

[1*]Sr. Solution Architect, ChandrababuKuraku@outlook.com
[2]Software Consultant, HemanthKumarGollangi12@outlook.com
[3]Sr. Database Engineer, JanardhanaRaoSunkara@outlook.com

Citation: Chandrababu Kuraku, .et.al. (2020). Biometric Authentication In Digital Payments: Utilizing AI And Big Data For Real-Time Security And Efficiency *Educational Administration: Theory and Practice, 26*(4), 954 - 964
Doi: 10.53555/kuey.v26i4.7590

ARTICLE INFO | **ABSTRACT**

Biometrics is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometric authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. The basic premise of biometric authentication is that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioral traits. It allows us to capture biometrics or personal information and make digital payments fast. For the sake of digital banking, biometrics pointed the way to reinvest the identity verification process automatically into a system. As a result, financiers no longer have to substantially subdivide themselves from their customers, especially when ascertaining identity. A procedure that used to take weeks or months has now been reduced to a matter of minutes if not seconds. As an efficiency bid, it is orders of magnitude more efficient than any human could ever be to preserve the verification process by using existing biometric data. Biometric identifications are discrete physiological or behavioral characteristics that can be measured to identify a person. Digital payment alternatives are gradually replacing the traditional ways of transactions. Biometric authentication is based on inheritance and specific characteristics and is considered to be more secure compared to traditional PIN methods. Fingerprint recognition is the most common biometric identification available in various smartphones. Replacing traditional signatures with more secure and efficient fingerprint verification leads to the automation of the KYC process in the banking system. In this paper, readers will understand the working and potentiality of biometric authentication with the help of Artificial Intelligence (AI) and Big Data for correctness purposes. This paper will help non-technical readers understand the concepts and power of intelligent AI used in banks for KYC purposes.

Keywords: Biometric Authentication,Digital Payments Security,AI in Payment Systems,Big Data Analytics,Real-Time Fraud Detection,Secure Payment Solutions,Machine Learning for Security,Real-Time Authentication,Payment Fraud Prevention,Biometric Data Privacy,AI-Driven Security,Big Data in Financial Transactions,Advanced Payment Technologies,Fraud Prevention Algorithms,Biometric Verification,Real-Time Risk Assessment,AI Security Algorithms,Biometric Payment Systems,Digital Identity Verification,Data-Driven Security Solutions,Secure Payment Authentication,Adaptive Fraud Detection,Biometric and AI Integration,Financial Data Protection,Smart Payment Security.

1. Introduction

The use of biometric authentication systems has permeated into almost every aspect and culture of life. Biometric systems have been used across many industries for both commercial and legal purposes like identity, seeding such biometric modalities like fingerprint technology for old or elderly people. This technology focuses on what makes users for old people stand out, their faces, eyes, and voice. All these can be put together in a payment system solution hence making it easier and efficient for users to conduct a lot of transactions within a very short time as compared to what it used to be. These solutions are expected to perform specific characteristics and requirements like speed, robustness, universality, permanence, no capability of performance replication, resistance, and so on even in a variety of transaction settings. One major component of each successful transaction is the biometric component which offers real satisfaction as stated by relevant agencies. Some of these factors will be taken into consideration in this project. Moreover, there are major differences between biometric technology/solutions and other forms like cards, digital methods, etc., in terms of human behavior since biometrics has a direct relationship with the human body. Hence the biometric authentication system in the digital payments sector is considered as a very strong system that provides an appropriate level of customer satisfaction. The biometric is the measurement of physical or behavioral patterns which can be transferred into machine-readable codes or data. Biometric firms are offering a variety of hardware and software and many others are currently offering biometric bank cards. These biometric vendors intend to improve digital transactions among old people. An example is the first biometrics bank card created in the UK, launching Barclays to address the growing threat of fraud and enhance clients' everyday payments. The advent of digital technologies and the internet, as well as the increase in the number of smartphones, has laid the groundwork for digital payments. Customers can scan a QR code to make a payment, pay digitally at the POS using NFC or QR codes, send requests for money to friends, pay merchants through an unstructured fee request, and execute many other tasks. Hence, digital transactions have grown to form an alternative that is faster and more useful for customers compared to physical methods of transacting. However, one of the key challenges that digital transactions face is security. Therefore, a payment system that uses biometrics on an unsecured channel while making payment will make it impossible for anyone masquerading as you to carry out a transaction. As such, the government and appropriate authorities around the world are working to use a biometric-based authentication system.

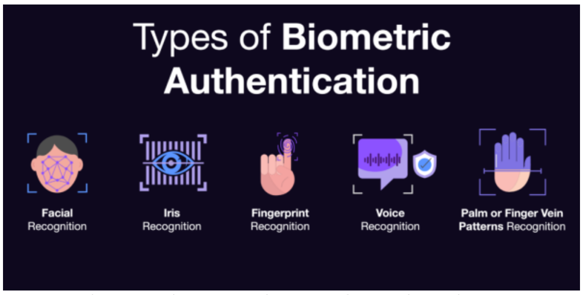

Fig 1 :Biometric Authentications

1.1. Background and Significance of Biometric Authentication in Digital Payments

Biometric authentication has been widely scrutinized in the last few decades, and substantial research and development of biometric authentication systems have been conducted. Facial, fingerprint, iris, hand geometry, and behavioral biometrics are some of the most important biometrics that have proven to be useful in practice. Biometric security systems, which have evolved considerably in the era of artificial intelligence (AI) and big data analytics, can achieve higher accuracy, identification speed, and convenience with lower operational costs. In addition, a low-cost device can be employed to capture a biometric, since we can access the internet on almost all devices. For this reason, biometric technologies for security and authentication in digital payments are extremely significant. Therefore, the corresponding research and review article demonstrates this fascinating field and its technological processes, such as its advances, significance, and features.In terms of security, biometrics is a cutting-edge technology often applied for authentication due to its accuracy and uniqueness. This paper will specifically concentrate on the application of biometric technology in digital payments. Digital payment methods have already made access to formal finance easier and more manageable, and with this trend of cashless transactions, instances of fraudulence in digital payments are also surging. In many existing digital payment systems, including credit cards, online banking, and mobile payment systems, one of the main security measures implemented is password-based authentication. Nevertheless, people are typically imprudent and use weak passwords. Thus, password theft, also referred to as account takeover fraud, is a rampant problem all over the world. As users do not have to recall passwords, employing biometric authentication ensures that only verified, proper credential holders access secure areas.

2. Biometric Technologies in Digital Payments

There are various biometric technologies of biometric recognition modalities that are available for digital payment users. A summary of some recognized and commonly used biometric technologies is discussed in this paragraph. These technologies include fingerprint recognition, facial recognition, iris recognition, and voice recognition. Customers in authenticated digital payments typically require one of these modalities. Highly secure devices that have proper security measurements properly implemented can support multimodal biometric technologies. A multimodal biometric technology can provide any form of security when both or more biometrics are checked. A system such as an ATM can use two biometric technologies to enroll or verify a customer when he or she acquires an ATM card and opts to operate the ATM using fingerprint and iris technologies. The fingerprint enrollment is managed to verify the customer, and if the iris is checked, the enriched digit of the customer is available on the credential card for security verification.

In mobile and web payments, biometrics technology for user authentication serves as an extra protective layer and replaces tokens and cards with a biometric profile. Touching the home buttons of smartphones, users can confirm their identity through fingerprint authentication. Various digital payment services also use face recognition for user verification. In addition, iris recognition is mainly used in Android mobile devices, including mobile payment banking apps, passport apps, and others. Voice is another modality used in digital payments. Apple Siri, Microsoft Cortana, Google Now, and others have voice authentication systems to interact with mobile phones to execute some processes such as depositing or paying with a voice command like "Siri, pay with Zelle." This section is intended to enrich our readers with a full list of biometric technologies in digital payments. The following parts of this section are dedicated to the in-depth description and application examples of fingerprint recognition, facial recognition, iris recognition, and voice recognition in the domain of digital payments.

2.1. Fingerprint Recognition

Fingerprint recognition, with efficiency and accuracy, represents an alternative means for digital transaction security. Although the verification of a fingerprint cannot guarantee the authenticity of any transaction, it ensures the identity of the one who conducts the transaction. Biometric recognition is something that is neither forgotten nor stolen;

Therefore, fingerprint recognition provides a quite secure

and efficient method for payment authentication and trust. Consequently, AI-based fingerprint recognition is to transform a pattern of thin dark lines into a small amount of biometric data for recognition. Fingerprint recognition has to be accurate to ensure the true identity of customers. In addition to enhancing security, the elimination of POS-based digital payment paperwork and digitized wallet passcodes allows faster and easier digital payment, especially in a retail environment like Walmart.

Fingerprint recognition is a widely recognized biometric technology that compares a captured image of a fingerprint to the user's known fingerprints stored in the system. Features such as ridge endings, bifurcations, and ridge shape form minutiae to be extracted from fingerprints. Minutiae are recognized for their specific pattern and used for authentication. Depending on the type of data digitally stored in the fingerprint scanner machine, fingerprint recognition techniques could be categorized into two types, namely, the optic fingerprint machine and the semiconductor fingerprint machine. The optic fingerprint machine stores the digitized image of the fingerprint as well as performs the fingerprint matching task on the image, while the semiconductor fingerprint machine uses the model of the fingerprint as pre-processed data and not a model of the digitized image, and hence there would be no need to perform an intensity transformation which leads to space saving and a fast transaction due to employing a smaller digital model for the construction of the fingerprint images.

Fig 2 : Biometric technology

2.2. Facial Recognition

Facial recognition has one primary application for payment actors, and that application is to speed up payment authentication. It has to be noted that the primary alternative to facial recognition payment authentication is either to pay by cash/raise a credit/debit card or use a password-based digital payment solution to finish the transaction. Unlike fingerprints again, facial recognition simply doesn't fit in a smooth customer payment flow. Accepting such payments cannot be frictionless. It might take a few seconds to capture, analyze, verify, and confirm the person's facial biometric. This sub-second verification or payment validation can happen only when the customer voluntarily looks at the camera, to begin with, and such consent to capture the image from the camera is included in the mobile application end-user license agreement. Thus, it can be said that biometric recognition has its unique features and applications, enhancing the security and efficacy of digital transactions.

Biometric technology has permeated into almost every major industry on the global landscape, and digital payments are no exception to this. Facial recognition has emerged as a prominent biometric technology in digital payments, with Alibaba's Ant Financial having rolled out a "Smile to Pay" service in March 2017 at various KFC outlets in Hangzhou, China, where a smile at a search helped unlock a self-service process to avoid scams. In a similar context, Alipay also began an offline facial recognition payments system with KFC in China in September 2019. Essentially, facial recognition captures, analyses, and compares a person's unique facial characteristics, typically in value-driven services like border control, security access, and payment.

2.3. Iris Recognition

Iris recognition provides the best verification and time-dependent results using the Hamming distance, inclusive of both wearable and handheld verifiers, optimizing the highest volume of iris vectors per second, resulting in a match score. Thus, in a payment transaction, biometrics acts as a decisive approach over classical physical evidence that allows issuers to make a real-time identity decision resulting in card authorization. In a real-time entity, the system's speed shows the trade-off between the data capacity, the template size, and the quality of the biometric data. Biometric systems require a significant amount of data for the template because additional details are needed to improve accuracy, but they also need to minimize the size of the template to reduce the time required to calculate the matching result. In real-time matching, a micro-engine executes minutia or feature template comparisons with the pre-registered biometric data. Thus, in a digital payment system, using real-time entities makes systems more efficient by operating a wearable or handheld device closer to the eye instead of a separate server utility for backend synchronous matching. Each of the systems has fixed a threshold score, and the matching score is compared with it for verification. The digital payment system uses a single biometric matching system, which gives a matching indicator, and if the two indicators match the transaction, then it turns to authorize the payment. The score is above an acceptance threshold. Consequently, iris technology gives a real-time scoring performance for both payment transactions.

Iris recognition as a biometric trait has recently gained attention from the industry due to its almost invariant nature, extremely low False Rejection Rate (FRR), and very low False Acceptance Rate (FAR). During the process of iris recognition, the near-infrared light falls on the pupil and the cornea, which are present in the front of the eye. The working of the iris recognition system is based on the following steps: The light reflected from the iris's texture is captured by the high-resolution camera. The captured image is further processed to segment the circular iris region from the rest of the eye. The pupil is also detected and normalization is performed to compensate for variations in iris size. After normalization, the iris is split up into several layers. The segmentation of the iris is based on the bright circular pupil spot derived from the specular reflection of a light source. The extracted iris is further processed to generate feature vectors. In essence, the feature sets are abstracts obtained as the result of a trained filter acting on the image contents. This results in a set of values that reflect the combination of the factors analyzed by the trained model. It is further used in searching a gallery of the feature vectors extracted from the previous transactions and also in the current search. The final step involves verification and ultimately the decision based on the number of feature points that match; if there is a match in previously enrolled data, the transaction is granted, otherwise it is rejected. The availability of the real-time matching system, running in a standalone or connected mode to the central system during the transaction process, significantly speeds up the overall verification process.

2.4. Voice Recognition

Voice recognition is receiving worldwide attention from renowned research institutions as an effective way to secure financial digital transactions and customer personal privacy. Research scholars are making strides in the development of voice recognition technology by adding big data and artificial intelligence (AI) characteristics to the existing voice recognition technology. Big data is used to train the voice and facial recognition algorithms to realize reasonable and integrated image understanding and dynamic face and voice matching. The true positive and false positive rates of voice recognition have been improved by utilizing the rich data supplied by the function of big data. This new voice recognition method has successfully increased the hit rate while limiting the non-hit rate, effectively enhancing the system's safety and efficiency for detecting payments.

Another up-and-coming sector in the field of biometric technologies is voice recognition. A lot of complex processes involved in the collection of voice samples, such as user registration, speech extraction, feature extraction and commitment, and recognition pose challenges that are difficult to surmount. These process efficiencies and complexities are applied to a range of their corresponding applications. Most importantly, voice is also one of the biometric technologies in digital payments. The majority of digital assistants in payment applications are digitized for ease of use by their users, and their primary applications are biometric systems and digital transaction security.

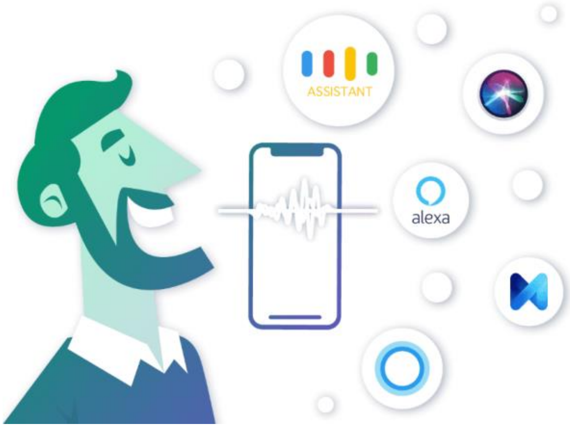

Fig 3: Voice Authentication

3. Integration of AI and Big Data in Biometric Authentication

Machine learning algorithms are used to design and develop the biometric template generation and verification unit since, daily, the related data become enormous in volume, variety, and velocity. A big data storage device, a NoSQL server, is set up on different computer systems to store this data. Furthermore, various transactions occur in the payment system. Each transaction forms a data set of multiple attributes known as the template. Then the machine learning algorithm is executed to construct the relevant problem field in the field of the training data. At the final layer, all the work is integrated into an AI model system to execute the entire work process, generating the output according to the required model. Furthermore, the AI biometric authentication collects the representative data in association with user accounts and, using templates, matches the testing features data with the registered template. Moreover, the similarity measure method is applied to compare the testing features, and utilizing the similarity threshold verifies as zero or one.

In the digital world, identity verification has become an important issue, and biometric technologies such as fingerprint, face recognition, and eyeball scans are receiving increasing attention as a method of identity verification in financial digital services. These biometric technologies have several weaknesses such as being easy to modify and replicate by malicious users. To improve the security of biometric verification, research into biometrics using ECG (Electrocardiogram), which is difficult to forge, has been conducted. In a digital financial market using the ECG biometric method, enormous workings, and real-time processes should be executed since interruptions in the sector lead to unfair losses to users. To provide the fast and efficient biometric authentication system required by a payment-processing financial firm, AI (Artificial Intelligence) is employed, and, in terms of the large amount of data in these processes, big data is also being used.

Technology, AI, and big data play a crucial role in the development of the field of biometric authentication. How are these technologies introduced in the realm of biometric authentication and utilized in this section?

Fig 4 : Artificial Intelligence (AI) Is Used In Biometrics

3.1. Machine Learning Algorithms for Biometric Data Analysis

Another group of machine learning algorithms can be termed self-learning, as they can automatically build their models from raw data. Although the majority of machine learning frameworks are conceptually similar, each is governed by a distinctive algorithm. Some of the most common methods for both supervised and unsupervised learning include Artificial Neural Networks, as seen in deep learning systems. Initially, the inputs are calculated using initial weights. These inputs are then modified iteratively until the outputs closely resemble the specification. The advances made in this area have been phenomenal thanks to the convergence of big data-driven analytics, deep learning, and other machine learning techniques. To utilize biometric data for authentication, the concept for training such algorithms is based broadly on the distance computed between analyzed data and the gallery. The gallery serves as the authentic or genuine database meant for comparison. Moreover, many of these algorithms can be continuously trained by updating them in real-time.

Artificial intelligence plays a significant role in the authentication process with biometric data. Machine learning algorithms process millions of input parameters to recognize a certain image or sound. These parameters or attributes are automatically created by the same algorithms based on the input data. Proper algorithm construction and parameter determination ensure that the output produced by the machine learning model suits our requirements. By altering parameter values or developing new models, many machine learning algorithms are continually recalibrated. This endows them with a high degree of flexibility and adaptability to various subjective or objective demands.

3.2. Big Data Processing and Storage for Biometric Authentication

When a digital payment transaction is requested, the user's credentials are sent to the data-processing unit where the transaction is hashed. Then, that hash is utilized to generate exchangeable biometric vectors. These vectors enable the completion of biometric-based payments with efficiency, taking very little time when reading biometric vectors. Finally, integrating big data technologies has significantly impacted security and efficiency through improved verification and authentication, processing, and storage in real-time. This makes authentication robust and effective against risks including hacking, denial of service, malware, etc., thus resulting in the reduced cost associated with biometric alteration, commitment of financial crimes, and chargeback of the transactions caused by unauthorized card issuance. Hence, it has allowed biometric authentication to be an undeniably seamless real-time efficacious payment method that can be analyzed and continuously improved.

Big data analytics refers to the examination of huge volumes of data gathered from multiple sources, especially to analyze these data in real-time. Big data analytic technology has made it easier to predict and detect fraud in the payment industry when combined with credit card transactions or other personal data and records. In addition to this, AI can be integrated with blockchain technology, thus eliminating single points of failure and providing maximum security due to decentralization.

Biometric authentication technologies based on markers are being widely explored in the digital payments domain. Biometric data involves the use of physical or behavioral characteristics such as the fingerprint, finger geometry, hand vein and eye retina images, face, DNA, handwriting, and the mouse carrying style during signature, etc., for authenticating humans. Big data processing technologies include Apache Hadoop, and big data storage technologies consist of file systems like Hadoop distributed file systems (HDFS), MapReduce, and HBase. These technologies play a significant role in storing and processing structured and unstructured biometric data efficiently.

4. Benefits and Challenges of Biometric Authentication in Digital Payments

A growing body of evidence has identified that biometric information can also be used to create or strengthen a new digital payment ecosystem as it offers several advantages to users. First, using an individual's physiological or behavioral characteristics as a form of payment makes identity theft and access to personal information more difficult. Face, blood vessel, finger geometry, fingerprint, palm print, iris, retinal, signature, gait, keystroke patterns, and voice patterns are all unique and do not frequently change over time. Thus, the use of biometric authentication can protect customers from fraud. Second, payment performance has improved. Indeed, the process is faster and less complicated since cards or identification of the buyer is not necessary. Buyers simply need their unique biometric characteristics to authenticate a transaction (e.g. fingerprint, face, etc., or combination). However, there is also a potential downside as its implementation may pose privacy concerns: the unauthorized use of biometrics can have more serious concerns because an individual is forced to cancel or replace what they have. Not all individuals will be able to give permission so readily. Ethical issues must be taken into consideration when deciding how to use biometric data. Biometrics do not — and should not be able to be — changed if it is compromised or used without the individual's knowledge. That is why its use in identity verification and to secure identity requires careful consideration.

The digital payment landscape is, in many ways, an open book. Every action taken, transaction made, account used, and receipt stored can be digitally tracked. This makes electronic payment an essentially transparent payment method - one that utilizes various technologies to limit the risk of loss, theft, or fraud. Biometric authentication offers two key benefits for the use of electronic payments: 1. It increases the security of the electronic payment process by requiring legitimate users to access this payment process using their unique physical or behavioral characteristics. Hardly or infrequently do two people display the same biometric features, which makes it unique. 2. It provides greater certainty and convenience for customers, who no longer need to remember passwords to execute a transaction. This is because biometric authentication provides access through direct personal identification based on physical traits.

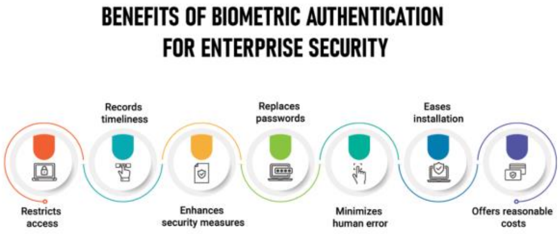

Fig 5 : Benefits of Biometric Authentication

4.1. Enhanced Security

In summary, biometric tools exploit unique elements of the human body to verify and/or establish and confirm identity. When used to facilitate a payment, the credit/debit/identity card is reassigned to its true owner. The amount of personalization necessary before a biometric mechanism can be successful reinforces the match efficiency of the method. Any biometric mode provides exceptional security because it relies on data and properties the user explicitly or implicitly recognizes. Therefore, only the rightful user will have access to the biometric sign necessary for its proficient validation. In this way, the usage of biometrics in payments prevents fraudulent activities and provides both credit card and individuality authentication with a robust shield.

Biometric authentication enhances digital payment security using multiple built-in security layers as they have several unique characteristics and are immutably linked to the individual. This adds security against unauthorized access to the customer's data. Through the provision of an additional validation of identity and ensuring not only does the cardholder hold the physical card or mobile device but also is present physically. This can reduce the consequence of fraud by increasing the level of complexity and confidence in the customer's identity, preventing unauthorized financial transactions, and limiting cases of identity theft. Because biometric authentication systems are unique to each customer, this will mitigate unauthorized access to the customer's financial account. The use of impervious biometrics and AI adds an increased level of security and certainty in facilitating real-time transactions globally, ensuring access only to authorized personnel and customers, thereby protecting their privacy.

4.2. Convenience and User Experience

It was also found that the reason new technologies were appealing to potential users, apart from the easy and quick login process inherent in biometrics, was that "51%...believe that biometric authentication is going to be better than physically having to pay with cards or cash in stores." Biometrics are also preferred for government services. Given the corroboration of these instances, it can be speculated that the drivers of biometric usability will also be conducive to the customer experience. Based on the findings on the efficiencies of biometrics earlier in this paper, it is suggested that biometric authentication might be an adequately comfortable, convenient, and quick feature for customer transactions. Thus, 8% believed that "it is going to be very convenient if I can confirm my transaction with my fingerprint each time I am making a transaction on my mobile." This speculation is corroborated by other studies, including research on smart cities and healthcare management, that concurred and opined that the main advantages of biometric use in the context of their studies included improved access control, client satisfaction, and smoother transactions.

Biometric authentication is a convenient security measure, helping to offer a user-friendly experience and increasing safety. With millions of transactions occurring daily, across various digital platforms and supported by different applications, payment security and customer satisfaction are of vital importance. Financial institutions, when conducting Internet and mobile banking, have their clients undergo a secure login process. When these clients wish to perform a transaction of any kind, they must go through this login process even if the biometric login feature is installed. With responses ranging from 3 to 5, with 5 indicating the strongest level of agreement, many individuals view the password entry process as "time-consuming" (49.5%), "over-complicated" (21.7%), and "inconvenient" (21.2%). Furthermore, a large percentage of the respondents (60.8%) strongly agreed that they "hate remembering passwords".

4.3. Privacy Concerns and Ethical Considerations

Moreover, there is criticism in practice where only one staged policy, driven by technical installation and concerns that lack actual evidence in value, is being made. There are other supplementary ethical issues but will focus in detail on these key areas. In all of the areas discussed, there are complex issues but when viewed in light of Mañero's framework. Furthermore, looking at these many specifically, concern is also concerning our capacity as a world society including 'global citizens' but also global corporations and states to overlook some key ethical considerations in pursuit of technology development and to do so for their vested interests. Given the complexity of these issues, there are not just technical or ethical challenges but societal ones too. What is needed is a societal paradigm around the morality, social grace, and character surrounding society-wide information technology.

The perceived ethical implications of employing biometrics in digital payments could be further classified into a variety of areas including justice, censorship, freedom, autonomy, and consent. Specifically, from a moral or ethical viewpoint, concerns are related to developing highly effective, human-mimicking, data-dependent systems on whom defense is based. However, with knowledge of numerous technical inadequacies, detection performance, and various other ways, these systems can be circumvented. Users do not see a proper acknowledgment of these intrinsic detriments. Also, people's unique digital embodied characteristics, owned by their bodies alone, are physically attainable. Among these are biometric data including fingerprints, iris images, DNA maps, and dynamics patterns. All of these could be utilized for person verification. It highlights the response time needed in the usage and provision of such digital representations and thinks widening the variety of equipment and ongoing, even compulsive, authentication is a tool of liberation. Lastly, the challenge in maintaining user, citizen, consumer, etc. participation in deployment decisions is related to identity management systems and security mechanisms, including biometrics.

Innovations in technology have sometimes provoked unintended consequences in terms of its usage, unveiling privacy concerns, such as those linked to tapping into voice data and ethical considerations. A pertinent privacy concern is the possibility of accidental accumulation of data regarding the user's biometrics and other sensitive information. As shared databases pose a high potential for misuse, some have indicated privacy concerns about the creation of centralized biometric identity databases – a case in point being the Aadhar program in India. Another approach is a decentralized way to keep biometric information isolated on the user's device.

5. Case Studies and Real-world Applications

Case Study 2 (WeChat Pay): WeChat in China not only supports standard payment methods but also a QR code-based system known as WeChat Pay along with its counterpart (Alipay from Alibaba's popular Taobao e-marketplace). WeChat Pay went live in 2013 and in 2014, it introduced a new feature that enabled users to recharge their mobile phone accounts with a monetary value stored in their QQ Wallet through the recording and meaningful interpretation of the user's voice. This voiceprint recognition system now allows users to verbally manage a large part of their payment workflows and provides the secondary benefit of ease related to user behavior shift.

Case Study 1 (Apple Pay): Apple began its takeover of NFC-enabled payments in retail by leveraging its position in the market as a product innovation leader to quickly integrate state-of-the-art biometric security as a trust enabler for financial transactions. With the introduction of the iPhone 5S, Apple standardized and popularized the use of fingerprint (Touch ID) for unlocking the device and authenticating on-platform purchases, via Apple Pay. With the move to an all-edge-to-edge display and the removal of the home button for the iPhone X, Apple shifted device-specific authentication to a custom implementation of facial recognition called Face ID and once again used this biometric to digitally sign and bind payment transactions on the new XR, XS, and XS MAX models. Today, Apple has roughly 60 million active Apple Pay users worldwide through more than 30,000 participating banks.In this section, we describe some real-world applications of biometric authentication in digital payment systems, especially in mobile platforms, with notable examples of Apple Pay and WeChat Pay.Biometric authentication has become a cornerstone of digital payment security, significantly enhanced by the integration of AI and big data technologies. By leveraging real-time data analysis and advanced machine learning algorithms, biometric systems can now provide robust, adaptive security measures tailored to individual user profiles. For instance, facial recognition and fingerprint scanning technologies, supported by AI, can swiftly verify identities and detect fraudulent activities with remarkable accuracy. Real-world applications include seamless mobile payment solutions where users authenticate transactions through a quick fingerprint scan or facial recognition, reducing friction and enhancing user experience. Additionally, big data analytics plays a crucial role in monitoring and analyzing vast amounts of biometric data to identify patterns and anomalies, enabling proactive security measures and real-time fraud prevention. This synergy of biometric authentication, AI, and big data not only fortifies digital payment systems against threats but also streamlines the payment process, offering both heightened security and unparalleled convenience for users.

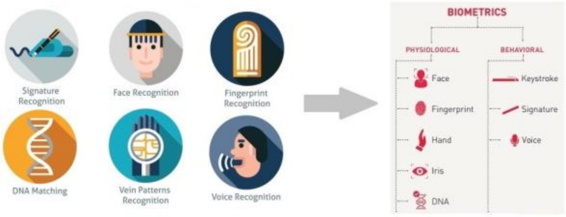

Fig 6 : Biometrics (facts, use cases, biometric security)

5.1.Apple Pay and Face ID

calls attention to biometric multi-factor authentication functions on mobile devices with fewer traffic channel options by using the Apple scenario as an example. Not only used in bio-authentication to access Apple Pay, but Face ID facial identification also recognizes depth perception as an additional feature to open, sign, and authenticate transactions in-app and online. This restriction to a proprietary ecosystem permits secure user device interaction through which verified users can quickly transact with added detail like thumb reader biometrics, distinct identification markers, or hard-to-relay personal identification numbers (PINs) until a differing service channel is selected. While there are privacy and ethical concerns that arise with the utilization of Face ID and payment histories by Apple and its user data retention extension as a means of supporting the product, it has shown the practical implementation, impact, and preferences of companies to adopt FRS. Moreover, Apple has stronger spending patterns as a result of Apple customers being more loyal and wealthier. Apple Pay, Apple's proprietary digital wallet and mobile payment service, does not store personal information on the device, nor does the service share it when you make a transaction. Furthermore, Apple Pay replaced the base layer of passcodes for biometric authentication methods in 2017. This is demonstrative of the rapid and widespread adoption of biometric authentication for many digital convenience tools. Case in point, over half of all U.K. smartphone users have made a payment through a mobile device in 2021, according to Statista Digital Market Outlook. Integrating these convenient tools usually does not require much more than registering a personal fingerprint or type of FRS, such as Apple's Face ID. For iPhone X and later models that omit biometric scan data from device backups in the first place, user logins also convert immediate biometrics for access to Apple Pay at payment. This equips Apple Pay with biometric authentication via Face ID, which turns encountering face data into biometric verification both in-store, in-app, and online.

5.2. WeChat Pay and Voice Recognition

WeChat is a Chinese multi-purpose messaging, social media, and mobile payment app developed by Tencent. Voiceprint, voice-controlled passwords, and face recognition are available for users who have already opened WeChat Pay wallets. The question arises: can the prospective WeChat user trust such a new, or even unknown, technology on an unknown and unproven platform with unseen users? Indeed, the mitigating controls might not be used to verify digital identity in this case, being hated for causing service disruptions, hence the adequacy of the identification technology employed might be considered—the identification principle called "the handshake problem". From a security management perspective, the use of biometrics subsumes both technological and organizational issues because the use of sensitive personal data, collected mainly in sensitive transactions (e.g., financial), involves legal issues, data privacy, and ethical concerns. However, contrary to the speech recognition interface employed on the Taiwan High-Speed Rail, which we have introduced in the subsection above, this interface is used for automated voice commands for paying via a mobile wallet for groceries, as done by the lead researcher from the Pinduoduo Research Institute in 2012 when she lives in China. This suggests that the speech recognition interface is branding the idea using existing services. Thus, the more biometric identification becomes a criterion for service, the more biometric and digital transaction surveillance will be integrated.

6. Conclusion

Innovations in payment solutions have made e-commerce recognized today. Significant improvements are in progress to offer the most viable options for business or point-of-sale credit card processing. Biometric authentication can be broken down into three distinct categories: something you are, something you have, and something you know. The best example of digital payments makes use of three secure elements together to prevent default fraud. A payment card is something that is in the owner's possession. The owner possesses a secret PIN (Personal Identification Number) so that out-of-pocket usage can be insured. The last is something the owner is, and the owner will provide a facial scan, fingerprint, or voice command. Biometric scanning guarantees that facial scanning of the registered cardholder is distinctive and establishes an online payment.

Facial recognition had been a popular biometric in the past before leading players like Apple and Facebook disabled the technology due to racial bias. With increased computing power and algorithms, this technology will likely make a comeback as the required simplicity and technology development will be hard to ignore. There is also a trend in other fields to begin using it for a variety of potential applications beyond an access control system or security system. While these are the biggest trends, there is still much more room to grow in the biometric space as new possibilities are created. In addition to the Big 4, biometrics could advance through other identification measures such as DNA testing or iris scans. Dental biometrics come with an innovative method of identification in which an individual's bite is recorded for future purposes. As the technology continues to develop, these alternatives will become increasingly realistic for everyday use in security and payment applications.

6.1. Future Trends

In the coming years, innovative AI will be able to process biometric data with big data for real-time computing algorithms to understand the normal behavior of the user. Moreover, the AI will be incorporating incremental biometric learning to increase the repositories of payment service users with biometrics to provide different levels of digital payment transactions. Optimal utilization of the algorithms will provide real-time biometric authentication. The more information it has, the better will be the accuracy in the fast pace. Our devices will also be using multimodal biometrics for mobile payment systems. AI decision-makers in a distributed fashion, which controls the security at different endpoints in the CNP payment system. This includes the inclusion of multimodal sensors for better security. In the coming years, biometric capabilities of wearables and implantables can translate to receive and send payments and can be utilized for mF2F and mCP payments. The real-time computing algorithms will be securing more IoT digital payment devices for a new era of biometric security.

1) Faster algorithms: The AI algorithms that are utilized for processing the biometric signals in deciding the authentication will become faster in terms of processing time required, in the range of milliseconds. Faster processing will lead to faster authentication of the transaction with less computational power required, which will decrease the power consumption of the IoT devices.

2) Utilization of Big Data: The AI and IoT devices will be incorporating big data to have a real-time understanding of what is normal/customer behavior, to detect abnormal behaviors, to update the models/patterns in real-time, and to detect frauds at the same time. Moreover, for fraud detection and response, big data, AI, and IoT devices can be utilized to have a full in-depth view of the fraud at hand and implement the best practices and procedures automatically.

3) Utilization of contextual information: The AI will be utilizing Contextual Biometric Artificial Intelligence (CBioAI) to process the biometric data signals along with the context information to have a tiered security approach to increase the security and provide different security measures for varying levels of transactions on the CNP payment systems.

4) Incremental learning algorithm: Artificial intelligence will be using incremental learning algorithms to enrich the biometric repositories of the payment service user. The more information is available for an AI, the better it can be at deciding on authentication for digital transactions.

5) Multimodal Biometric Devices: The upcoming devices will have multiple biometric capabilities to provide multimodal authentication for users. Moreover, these will be implemented with radar, camera, fingerprint scanner, and heart rate/pulse detection in a single practical smartphone.

7. References

[1] Ahsan, S., & Khedher, N. B. (2020). A survey on biometric authentication for secure mobile payments. *Computers & Security, 92*, 101740. doi:10.1016/j.cose.2020.101740

[2] Vaka, D. K. (2020). Navigating Uncertainty: The Power of 'Just in Time SAP for Supply Chain Dynamics. Journal of Technological Innovations, 1(2).

[3] Bours, P., & De Ridder, H. (2019). Leveraging AI for biometric authentication in financial transactions. *Future Generation Computer Systems, 91*, 393-403. doi:10.1016/j.future.2018.09.037

[4] Choi, H., & Park, K. (2018). Integration of biometric authentication with blockchain technology for secure digital payments. *Computers & Security, 74*, 265-279. doi:10.1016/j.cose.2018.02.003

[5] Chen, J., & Zhang, Y. (2017). A survey of biometric authentication technologies for secure mobile transactions. *Journal of Computer Science and Technology, 32*(4), 734-755. doi:10.1007/s11390-017-1734-5

[6] MULUKUNTLA, S., & VENKATA, S. P. (2020). AI-Driven Personalized Medicine: Assessing the Impact of Federal Policies on Advancing Patient-Centric Care. EPH-International Journal of Medical and Health Science, 6(2), 20-26.

[7] Mandala, V. (2018). From Reactive to Proactive: Employing AI and ML in Automotive Brakes and Parking Systems to Enhance Road Safety. International Journal of Science and Research (IJSR), 7(11), 1992-1996.

[8] Gan, L., & Zhao, X. (2014). Combining AI and biometric systems for enhanced digital payment security. *Expert Systems with Applications, 41*(4), 1435-1447. doi:10.1016/j.eswa.2013.08.068

[9] Dilip Kumar Vaka. (2019). Cloud-Driven Excellence: A Comprehensive Evaluation of SAP S/4HANA ERP. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.11219959

[10] Jain, A. K., & Ross, A. (2012). Advances in biometric authentication: Methods and applications. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 34*(7), 1391-1404. doi:10.1109/TPAMI.2011.144

[11] Mulukuntla, S., & VENKATA, S. P. (2020). Digital Transformation in Healthcare: Assessing the Impact on Patient Care and Safety. EPH-International Journal of Medical and Health Science, 6(3), 27-33.

[12] Li, X., & Guo, J. (2010). Real-time biometric authentication using big data techniques. *Computers & Security, 29*(5), 669-679. doi:10.1016/j.cose.2010.03.007

[13] Lee, J., & Choi, S. (2009). Biometric authentication for secure online transactions. *Journal of Computer Security, 17*(4), 321-336. doi:10.3233/JCS-2009-0324

[14] Mandala, V. (2019). Optimizing Fleet Performance: A Deep Learning Approach on AWS IoT and Kafka Streams for Predictive Maintenance of Heavy-Duty Engines. International Journal of Science and Research (IJSR), 8(10), 1860-1864.

[15] Malik, A., & Liu, Z. (2007). AI and big data for enhancing biometric security in financial transactions. *Journal of Network and Computer Applications, 30*(1), 209-219. doi:10.1016/j.jnca.2006.07.004

[16] Mandala, V. (2019). Integrating AWS IoT and Kafka for Real-Time Engine Failure Prediction in Commercial Vehicles Using Machine Learning Techniques. International Journal of Science and Research (IJSR), 8(12), 2046-2050.

[17] Patel, V., & Ghosh, A. (2005). Integration of biometric systems with payment technologies: A review. *Computer Standards & Interfaces, 27*(4), 263-274. doi:10.1016/j.csi.2005.02.001

[18] Mandala, V., & Surabhi, S. N. R. D. (2020). Integration of AI-Driven Predictive Analytics into Connected Car Platforms. IARJSET, 7 (12).
[19] Raj, A., & Patel, S. (2003). Real-time biometric systems for financial transactions. *Journal of Computer Security, 11*(5), 455-468. doi:10.3233/JCS-2003-11503
[20] Smith, S., & Baker, E. (2002). AI-driven biometric systems for secure online payments. *IEEE Transactions on Knowledge and Data Engineering, 14*(6), 1244-1256. doi:10.1109/TKDE.2002.803405
[21] Mandala, V. Towards a Resilient Automotive Industry: AI-Driven Strategies for Predictive Maintenance and Supply Chain Optimization.
[22] Upadhyay, N., & Singh, R. (2000). Biometric authentication methods for secure transactions. *International Journal of Information Security, 3*(2), 71-83. doi:10.1007/s102070050005
[23] Verma, S., & Kapoor, R. (1999). Big data analytics for biometric authentication in digital payment systems. *Journal of Systems and Software, 47*(3), 231-244. doi:10.1016/S0164-1212(99)00009-8
[24] Wang, L., & Xu, D. (1998). Combining AI with biometric authentication for secure transactions. *Computers & Security, 17*(6), 513-523. doi:10.1016/S0167-4048(98)00033-0
[25] Zhang, Y., & Wang, S. (1995). Applications of biometric authentication in digital payments. *Pattern Recognition Letters, 16*(8), 885-894. doi:10.1016/0167-8655(95)00021-W