Artificial Intelligence for Futuristic Banking

Moksha Thisarani
Faculty of Information Technology
University of Moratuwa
Sri Lanka
moksha.17@itfac.mrt.ac.lk

Dr Subha Fernando
Faculty of Information Technology
University of Moratuwa
Sri Lanka
subhaf@uom.lk

2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) | 978-1-6654-4963-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICE/ITMC52061.2021.9570253

Abstract*—Artificial Intelligence (AI) has become an essential resource for large banks that deal with regulatory changes, new Anti-Money Laundering (AML) obligations and vulnerable fraud-prone clients. Cybersecurity has thus become a hot topic due to security failures using traditional methods and concerns about how companies use the personal data collected from clients or their regular users. The most obvious apparent reason why cybersecurity is critical in banking sector transactions is to protect client assets with a high level of data privacy. The main approaches in the front office conventional banking such as AI chatbots, smart virtual assistants and biometric user authentication are discovered to answer security challenges and to enhance prosperity in the field. Concurrently, advanced AI applications in fraud detection, fraud risk monitoring, anti-money laundering techniques and cross-border payments handling are observed under the back-office operations. The paper reviews the conceptualizations of privacy concerns and the antecedents and consequences of using AI-power in the banking sector. Moreover, overlooked limitations of AI such as scarcity of quality data, a rise of hidden-bias in suggestions and obliviousness of lacking knowledge are discussed with several thriving solutions.

Keywords*—Artificial Intelligence, Banking, Cybersecurity, Information Privacy

I. Introduction

With the introduction of Computer Technology, Electronic Communications Technology, and Information Technology, banking experiences have been upgraded and expanded into Mobile banking and Online banking, in addition to traditional walk-in Offline banking operations. Electronic banks, Mobile banks and the Internet bank are considered as virtual banks. Virtual banking operations do not necessarily require a face-to-face trade with the customer. This provides banks and customers with great convenience. However, it introduces risks when accurately validating the legality of customers, and it becomes an important concern for avoiding potential illegal interference and damages.

Internet banking brings convenience and significant risks concurrently. Meanwhile, the security of Internet banking has been the focus of attention from all quarters of society. Although, the vast majority of reasons why customers disclaim or abstain from Internet banking is the reliance of uncertainty in transaction security among net citizens who refuse to operate with Internet banking. As online banking safety studies need to be improved to strengthen the security of the system, many commercial banks have also introduced several security initiatives. User account details privacy and transaction details privacy are the two main areas which have a more significant impact on managing banking information security under the aspect of maintaining data privacy. Over the years, endpoint security has come a long way from using an antivirus solution to using AI for data protection. The endpoint security is taken to the next level as AI can identify, block and evaluate attacks quickly and accurately. Also, AI can conduct comprehensive behavioural analysis using sophisticated AI algorithms in user recognition and authentication over existing approaches[1] such as password based systems.

Customers should be given quick access to frequently requested data for their convenience using smart approaches as digitized information provided in web and mobile applications might be scattered. Chatbots and smart virtual assistants are some intelligent systems that are capable of understanding user queries given in natural language and respond accordingly to maintain the conversation. These fulfil the requirement of talking to a real person actively and quickly when retrieving adequate information. Such systems eliminate waiting time at inquiry officers as well as repetition of officers on similar queries to several clients.

Banks are currently making significant investments in artificial risk-reduction capabilities, including fraud prevention, enforcement and cybersecurity. These are some implementations of anomaly detection methods in machine learning. Anomaly detection saves time when automated processes at scale, preserves reputation by strengthening great loyalty of customers and avoids regulatory fines for compliance lapses. Traditional rule-based fraud detection systems often deliver false-positive warnings for acceptable transactions, mistakenly marking guilty. However, the latest applications in Deep learning techniques for identifying anomalies can be implemented to understand what comprises ordinary behaviour and to recognise unusual behaviour that has not occurred in the past.

In today's technology-driven society, criminal elements use all the available means to dispose of their illegal activities. Although there are many anti-money laundering approaches in the financial community for some time, they can not adjust to the ever-changing financial laundering threats and methods. Intelligent agent technology is used to provide a more versatile, autonomous and scalable solution for Anti-Money Laundering(AML). In designing successful methods for anomaly monitoring of transactions, supervision authorities and financial organizations have been particularly involved in their battle against money laundering. Many of the previous AML schemes were rule-based, with poor performance and less efficiency, such systems could be easily learned and evaded by money launderers.

Throughout this era of globalization, the key to sustainability is technological globalization in creating strategic alliances among financial companies to offer various services to a global customer base. However, user privacy-centric regulations and drawbacks of the middleman third-party services compelled banks to discover trusted alternatives. Blockchain is one of the most promising technologies currently in financial services and has revealed that blockchain is a top priority for bank leaders in finance. The most prominent key to realizing the potential of blockchains is to build the networks needed to support global payments through collaboration between banks. Banks ought to look at the bigger picture and partner with non-banks to help identify the framework of an internationally agreed universal payment network that changes the implementation of transactions by banks.

The motivation for this review is based on the following aspects:

(1) AI-powered applications in banking and finance have been developed and deployed in the recent past. They continue to offer user authentications, automated transactions, fraud detection, market research, investment management, personalization, customer service, and many more.

(2) After investigating the gradual research regarding the transformation of traditional banking to futuristic banking, the necessity for a systematic literature review is observed. Hence, the present work is based on why and how AI is used in the financial context and the advantages and limitations in applications.

This review has made three core contributions: (1) providing a discussion on why the applications of AI in the field of finance is essential; (2) presenting an overview of the existing AI-powered methods that are used especially in banking; (3) investigating research and other approaches for the sustainability of commercial banking.

The organisation of the paper is as follows. In section II, the critical significance of privacy, confidentiality and accuracy in the finance industry is discussed along with some use cases on officially reported global data breaches. Subsequently, in section III, a comprehensive review of Artificial intelligence approaches in the banking industry is discussed. Section IV is dedicated to AI applications in Front Office conventional banking including AI chatbots, virtual assistants and biometric user authentication. Fraud detection, fraud risk monitoring and anti-money laundering using AI and application of Blockchain in cross-border payments handling are discussed under the applications in Back Office operations in section V. Afterwards, limitations of using AI are discussed in section VI. VII discusses how to overcome the limitations identified in the previous section. Section VIII concludes the paper with an extensive discussion on how AI can enhance the security and prosperity of the banking industry.

II. Why privacy, confidentiality and accuracy are critical in the finance industry

People share more and more data online than ever before due to social networking, search engines and online financial services, causing billions of unintentional personal data exposure. Globalization and enormous internet usage have created an ongoing trend of data breaches. Reduction of accuracy measures and the increasing privacy risks becomes a national and international concern because cyber attacks and infringements of privacy are becoming more and more frequent. With the adaptation of the General Data Protection Regulation (GDPR), data breaches have increased and many more infringements have been reported in the media, as per the insight into the main international data breach policy factors provided by Helen Davenport [2]. Therefore, banks and other financial institutions holding sensitive data of customers have taken actions to improve the cybersecurity of their systems.

Personal information, Credit-eligibility information (obtained from an external credit reporting agency about individual creditworthiness) and Credit information (all current or terminated consumer credit accounts) are the main types of information that each bank keeps about individual customers. Several countries have enacted comprehensive legislation to protect the provided three categories of customer sensitive information however, potential security breaches persist. The main requirement of data security and confidentiality falls under verification of privacy by preventing unauthorized access and restriction of data corruption by revealing sensitive data to the outside. From that confirmation of data privacy can be achieved through information technology applications and could be further improved by AI applications.

Following are some of the officially reported data breaches regarding financial institutions globally [3].

A. ECB BIRD Site Data Breach

The Integrated Reporting Dictionary (BIRD) platform of the European Central Bank (ECB) was shut down after routine maintenance uncovered a cyber-attack that compromised web newsletter subscriber information. The ECB announced that the attack did not compromise market-sensitive data. However, names, email IDs and titles of 481 individuals have been illegally accessed by hackers.

B. Capital One Data Breach

Capital One reported a data breach that affected the credit card applications of nearly 100 million people after a software developer reached a cloud-based server. The documents included names, date of birth, credit scores, contact details and certain social security numbers of the United States and Canada. A hacker used an inappropriately designed firewall to gain access to Amazon Web Services Personal Server. After the hacker gained access to GitHub, Capital One was alerted by an anonymous person of the GitHub database. The authorities arrested one person in direct connection with data theft.

C. Banco Pan Data Breach

Researchers working on security violations found an online file containing 250 GB of personal and financial information, primarily related to Banco Pan, a Brazilian financial institution. The records claimed by Banco Pan are

978-1-6654-4963-2/21/$31.00@2021 IEEE

owned by a partner including scans of ID cards and social security cards, proof of address documents and service request forms.

D. Crypto Exchange Theft

Europol officials, British law enforcement agencies and the Dutch law enforcement authorities detained six suspects for cryptocurrency fraud in the sum of € 24 million (over $26 million). The suspects have employed a technique called 'typosquatting' that replicates the exchange of information online to capture and manipulate the Bitcoin wallets of offenders. This assault has affected over 4,000 citizens in at least 12 nations.

E. SBI Breach

The State Bank of India, the largest bank in India, lost the protection of its server allowing attackers to enter the network without the authority to do so. Hackers were able to access customers' personal data, given that the bank has a customer base of over 4.5 trillion.
Reported in India, 4 February 2019

III. Review of Artificial Intelligence Approaches in the Banking Industry

Digital innovations redefine markets and change operations in businesses. Growing innovations explore options and take approaches to create value in the world powered by technology. Depending on the rise of consumer awareness and expectation, the banking sector undergoes customer centricity service model. Banks have expanded their business for conventional banking to information technology and telecommunications to fulfil these demands providing mobile banking, e-banking, and real-time money transactions. Although this change made it possible for consumers to use the bulk of banking services anywhere at their disposal, they also have a cost for the banking industry. The collaboration of the financial industry and other sectors such as IT, telecommunication, and retail, critical information has been transmitted through virtual networks susceptible to cyber-attacks and frauds. Such events have not only an impact on bank competitiveness but also bank assurance and consumer bonds. Artificial Intelligence cognitive technology provides banks with the benefit of digitalization and lets them face rivalry among FinTech(Financial technology) players.

The future of the banking industry is artificial intelligence, as advanced data analytics have the strength to fight fraudulent transactions and boost enforcement. The AI algorithm requires seconds to complete money laundering detection operations which otherwise takes hours and days. AI also helps banks to handle vast amounts of record data and gain valuable insights. Applications including AI features, virtual assistants on customer service and biometric authentication systems lead to better service quality for a broader client base. All of this means higher earnings and increased profits by accelerating customer attraction and retention.

Chatbots recognise and react most accurately to the meaning and emotions in the text chat with human clients. These cognitive machines allow banks not only to save time and improve productivity but also save millions of dollars by accumulated cost savings. Cognitive systems, which think like human experts and react like them, offer optimal solutions real-time based on data as human assistants respond to client queries. AI provides a better understanding of clients and their conduct, based on past experiences. This allows banks to provide meaningful client interaction, through the introduction of personalized functionality and responsive engagement. By evaluating previous actions AI can predict future scenarios and can assist banks in predicting future results and patterns. It allows banks to recognise theft, spot money laundering trends and monitor customers. AI detects these horrific acts and helps to save millions for banks by using its strength in machine learning. Likewise, to perform risk detection, AI identifies fraudulent data models in humongous quantities while accommodating a trusted, borderless and transparent network of monetary circulation.

Not only will AI motivate banks by automating their know-how staff, but it will also intelligently make the entire development cycle adequate to eradicate FinTech's cyber danger and rivalry. AI is a crucial extension to existing systems and activities of banks and continues to evolve over time without any manual intervention. AI would allow banks to optimally exploit the ability of people and machines to function cost efficiency and offer personalized services. All these advantages for banks are no longer a vision for the future. By employing AI solutions, banking executives have taken due diligence steps to leverage these advantages. Fig. 1 summarizes how banks are expanding their use of AI technologies to improve customer experiences and back office processes.

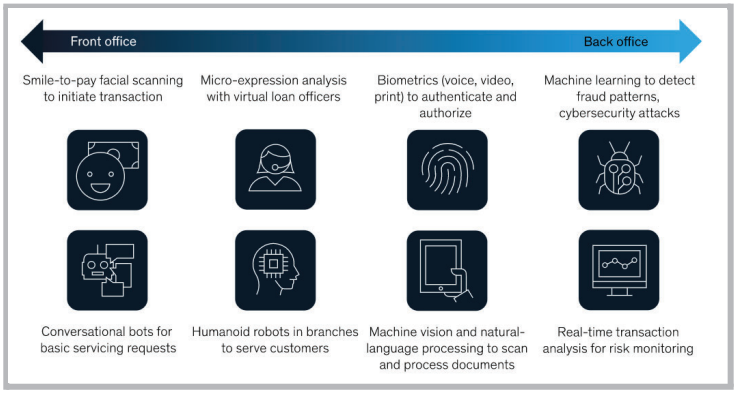

Fig.1: Summarized version of AI applications in banking[4]

IV. AI Applications in Front Office Conventional Banking

IB (Investment Bank), capital markets, property management as well as sales and trading divisions build the front office. Research divisions for finance, investment and acquisitions are also seen as in the front office, although they do not produce direct revenue or communicate with consumers. Services offered by the front office are basic financial trading, property broker, wealth management assistance, and corporate investment. The front office has the highest number of customer interactions in investment banks. When interacting with millions of clients it is profoundly important to provide exceptional service with high accuracy and efficiency while managing any kind of

frauds and risks. Consequently, Banks are leveraging AI in the frontend to smoothen customer identification and authentication to address security concerns, and mimic live employees through AI chatbots and virtual voice assistants in response to user queries to improve the quality and efficiency of the service.

1. User authentication using AI

The online services have struggled to keep up with the sophistication and reliability of user authentication technologies over the past decade. Recent advances in Artificial Intelligence have given new systems authentication approaches that can quickly and accurately identify and authorize users by using their biometrics. Biometrics is a field of science that measures characteristics of human beings by analysing physical characteristics such as fingerprints[5], or retina[6] and behavioural characteristics such as voice[7] and handwriting[8]. Physical characteristics are unique and constant to a degree for everybody even for identical twins, while behavioural characteristics are inconsistent throughout the lifetime.

A. Fingerprint Recognition using Artificial Neural Networks (ANN)

Above all biometric characteristics, fingerprints are one of the most reliable measures, which is widely used by forensic experts in defining and confirming individualities. Research is carried out to build sophisticated fingerprint user authentication systems using Artificial Neural Networks(ANN)[9]. Artificial Neural Networks(ANNs) are recognized as one of the main techniques used in machine learning. They are brain-inspired structures that are intended to mimic how we humans learn, as the 'neural' aspect of their name implies input and output layers and, in most situations with a secret layer composed of units that turn the input into something the output layer can use. They are excellent tools for finding patterns that are far too difficult to isolate and too complex to train without computers.

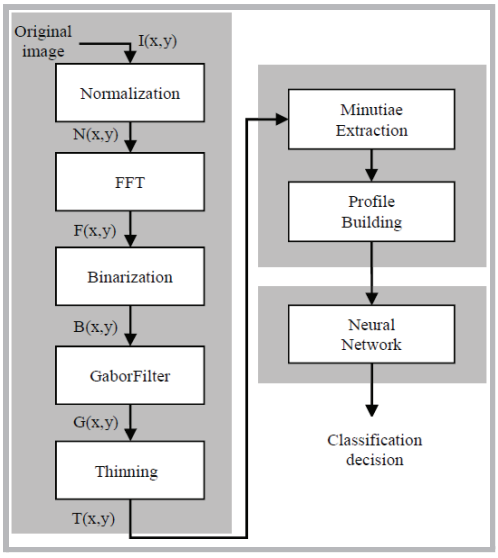

Fig.2: Fingerprint Recognition system[10]

Noise and poor quality of images caused anomalies in the identification of fingerprints. To improve detection results, pre-processing of fingerprints is required to transform the primary image into a thinned image that is used to extract minutiae. It is a five-phased process, namely normalization (standardize fingerprint grayscale values), enhancement (connect falsely broken points using Fourier Transform), binarization (transformation of 256-level of grey into black and white), filtering (eliminate noise and preserve actual ridge and valley structures) and thinning (eliminate the redundant pixels) as shown in Fig.2. Then the unique features of each image are quantified using Minutiae Extraction cross number method[10]. Finally, a feedforward backpropagation ANN is trained to classify the various fingerprint images as belonging to its legitimate owners.

Royal Bank of Scotland and NatWest - Fingerprint based Biometric Payments Card system [11]: In 2019 the Royal Bank of Scotland (RBS) launched a pilot of biometric fingerprint cards. The trial took place with nearly 200 clients of the bank NatWest and the following phases will be held in the UK. The fingerprint replaces the PIN entries and verifies transactions in excess of £ 30, enabling customers to make their payments faster and more comfortably. The United Kingdom's first biometrical innovations for user authentication are RBS and NatWest. Such banks can recognise fingerprints on mobile banking applications by touch ID.

B. A Neural Network-Based Approach for Iris Recognition Based on Both Eyes

Because of its high personal identification reliability, iris recognition is one of the most promising solutions for the authentication of biometric identities. The human iris has a complex structure with minute features such as furrows, crypts and corones, which is a small, circular diaphragm between the cornea and its lens[12]. The iris is a colored part of the human eye and has a characteristic appearance, which allows the iris easily to be used for personal identification. The iris patterns of the same person's eyes or identical twins are totally independent. In addition, the iris stabilizes the use of iris recognition for personal identification throughout the lifetime of a person as it is non-intrusive and non-invasive. In general the iris recognition systems contain four stages: acquiring an image, segmentation of the iris, standardization of the iris and recognition.

Wells Fargo - Eyeprint Authentication [12]: The Mobile banking application from Wells Fargo allows commercial customers to monitor bank balance sheets, make deposits, and accept payments from their mobile devices. Advanced security features like encryption, secondary authentication and token creation are part of the solution. The use of eye-print biometric features promotes accurate identification of uniqueness in each individual. This feature allows users to log in via iris scanning through mobile devices. Authentication of an eyeprint eliminates the need for a password or token while simplifying secure logins.

Bank of America - Fingerprint Authentication, Iris-Scanning, and App Linking [11]: In 2018, mobile application by Bank of America launched with touch-ID

authentication and a short term pilot of iris scanning. Recently, the financial institution announced the addition of a new App Linking feature. It is included in all mobile applications belonging to the Bank of America (Bank of America, Merrill Lynch, Merrill Edge and the US Trust). Users authenticate once, by means of a fingerprint scan or face recognition, can switch between dedicated apps with a single click, without having to authenticate it again.

C. *Biometric Signature Verification using Pearson Correlation Features and Artificial Neural Network*

Handwritten signatures are widely used as a type of biometrics to authorize documents or to authenticate online agreements, especially financial transactions. Signature is a biometric trait that is not dependent on the individual's physical properties, such as fingerprinting or facial recognition, but rather a feature of behaviour. Biometric signature authentication has become popular as a more trustable alternative to password-based security systems. But signature could change its design over time, which makes it difficult to recognise unique patterns. Depending on the input data available, signature based authentication can be divided into two types as online signature authentication and offline signature authentication. Offline verification(static) of signatures takes input as an image and is useful to verify signatures found in bank cheques and documents automatically. Authentication of the digital(dynamic) signature uses signatures obtained via pressurized tablets to obtain dynamic signature characteristics in addition to their shape. Some complex features including the number and order of strokes, the overall signature pace, the pen pressure in each stage adds uniqueness for each signature making it difficult to forge. It makes online signature verification much more effective than offline signature verification. Therefore, online signature verification is applicable in many security applications[13].

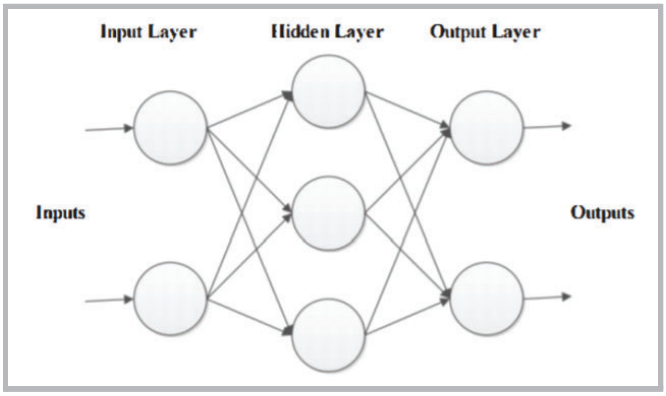

Fig.3: Multilayer neural network architecture used in signature verification[14]

Research is in progress to detect applications of characteristic extraction methods for online signature of a person based on the Pearson correlation coefficients[14] in ANN to identify the mechanism of transforming inputs to outputs using neural models in the hidden layer of the network(Fig.3). Then a feedback network is used to differentiate between fake and genuine signatures, using the derived features. The correlation coefficient of Pearson is the measure of statistics which calculate the statistical relationship between two continuous variables. It is known as the best tool for calculating the association between variables of interest, as it is based on the covariance principle. This knowledge provides information about the magnitude and the nature of the interaction or connection.

D. *Palm Vein based Identification using Support Vector Machine Algorithm in Artificial Neural Networks*

Palm vein-based recognition is an evolving biometric phenomenon that has focussed the attention of researchers. The main idea for concentration in the palm vein is that studies revealed that most of the vein patterns of the body end up in the palm, making it easy to study the characteristics of veins either through structure-based or texture-based analysis. This biometric system provides a high degree of accuracy at a reasonable cost. As palm vein recognition is accurate, many crime labs use the technique of fingerprinting in the initial stage, and the identification of palm veins is made as part of the conclusion process. This process is also known as vascular recognition. It uses optical scanning technology to capture vein images in palm. Some research is executed on vein pattern verification[15] using palm dorsum. Palm vein images are enhanced first, then features are extracted with neural networks, later a feed-forward algorithm and Support Vector Machine (SVM) algorithms are used to make predictions with high efficiency and accuracy. SVM is a supervised machine learning algorithm that uses classification techniques for two-group classification queries.

Barclays - Finger Vein Reader Technology [11]: Barclays partnered with technology giant Hitachi to supply Finger Vein reader technology to its company banking customers. Business customers simply put a finger into a small desktop scanner to allow transactions rather than entering passwords and PINs. That finger, which grows in the womb and largely unchanged throughout its entire lives, has the beauty of the technology. The Barclays biometric reader integrates advanced protection with a user friendly interface for a groundbreaking authentication experience for many financial institutions.

E. *Facial Recognition using Convolutional Neural Networks*

Facial recognition is important for the provision of biometric authentication used especially in security applications. Security is one of the most important concerns in the banking industry, as people expect the security of their assets and identity. Facial recognition used to be among the most contemporary and widely used applications employing image processing technologies due to extensive use of the biometric system having significant popularity in recent years. Instead of using passwords, keys and Personal Identification Number(PIN) that have been difficult to recall for a long time and can easily be lost, biometric based strategies emerge and eventually get promoted. Therefore, the most economical and simplest way to solve these challenges is facial recognition with Convolutional Neural Networks(CNN). Artificial intelligence usually includes machine learning to allow the system to learn things and automatically develop its experiences. The main focus of this approach is to create systems that can access data independently and then use it for their learning. The use of

978-1-6654-4963-2/21/$31.00@2021 IEEE

deep learning as a subset of machine learning, uses multi-layer non-processing tools to transform and extract diverse features, and CNN as one of the powerful approaches for image processing algorithms, programmed in Python for Facial Recognition in deep learning [16].

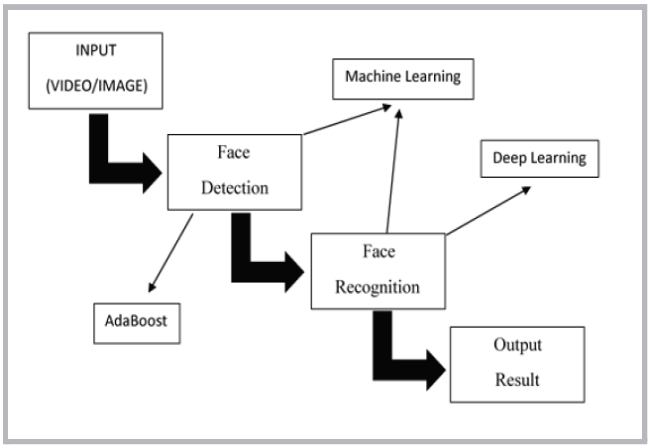

Fig.4: Steps of Facial Recognition process[16]

According to research, at first a picture or video data will be provided to initiate face detection process, the region in which the face is positioned is sliced and used as the reference for face recognition. Findings/ output results are shown after the identification process is completed using the machine learning model. A simple facial recognition system architecture is shown in Fig.4.

F. Speech and Speaker Authentication System using Voice Signal Feature Selection and Extraction

Voice recognition systems have an important role to play in and across all implementations of human electronics. In many applications, noise elimination, safety telephoning, voice authentication[17] and voice locking are extremely useful. These are also helpful as a security key. Voiceprint Identification System may be used for speech recognition and speaker authentication. There are a wide range of methods used for voice recognition. The process of speech recognition can be narrowly divided into two levels. The first step is the extraction of the characteristics, is to interpret digital speech and analyze the digital acoustic signals. In order to analyze and derive information from signals, spectral analysis techniques are applied. Phonemes and other special terms are identified in the next step. This is the norm which can be done by many approaches, such as Dynamic Time Warping[18], Hidden Markov models[18], artificial neural networks and expert systems.

Citi - Voice Authentication[11]: In 2016, CitiBank of the United States launched speech biometrics for the identification of customers using the system at call centres. Authentication of the speech uses biometrics to validate user identification, so that they answer some questions customer service officials raise. It analyzes and cross-checks unique characteristics of a person's voice patterns against a pre-registered voice file to check their identity. This lengthy process of confirming the customer's identity replaces voice authentication by using identification numbers and personal information, also reduces customer frustration and makes it easier to provide practical help for officials. Within a year of their publication, more than one million customers in the area of the Asia Pacific have used this authentication technique. The client takes less than a minute to build up their voiceprint to be validated, to make it applicable for a long time in future.

2. Chatbots and virtual assistants in the front office

The use of banking services by virtual banks has contributed to a real revolution in the field of global monetary circulation. Millions of people became persuaded that the whole spectrum of financial services they might take advantage of would not entail a daily visit to bank branches. Many convenient services are widely available on the internet including opening an account, saving or even borrowing. The assistance services include chatbots and automated assistants, computer applications that are equipped for conducting interviews, answering questions, providing advice and collecting data to solve the user reported issue.

A. Chatbots forIntelligent Assistant Systems

Chatbots are intelligent systems capable of understanding user queries given in natural languages acting as a virtual assistant. Digitalization has transformed banks to introduce internet banking, mobile banking facilities but sometimes, these sources can be a bit overwhelming for most of the users as information is too scattered to search for easily. Although inquiry counters are available, considerable delays and redirections are involved in simple informational query suffers customer satisfaction. Bank employees often face problems answering time-consuming repetitive client questions. Hence, integrating a chatbot will provide a smart solution to answer such queries.

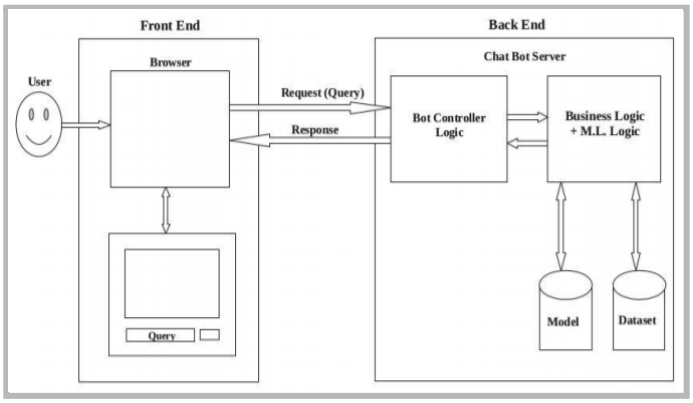

Fig.5 : Architecture of NLP and ML based intelligent assistant system[19]

The bot controller logic[19] is used to send and receive responses using the Flask framework for web applications. The user inquiry is sent in text format into business logic(Fig.5) through a bot controller logic. Such text data are pe-processing using Natural Language Processing (NLP) techniques before feeding into the system. NLP is a field covering the relationship between the machines and humans and applications for processing and interpretation of a large quantity of natural language data query and extracting the essence of each NLP data token by removing

unnecessary space and terms. Then text-format will be converted to vectorized format using vectorization followed by a classification algorithm to find the class of inquiry it belongs to. The user will receive the most similar response according to the similarity of values obtained from the input query.

Chatbots by Kasisto[20]: In the construction of its own chatbots and virtual assistants, Kasisto made a major contribution to the banks. These conventional AI platforms have their roots in AI reasoning and understanding natural language comprehension, which means that sophisticated financial management questions and regular customer service conversations are handled. Kasisto has assisted a number of prominent banks including the UAE Virtual Bank and Bank of America's Erica with their AI assistants so far.

B. Virtual Assistants for Payment Processing using Deep Learning in Natural Language Processing

The evolution of business synergies with customers has established a new paradigm of experiences between humans and machines by employing AI. In these cases, the computer communicates with humans(also known as customers) utilizing NLP (Natural Language Processing) composed of NLU (Natural Language Understanding) and NLG (Natural Language Generation). NLP is one AI division which uses natural languages to discuss the interaction between computers and humans. The ultimate aim of NLP is reading, decoding, learning and understanding of human languages in a useful manner. NLU is a computer software to understand input made in the form of sentences in text or speech format. NLU directly enables Human-Computer Interaction (HCI). NLG is a process of transforming structured data into meaningful content in natural language enabling organisations to create long-form material for custom publications as well as for developing unique products for online or mobile applications. The direction of discussions on these technologies is complex and rapidly changing to maintain interest and rationality of realistic nature. The changing landscape allows today's NLU and NLG elements through the new profound learning algorithms to make them more appealing to consumers who want to recognize themselves, to react actively to them or to take appropriate actions. Nevertheless, these specialized methods require good model examples to be mastered in handling real-life situations. The NLU behind the AI virtual assistants robustly interprets consumer utterances to help customers to manage their due inquiries, which is an integral part of a variety of industries such as finance, insurance, telecommunication, supermarkets with constant two way interactions with clients.

The types of communications have developed far more than any chat based conversations utilizing keyboards/keypads toward novel solutions powered by extremely precise computer algorithms for speech recognition. The adequate interpretation of natural language, conversation management and response formation are three main dependencies in developing a virtual assistant[20]. Confusion in the language utilized by the consumers is the biggest obstacle in addressing all three dependencies, and the literal nature of the sentences is the greatest reason for the confusion. The second is a combination of various objectives, sometimes there are several objectives in one paragraph combined without giving specific expectations. Ambiguity should be managed to overcome those issues. Deep learning has created a remarkable impact in effective interpretation of natural language avoiding ambiguity.

Distributive vectors[22] often referred to as term embeddings based on so-called distributional theory referring to words appearing within similar contexts that possess similar meaning. Word embedding is pre-trained where the aim is to predict a word using a shallow neural network based on its context. Variable representations for phrases are one of the problems of embedding approaches. Phases can not be merged simply as the individual word vector representations because they do not reflect the combination of the meanings of each word. And the complexity arises as the word length increases.

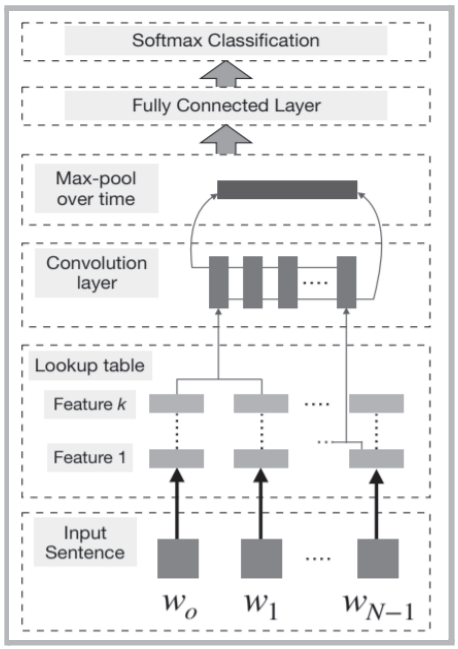

Fig.6 - Word embedding approach[22]

A neural based approach of CNN (Convolutional Neural Network) describes a computational method used to construct terms or n-grams to obtain higher levels of characteristics. The goal of this method was to turn words into a vector representation via a look-up table, resulting in an initial word embedding approach that learns weight during network training (Fig.6). CNN is a deep neural network form, which is most widely used for visual analysis. They are also classified as artificial neural networks based on shared weights and the invariance of translation characteristics of invariant shifts or volume. CNN shows the network is using convolution mathematical processes. Convolution is a continuous process of a special nature. Convolutional networks are essentially neural networks, which are transformed in at least one layer instead of standard matrix multiplication.

First, sentences are tokenized into words to carry out sentence modelling with a simple CNN that is further transformed into a word embedding matrix. This input embedding layer consists of a filter of all conceivable window sizes, to create what is considered a feature map. This proceeds a total-pooling process to obtain a

fixed-length output and the dimension of the stream and requires a limit operation at each stage then the final sentence is reflected in this process. The inability of modelling long-distance dependency which is essential to numerous NLP activities reflects one of the limitations with simple CNNs. CNNs were coupled to Time Delayed Neural Networks (TDNNs) which allow a broader contextual range simultaneously while training to tackle this issue. The Dynamic Convolutional Neural Network (DCNN) is another useful form of CNNs that have been effective in various NLP tasks such as sensation prediction and classification in the query. A dynamic k-max bundling technique is utilized by a DCNN, where filters can expand variable ranges dynamically during sentence modelling.

Erica in Bank of America (USA) [23]: Erica offers essential banking services such as searching past transaction data, inquiries on cheques received and written, credit scores, credit card payments. Furthermore, additional details on the device and control such as routing codes, the nearest bank or financial centre, arranging face-to-face interactions with more than 25,000 financial center experts, checking the bills and scheduling transfers, locking and unlock of debit cards, and transferring funds to accounts or sending money to friends and families through Zelle, Bank of America's money transfer application.

V. AI APPLICATIONS IN BACK OFFICE OPERATIONS

The back office may not trade or directly interact with clients, but it contributes vital support to the front office in handling accounts, operations, strategic planning, data warehouse maintaining and anomaly detection. Fraud detection, fraud risk monitoring, anti-money laundering and cross-border payments handling are some of the critical operations carried out by the back office. Because of the significance and complexity, such sensitive operations should be managed decently. Therefore, some prominent organisations in the financial industry have adapted advanced technologies in AI.

A. Fraud Detection using Data Mining

The word fraud involves one or more individuals, where they deliberately operate illegally to take important information for personal benefits. The improvement of new technologies and techniques has become an advantage for criminals to commit frauds[24]. Hence, fraud detection has become a major concern in the corporate finance world. Fraud detection is based on simple comparisons with association, clustering, perdition and outlier detection techniques. Anomaly detection is one AI technique that may assist banks to recognise purchases and transfers that are fraudulent. Through the way of predictive analysis, banks may diagnose frauds and rate transactions on the basis of a broader range of client data at a risk level. Some researches propose automated fraud detection frameworks using data fusion and data mining techniques. The fraud detection approach is somehow improved by using data mining methods but the model is based on manual inspection and estimation capabilities that improve with experience. Because the manual process requires more user interaction, domain knowledge, profound monitoring through different phases with different techniques for data mining. Many organizations acquire and analyze massive amounts of data in the financial world. The rapid use of data mining with existing software and hardware platforms enhances the value of historical information. Data mining applications may find large datasets to extract conclusions based on data by implementing mining techniques on high-performance application servers or in parallel processing machines. Pre-processing data is generally used as a preliminary practice for data mining. This translates data into a format that is interpreted for consumers more comfort and efficiency.

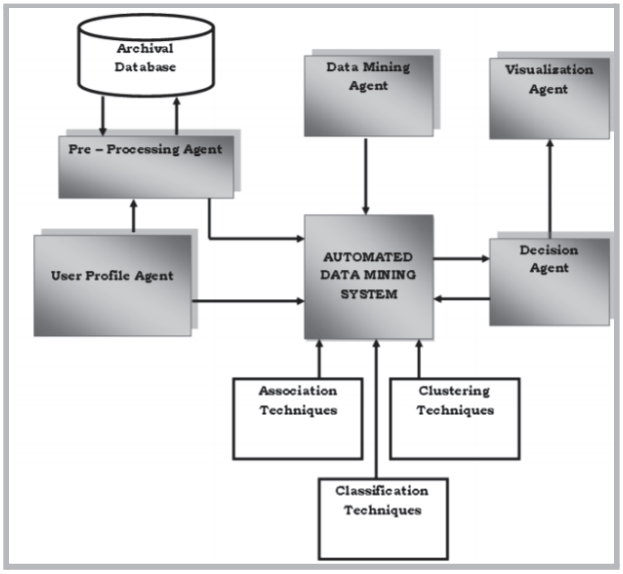

Fig.7: Fraud detection system architecture using automated data mining techniques[25]

All new user entries are validated autonomously by the user profile agent in collaboration with the archival agent on the basis of user profiles stored in data warehouses as shown in Fig. 7. Once the validation process is completed, the archival agent will be updated whether the particular user is a new user or an existing user. User information is further investigated by the pre-processing agent and the data mining agent, eliminating noisy data and injecting missing values based on the sequence and data types. Then the data mining agent sends a request to the archival agent to check for any historical data in the data warehouse for a special user. If any existing pattern matches respective decisions are made. Otherwise, the data mining agent will automatically detect new patterns for future decision making processes. When any new pattern is created by a data mining agent, it is validated by the decision agent authorized to approve or reject new patterns. Clustering algorithms such as Dunn's Validity Index and Davies Bouldin Validity Index algorithms are used in decision making. After processing critical decisions, patterns are forward to the visualization agent for further processing. The visualization agent used to visualize results using decisions made by the decision agent. When any existing user interacts with the system, it will be automatically identified by the visualization agent and detects any anomalies.

Teradata AI-powered fraud detection system in Danske Bank, Denmark[26]: Teradata machine learning platform recognizes potential fraud cases avoiding purported 1,200 false positives reported per day(60% of total false positives

detected) with acceptable deviations. This system is expected to reach 80% accuracy as the model continues to learn.

B. Anti Money Laundering using Intelligent Agents

Anti-money laundering (AML) is a series of policies, laws and regulations to avoid income generation through illegal actions. In most cases, money launderers cover up their activities by a series of steps which make money appear to be legitimately obtained from illegal or unethical sources. Many leading banks worldwide move from rule based software systems to more robust AI systems to detect money laundering patterns. Anti monetary laundering systems are expected to become more reliable over the coming years with a high level of accuracy due to continuous improvement.

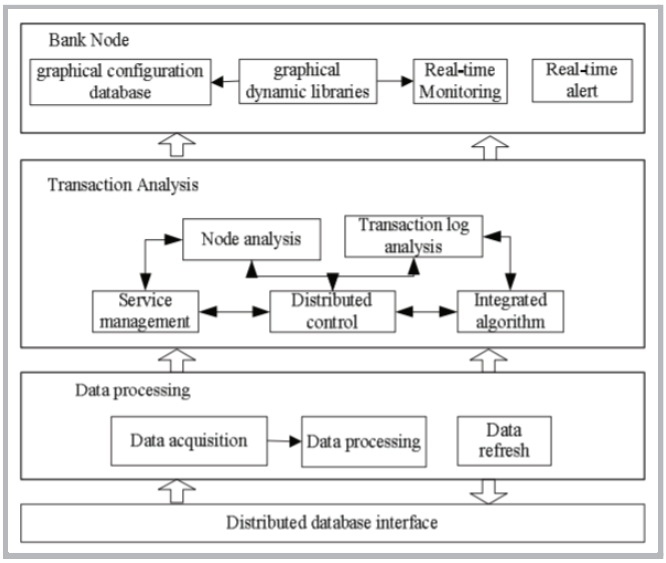

Fig.8: Architecture diagram of Anti-Money Laundering real-time monitoring system[27]

Bank Node includes a real time monitor and graphical configuration database, real time alert module and graphical dynamic libraries. The real time alert module can detect suspicious transactions using data mining algorithms and recorded to the dynamic graphics library. Suspicious transaction alerts are received by Transaction Analysis and displays through the graphical interface. Transaction Analysis includes the organization of parser, service management device, the transaction log analyzer, algorithms Integrator and distributed control. Transaction Analysis sends the results to the transaction log analyzer while updating the historical database(Fig.8). The analysis of data, including data acquisition, data processing and data refresh are primarily responsible for in-house development and processing of data.

AML at HSBC[28]: HSBC announced its innovative partnership with an AI tech start-up, Ayasdi to integrate an AI-powered anti-money laundering system. Data mining and machine learning algorithms are used to reduce the number of false alerts by using a large data set to distinguish complex criminal activity in various products, business lines and customers.

C. Fraud Risk Monitoring System for e-banking using Machine Learning Techniques

Modern commercial community highly relies on paperless monetary transactions using e-banking and cashless payment systems. Online banking, mobile banking and ATM(Automatic Teller Machine) and CRS(Cash Recycling Systems) fall under e-banking. Such services have provided greater convenience for the customers on a lower cost with high accuracy and reliability. On its massive expansion of usage, security has become a significant concern of e-banking transactions because of vulnerabilities in systems. Hence, it is urgent to build an effective fraud detection and risk monitoring system to address a broad variety of partly severing security issues.

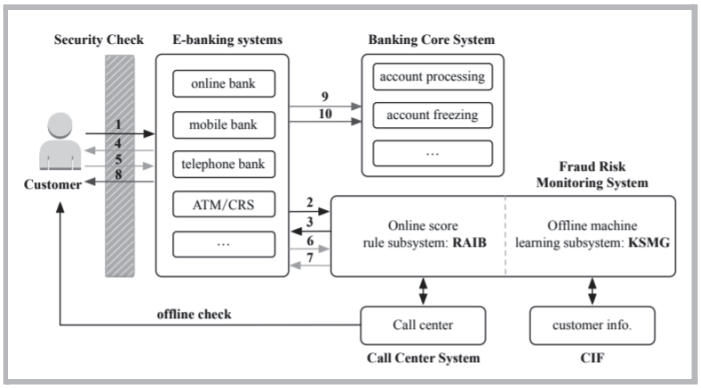

Fig.9: Framework of the Fraud Risk Monitoring System[29]

Researchers propose fraud risk monitoring systems for e-banking transactions consisting of an online scoring subsystem based on expertise and an offline subsystem based on big data, as shown in Fig.9. The online subsystem generates the RAIB (Risk Activity Identity and Behaviour) score of the transaction returning its level of risk. The offline subsystem driven by the big data framework handles historical transactions. The Parallel Random Forest algorithm is used in identifying fraudulent transactions. A random forest is a collection of random decision trees created using training data samples. An arbitrarily drawn subset of functions on each node of the decision tree, will test different threshold values and see how they separate samples according to a given set of criteria. Then each function and its threshold is saved to evaluate data and to separate accordingly then write sample data to the respective node. Since each node is built from random functions, this algorithm facilitates a good compromise between displacement and dispersion. In test mode, the test sample will go through each tree, giving labels for each tree. The most accurate label is usually the final result of the classification.

When a customer invokes a transaction using any of the electronic transaction channels, it will pass to the fraud risk monitoring system after an initial security check. Then the online subsystem will calculate the RAIB score of a particular transaction and return the response with the next operation, continue as a regular transaction or challenge the suspicious transaction. When a suspicious transaction is detected, customer information will be backtracked using CIF(Customer Information File) and passed to the customer.

The monitoring system receives customer responses for validation and its results will be prompted by the e-banking channel. If the customer deserted, the suspicious transaction is rejected and the account made the fraudulent transaction will be frozen.

OpenML engine software at Citibank by Feedzai[30]: Feedzai is an agency in data science that predicts omnichannel exchange frauds using machine learning in real-time to evaluate large amounts of data to identify suspicious payment transactions and reduce financial sector outrage. Feedzai Software has reportedly become the main decision making tool of the new customers onboarding cycle and could validate authenticity, acceptability and the level of fraud risk.

Data analytics software at the Danske Bank, Denmark[30]: Teradata is an AI company that trades solutions for fraud detection in the financial industry. The learning platform offered by Teradata will enhance the identification of banking fraud at the Danske bank by allowing their data analysis to identify potential cases of fraud and prevent appropriate variations from the standard. Teradata has been supporting Danske Bank to modernize its fraud detection mechanism and recognise 1,200 false positives a day. The fraud detection software has reduced false positives by 60% and expected to reach 80% as the machine learning model continued to learn. Also, this model has increased detection of real fraud by 50%.

D. Blockchain in Cross-border Payments Handling

After the introduction of Bitcoin, virtual currency in 2008[29], Blockchain Technology received significant attention. The capability of secure decentralized recording and validating every transaction without a third-party authorization promotes blockchain technology to use in almost every industry, especially in finance. In the financial services industry, particularly the distributed ledger technology, sought to capitalize on the underlying technology to generate new products, services and innovative business models. For every bank and/or financing institution payments are the first and foremost application scenario. With regards to blockchain finance, the emerging system has also been utilized with terms of the money collection and future issue of its digital currency by commercial banks around the globe[31]. This trend also includes international payments, mainly carried out by Swift or Western Union. Cross-border transfers via bank blockchain are quicker than traditional networks and are less costly.

A digital cloud is constructed hierarchically on multiple security servers in different countries. The global cloud integrates data stored in datacenters organically to supply stored data to different types of applications as per queries requested. Security gateway manages protection and privacy when entering a particular zone. Applications can access data to various countries, conduct multi-scale analyzes, and compare among countries by using the platform. Application queries and query results from the data hub are exchanged through a security gateway placed as the network portal for the global cloud in each area. On request from an application to access the data hub, security gateway generates a token allowing access till the token expires.

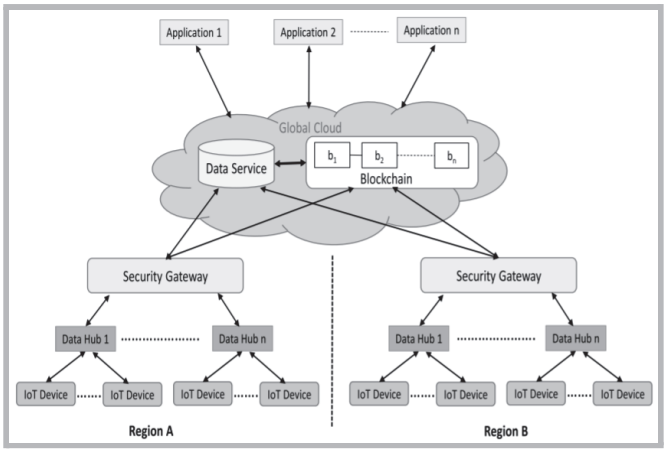

Fig. 10 - Cross Border data sharing architecture[32]

The application shall then define the ID of the data hub or the forms of data to be accessed and its certificate of membership. The security gateway refers to the membership certificate and security policies issued by both countries when issuing the access token having the complete authority of permitting access to the data. Every data transfer towards the service module record in the blockchain maintained by the global cloud. On a report from an application to the service module about misbehaviour, the service module validates the case checking the blockchain. This architecture[32] facilitates cross-border transactions in a secured manner utilising a shared global cloud, Fig.10.

Cross-border payment in Westpac[33]: In 2016 Westpac also affiliated with Ripple(a multinational payments firm) to introduce a low-cost cross-border payment network focused on blockchain technology. The US Federal Reserve partnered with IBM in 2016 to develop a decentralized payment network focused on blockchains. Besides, Deutsche Bank, Barclays Bank and BNP Paribas are other well-known banks which incorporated blockchain technologies.

VI. Limitations of AI in Banking

The application of AI is primarily driven by economic and social needs and progress is being made in almost all sectors of society and industry. In some cases, AI may modestly challenge the values of privacy while in others it may be viewed as wider and more controversial. An expressed concern with advanced AI is that the outcome is not always understood, also called "the question of the black box." Access to data algorithms and machine logic should be purposely restricted by commercial interests, national security etc. The structure of the system and the neural networks algorithms are complicated and difficult to explain. Non-guided learning also helps systems to identify new patterns and associations that can be difficult to explain in data. Automation of AI systems may increase cybersecurity. Nonetheless, alongside automation, human

intelligence is still needed to better detect risks, evaluate patterns and make fast use of available resources. When new software updates are available several automation tools show pop-up messages. Sometimes the updates only include new features, but they are usually dealing with vulnerabilities that could compromise security. Thankfully, many software titles enable people to select the correct period for the upgrade to occur or automate the maintenance of automation software because an outdated system can infringe on the privacy of user information.

Some of the leading banks have initiated to incorporate with Biometric Authentication to develop next-generation user identification mechanisms before enabling customers to proceed with transactions. Whereas the word biometrics evokes physical human measurements such as fingerprints, iris, retina and unique facial features, biometrics also covers behavioural characteristics present in keystroke patterns, personal signatures, voice and palm vein identifications. Using these distinguishing human qualities, Artificial Neural Network powered user authentication systems are developed with the capability of quick and accurate customer validation. Such approaches combat frauds while ensuring high secured transactions and enhanced customer experience.

However, all technology-based systems have boundaries and biometrics is not an exception. As most of the biometric characteristics are permanent, are already exposed and can be stolen without the consciousness of the proprietor, therefore identical frauds could challenge the accuracy of these systems. Another challenge in front of biometric identification is population coverage due to physical labour, diseases, accidents which may cause biometric identifiers to deteriorate eventually. Furthermore, most of the deployment and implementation of biometric systems are complex and expensive. However, it always depends on a particular use case that it will become advantageous or disadvantageous. As more and more biometric systems are being introduced, improvements in demand and economies of scale are expected to make them even cheaper. Touch gesture based authentication, vocal resonance recognition and blockchain authentication are some of the areas under the future of user authentication using AI which are still under research level. Furthermore, quality and quantity of relevant data has limited the performance of AI while encouraging false predictions and biased results.

Online banking systems process tens of millions of concurrent transactions every millisecond. In order to meet the processing power demands, AI applications need high cost robust computer systems. The rapid increase of the capital investment in hardware and software systems discourages potential financial institutions to incorporate AI systems into their ecosystems despite all benefits the system could deliver. However, it is observed in some situations collaborative computational approaches such as flexible interface configuration, load balancing weight distribution, communication link health status check, and routing parameter configurations [34] are occupied. When various intelligent services share computational power and resources, they no longer need high performancing hardware dominated for a particular process.

Although the decentralized nature of blockchain is often seen as its core advantage, some limitations can be found[35]. Since blockchains do not accommodate central decision-maker, participants of blockchain-powered transactions may get misaligned motives imposed by the governance less nature. Apart, the growing popularity of blockchain only reveals the problem of scalability. Even though many scaling methods have been proposed each of them has limitations. Furthermore, applications of blockchains are limited by regulations and policies. There is also a lack of consistency in regulatory issues for financial institutions under cryptocurrencies and smart contracts. Proper regulatory frameworks are required to be established for financial institutions to use blockchains at its highest returns.

AI has many benefits to deliver to the financial industry presenting revolutionary changes to the banking sector. Banks can consider the customer's conduct using many interactive platforms powered by AI such as mobile and other applications in order to deliver them personalized experience. Analysts is a leading supplier of IT solutions providing personalized business solutions by combining innovative technology such as AR (Augmented Reality), VR (Virtual Reality), AI (Artificial Intelligence) and Blockchain.

VII. Discussion

The FinTech industry is working closely with AI constituents to ensure new concepts are captured, developed and commercialized earlier than the competitors[36] and secure themselves from hacking and security breaches affecting highly sensitive data. The obvious reason for the significance of cybersecurity in the banking sector operations and services is to safeguard customer assets and identities. As many individuals and organisations perform most of their transactions through online banking, the risk of a data breach increases daily. Consequently, maintaining a robust security mechanism with AI applications has become one of the highest priorities. In the past, most virtual assistants focused on the field of connectivity with questions before deep learning emerged, and this was achieved by creating a back-end information map and responding to questions through finding answers to the most similar questions. However, recent advances in machine learning and deep learning algorithms have made language systems more effective and accurate in understanding human expectations. The new customer interaction processes allow developers to split complex processes among multiple virtual assistants in single business interaction, so that each virtual assistant may concentrate on a small piece of information and be an expert in the field.

Even though AI has become the most promising technology in terms of security and efficiency with the capability of evolving over learning through the experience of the environment, it has a limitation as discussed in section VI. The quality AI solutions depend on the model and its training data set. However, acquisition and

978-1-6654-4963-2/21/$31.00@2021 IEEE

preservation of bulk of data produce few obstacles such as dissemination, insufficiency and loss of data. Hence, an adequate amount of relevant data needs to be administered properly labelled and updated. Deficiencies in data privacy standards and legislation imposed on data privacy are other data related restrictions. Regulations are to be established to monitor the use by organizations or government bodies of personal or consumer information. Also, organizations should determine appropriate criteria to analyse data without violating federal, state or global data privacy policies. Moreover, data exchange policy schemes should be revised accordingly ensuring the most reliable corporate partnerships among organizations to secure identities of clients. A further downside of AI is that computers are often oblivious of their lack of knowledge. Although AI is good for vast volumes of data, the system can not guarantee that all the data are understood. The solution is Human Centered AI, a series of studies and architectural development and deployment in a deep and meaningful way of learning and collaborating with humans. This ensures continuous improvement of the AI model by establishing an efficient and satisfying relationship between humans and robots resulting in optimal use of resources. Over the training AI model develops hidden bias phenomena, oftentimes bias is transferred from humans when giving instructions. To overcome this problem, a memory refreshing approach can be introduced opening opportunities to generate solid unbiased predictions.

AI is still a developing technology, and one which potentially raises suspicions with the public, particularly in how it will be used by the banking and financial services sector. Nevertheless, the speed at which technological developments occur, coupled with the growing threat of cyber and financial crime. Which means the financial institutions cannot afford to discount the effect of increasing security of their systems. This made AI and machine learning a ‘must have’, rather than a ‘nice to have’, despite the uncertainties surrounding its application and results.

Advancements in technology and affiliated practices and resources will drive FinTech to calibrate themselves for the next level of the Internet of Things (IoT) and will be further supported with multi-fold growth in the next few decades by quantum computing[37]. This transformation will enable the creation of an entirely new ecosystem and technological capabilities which in turn will induce the creation of new business practices and even business models within the banking and financial services industry. FinTech companies would be able to combine data from many sources including mobile devices, social media platforms, other online interactions, and billions of new sensors to create new allied businesses to optimise their services inside and outside of the organization.

VIII. Conclusion

In the past decade, applications of AI in banking has been an unheard word. However, as the usage of AI in other sectors became more and more popular, ratification in the banking sector became very unavoidable. AI's effects on banking continue to expand worldwide across the whole banking landscape introducing many incredible applications including biometric user authentication, AI chatbots and virtual assistants, fraud detection and risk management and anti-money laundering. With embedded AI software, data can be obtained from all channels and the consumer experience can be acknowledged correctly. To improve interaction and allow real time decision-making, banking systems should be automated client engagement through all platforms. Machine learning methods are used to determine what kinds of financial transfers are likely to be fraudulent. Techniques including predictive master learning and unattended smart officers, AI may anticipate suspicious transactions based on shifts and anomalies in consumer behaviour while reducing false positive detections improving the loyalty of consumers. AI witnessed a remarkable transformation in the financial industry, along with some limitations, most businesses tend to overlook. They are scarcity of quality data, arise of hidden-bias phenomena in suggestions and obliviousness of lacking knowledge. However such limitations can be overcome by applying novel solutions such as conventional data management, human centric learning and self refreshing memory.

In summary, not only will AI allow banks to automate the role of technical staff but also make the entire automation cycle smart enough to reduce FinTech's cyber danger and competitiveness. AI is central to the bank's activities and processes and continues to develop and grow over time without minimal human intervention. AI would allow banks to maximize the ability of man and machine to drive operations, improve cost effectiveness and to provide customized services. All these features are no longer a revolutionary dream for banks. Through the implementation of AI, banking executives have already taken deliberate steps to harvest such advantages.

References

[1] Abdul Samad Shaikh and Mohammed Waseem Ashfaque, “Analysis of User Authentication Methods & Impact on Identification Especially in Banking”, International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 2, February 2015

[2] GOWLING WLG - International data breach strategies by Helen Davenport (02 May 2019), Available in: https://gowlingwlg.com/en/insights-resources/podcasts/2019/international-data-breach-strategies/

[3] Timeline of Cyber Incidents Involving Financial Institutions on Carnegie Endowment for International Peace (2019), Available in: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

[4] AI-bank of the future: Can banks meet the AI challenge? Article by McKinsey group, Available in: https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge# (September 19, 2020)

[5] Jain, L.C., “Intelligent Biometric Techniques in Fingerprint and Face Recognition”, Boca Raton, FL: CRC Press. (1999)

[6] Retina and Iris Scans. Encyclopedia of Espionage, Intelligence, and Security,The Gale Group, Inc (2004)

[7] Jean-Francois Bonastre, Frédéric Bimbot, Louis-Jean Boe, Joseph P. Campbell, Douglas A. Reynolds, Ivan Magrin-Chagnolleau, “Person Authentication by Voice: A Need for Caution”, 8th European Conference on Speech Communication and Technology. Geneva, Switzerland: isca-speech.org in September 2003

[8] Alisher Kholmatov, “Identity authentication using improved online signature verification method”, Berrin Yanikoglu Sabanci University, Faculty of Engineering and Natural Sciences, Istanbul, Tuzla, Turkey(2005)

[9] Ridouane Oulhiq, Saad Ibn Tahir, Marouane Sebgui and Zouhair Guennoun, “A Fingerprint Recognition Framework Using Artificial Neural Network”, 10th International Conference on Intelligent Systems, Rabat, Morocco, October. 2015

[10] Jing Wang, Jingcui LI and Liulin Cao, “An Improved Fast Thinning Algorithm for Fingerprint Image and Its Application”, Journal of Computational Information Systems, 2000

[11] Five Examples of Biometrics in Banking posted by Alison Arthur and Bethany Frank (08 May 2019) Available in: https://www.alacriti.com/biometrics-in-banking

[12] Maha Sharkas, "A Neural Network-Based Approach for Iris Recognition Based on Both Eyes", 2016 SAI Computing Conference (SAI), London, UK, July 2016

[13] S. Nanavati, M. Thieme, and R. Nanavati, "In Biometrics: Identity verification in a networked world", New York: John Wiley & Sons (2002)

[14] Vahab Iranmanesh, Sharifah Mumtazah Syed Ahmad, Wan Azizun Wan Adnan, "Online Signature Verification Using Neural Network and Pearson Correlation Features", IEEE Conference on Open Systems (ICOS), Kuching, Malaysia, December 2013

[15] Wei Wu, Stephen John Elliott, Sen Lin, Shenshen Sun and Yandong Tang, "Review of palm vein recognition", IET Biometrics on 16 January 2020

[16] Suleman Khan, M. Hammad Javed, Ehtasham Ahmed, Syed A A Shah and Syed Umaid, "Facial Recognition using Convolutional Neural Networks", International Conference on Information Science and Communication Technology (ICISCT), Karachi, Pakistan, March 2019

[17] Dr. E. Chandra, Mrs. C. Sunitha, "A review on Speech and Speaker Authentication System using Voice Signal feature selection and extraction", IEEE International Advance Computing Conference, Patiala, India, March 2009

[18] Chee Peng Lim, Siew Chan Woo, Aun Sim Loh, and Rohaizan, "Speech Recognition Using Artificial Neural Networks", Proceedings of the First International Conference on Web Information Systems Engineering, Hong Kong, China, 19-21 June 2000

[19] Chaitrali S. Kulkarni, Amruta U. Bhavsar, Savita R. Pingale, Prof. Satish S. Kumbhar, "Bank Chatbot – An Intelligent Assistant System Using NLP and Machine Learning", International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 05,May 2017

[20] Builtin - KASISTO, AI in banking (2019) Available in: https://builtin.com/artificial-intelligence/ai-in-banking

[21] Sam Albert, Brijesh Singh and Ananda Swarup Das, "Robust Methodology for Building an Artificial Intelligent (AI) Virtual Assistant for Payment Processing", IEEE Technology & Engineering Management Conference (TEMSCON), Atlanta, GA, USA, June 2019

[22] Tom Young, Devamanyu Hazarika, Soujanya Poria, Erik Cambria, "Recent Trends in Deep Learning Based Natural Language Processing", IEEE Computational Intelligence Magazine (Volume: 13 , Issue: 3 , August 2018, Pages: 55 - 75)

[23] Fintech News, 10 AI-powered virtual assistants making banking easier for everyday consumers (September 26, 2018) Available in: https://www.fintechnews.org/10-ai-powered-virtual-assistants-making-banking-easier-for-everyday-consumers/

[24] Abdullah A. I. Alnajem and Ning Zhang, "A Copula-based Fraud Detection (CFD) Method for Detecting Evasive Fraud Patterns in a Corporate Mobile Banking Context", International Conference on IT Convergence and Security (ICITCS), Macao, China, December 2013

[25] Dr. R. Jayabrabu, Dr. V. Saravanan and Dr. J. Jebamalar Tamilselvi, "A framework for fraud detection system in automated data mining using intelligent agents for better decision making process", International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), Coimbatore, India, March 2014

[26] AI-Based Fraud Detection in Banking – Current Applications and Trends published by Niccolo Mejia (January 21, 2020) Available in: https://emerj.com/ai-sector-overviews/artificial-intelligence-fraud-banking/

[27] Cheng-wei Zhang and Yu-bo Wang, "Research on application of Distributed Data Mining in Anti-Money Laundering Monitoring System", 2nd International Conference on Advanced Computer Control, Shenyang, China, March 2010

[28] Future digital finance - Here's How HSBC is Using Artificial Intelligence to Take Money Launderers to the Cleaners by WBR Insights (2019) Available in: https://netfinance.wbresearch.com/hsbc-artificial-intelligence-strategy-to-beat-money-launderers-ty-u

[29] Chaonion Guo, Hao Wang, Hong-Ning Dai, Shuhan Cheng and Tongsen Wang, "Fraud risk monitoring system for e banking transactions" , IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing", 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, Athens, Greece, August 2018

[30] Priya D. Dozier and Troy A. Montgomery, "Banking on Blockchain: An Evaluation of Innovation Decision Making", IEEE Transactions on Engineering Management, November 2019

[31] Aabhas Sood and Rajbala Simon, "Implementation of Blockchain in Cross Border Money Transfer", 4th International Conference on Information Systems and Computer Networks (ISCON) in Mathura, India, November 2019

[32] Mohammad Shahriar Rahman, Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Anirban Basu and Shinsaku Kiyomoto, "Accountable Cross-Border Data Sharing Using Blockchain Under Relaxed Trust Assumption", IEEE Transactions on Engineering Management, January 2020

[33] Use Cases of Blockchain Technology in Banking 2020 by YouTeam Editorial Team. Available in: https://youteam.io/blog/10-use-cases-of-blockchain-technology-in-banking/#:~:text=In%202016%2C%20US%20Federal%20Reserve,Bank%2C%20BNP%20Paribas%2C%20etc

[34] Luo, G., Li, W., & Peng, Y. , "Overview of Intelligent Online Banking System Based on HERCULES Architecture", 2020

[35] 3 Major Roadblocks to Blockchain Adoption in Banking by Ivan Kot on 02 December 2019. Available in: https://www.finextra.com/blogposting/18197/3-major-roadblocks-to-blockchain-adoption-in-banking

[36] Mehrotra, A. , "Artificial Intelligence in Financial Services – Need to Blend Automation with Human Touch" at International Conference on Automation, Computational and Technology Management (ICACTM), 2019

[37] Agarwal, P., "Redefining Banking and Financial Industry through the application of Computational Intelligence", Advances in Science and Engineering Technology International Conferences (ASET) , 2019