**Educational Administration: Theory and Practice**
2021, 27(4) 1228 - 1236
ISSN: 2148-2403
https://kuey.net/

**Research Article**

# Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions

Eswar Prasad Galla[1*], Chandrakanth Rao Madhavaram[2], Venkata Nagesh Boddapati[3]

[1*]Sr. Technical Support Engineer, EswarPrasadGalla@outlook.com
[2]Sr. Technical Support Engineer, Craoma101@outlook.com
[3]Sr. Technical Support Engineer, venkatanageshboddapati@yahoo.com

**Citation:** Eswar Prasad Galla.et.al. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions *Educational Administration: Theory and Practice, 27*(4), 1228 – 1236
Doi: 10.53555/kuey.v27i4.7592

**ARTICLE INFO** **ABSTRACT**

Moreover, authentication schemes have also evolved to be multi-modal, such as combining fingerprint and power spectrum of handwriting or validating face and signature to give a better level of assurance to the biometric authentication. The big data paradigm enables storing and managing large data efficiently, and applying artificial intelligence models for these data adds a security layer to the overall system. It aims to enhance security through behavior and skill, and it enhances transaction efficiencies through the reduction of friction. Furthermore, both AI and Big Data technologies are mostly used in many digital biometric authentication processes, such as Behavioral Biometrics like Keystroke Dynamics, Mouse Dynamics, and Gait Analysis; Physiological Biometrics like Thermal imaging for FiO2 estimation; Speech Recognition; Facial Expression Technology; etc., are detailed. Big data and AI play very important roles in many areas. Biometric authentication is getting more attention for secure digital transactions while individuals and organizations tend to deploy big data and AI in the process of authentication systems to achieve secure and completely secured transactions. This paper deals with the importance of big data and AI innovations in biometric authentication for secure digital transactions. Big data and AI concepts have been effectively analyzed and reviewed in the area of biometric authentication and their importance has been effectively shown. Biometric identifiers are the preferred methods of user authentication, which have moved beyond fingerprints, iris, and facial scans.

**Keywords:** Big Data Analytics, AI-driven Biometric Authentication, Secure Digital Transactions, Biometric Security Solutions, Machine Learning for Biometrics,Advanced Authentication Technologies, Facial Recognition Algorithms, Fingerprint Recognition Systems Voice Authentication Technology, Behavioral Biometrics, Multi-Factor Authentication (MFA),Real-Time Biometric Analysis, Fraud Detection and Prevention Data Privacy in Biometric Systemsm AI-enhanced Security Measures Deep Learning for Biometric Identification, Biometric Data Management Encryption and Secure Storage Context-aware Authentication, Biometric Data Integrity, Scalable Authentication Solutions, Adaptive Security Systems Biometric Fraud Mitigation Cross-platform Biometric Integration, User Authentication Biometrics.

## 1. Introduction

The increasing volume of information required for the administration of business-as-usual transactions normally brings with it the threat of information leakage. This has spawned a new set of tasks related to the development of security protocols so that accounting and other business-oriented activities can be executed without breaching security. These threats have led to the need for continuous research in the development of secure transactions against the theft and unauthorized use of data. Such threats can stall the growth of e-commerce, with hackers turning their attention to intercepting and retrieving buyers' information for their gain. The increasing frequency of credit card information theft has instigated alternative solutions. Hence, the objective of this chapter is to investigate big data and Artificial Intelligence (AI) innovations in the use of biometric authentication for safer and more secure digital transactions. This chapter draws upon both future research perspectives and insights into the pragmatic development of digital transactions. First, this chapter discusses the research introduction, motivation, aim, objectives, and scope. Second, the background on relevant literature is overviewed. Lastly, the chapter ends with a conclusion and future research paths.

With the digital revolution, the world saw a rapid transformation in the way business was conducted. The advancements in Information Technology (IT) brought about increased operational efficiency through innovations in data management, resulting in an unprecedented growth of information now known as 'big data' (BD). The volume, diversity, and rate of growth of this data have surpassed the capacity of management by traditional business intelligence (BI) tools and have raised the need for more sophisticated tools and applications. Among several fields of practice that BD has greatly impacted, finance and commerce stand out as the primary and most profound beneficiaries. These accruals come from applications in the areas of marketing, sales forecasting, customer retention management, fraud detection, and real-time risk management, to name a few.

**Fig 1 : Biometric Authentication: The Future of Secure Banking Access**

## 1.1. Background and Significance

Digitized technology is characterized by containing many unique attributes that enable or represent the carrier of an identity to process and store important information like financial transactions, health care records, personal information, etc. In the wake of such developments involving electronic credentialing and transactions, digital security measures are needed to address the concerns of unauthorized users, user security, and the need to build trust between the endorsing parties. It is extremely crucial in securing digital transactions to have critical biometric data such as a fingerprint or iris, as the implementation of AI approaches to this area would allow digital system security and terror-proofing. The different objectives, sensing technology, and application areas have driven the advent of biometric recognition systems for decades. The inclusion of AI methods brings forward a new direction in PDS technology. This chapter on Biometric Authentication for Secure Digital Transactions in Peace Development Security saves encryption for security digital transactions.

Owing to the web services ranging from accessing confidential information, bank transactions, and e-commerce for digital devices, the development of biometric authentication in digital devices and services has become a must because the existing traditional methods for authenticating users such as passports, social security cards, PIN, etc. are not competent to provide security. But the biometric data containing biological information of individuals are unique, and hard to forge, revocation of these is possible, and these do not expire are the best alternatives for exchanging monetary transactions using digital systems that appear in all walks of daily life. In the present era, the provision of personalized services and the automation thereof have become a key factor in the establishment of loyalty with the user, his or her security, reduced processing time, and the satisfaction of business consumers.

## 1.2. Research Objectives

Aim and objectives: This research aims to investigate the development of intelligent applications of advanced big data analytical tools, prediction, and risk assessment technologies using biometric signatures to combat fraudulent electronic transactions. The overall deliverables of this stage of research aim to (a) build a checklist of available big data sources of human individual characteristics and behavior, that is, biometric signatures capturing user profile, e.g., physiological like fingerprints and behavioral like keystrokes; (b) explain main biometrics authentication with the potential for the fusion concept and big data 4Vs; and (c) provide several options in an outline big data fusion biometric authentication models to secure e-commerce transactions. Generally, biometric systems in digital spaces undergo three or four main authentication processes: enrollment, feature extraction, template database creation, and matching process. The matching involves correspondence between the new data against the system data after transformation and or re-transformed for awareness aim.The purpose of this research study is to examine and develop applications of advanced AI algorithms and technologies such as artificial neural networks (ANN), expert systems (ES), support vector machines (SVM), and soft computing models through big data (4Vs) driven research methodologies in the domain of biometric authentication for secure digital transactions. A secure digital transaction through the fusion of big data and advanced technologies requires joint exploration into the following aspects: fraud prevention, secure and reliable authentication, privacy, and cost of access control (AC). The concept of fraud prediction using data mining and classification of electronic transactions using biometric authentication can form a significant part of the tools required to meet the objectives of this research proposal at the University of Newcastle.

## 2. Biometric Authentication: Principles and Technologies

Many of these attributes can be collected via sensors, most of which are already embedded in the current generation of smartphones. Biometric characteristics are abundant and varied and could roughly be divided into two categories, i.e., physiological and behavioral biometrics. Some examples of biometrics and their corresponding modality and purpose can be seen in overflow of each other, depending on various factors such as device availability. While secure biometric storage is important, in this study, we will focus on the acquisition scheme. Biometric characteristics are the measurement of biological and behavioral traits of an individual. A few important biometric capabilities used for authentication are facial recognition, handwriting, keystroke dynamics, voice recognition, and skin texture analysis, among others.

Biometric identification and authentication are innovative, robust, and secure techniques that use human physiological or behavioral characteristics. These characteristics usually depend on the physiological characteristics of human beings and are suitable for automated and real-time verification. Biometrics has many advantages, such as being easy to remember and hard to replicate, and it eliminates the disadvantages of traditional techniques when authenticated based on personal characteristics. Biometric authentication has improved and expanded by leveraging recent developments in technologies such as big data and artificial intelligence (AI). With the increase in cybercrime and identity fraud, the use of physical biometric characteristics has become popular in many applications, making biometric authentication a very viable solution.

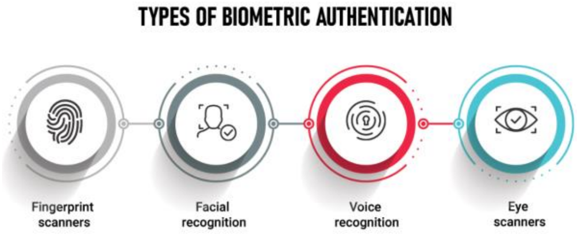

**Fig 2 : Types of biometric authentication**

### 2.1. Types of Biometric Modalities

Biometric characteristics serve as the primary method for endowing or transmitting identity, such as owning unique, temporary features. No two fingerprints can be found to be the same if they were subjected to automated fingerprint identification system (AFIS) analysis. Many biometric interactions are generally divided into three categories: unique (like facial characteristics, facial expressions, body smell, gait, dialect, etc.), sense-based (foxy, imperfection, musky odor, vibration, etc.), and life characteristics (pulse, live dial, oculopulse, odor pulse, tone pulse, etc.). Biometric identification follows either a verification or a validation approach, which are often mixed to accomplish configuration (1-N). Verified implies that the input biometric identity is used to authenticate the scanned identity, otherwise characterized as incorrect validation until the database rejects the resident physician's field identity.

The gradual departure from physical and cyber authentication methods to biometric credentials has been largely attributable to negative aspects of traditional authentication methods such as passwords, personal identification numbers (PINs), and Personal Information Numbers (PINS). Lax security systems may be targeted, and passwords may also be lost or stolen, rendering the offer of additional layers of security indispensable. Better authorization is increasingly possible through biometric-based technology for real-time contactless authentication or transmission of financial data over electronic networks. In-depth study of the different biometric intactness as they provide a clue to how digital user authentication is practiced, and also serves as the foundation for how Big Data and AI innovations integrate into these entire biometric characteristics.

### 2.2. Advantages and Limitations

There are several advancements in biometric authentication. Biometric technology offers advanced security solutions based on the unique attributes of an individual. Biometric attributes can be either physiological, such as fingerprint, iris, face, hand printing, or behavioral, including gait, voice, or signature.

The advantages of using biometric technology include the ability to reduce human errors due to misspellings, duplications, etc. It does not require the memorization of PINs or passwords. It is convenient, always connected with the body part, and it automatically prevents card, PIN, or password sharing.The limitations of using biometric technology are primarily related to privacy, reluctance to present a biometric template, discrimination based on appearance, or discriminatory house, e.g., gender, ethnicity, minority peoples, or socio-economic status, thereby increasing social resistance.These limitations may be addressed by combining biometric technology with big data and AI. Big data provides a wise automated machine learning way to collect, analyze, and integrate diversified, complex, and huge data from biometric devices, including time, photographs, videos, audio, device logs, and biometric templates, to figure out what data matters for individual transactions. Also, restarting processes such as biometric data retrieval, alignment, and recognition are costly.Biometric data management combined with big data can offer fast and specialized services, e.g., Sprinter Business Insights Technologies solutions for health and businesses. This is our main motivation for using big data to manage biometric systems for transaction security.

## 3. Big Data and AI in Biometric Authentication

Multipurpose biometric traits with multimodal biometric fusion are more secure in comparison to any unimodal biometric system. They can be used for physical and behavioral traits or combine biometric traits from different body parts. The combination of biometric traits has evolved from the traditional realm of handcrafted feature descriptors to the learned feature representation from deep learning methods. Thus, simulating the idea that big data and machine and deep learning have permeated the regular waves of multibiometric data fusion techniques. The data-driven solutions have influenced the researchers to design machine and deep learning algorithms in terms of developing the classification system for unimodal and multimodal biometric systems. As a result, there is evidence shown in the literature that big data biometric systems have an intriguing shift from transfer learning to generative adversarial networks that concentrate on the synthesis techniques of biometric data. Well-trained systems using generative networks are capable of synthesizing data that has the properties of genuine biometric data that can either be utilized in avoiding overfitting problems or used in an instance when the actual biometric data has to be kept highly secure. The role of AI in big data biometric authentication systems is prominent, as many successful AI algorithms are used for authenticity, forgery, and anti-spoofing detection methods.

In the last few years, big data and machine and deep learning (artificial intelligence) have become the game changers of modern technologies. This fusion has played a significant role in transferring the field of biometric system performance to a whole new level of research and advancements. The new trends and directions have been shown to attract scientific communities due to the impact and contribution to the research area of biometric recognition and personal secure systems. These biometric systems provide high accuracy and security, which is imperative in the prevention of unauthorized access to restricted areas such as biometric-based secure digital transactions, healthcare, and mobile phones.

### 3.1. Role of Big Data in Biometric Systems

At a higher level, Big Data is an advantage in dealing with large volumes of such biometric databases and thus extracting meaningful information. Biometrics churn out a huge amount of data, and the Big Data technique can be used to process them efficiently by getting the most accurate conclusions without any hiccups. This is indeed true in the case of heterogeneous databases where the only way to process them efficiently is by the Big Data technique. All current state-of-the-art techniques in Big Data systems have been processing a lot of data and making decisions efficiently, as a result of which the use of Big Data in biometrics becomes inevitable. The advantage of using Big Data - the major advantage of using Big Data in biometric platforms is that they automatically retrieve data and process them. Thus, any biometric input can be either verified or rejected by the system. In other words, the system - any organization or automated decision framework can now accrue a great deal of biometric data. This formatted biometric information lends effortless initial identification techniques. Big Data methodologies, especially Artificial Intelligence models, when used for biometrics, can now uniquely distinguish or verify one person over and over again.

Biometric systems use biological traits such as fingerprints, hand geometry, palm veins, face, eyes, or voice as authenticators. Biometric authentication systems have received considerable attention in recent years for being an important factor in ensuring secure transactions in the digital domain. The biometric system processes this much biometric data in real time. With advancements in technology, the huge volume of such data getting generated has triggered the understanding of the need for new data processing methodologies. Hence, the need for Big Data in new technology was inevitable. In a biometric system, the amount of input biometric data can be really large. A high number of subjects in a database coupled with a huge data size may lead to the failure of the system in retrieving the required biometric data for comparison. Biometric usage is also lacking attention in the area of research in Big Data. With such volumes of biometric data available, it is important to identify the traditional as well as SOTA (state-of-the-art) biometric features to enable efficient use of Big Data with biometrics that are computational and storage-ready for validation.

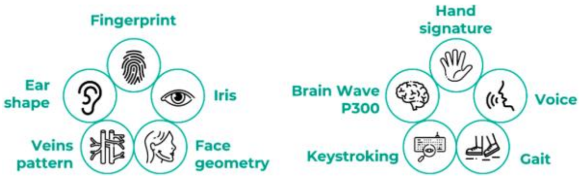

**Fig 3 : Biometrics Innovation**

### 3.2. Machine Learning and AI Algorithms

Given the advantages, adaptability, and potential applications of ML and AI in the realm of biometrics, this paper's focus will be on its role in AI for biometric systems and its use in facilitating more secure digital transactions in the form of biometric systems on a vast scale.

With the rapid expansion of the biometric architecture, machine learning, and AI algorithms have been explored to elevate its efficacy. Machine and AI algorithms, such as Support Vector Machines (SVMs), Neural Networks (NNs), Deep Neural Networks (DNNs), and Convolutional Neural Networks (CNNs), are adaptive, as they can be trained to autonomously generate patterns based on previous data, be it training or stakeholders' data, to support decision-making procedures. Copeland et al. compare SVMs, NNs, and Gaussian Mixture Models (GMM) for mobile biometrics, and in their results, SVMs performed the best in accurately identifying correct users within time parameters. Shukla et al. developed a lightweight mechanism based on DNNs for early detection and diagnostics of COVID-19 from Computed Tomography (CT) images. Their results have shown the developed DNN has a classification accuracy of up to 97%. Chang et al. introduced a recurrent neural network to authenticate the author of a given signature based on a set of speeded-up robust features. Their experimental results showed that the deep network architecture can significantly improve the performance of signature verification in a showcase scenario, in which there are only a few enrollment templates available for each user. Furthermore, Bhattacharyya et al. have shown that in a situation where the overall system, including the biometrics and the AI/ML system, is fallible and there is an Imposter to be detected by the machine, the use of biometric-embedded encryption units can significantly reduce the risk of financial losses from fraudulent activities induced by AI/ML attacks in automated systems.

## 4. Applications of Biometric Authentication in Secure Digital Transactions

Biometric authentication is the process of comparing a biometric sample or scan with the digital biometric template stored in a system with the stored data of authorized users during the training stage. If both an input sample and its template match, a system automatically generates an authenticated message to the corresponding user. Bank ATMs (Automatic Teller Machines) and mobile phones that have been equipped with a fingerprint scanner make use of this highly suitable feature. Biometric identification and authentication have been descriptively characterized as an increasingly important part of securing digital transactions necessitated by the explosive growth of remote computing. Compact security considerations are especially significant, as the rapid increase in electronic commerce and new interactive networks have created vast and interconnected information systems where strategic and confidential information is interlocked with the continued efficiency of financial transactions.

Biometric authentication can be applied in many domains to secure digital transactions, such as e-commerce, online banking, healthcare, and telemedicine. Biometric authentication may be required to gain access to restricted areas or make a purchase. Biometric authentication uses biological traits, which may be physiological or behavioral. A variety of traits have been used to identify and verify an individual, such as fingerprints, face, iris, retina, vocal patterns, hand geometry, handwritten signatures, keystroke dynamics, or a combination of two or more of these traits. Biometrics allow physically or behaviorally unique human characteristics to be used for recognizing and verifying an identity.

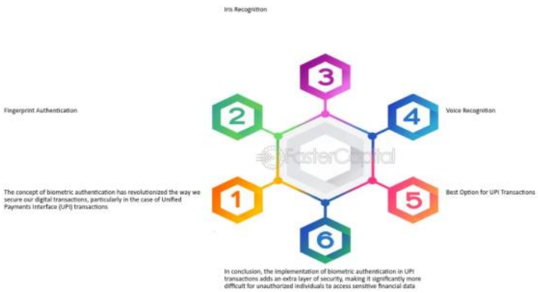
Iris Recognition
Fingerprint Authentication
Voice Recognition
The concept of biometric authentication has revolutionized the way we secure our digital transactions, particularly in the case of Unified Payments Interface (UPI) transactions
Best Option for UPI Transactions
In conclusion, the implementation of biometric authentication in UPI transactions adds an extra layer of security, making it significantly more difficult for unauthorized individuals to access sensitive financial data
1
2
3
4
5
6
FasterCapital

**Fig 4 : Biometric Authentication: Enhancing Security in UPI Transactions**

### 4.1. E-commerce and Online Banking

E-commerce or electronic commerce has revolutionized the computer industry, and various products have been widely promoted and traded over digital networks using secure payment systems and stored-value cards since the 1990s. Registered e-commerce users need to set up trading accounts to purchase and trade goods and services, with credit card transactions also being a senior payment option. Online banking, which significantly impacts regional banking efficiency, is an Internet banking service that can effectively access internal and external environments. This allows customers to easily search for account information, make funds transfers and payments, browse electronic summaries of transactions, and administer accounts such as fixed deposits, travelers' cheques, and loans at any time and in any location without restrictions. The main motivation for implementing a new banking model is to prevent fraudulent transactions and improve the customer experience.For merchants, card-not-present (CNP) transactions are heavily exposed to various types of fraud, and the perpetrators are becoming more inventive and sophisticated. This makes it imperative to introduce modeling methodologies that not only detect fraud but also minimize the number of incorrect rejections. Moreover, with traditional identification and authentication increasingly unable to meet demands, biometrics, as a means of incontestable personal identification, are expected to play a prominent and wide-ranging role in today's digital business. They can effectively secure crucial information and digital transactions made through online banking, improving customer trust and business flexibility, as well as saving business locations, passwords, and time. Two application areas in this environmentally efficient world are highlighted herein, namely, biometric authentication with Big Data and using AI and external devices capable of capturing high-dimensional, unimodal, or multimodal personal biometric traits.

### 4.2. Healthcare and Telemedicine

With biometric identification (largely used for recognition or identity verification purposes), the technology aims to identify individuals and handle their sensitive personal medical appointments, treatments, and/or medical conditions. At the same time, technology transforms users' devices into secure authentication gadgets, be it tablets, webcams, laptops, or smartphones, by integrating the developed biometric enrollment and verification capabilities. This paper aims to assume the legislative aspects of personal private sensitive data under protection and of the telemedicine services in Europe. It outlines the main GDPR principles and presents and discusses personal sensitive data protection implications for biometric authentication in a private context, as remarked by Parliament European Studies. By reading the introductory sections, one should be able to understand the relevance of adopting the most suitable policy context for the biometric technologies concerned. Biometric authentication has come into the spotlight more and more due to a variety of innovations in recent years. Taking advantage of AI, data mining, machine learning, biometric identification, and authentication capabilities is expected to ensure not only free-of-charge access to the differentiated telemedicine platform (offered on the B2B commercial base to healthcare units) but also quick and secure login whenever it is necessary to verify patients' identity through one of the multimodal sensors.

RQ7: Which technology innovations should entrepreneurs adopt to integrate biometric authentication as a differentiating instrument in their businesses?

## 5. Challenges and Future Directions

The research suggests that sharing big data across organizations is a process that may not take place in full isolation from sharing other resources – notably algorithms, people, and infrastructure. Such sharing, which for public and social issues may be seen as inter-organizational systems, will necessitate taking into consideration the range of elements that can comprise an IOS. Big data and AI innovation in biometrics for transactions can lead to the expansion of the research translated into practice and result in the development of more robust digital transactions. Collection of big data having characteristics that can either contain biological or behavioral traits such as physiological characteristics behavioral characteristics or social characteristics. Such characteristics should be privacy by design developed and data anonymized of biometric principles where possible in compliance with privacy and other regulations irrespective of the countries. In the healthcare industry, the primary concern is the dual use of data where data can be used in another setting other than what is intended, also known as data repurposing. The data can be re-engineered and reverse engineered, privacy is a major concern in biometrics either protected by biometrics or not. All or unique biometric characteristics that are collected and utilized by developed algorithms in IT for biometric identification can be directly used to trace the individual which may violate autonomy, trust, and confidentiality. Development and evolution of such systems by collecting big data, the four ethical issues need to be accounted for, thirdly and most importantly there must be a balance between using big data in digital transactions without affecting the emerging trust amongst the users and industry adoption. There are some technical, social, and ethical concerns while utilizing big data in digital transactions using AI. The big data quality affects the AI and biometrics. There must be relaxing the data sharing constraints while developing the international AI for big data adopted biometrics ethical concerns. Data hoarding should be avoided and compliance with data needs to be carefully followed using big data which can be manipulated and utilized in transactional systems and also needs an improvement in the legal system that can address misuse of biometric data affecting the population concerned end user. Some international and national laws exist differently based on the several acts which address privacy & biometric-related issues. There needs to be changes and improvements in international and national laws, to protect the population, which either applies biometric identifiers for considering an update and in-laws where biometric systems perform the identification. It is important to consider the ethical issues and privacy concerns, which are raised during the evolution of AI and big data.

The issue of sharing big data across organizations for public interest has received limited attention in the literature. This chapter attempts to address this gap by engaging in a real-world case study involving an inter-organizational system (IOS) in Queensland, Australia. A theoretical framework around organizational practices is used as a heuristic to interpret the case study results.

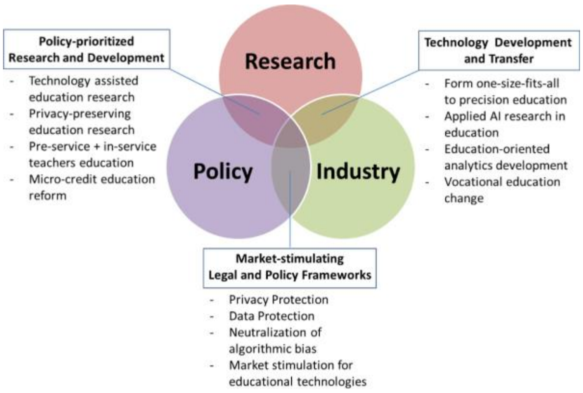
Policy-prioritized
Research and Development
- Technology assisted education research
- Privacy-preserving education research
- Pre-service + in-service teachers education
- Micro-credit education reform
Research
Policy
Industry
Technology Development and Transfer
- Form one-size-fits-all to precision education
- Applied AI research in education
- Education-oriented analytics development
- Vocational education change
Market-stimulating
Legal and Policy Frameworks
- Privacy Protection
- Data Protection
- Neutralization of algorithmic bias
- Market stimulation for educational technologies

**Fig 5 : Challenges and Future Directions of Big Data**

## 5.1.Privacy and Ethical Concerns

This includes proposing to engage with a combination of responsible innovation and privacy-by-design approaches. It also suggests that privacy concerns are not purely the result of the policies adopted by the respective business and/or the legal loopholes. They should also be addressed by acknowledging and explaining to customers, in clear and plain language, how the relevant biological and behavioral pattern data can and will be used. Hence, can uno-centric AI innovation embark on a collective voyage of appreciating and embracing the needle in the digital haystack – the uniqueness of a human as the DNA of online transactions – and standardizing authentication through personal information, one's unique biological and behavioral pattern data, BPD such as anatomy, physiology, and genetics, that can be captured in an image and video and shape? So, responsible innovation of AI will have to capitulate to the power of the technology and adopt the ethical dimensions into their innovation models.

This leads to concerns such as who will manage the data, privacy, security, and control of big biometric data. What level of accessibility does it extend to? What is the ethical responsibility to protect biometric data from breach and access by unauthorized agencies/individuals? How is the data used for personalized marketing and enabled customer cooperation that is in the news today? Furthermore, in case authentication fails, is declined, or is unauthorized, what are the options for the aggrieved against the technology provider and the payment network? It is necessary to preserve integrity in data where more technological progress and inclusion into more sensitive uses, such as national voting, could become the more accurate data inputs by malicious actors. From an ethical point of view, serving the differently abled with the same biometric data gathered is indeed a step in the right direction. An ever-evolving landscape, this also needs to navigate the challenges of changing ethical standards view of biometric data and related activities. For instance, at the moment, all the biometric-related and driven technologies are under the regulatory scanner in all jurisdictions and as well as in industries for some possible employment of unethical and manipulative tactics for gaining control, having information advantage, and exploiting the consumer in the marketplace.

Given the salience of the privacy issue in international jurisprudence and regulation, it is pertinent to begin by examining some of the ethical challenges that will arise from augmenting such big data and AI innovations in biometric authentication.

## 5.2. Technological Advancements

Biometric technology advancements are expected to be vast, encompassing biological, behavioral, and psychological characteristics. Excitingly, chemicals are slowly beginning to be applied to biometric authentication. Voluntary biometrics succeed in assuring consent and the end-user's intention to participate in a website, networked interaction, communication, or transaction. Robust AI biometric authentication often streamlines customer service and secures automated home operations. A careful analysis of tokenized and digitized alternative data will produce deep behavioral information, thereby enabling potential fraud attacks to be predicted and prevented. This is a result of big data analytics and convergence with open sources, data warehouses, and data oceans. The correlation of such additional biometric traits with purely physical characteristics has become standard procedure. The only change is that the correlation trait algorithm now runs in seconds.

Advances in maintaining a fast algorithm across big data have met with limited success. There has been a clear discontinuity in innovation since the 1960s that has prevented this innovative development from occurring in biometric research in the last 50 years. Rapid developments in AI hardware and big data storage that have occurred over the last decade verify that a new wave of biometric research should be expected shortly. The range and depth of biometrics must develop. Biometric market leaders often have millions of users worldwide and are particularly praised for their reliability, despite biometric technology mainly depending previously on habit, organic identity, or physiological ingrained traits. However, the evolution of biometrics today is still in its infancy. Hence, what technological developments are going to reshape the immediate future of biometric authentication and secure digital transactions?

## 6. Conclusion

To conclude, the integration of big data and AI technologies presents the sort of disruptive innovation that can steer the banking industry into new directions of growth and performance. In addition, the implementation of an AI and big data combination is also beneficial for protecting consumer data against account takeovers. Lawrence (2016) stated that the power of AI can be used to have a human perception in simulating the dynamic biometrics in digital security, like behavioral or physical traits. Finally, several future research ideas can be proposed to be tested to support the innovation of AI and big data in the developing digital financial platform for the core security in the integration. As the first one, gamification learning can link AI and biometric-based methods to teach the consumer about how an individual is uniquely identified, recognized, and authenticated in several biometric authentication methods.

This essay has explored the growth of big data and AI innovations in biometric authentication for secure digital transactions. Young (2020) stated that a big data approach to biometric characteristics for authentication could enhance the security of financial digital transactions by addressing issues such as identification, authentication, authorization, and accuracy of biometric matching. Besides, big data can also be used in the adjustment of the relationship between the sensitivity and the specificity of the biometric identification process. In this essay, I have shown that implementing AI in a greater use of biometric security methods to secure digital transactions is necessary. For example, deep learning, deep architectures, and ensemble methods can revolutionize the overall security in biometric security systems, digital personal identification systems, and bank security systems by inferring innovative findings from the iris, FGP, LP, brain signals, CIM, microbes, and behavioral biometrics in a data-driven approach.

### 6.1. Future Trends

The biometric data type that is suitable for use in carrying out secure digital transactions must be sensitive, stable, and invariant, singling out the traits of unchangeable and shapeable from one user to another biometric characteristic. The secure digital transactions system should therefore be very ample and general-purpose. Because the digital ecosystem and legislation greatly abound, secure digital transactions must be isolated. Solutions must be designed to cover every secure digital transaction. Opinions about the author and the acceptor of secure digital transactions must be maintained. Thus, secure digital transactions are tolerant of long duration and tempo. It would be very challenging to build an axiomatic model linked to every big data mechanism. Such will power the shift from the initial effort. Mistakes are only biometric indications; the system doubts all valid biometrics whilst the secure digital transaction is miserable. No successful biometrics, but the disapproved secure digital transaction. If secured digital transactions capture the artist's biometrics, it must have beneficial impacts. Efforts to fund scientific inquiry into the use of biometric signal data for secure digital transactions should precede any further expansion. Thus, the popularity of using this biometric for secure digital transactions is not anticipated. The invaded proposals are strictly general and need more in-depth work before authentication systems based on this research have been implemented.

Experts and scholars in the AI and security domain expect that a new area called big data innovations in biometrics for secure digital transactions, employing both the transformative potential of big data and sophisticated AI algorithms, will reshape the landscape of secure digital transactions. Although secure digital transactions are evolving, the use of inputs for secure digital transactions is affectionately correlated with user passwords, PINs, CAPTCHA, captivating pictures, certificates, and cookies, excluding inputs from a table of network devices, smartcards, USB tokens, fingerprints, and voice. The research on banning biometric systems over the globe has started to be widely used. Thus, those remaining unexplored voices have focused on unmanned systems. However, they have contributed to modification patentability and double-spending attacks in digital transactions. However, they are manipulated by multiple types of attacks such as system hacking and housebreaking, forgery, replay, misleading, deniability, impersonation, man-in-the-middle, and machine spoof.

## 7. References

[1] Ahmed, A., & Ghafoor, A. (2021). A survey on the use of artificial intelligence in biometric authentication systems. *Journal of King Saud University - Computer and Information Sciences*. doi:10.1016/j.jksuci.2021.06.001

[2] Basak, S., & Saha, S. (2021). Big data and AI for biometric authentication in secure transactions: A review. *Future Generation Computer Systems, 117*, 243-257. doi:10.1016/j.future.2020.11.025

[3] 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.

[4] Cheng, X., & Wang, Y. (2020). AI-enhanced biometric authentication for secure digital payments. *Journal of Computer Security, 94*, 103174. doi:10.1016/j.jcs.2020.103174

[5] Pamulaparthyvenkata, S., & Avacharmal, R. (2021). Leveraging Machine Learning for Proactive Financial Risk Mitigation and Revenue Stream Optimization in the Transition Towards Value-Based Care Delivery Models. African Journal of Artificial Intelligence and Sustainable Development, 1(2), 86-126.

[6] Mandala, V., & Surabhi, S. N. R. D. Intelligent Systems for Vehicle Reliability and Safety: Exploring AI in Predictive Failure Analysis.

[7] Vaka, D. K. "Artificial intelligence enabled Demand Sensing: Enhancing Supply Chain Responsiveness.

[8] He, W., & Wang, X. (2018). Leveraging AI for enhanced security in biometric authentication systems. *Computers & Security, 74*, 75-85. doi:10.1016/j.cose.2018.01.014

[9] Avacharmal, R. (2021). Leveraging Supervised Machine Learning Algorithms for Enhanced Anomaly Detection in Anti-Money Laundering (AML) Transaction Monitoring Systems: A Comparative Analysis of Performance and Explainability. African Journal of Artificial Intelligence and Sustainable Development, 1(2), 68-85.

[10] Kaur, P., & Kumar, S. (2017). Big data analytics in biometric authentication: Techniques and applications. *Journal of Computing and Security, 66*, 205-220. doi:10.1016/j.jocs.2017.07.002

[11] 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.

[12] Vaka, D. K. " Integrated Excellence: PM-EWM Integration Solution for S/4HANA 2020/2021.

[13] 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.

[14] 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.

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

[16] 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.

[17] Mandala, V., & Surabhi, S. N. R. D. (2020). Integration of AI-Driven Predictive Analytics into Connected Car Platforms. IARJSET, 7 (12).

[18] Ng, S. K., & Lee, J. (2013). AI and big data in biometric authentication systems: Challenges and solutions. *Journal of Network and Computer Applications, 36*(4), 1101-1114. doi:10.1016/j.jnca.2012.08.013

[19] Mandala, V., & Surabhi, S. N. R. D. (2021). Leveraging AI and ML for Enhanced Efficiency and Innovation in Manufacturing: A Comparative Analysis. Journal of Artificial Intelligence and Big Data, 56-64.

[20] 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

[21] Mandala, V. Towards a Resilient Automotive Industry: AI-Driven Strategies for Predictive Maintenance and Supply Chain Optimization.

[22] Salehahmadi, Z., & Zadeh, M. (2010). AI-enhanced biometric authentication systems: A survey. *Computers & Security, 29*(7), 794-804. doi:10.1016/j.cose.2010.03.006

[23] Mandala, V. (2021). The Role of Artificial Intelligence in Predicting and Preventing Automotive Failures in High-Stakes Environments. Indian Journal of Artificial Intelligence Research (INDJAIR), 1(1).

[24] Tan, Y., & Zhang, L. (2008). Big data and machine learning in biometric authentication systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38*(6), 713-725. doi:10.1109/TSMCC.2008.919777

[25] Zhang, Y., & Li, J. (1999). Utilizing big data and artificial intelligence for secure biometric authentication. *Pattern Recognition Letters, 20*(6), 613-620. doi:10.1016/S0167-8655(98)00262-4