Migration Letters

Volume: 21, No: 8 (2024), pp. 574-590

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Leveraging AI And Big Data For Enhanced Security In Biometric Authentication: A Comprehensive Model For Digital Payments

Sri Sai Krishna Mukkamala[1] , Ankur Mahida[2] , Vishwanadham Mandala[3] , Mohit Surender Reddy[4]

Abstract

The paper offers an epitomized overview of the state-of-the-art frameworks, algorithms, and methods in the domain of biometric cryptography for mobile transactions. The rapid technological advancement has led to the popularity of various biometric systems. The association of these systems in different fields of digital life, such as banking, e-commerce, or m-commerce, cannot be overlooked. However, daily digital transactions have augmented the risk of breaches of security and privacy concerns, which have found their solution in biometric authentication[1] systems. These diverse applications encounter many challenges, including the trade-off between recognition accuracy and computational complexity, advanced fake attributes, privacy issues, and continuous efforts for enhanced estimation of entropy. To address these issues, many companies are leveraging oncoming technological paradigms like the Internet of Things, cloud computing, big data, and artificial intelligence. Among them, AI and big data have been researched the most by industry, since they can add significant value.

Keywords: *Biometric Cryptography, Mobile Transactions, Biometric Authentication, Digital Security, Privacy Concerns, Recognition Accuracy, Computational Complexity, Internet of Things (IoT), Artificial Intelligence (AI), Big Data.*

1. Introduction

The application of artificial intelligence (AI) and big data has undergone abrupt acceleration in modern digital technology across diverse research, development, and operational sectors ranging from finance, insurance, healthcare, social media, advertising, transportation, diagnostics, automation, e-commerce, human resources, and cybersecurity, among others. The inroad of AI and big data into biometric authentication has particularly narrowed the gap of significant security vulnerabilities of traditional PINs and passwords used for transaction authorization. The narrow gap is critically important for popular means of digital transactions such as electronic banking, mobile banking, internet banking, and point of sale, among others. However, an inherent vulnerability of the present state-of-the-art biometric traits, which AI and big data employed models are extensively involved with, rests in the exposure dilemma of biometric artifacts—outsiders' real-time capturing, printing, lifting, and reapplication along with pre-acquired biometric templates of a legitimate person in tasks of transaction impersonation.

[1]Software developer, SriSaiKrishnaMukkamala@outlook.com
[2]Site Reliability Engineer, Ankurmahida@outlook.com
[3]Service Delivery Lead, Cummins Inc, vishwanadh.mandala@gmail.com
[4]Sr Technical Support Engineer, mohitsurenderreddy@outlook.com

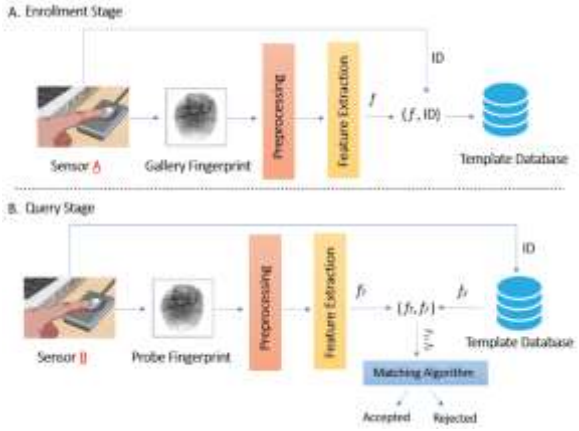
As biometric artifacts are known to exploit unique physical and anatomical characteristics of portrait subjects and subsequently exhibit the same for real-time capture and/or inculcation, the continuous innovation and adaptation of AI and big data in mitigating the exploitation of biometric traits in financial transaction authorization matrix modeling are non-delegable aspects of the present research and other future quality research investigations. To accomplish this goal and allow for the removal of dysfunctional templates, a comprehensive, secure biometric cryptography model for transaction authorization, which leverages deep convolutional neural networks, variational autoencoders, big data, and cryptogram generation models, has been introduced. The in-depth layering and detailed performance of the individual models, which collaboratively blend to achieve optimal atmospheric performance in initiative propriety confirmation along with multi-step operation, expound the intricate potential configuration of the proposed model both for its elevated data reduction advantage for system complexity and reduced risk of vulnerability to various attacks.

1.1. Background and Rationale

In recent years, rapid advancements in technologies have led to an increase in the level of digitalization of work and life at a global level. Consequently, with the digital revolution, the level of spending in the industry and decisions about payment and purchase has increased. Despite increasing awareness and concern about security, this increase in trade has resulted in increased security concerns, for example, personal identification or financial systems that have proven useful in a digital world. Inaccurate and illegal uses of someone else's physical and financial resources may result in significant financial losses.

Biometric technology enhances the development of the security of the systems used by simply employing biological characteristics for automatic recognition purposes. It is simpler than traditional security techniques used in computer fields. The system just verifies the identification of the user by different biometric methods, including their face, fingerprint, voice, DNA, keyboard dynamics, and others. The method can be classified as the device of the patent based on an immediate turn of biometric features in their physiological traits. For reasons such as emotional recognition, computer graphics, and social anthropology, biometric recognition of facial data is on a rapid increase. Among all these techniques, portable facial biometric recognition is used in different fields such as research, public security management, and customer service.

Equation 1 : Cross-sensor fingerprint matching system.



1.2. Research Aim and Objectives

This study aims to develop and evaluate the performance of a new comprehensive model of biometric user authentication for digital payments that leverages artificial intelligence and big

data for enhanced user verification. The development involves not only the integration of AI, big data, and security elements but also the improvement of their interactions. We also seek to closely examine how the evaluated security elements, their suggested interactivity, and their applied underlying controllable states impact biometric user authentication and the model's framework. Doing so is crucial to exploring the next phase of biometric user authentication for digital payments and, therefore, contributes to biometric payment security to promote widespread acceptance, trust, use, and robustness.

Element 1: Improving the user decision-making process of biometric modulus encryption by using an AI analysis engine. Element 2: Detecting and preventing spoof measurements that the current biometric encryption inspection hardware fails to identify by using AI analysis. Element 3: Since the information collected from a biometric login attempt will be used for both biometric payment and personalization, big data analytics will facilitate the connection; mapping will be performed through our artificial intelligence model. The objectives are combined to qualitatively explain how the implementation of AI, big data, and underlying variables adds to existing theoretical frameworks and recognized security suggestions for biometric user authentication. Since user transaction choices involve interacting security elements, the objectives primarily delineate the levels of users' commitment to authenticating by using AI and big data for all of the biometric logon phases performed, and the implemented recommendations to enhance biometric payment security by quantifying potential combinations of how the recommended interactions, big data input, and their suggested environmental cues impact biometric user authentication and the applied framework. The model is not applicable until clear and measurable recommendations are elaborated. This research objective is valuable because a well-specified interaction of high-quality biometric design principles and security models is essential to the development and enforcement of best practices.

2. Biometric Authentication in Digital Payments

The unprecedented expansion of advanced digital technologies and mobile communication devices in recent times, facilitated by favorable regulatory and legal frameworks, has revolutionized the payment industry. Nowadays, digital payment is a fundamental component of electronically mediated, financially inclusive, and formal economy-fueled legal transactions. Governments, businesses, and people have found themselves increasingly dependent upon these means of conducting financial transactions. However, this dependence has been matched by a commensurate rise in the complexity and variety of threats that affect the use of digital payment instruments. The most basic of these, affecting all digital payment mechanisms without exception, is the fraud that uses the true card details of one person for the financial gain of another. More sophisticated threats involve malware inserting or substituting forms to enable unauthorized transactions, interception of online passwords in a man-in-the-middle or man-in-the-app attack, and holding data to ransom using ransomware. News stories of headline security intrusions to systems mean there is a continuously unfavorable risk perception of digital payment systems.

Realizing the severe challenges faced by legacy digital payments, governments, businesses, and academic researchers embarked on creating the next generation of digital payment systems with the twin objectives of improved security and the provision of a trusted identity-based relationship between the individual holder of a purported trust root identity and the issuer of this trust root identity. The next generation of digital payment systems was based on the identification, authentication, and verification of a remote person’s identity through the use of biometric authentication methods. Unlike secret knowledge such as passwords, biometric characteristics, also termed biometric features by some, are classified as 'something that a user possesses' and 'something that a user is,' respectively. Biometric technology is perceived by many experts as providing superior identity assurance in comparison to passwords and PINs.

As a result, the issuance of trust root identity by legal authorities and the acceptance of these legally issued trust roots by relying on parties for the provision of strong identity proofing of citizens transacting in digital e-services portals, experiencing enhanced citizens' online journeys, including enhanced digital bank account opening, digital bank services taken up in a mobile environment rather than at the branch counter, personal identification, and identity verification undertaken in high-traffic control contexts, are predicated on the presentation of biometric evidence of a user's identity.

Fig 1 : Biometric Authentication Process with AI

2.1. Definition and Importance

Authentication is the most efficient approach to protect against cyber threats and attacks. It is the process of verifying the person, application, or electronic system requesting access to resources. Authentication is entirely based on the knowledge of what the individual knows or on what the person possesses. One of the major weaknesses in existing authentication technologies is that the majority of existing passwords are already known by attackers. The alternatives, such as biometric systems and smart card systems, involve other weaknesses, including false rejection, theft, or identity fraud. There are three different types of conventional authentication: password-based, token-based, and biometric-based authentication systems. The password-based authentication scheme is a traditional method but is still popular and fast for verifying the user. The differences include something the user knows, something the user has, or something the user is.

Biometric systems allow personal recognition based on physiological or behavioral characteristics, such as fingerprint, iris, voice, hand, palm, and face recognition. As biometric-based systems have gained increased interest in the security field, the biometric system market is expected to grow in the forthcoming years. Biometric authentication techniques have generated significant interest because of their unique potential: the replacement of passwords. Users dislike passwords. They lose them. They forget them. They are easily hacked. Biometric authentication uses "who you are" as your password. A second style of biometric authentication is its use in two-factor authentication, as in something you have plus something you are. Here, the biometric is the second factor as well as the technique to authenticate that you have possession of the "first-factor" device you have registered.

2.2. Current Challenges

Unfortunately, few biometric databases can handle natural changes in attributes over time. External effects such as haze, sunscreen, skin modifications, and plastic surgery can cause the performance of initial biometric samples to degrade significantly due to factors like facial amplitude, social demographics, ambient lighting, and other influences. The credibility of facial recognition services generally deteriorates or becomes ineffective under different lighting conditions at various address points. Performance degrades rapidly even with minor modifications. Since facial biometric models are heavily dependent on updates, a practical approach is to use this type of perceptible trait for challenging conditions. Given that facial challenge databases are scarce, they often present adverse effects. Training biometric systems with variations such as pose, light, trauma, and age can lead to unique errors of unprotected

moral intent and possibility. Clothing and hairstyle variations also contribute significantly to these challenges. It is known that hostile individuals often try to change their gender and age to adapt to the template. If current megapixel cameras are further developed, the operating distance will be extended, leading to a general increase in later risk evaluation exams. Multibiometric systems can enhance matching accuracy and the likelihood that the results of noise, age, plastic surgery, and other issues can be confirmed. Some statistical algorithms can be easily fooled by everyday objects when the noise is too large. Information changes require expert knowledge and can only be partially addressed, limiting the effectiveness. Publicity poses a threat to broadband and narrowband wireless broadcasts as lobby utterances. Particularly in dim lighting, many existing high-end facial models exhibit low reliability, and the errors of line algorithms will increase. A recent survey on deep face identification also reveals that large textured clothing can mask facial biometric models, but slashing or inspection measures may fail to catch resource substitution. High-resolution photos can spoof face recognition by effectively scanning advanced holographic glasses. Fibers within thin synthetic materials are being exploited in a new class of face alternatives because of their branding capabilities. The disadvantage is that more views of suspicious individuals increase the opportunity for more speakers.

3. Role of AI in Biometric Authentication

The role of AI is increasing in the context of biometric systems. The use of multimodal biometrics is growing rapidly in various sectors due to its high robustness and discrimination. Fusion at the deep level can be sensed in the form of multilayer perceptrons, ISC, Gram, etc. These fusions dealing with the change of global data are faster and can improve the result by increasing the discriminative capacity. Cryptographic hashing on a multimodal biometric is recognized for its privacy and transparency. In the situation of the deep learning model, the idea of transferring traditional annotation and image categories to study neural network estimating models is proposed and used. For the creation of this recognized multimodal data, there is an extended deep-learning CNN network.

A semi supervised AI method by signal diversity is made to verify MASR biometrics. The use of AI forensic techniques, in combination with other technologies, presents numerous open issues and technical opportunities. The identification of a person's identity using soft biometric traits is performed using deep learning models. After the person was identified, the model was modified based on the identified characteristic. The advances in the application of deep learning techniques to detect some aspects of identity in particular, and therefore the automatic recognition of a person in general, are discussed.

Fig 2 : Types of Biometric Authentication

3.1. Machine Learning Algorithms

Machine learning is the science of getting computers to learn and act like humans do, and improve their learning over time in an autonomous fashion. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns, and make decisions with minimal human intervention. According to the way supervised algorithms are trained and tested, three models are the best to work with classification models, regression models, and recommendation models. In supervised algorithms, important supervised learning models include support vector machines, nearest neighbor algorithms, Gaussian mixture models, Bayesian networks, decision trees, neural networks, etc. In unsupervised algorithms, vital methods that are generally used include clustering through means of grouping the data, k-means algorithm, mean-shift algorithm, hierarchical clustering algorithm, and association rules model, which find the hidden patterns within the data.

The machine learning algorithm, random forest, was also developed for considerations of nonlinearity, high accuracy, high versatility, and bias-variance analysis, ensuring that all potential conditions can be solved at all times, avoiding the occurrence of singular cases. The random forest model is thus more robust, with no need for data pretreatment. With potential, the scale parameter of this model can also be reduced, if necessary, reducing the training time; data within relevance will be increased. Within random forest applications, the importance of each type of data is evaluated differently. These types of data are evaluated uniquely to represent significant structures; they include variable importance, misclassification rate, reducibility of size, and proximity measure.

3.2. Deep Learning Techniques

In recent times, with the development of big data and Internet technology, network in-depth learning has shown great potential in the field of biometric recognition and has great advantages in many cross-modal recognition tasks. In the field of face recognition, the target dataset of current network in-depth learning research is mainly some large-scale labeled face image datasets, and the current research for cross-modal face recognition is mainly complete for visible and infrared light images of face modal recognition. Few of them are dedicated to other cross-modal face recognition tasks, such as cross-modal photo-to-sketch face recognition. In this paper, we use in-depth learning technology to transform the two modes of cross-modal face images into feature space that meets the distribution consistency and decision consistency

between the two modes, and then design a large-margin loss function for end-to-end training to realize photo-to-sketch face recognition.

Our research work proposes a local model alignment and dense feature mapping loss function, aiming at achieving high originality and large differences between intra-class clusters and inter-class clusters within the batch. Simultaneously, with the help of domain-specific dense connections, this work builds a mapping relationship between the two-dimensional features of the photo and the sketch, realizes the conversion between the two modes via the network cascade operation, and finally realizes the visual-to-sketch face recognition conversion task in an end-to-end manner. Extensive experimental results have shown the validity and effectiveness of our approach. Compared to the numerous facial recognition projects that have garnered significant attention in network in-depth learning research, existing studies on cross-modal face recognition mainly focus on visible light and infrared light images. In recent years, with the rapid development of network depth learning algorithm technology, the research of cross-modal recognition has been considered by some scholars, but few of them have paid attention to the research on visible light and sketch photo-to-sketch cross-modal face recognition. In this work, our research focuses on the development of visible light to sketch face recognition. There are considerable difficulties, and there are still some specific challenges and objectives: first and foremost, the face specimens of the two modes have greatly different features. Second, there are great differences between sketch drawing and photo humanistic representation methods, and the two modalities are very different in similar and different aspects.

4. Big Data Analytics in Security

Leveraging Big Data for Security: With the social trend of associations gravitating towards AI, investment, and practice in the field of big data security based on machine learning and cloud storage is incessantly sweeping numerous commercial banks and governments, in addition to massive organizations. The implications of big data technology in the field of security are mostly seen in the following dimensions. 1) Big Data can improve security analysis and judgment. 2) Based on Big Data cloud storage, AI outputs security knowledge and resources. 3) Large data sets and strong correlation rules, in the case of truths involving important data, help to develop high-level security decision-making systems. The development of big data technology can lead to valuable investments that not only provide a professional technical basis to those involved in data security but also better maintain data flows in the big data era.

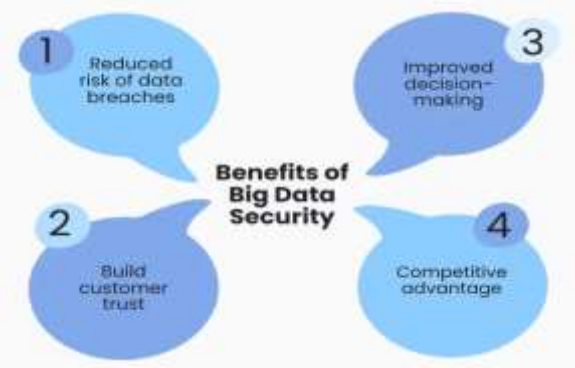


Fig 3 : Benefits of Big Data Security

Big Data Can Improve Security Analysis and Judgment: In the generation of big data, numerous information retrieval technologies have been amplified, including the coverage of deep learning in conjunction with big data technology in the field of security. Big Data has made significant breakthroughs and launched a more sophisticated search experience for pattern recognition, aiding in speeding up the development of information index queries as well

as structure queries. Data pyramid caching configuration is based on the distribution of data and machine learning for acceleration. In the concepts of cloud storage and organization, cloud storage based on anti-gender index and anti-gender query proposes more favorable and far-reaching storage management techniques. As the effect of studying big data analytics, database utilization of data, and big data technology applied in fields such as anti-global search, database security, and anti-theft storage is broadened, providing security technology for big data.

4.1. Data Collection and Storage

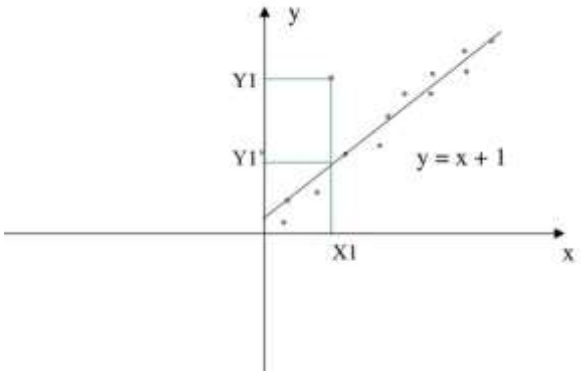
Biometric data are physical or behavioral human characteristics used to confirm or determine an individual's identity. This type of identification is frequently utilized in several fields such as authentication of access, e-voting, and e-banking. Biological data include fingerprints, facial features, the iris, DNA, palm print, and voice recognition. The increasing use of biometric technology everywhere is expected to save lives and fight identity theft in the economy. This deployment has opened up awareness of the threats that may significantly affect national and personal security if the biometric information being recorded, saved, and retrieved is not correctly governed.

Fingerprinting, like facial characteristics, generates discrete pictures that are electronically stored in a database. How these biometric samples are drawn, encoded, and transferred to the credential in the server is called data collection and storage. The significant disadvantage of biometric procedures is the number of fingerprints and images on a face that can potentially be included as lifelong personal identity verifiers. A hacker who uses a collection of unique biometric identifiers stored in a database can impersonate a new profile, invalidate the information, and compromise the integrity of the credential. The private rights to biometrics, even with proper de-identification, are not influenced by using biometric identifiers of a person who has not yet been considered to be involved in anything with sensitive identity information. It is in this context that it is assumed to be of critical significance that security aspects must regulate the individual's vital attributes before that data is distributed and stored.

4.2. Data Processing and Analysis

The data collected are then filtered to remove errors, either by classifiers or by removing or modifying any data that signal the possibility of error. This step is particularly important when processing mobile-based transactions, as mobile users are moving around and may change in unexpected ways between the time they enroll and the time they scan. This could potentially affect the performance of the biometric recognizer during a real scan. The biometric data extracted via mobile users' information are first brought into the template level by using an appropriate error learning approach. This can be done by transforming the raw data into an uncorrelated signature; then through normalization and threshold processes, a binary array is produced from the pattern, and this array is matched with the pre-existing user's array. In case of a binary mismatch, a new facial binary array is created and updated in terms of the template. The validation process is an essential phase in choosing a better facial biometric identification algorithm, which in turn impacts the performance of the system. It is a very important step to determine the list of algorithms that are best suited to be deployed in processing the data of the system. Once the extracted biometric image passes validation, the facial image is stored securely in the database. In case of a match at the template level, the measured raw data stored in the database is declared a match for the authorized user since it must be the owner of that raw data.

Equation 2 : Data PreProcessing (Pra Proses Data)



5. Proposed Comprehensive Model

Given the challenges of security in digital payments, the current paper has explored the concept of digital security. It has investigated the present status of digital payments in India, their benefits and associated risks, deterrence for security in digital payments by enterprises, current security measures, human, organizational, and legal measures for security, security architecture of the business ecosystem, biometric authentication and security in digital payment, AI, and big data for enhanced security in digital payments, and the comprehensive model for enhanced security in biometric authentication for digital payments. A comprehensive model for enhanced security that stems from a deep understanding of the constituent and allied issues governs the enhancement of convenience and the reduction of vulnerabilities in the e-banking structure. Since the literature has not identified a critical comprehensive model based on AI and big data for enhanced security in biometric authentication, the study embarks on identifying such a comprehensive model. While various kinds of literature speculate upon the criteria governing enhanced security in e-banking, our focus seemed unique as we used AI, big data, and a comprehensive model to sustain the enhanced security in biometric authentication for digital payments.

Digital technology has emerged as an important enabler of improved access, security, and affordability in financial services. With sustained innovation, digital payments might improve the business climate. As technology advances rapidly, contemporary security measures in digital finance must be coupled with AI and big data-enabled solutions to be robust. Given current resolutions being employed in digital payments, it is evident that the payment ecosystems must effectively shield against a growing number of threats that are being perpetuated by elements that align with interconnected digital technology and crime. AI and big data applied for security in digital payment require getting back to the proverbial drawing board to architect digital financial ecosystems that converge interoperable technological and administrative elements dressed for the myriad challenges portrayed by inherent risks in digital financial services. The result is an enhanced security model that calls for the use of advanced technology.

5.1. Integration of AI and Big Data

In the present dynamic threat landscape, AI and Big Data are changing the security paradigm by enabling pattern recognition intelligence, self-learning systems, and the ability to create anomaly detection engines that can detect unknown or hidden threats. AI provides predictive and learning models that can sense and predict events and provide feedback to enhance existing security checks. Big Data provides the capability of ingesting, processing, and understanding a massive amount of data in real-time, which is generated by different systems. In this way, Big Data has the potential to provide multiple hyperdimensional security solutions to solve conventional as well as new threats—for example, the unauthorized use of biometric identities. The integration of AI with Big Data opens up security opportunities based on the increased

availability of structured and unstructured data. As a consequence, next-generation data analytics, domain-specific insight-driven solutions, and decision support systems have the potential to change conventional security checks from reactive to proactive and, in some cases, even predictive. Currently, the most significant developments addressing security threats involve learning and predictive security models, risk intelligence, machine learning algorithms, and pattern recognition tools, all leveraging the science of AI. However, leveraging AI for predictive security is incomplete without Smart Data. AI and Smart Data need to be combined to create domain-specific models with tailored designs, visual and streamlined architectures, high-performance computing strategies, and new-generation preemptive and self-learning security engines for applications in biometric authentication security. Digital payments are one such demanding and innovative application for which conventional security checks are no longer sufficient. This new security biometric industry needs state-of-the-art security frameworks for improving security and privacy parameters. These can only be realized through the technology-intensive power of AI and Big Data.

Fig 4 : Improving Payment Processing with AI

5.2. Key Components and Features

Recent innovations in leveraging AI in biometric authentication include film and anti-spoofing technologies that help ensure detection, which can deter spoofing attacks. Furthermore, AI-enabled biometric templates reduce errors and tackle the problems of re-issuance for identification and smart card management. Anti-spoofing technologies result in a significant decrease in entry time. AI-enabled security elements have resulted in a more efficient identification process, with algorithms that can work quickly and accurately across data coming from many different kinds of sensors. AI-enabled security enhances both the accuracy and the requisite augmentation to withstand collusion attacks and cross-sensor spoof detection. Furthermore, customization available in AI-related security, such as algorithm attributes and finer control of an algorithm, results in more robust biometric characteristics.

6. Case Studies and Applications

The authors published a model with improved security in biometrics by taking advantage of the combination of big data and moderate AI and pointed to the possibility of recurring costly results with extreme AI. The contribution aimed at integrating big data features into biometrics by looking at changes in technology while mapping the trend of significant attention and the effects from the outside world. Featuring new concepts and meanings that lead to a strategic future model with a broad vision based on intelligence, focusing on value co-creation to reach a more digital approach. They reveal a comprehensive model for biometrics in digital payments thanks to strategic intelligence, encouraging investment to pave the way for expanding knowledge that is realized in social complexities and applications to everyday life that affect human beings.

Digital payment systems are increasingly a target of attacks, so security is an important and essential component in managing these systems. The models created in the different works

presented should integrate digital security into the essential, incorporating cryptographic attributes in combinations and configurations, so that only the correctly authorized individuals have access to the right use. Likewise, more and more solutions should include AI in conjunction with big data as a means of improving false detection rates and adapting access to trusted entities. It still aims to integrate functional intelligence that can contribute to understanding and, in some way, even interpret the real presumed feelings of customers in their different concerns and participation regarding the advances in security that are proposed to be carried out in these sensitive systems. The authors end this work with proper bibliographical research in a structured manner in various security domains combined with the synergies of AI and big data.

6.1. Real-world Implementations

There has been significant work in developing real-world security implementations locally and across the globe in the fields of banking and finance, e-commerce, healthcare, insurance, and monitoring and detection, using biometric data and artificial intelligence. However, there is still a dearth of scholarly research proposing solutions that combine biometric data, big data, and machine learning to provide comprehensive and state-of-the-art digital security models that consider transaction authenticity, transaction validation, and human impersonation threats. While some organizations may use other digital security techniques in combination with biometric data to further enhance security, it is important to investigate the security offered by solutions that solely use biometric data, big data, and machine learning.

We will undertake an experimental analysis of the proposed model by conducting an empirical study with a real-world organization that has a large user base globally and offers both mobile and web financial digital services. We will provide the model design semi-formal specifications to aid in the construction of the solution and field study implementation and highlight the key outcomes and benefits. This work aims to fill the gap in the literature by making the proposed model accessible to professionals in the field for product specification and design, software development, implementation, experimental analysis and testing, and subsequent value realization.

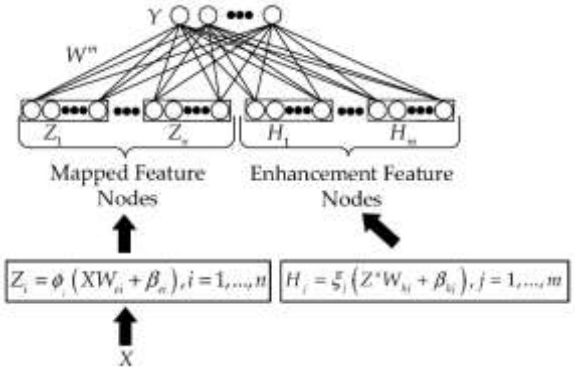
6.2. Success Stories and Lessons Learned

Our team has successfully developed four solutions based on combining biometric authentication and mobile payment systems. These solutions are used in the world's first national fingerprint-based mobile payment system in Vietnam and other countries. The experience that we have gained from collaborating with large data providers has inspired us to develop the Security Enhanced Compressive Sensing-Based Iris Recognition system in the next project. In this system, the one-time, one-use, zero decoding error rate encryption chaff images are created by the iris presentation attack detection system. Moreover, we have proposed an initial solution that securely matches two templates of any type in the biometric big data. In Particular, the learners could take advantage of the proposed chaincodes to improve the performance of deep convolutional neural networks.

The potential that we discover by developing these solutions has given us valuable lessons about authentication policymaking, technical aspects, and application. Specifically, the biometric authentication policy recommendations and flexible decision-making strategies have led us to propose the first biometric-based orchestrated payments concept. The experiences have also given us valuable insights to resolve the current biometric privacy and security concerns. We illustrate this by developing a theorem that could prove that the public template and the chaff images have no privacy for specific persons but still preserve the template security. The proposed chain code tools could be used to compute the biometric reversal of the hash for privacy protection purposes. We then complete the privacy and security enhancements

in the unique solutions. These experiences will give the readers meaningful heuristic advice in choosing similar matching strategies used in the solutions.

Equation 3 : Anomaly Detection Algorithm Based on Broad Learning System



7. Challenges and Future Directions

There are several challenges in implementing the proposed framework for the FinTech sector: The unavailability of contextual data and a lack of access to a dataset that is suitable for training and validating the innovative AI models so that penalty functions can predict in-progress attacks. The issue of limited availability of methods for enhancing continuous re-verification for transactions while enforcing security constraints in the online setting. Scalability issues can arise when an AI and Big Data framework is reused beyond a specific entity with many users. Operations must be streamlined so that the entity possesses software that enables efficient data processing. In the case of the similarity threshold constraint, a model's performance and an attacker's success are directly linked and are influenced by the size of the biometric sample. However, there are no regular intuitive ways of determining a threshold with these constraints. Threats by AI tools, scenarios, admissibility, fairness, and training quality, among other factors, should be considered. The transparency of the operations may also pose a challenge. Since the detection of in-progress attacks is performed in continuous time through user-device interactions, real-time constraints must be enforced. A lack of transparency through various activities may interfere with user satisfaction. It is necessary to maintain a balance between the need to maintain minimal interruptions in transactions and user authentication, and at the same time, protect user privacy. Consequently, an adaptive learning model that factors in such considerations would be highly desirable. Although user studies were conducted under lab conditions, a field-catalyzed model has been defined that will allow deploying the model safely. The methodology will motivate a user to challenge an in-progress attack by creating various scenarios. In addition, the results will provide estimates of the likelihood of in-progress attacks and explain why decisions were made. Ethical considerations must take into account the impact of a new biometric-driven AI approach that is transparent, fair, and accurate as usual.

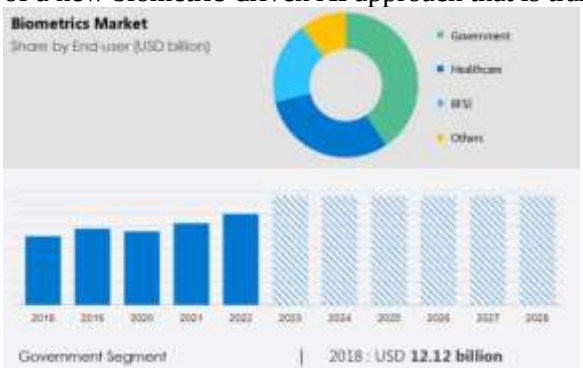


Fig 5 : Biometrics Market Size Growth Report 2024 - 2028

7.1. Ethical and Privacy Concerns

The unified Security, Ethical, regulatory, and policy model (SERP model) leverages seven ethical and privacy consequences. It is defined by a combination of four factors: the country factor, the policy and norms factor, the ID factor, and the biometric authentication update factor. The unified model identifies seven ethical and privacy consequences, including data breaches, data misuse, surveillance, transparency, stigma, economic performance, and moral/social norms.

Data breach is a privacy-related issue that involves the theft of sensitive, confidential, or protected data. The typical characteristics of the theft comprise unauthorized access, use, disclosure, and destruction. When such information is revealed to the public, consequences include protective responses from individuals, corporate responses, and legal consequences. Misuse of sensitive private data occurs when data meant for one purpose is put to another use without obtaining permission. This misuse can lead to various consequences, including stigmatization of individuals, causing significant social and moral concerns. Revelations about other individuals' sensitive data, such as race, religious affiliation, or a particular sexual orientation, have caused significant outrage, as such actions can seriously damage or destroy people's lives through public humiliation or persecution. Surveillance of individuals is similarly a major privacy issue raised by some surveillance technology. Rejection of biometric use can affect societal and economic performance. Data subjects may refuse to participate in large data processing programs, for example, that measure public opinion of law enforcement criminal strategies. Several surveys have shown public ambivalence concerning the extent of programs aimed at combating such activities. This situation leads to data-starved environments in which data-for-the-sake-of-analyzing techniques are deployed. Finally, failures to meet the required level of transparency do not identify concerns that would face high-performance standards during the development of surveillance recognition systems. The projections associated with the validity have been considered discriminatory, and these deficiencies have become ethical issues in the use of biometrics, both in its forensic applications and its applications to surveillance. Such deterministic categorization of people may generate stigma for those who have been 'chosen' as highly suspect of criminal intent, especially if profiling approaches are incorporated into the recognition system.

7.2. Technological Advancements

The confluence of AI/ML, next-generation biometric sensors, and fusion approaches, natively high-performing cryptography, tokenization, and underlying trust services ecosystems will represent fourth or fifth-generation biometric authentication payment capabilities. The path will be complex, but with cooperation and collaboration among device manufacturers, sensor scientists, technologists, algorithms, standards bodies, application developers, and local and global regulators and financial institutions, the biosensing future will be brighter. In the not-so-distant future, multi-modal capabilities will be available, possibly at the application level. Wider operational robustness will be the outcome of the genuine user experience while ensuring sufficient robustness against certain kinds of spoofs. Third or fourth-generation combinatory, cryptographic as a positive opposed to a defensive capability, AI/ML distributive self-training and governance capabilities will be developed and integrated into digital payments and digital commerce such that national and supra-national security – not just financial – is actively operational, thereby deterring the intention of conflicts and wars that result in national and supra-national referee-based organizations. Several scenarios have been proposed that both challenge the validity of the current and future payment methods, providing a stark examination into critical flaws in both people's perceptions and organizations' conception of levels of

security and the role of data and how fingerprint data as both a financial and security-focused enabler could be refocused.

8. Conclusion

This chapter focuses on the integration of diverse AI-driven technologies for optimized security in biometrics and provides a unified approach for enhancing security in biometric authentication systems. The various security threats of biometrics are shown. The standard security measures of biometric authentication, that is, template security and privacy protection methods, are discussed. The need to enhance security to withstand the present higher speed and sophisticated multi-pronged attacks is justified. It has been analyzed how various current digital technologies such as big data tools in contrast sensitive convolutional neural network preprocessing, and the use of trend-sensitive replicators in asymmetric cryptography that also have counter-personation and non-repudiation abilities in biometric applications can be cut off for enhanced biometric authentication system security features due to these unique possibilities. The chapter is structured in a meaningful manner and the narrative is insightful. The chapter throws light on the advancements in AI and big data tools, followed by the unified model. The significant section of this chapter is the model validation from differing dimensions. The evaluation of the quality and the computational complexity of AI features for biometric security applications. Then, several tactics for multi-engineering AI have also been recommended. The next logical step will be the creation of some prototype biometric authentication systems by the unified model to establish it as a reference model framework for biometrics security. The chapter concludes on the perceived benefits, applications, and challenges of the new paradigm of systems.

8.1. Summary of Findings

In this chapter, we initiated our study by presenting the limitations of traditional fingerprint-based authentication systems, particularly when used in real-time identification. We described how each traditional technique neglects its intrinsic characteristics to handle the problem. The wrong handling of these problem characteristics in large databases that have to be searched with finger images contributes to slowing down the identification time. We discussed how the current solutions that eliminate these characteristics to reach results have several times a worse level of success than traditional fingerprint recognition techniques that perform minutiae extraction as the first step before comparison.

We proposed our approach based on the philosophy that negative responses can eliminate several images with potential similarity from future comparisons. This is the concept of image simplification and its effectiveness in accelerating the processes of identification. Our methods are specifically designed to accelerate the fingerprint identification process by eliminating characteristics that contribute to slowing down the search for all fingerprint images, even though we are using characteristics to perform image comparisons.

8.2. Implications and Recommendations for Future Research

Implications of the findings from the proposed model are far-reaching and deserve considerable attention from relevant stakeholders. The model creates an interface between biometric authentication, big data analytics, and AI for digital payments. It leverages these technologies through feature extraction and transfer learning of encoded data to improve transaction certainty and security. Biometric physiological data ownership and security management are discussed. Ethical considerations could inform security policy. Besides reducing transaction uncertainty, however, the proposed system offers a business opportunity for the digital payments ecosystem. Firms employing this model, through the incorporation of ethical considerations, will derive maximum utility from innovations in the technology that underlies digital transactions.

Notwithstanding the plethora of advantages that biometric authentication systems offer, this study does not overlook the potential risks and limitations related to the usage of such systems in digital transactions. The findings are also presented as a basis for recommendations for future research. The direction for future research activities revolves around considering this model for more varied environments and investigating the potential for processing accuracy to become biased during transfer learning, such that possible differences could emerge in the ability of one user group to model another group. In an environment with a significantly larger number of biometric data traits, the extent of the benefits and significance of transfer learning could also be explored. Consideration of ethics stems from the benefits that come from the usage of technology. Addressing potential ethical issues at the discussion phase of big data and AI applications offers two advantages.

8. References

[1] Pillai, S. E. V. S., Avacharmal, R., Reddy, R. A., Pareek, P. K., & Zanke, P. (2024, April). Transductive–Long Short-Term Memory Network for the Fake News Detection. In 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-4). IEEE.

[2] Zanke, P., Deep, S., Pamulaparthyvenkata, S., & Sontakke, D. Optimizing Worker's Compensation Outcomes Through Technology: A Review and Framework for Implementations.

[3] Vaka, D. K. (2024). Procurement 4.0: Leveraging Technology for Transformative Processes. Journal of Scientific and Engineering Research, 11(3), 278-282.

[4] Manukonda, K. R. R. (2024). ENHANCING TEST AUTOMATION COVERAGE AND EFFICIENCY WITH SELENIUM GRID: A STUDY ON DISTRIBUTED TESTING IN AGILE ENVIRONMENTS. Technology (IJARET), 15(3), 119-127.

[5] Mandala, V., & Mandala, M. S. (2022). ANATOMY OF BIG DATA LAKE HOUSES. NeuroQuantology, 20(9), 6413.

[6] Bhattacharya, S., Najana, M., Khanna, A., & Chintale, P. (2024). Securing the Gatekeeper: Addressing Vulnerabilities in OAuth Implementations for Enhanced Web Security. International Journal of Global Innovations and Solutions (IJGIS).

[7] Mahida, A. (2024). Integrating Observability with DevOps Practices in Financial Services Technologies: A Study on Enhancing Software Development and Operational Resilience. International Journal of Advanced Computer Science & Applications, 15(7).

[8] Muthu, J., & Vaka, D. K. (2024). Recent Trends In Supply Chain Management Using Artificial Intelligence And Machine Learning In Manufacturing. In Educational Administration Theory and Practices. Green Publication. https://doi.org/10.53555/kuey.v30i6.6499

[10] Kommisetty, P. D. N. K., & Nishanth, A. (2024). AI-Driven Enhancements in Cloud Computing: Exploring the Synergies of Machine Learning and Generative AI. In IARJSET (Vol. 9, Issue 10). Tejass Publishers. https://doi.org/10.17148/iarjset.2022.91020

[11] Avacharmal, R. (2024). Explainable AI: Bridging the Gap between Machine Learning Models and Human Understanding. Journal of Informatics Education and Research, 4(2).

[12] Pamulaparthyvenkata, S., & Avacharmal, R. (2023). Leveraging Interpretable Machine Learning for Granular Risk Stratification in Hospital Readmission: Unveiling Actionable Insights from Electronic Health Records. Hong Kong Journal of AI and Medicine, 3(1), 58-84.

[13] Kumar Vaka Rajesh, D. (2024). Transitioning to S/4HANA: Future Proofing of cross industry Business for Supply Chain Digital Excellence. In International Journal of Science and Research (IJSR) (Vol. 13, Issue 4, pp. 488–494). International Journal of Science and Research. https://doi.org/10.21275/sr24406024048

[14] Manukonda, K. R. R. (2024). Leveraging Robotic Process Automation (RPA) for End-To-End Testing in Agile and Devops Environments: A Comparative Study. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-334. DOI: doi. org/10.47363/JAICC/2024 (3), 315, 2-5.

[15] Kommisetty, P. D. N. K., & Abhireddy, N. (2024). Cloud Migration Strategies: Ensuring Seamless Integration and Scalability in Dynamic Business Environments. In International

Journal of Engineering and Computer Science (Vol. 13, Issue 04, pp. 26146–26156). Valley International. https://doi.org/10.18535/ijecs/v13i04.4812

[16] 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).

[17] Balakrishnan, A., Jain, V., Chintale, P., Gadiparthi, S., & Najana, M. (2024). Blockchain Empowerment in Sanctions and AML Compliance: A Transparent Approach. International Journal of Computer Trends and Technology.

[18] Mahida, A., Chintale, P., & Deshmukh, H. (2024). Enhancing Fraud Detection in Real Time using DataOps on Elastic Platforms.

[19] Vaka, D. K. (2024). Enhancing Supplier Relationships: Critical Factors in Procurement Supplier Selection. In Journal of Artificial Intelligence, Machine Learning and Data Science (Vol. 2, Issue 1, pp. 229–233). United Research Forum. https://doi.org/10.51219/jaimld/dilip-kumar-vaka/74

[20] Kommisetty, P. D. N. K., & dileep, V. (2024). Robust Cybersecurity Measures: Strategies for Safeguarding Organizational Assets and Sensitive Information. In IJARCCE (Vol. 13, Issue 8). Tejass Publishers. https://doi.org/10.17148/ijarcce.2024.13832

[21] Avacharmal, R., Pamulaparthyvenkata, S., & Gudala, L. (2023). Unveiling the Pandora's Box: A Multifaceted Exploration of Ethical Considerations in Generative AI for Financial Services and Healthcare. Hong Kong Journal of AI and Medicine, 3(1), 84-99.

[22] Pamulaparthyvenkata, S. (2023). Optimizing Resource Allocation For Value-Based Care (VBC) Implementation: A Multifaceted Approach To Mitigate Staffing And Technological Impediments Towards Delivering High-Quality, Cost-Effective Healthcare. Australian Journal of Machine Learning Research & Applications, 3(2), 304-330.

[23] Vaka, D. K. (2024). Integrating Inventory Management and Distribution: A Holistic Supply Chain Strategy. In the International Journal of Managing Value and Supply Chains (Vol. 15, Issue 2, pp. 13–23). Academy and Industry Research Collaboration Center (AIRCC). https://doi.org/10.5121/ijmvsc.2024.15202

[24] Kommisetty, P. D. N. K., vijay, A., & bhasker rao, M. (2024). From Big Data to Actionable Insights: The Role of AI in Data Interpretation. In IARJSET (Vol. 11, Issue 8). Tejass Publishers. https://doi.org/10.17148/iarjset.2024.11831

[25] Rami Reddy Manukonda, K. (2024). Multi-Hop GigaBit Ethernet Routing for Gigabit Passive Optical System using Genetic Algorithm. In International Journal of Science and Research (IJSR) (Vol. 13, Issue 4, pp. 279–284). International Journal of Science and Research. https://doi.org/10.21275/sr24401202046

[26] Tabbassum, A., Chintale, P., Praveen, G., & Najana, M. (2024). The Impact of AI on Future Employment Patterns. International Journal of Global Innovations and Solutions (IJGIS).

[27] Mahida, A. Explainable Generative Models in FinCrime. J Artif Intell Mach Learn & Data Sci 2023, 1(2), 205-208.

[28] Vaka, D. K. (2023). Achieving Digital Excellence In Supply Chain Through Advanced Technologies. Educational Administration: Theory and Practice, 29(4), 680-688.

[29] Avacharmal, R., Sadhu, A. K. R., & Bojja, S. G. R. (2023). Forging Interdisciplinary Pathways: A Comprehensive Exploration of Cross-Disciplinary Approaches to Bolstering Artificial Intelligence Robustness and Reliability. Journal of AI-Assisted Scientific Discovery, 3(2), 364-370.

[30] Kommisetty, P. D. N. K., & Nishanth, A. (2024). AI-Driven Enhancements in Cloud Computing: Exploring the Synergies of Machine Learning and Generative AI. In IARJSET (Vol. 9, Issue 10). Tejass Publishers. https://doi.org/10.17148/iarjset.2022.91020

[31] Pamulaparthyvenkata, S., Reddy, S. G., & Singh, S. (2023). Leveraging Technological Advancements to Optimize Healthcare Delivery: A Comprehensive Analysis of Value-Based Care, Patient-Centered Engagement, and Personalized Medicine Strategies. Journal of AI-Assisted Scientific Discovery, 3(2), 371-378.

[32] Vaka, D. K., & Azmeera, R. Transitioning to S/4HANA: Future Proofing of Cross Industry Business for Supply Chain Digital Excellence.

[33] Manukonda, K. R. R. (2023). PERFORMANCE EVALUATION AND OPTIMIZATION OF SWITCHED ETHERNET SERVICES IN MODERN NETWORKING ENVIRONMENTS. Journal of Technological Innovations, 4(2).

[34] Kommisetty, P. D. N. K. (2022). Leading the Future: Big Data Solutions, Cloud Migration, and AI-Driven Decision-Making in Modern Enterprises. Educational Administration: Theory and Practice, 28(03), 352-364.

[35] Jain, V., Balakrishnan, A., Beeram, D., Najana, M., & Chintale, P. Leveraging Artificial Intelligence for Enhancing Regulatory Compliance in the Financial Sector.

[36] Mahida, A. (2023). Enhancing Observability in Distributed Systems-A Comprehensive Review. Journal of Mathematical & Computer Applications. SRC/JMCA-166. DOI: doi. org/10.47363/JMCA/2023 (2), 135, 2-4.

[37] Vaka, D. K. (2024). From Complexity to Simplicity: AI's Route Optimization in Supply Chain Management. In Journal of Artificial Intelligence, Machine Learning and Data Science (Vol. 2, Issue 1, pp. 386–389). United Research Forum. https://doi.org/10.51219/jaimld/dilip-kumar-vaka/100

[38] Avacharmal, R., Gudala, L., & Venkataramanan, S. (2023). Navigating The Labyrinth: A Comprehensive Review Of Emerging Artificial Intelligence Technologies, Ethical Considerations, And Global Governance Models In The Pursuit Of Trustworthy AI. Australian Journal of Machine Learning Research & Applications, 3(2), 331-347.

[39] Tilala, M., Pamulaparthyvenkata, S., Chawda, A. D., & Benke, A. P. Explore the Technologies and Architectures Enabling Real-Time Data Processing within Healthcare Data Lakes, and How They Facilitate Immediate Clinical Decision-Making and Patient Care Interventions. European Chemical Bulletin, 11, 4537-4542.

[40] 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

[41] Kodanda Rami Reddy Manukonda. (2023). Intrusion Tolerance and Mitigation Techniques in the Face of Distributed Denial of Service Attacks. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.11220921

[42] Bhardwaj, A. K., & Chintale, P. (2024). The Role of the Integral Driven Architect in Agile Project Management. In Practical Approaches to Agile Project Management (pp. 254-269). IGI Global.

[43] Mahida, A. (2023). Machine Learning for Predictive Observability-A Study Paper. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-252. DOI: doi. org/10.47363/JAICC/2023 (2), 235, 2-3.

[44] Vaka, D. K. (2024). The SAP S/4HANA Migration Roadmap: From Planning to Execution. Journal of Scientific and Engineering Research, 11(6), 46-54.