BULLET: Jurnal Multidisiplin Ilmu
Volume 03, No. 06, Desember 2024
ISSN 2829-2049 (media online)
Hal 731-743

Harnessing Big Data with AI-Driven BI Systems for Real-Time Fraud Detection in the U.S. Banking Sector

Ashok Ghimire
Westcliff University, USA
ashok.ghimire1991@gmail.com

Abstract

AI BI systems with integration to Big Data is going to help change the face of the detect fraud for banking sector in United States. This paper examines how these technologies make it possible to detect fraudulent activities in real-time: the novel being that mega yards of transactional data may have to be ingested and analyzed in near real-time to make way for machine learning, predictive models, and/or AI. Banks are on the receiving end of those more advanced techniques and with the use of AI and Big Data there is capacity to analyze of those fraud patterns, improve accuracy and eventually diminish the made losses. However, the actual application of these systems has its drawbacks: concerns for data protection, having algorithms with certain biases, a history of the corresponding system being meddled with and needing to be updated. The present work aims to consider a few examples of applying the AI solutions in practice to investigate actual and pilot cases of frauds in the big US banks, such as JPMorgan Chase, Bank of America, and Wells Forgot. It also includes an emergence of fraud detection systems which in form of block chain technology, enhanced biometric science, quantum technology and shared fraud detection platform. However, all these technologies are seen to offer a great potential for enhancing the security level of the banking sector, especially as regards the prevention of fraud activities in the field. These are the goal posts which financial institutions have to clear while adopting change, controlling frauds to combat new techniques in an environment that moves towards an online financial services consumer's environment.

Keywords: AI benefits, risks and applications, such as using AI for fraud control, Business Intelligence, Big Data, machine learning, predictive analytics, real-time fraud, the US banking industry, block chain technology, biometrics, quantum computing, algorithmic prejudice, data protection.

INTRODUCTION

The United States has witnessed enormous growth of technology in the banking sector in the last few decades and the use of Big Data and technology AI is one of the most pioneering changes. Consequently, with more and more economical organizations being threatened and challenged by the emergent and iterative digital environment, there has indeed never been a higher call for more novel strategies against such financial fraud risks tackled real-time. This paper offers the chance to connect Big Data with artificial intelligence powered Business Intelligence (BI) systems as a measure of safeguarding sensitive financial data and banking secure operations [1]. New types of risks including identity theft, credit card fraud and account take over have emerged in the banking sector in form of cybercrimes. This type of fraudulent behavior is on the rise because the mass of information gleaned from financial operations is on the rise too. Traditional methods of fraud detection as well as knowledge based and manually time-consuming and they do not detect and respond to fraud until it has already happened, and in addition to this the accuracy score that they offer is not very high which hardly enable the banks to fight fraud in real-time. As a result, the financial institutions have adopted the AI and the Big Data analytics in the identification of any unlawful activities and preventions of risks [2].

As the engine of this technological transition, BI systems are built using information technologies and, more specifically, artificial intelligence. These systems could handle transactional data at high speed in real-time to give far better results on trends, deviations and threats than traditional approaches. It also allows the banks to detect fraud in its infancy and besides it also allows the banks to counteract any further loss by immediately responding to new threats. Besides, they pointed out that Big Data can enhance the efficiency of AI systems because the data on which Big Data operates is diverse in terms of data type and, therefore, enhance the efficiency of fraud detection models [3]. The large volumes of transaction data means that AI can refresh its learning from the new patterns and the systems also have the ability to enhance the detection methods as new strategy are developed by fraudsters.

This paper is centered upon Big Data, AI and BI systems with a view to analyzing their real world applicability in real time fraud detection system in the banking sector of United States. The paper describes advantages of applying artificial intelligence to fraud detection, issues of financial organizations, and potential trends of such technologies in financial securities. In this section, the background to the material that will be presented in this article is presented by considering the relevance of Big Data, AI and fraud detection in the modern business environment of banking [4].

BIG DATA, AS WELL AS ARTIFICIAL INTELLIGENCE

When analyzing recent advancements in banking and their connection, two primary pillars may be distinguished: Big data and Artificial Intelligence. I will therefore briefly describe each technology to appreciate how they play a role in enhancing the fraud prevention in the United States banking industries before continuing with the paper.

Big Data in the Context of Banking: Big Data as defined a system that deals with the large amounts of structured, semi structured and unstructured data that is being generated at an incredible rate. In the context of banking business, this data can be obtained directly from customers within branch and ATM level, through mobile and internet banking channels, from social media platforms, as well as, from external sources of market data and third-party information [5]. The data is not only big data in terms of size and complexity but also poly-structured in terms of the data types that include text, image, voice and transactions logs. Banks perform petabytes of data on a daily basis and at the present, volume is only rising. The prerequisite to such amounts of information accumulation gives banks a lever that in turn shall enable them to understand the behavioral patterns of the customers, the efficiencies of the various branches and offices or even the existence of various new fraud schemes [6]. Old fashioned like databases and analytical software programs can deal effectively with such big data and big data as well but will need Big Data like Hadoop and Spark. Such degrees of freedom afford flexibility to banks to control, manage and compute data over the network so that the system itself can grow and accomplish the work on the mentioned scale. Big Data analytics will make the Big Data technology capable of doing identification of patterns, analysis of customers and assessment of other behavioral patterns, and identification of suspicious activity or fraud.

Role of AI in Modern Business Intelligence (BI) Systems: Artificial Intelligence, on the contrary, is the division of computer science, which is aimed on creation of systems capable to solve tasks which can be solved only Oriental intelligence, including pattern recognition and learning. Cognitive computing includes Machine learning (ML), Natural language processing (NLP) and Deep learning (DL) and all fall under AI but all have different uses in banking industry. When incorporated in Business Intelligence BI systems, AI makes it easier for banks to fully exploit their Big Data through intelligent decisions in operation [7]. For example the application of machine learning involves developing one that forecasts risk factors and identify suspicious activities in real time. They are constantly updated over time as the ‘AI models learn” from new data to make it effective at putting through fraud detection. With the help of AI-based BI systems, it is not only possible to analyze fraud attempts and prove them but also define the organizations or departments which should be under more careful control in the future [8].

The Synergy between Big Data and AI: Combined with the help of Big Data, the AI enhances the BI systems’ potential in detecting fraud when it happens, in real time. Big data coupled with an intelligent algorithm and intelligence enables the financial institutions to not only analyses past data strait but to also identify emerging threats and transition of fraud techniques. For instance, based on deep learning approaches, one can implement complex developments operating with enormous databases to explain in apparent patterns and outlying conditions that a human analyst or conventional anti-fraud systems cannot detect. However, AI heeds the ability to forecast future incidents due to the integration of real-time Big Data feeds to the learning job, while also providing a powerful way of refining the detection job frequently [9]. As new transaction data is fed into them, these systems learn and enhance over time, making the recognition of fraud patterns better even with increasingly complex heists. When it comes to application Big Data and AI can help the banks improve their mechanisms of fraud detection and prevention dramatically compared to regular means. This integration of the technologies not only assist the banks protect customer’s assets but also gains confidence and the overall security of the banking environment is also advanced [10].

REAL TIME FRAUD MONITORING IN BANKING

Anti-fraud measures have been crucial for banks in the past, and given the recent popularity of digital banking, the banks require better technological solutions to overcome modern sophisticated frauds. Pre to date financial institution used simple, rigid and once only based rule to detect suspicious activity. These systems compared the transaction data against predetermined rules for example transaction size, regular changes of the account details or geographical oddities which are suggestive of fraud. These methods were, nevertheless, usually slow, post hoc, and fault tolerant for a high throughput environment more characteristic of present day transactions [11]. On the other hand, real-time fraud detection is a relatively more modern and aggressive action that employs the most advanced tools for accomplishing the fraud as it occurs. This approach is particularly crucial in the context of frequent financial transactions where quadrillion of dollars are handled daily through digital instruments. In real-time system, every transaction can be validated within a snap of a finger thereby denying any dubious transaction a chance to go unnoticed [12].

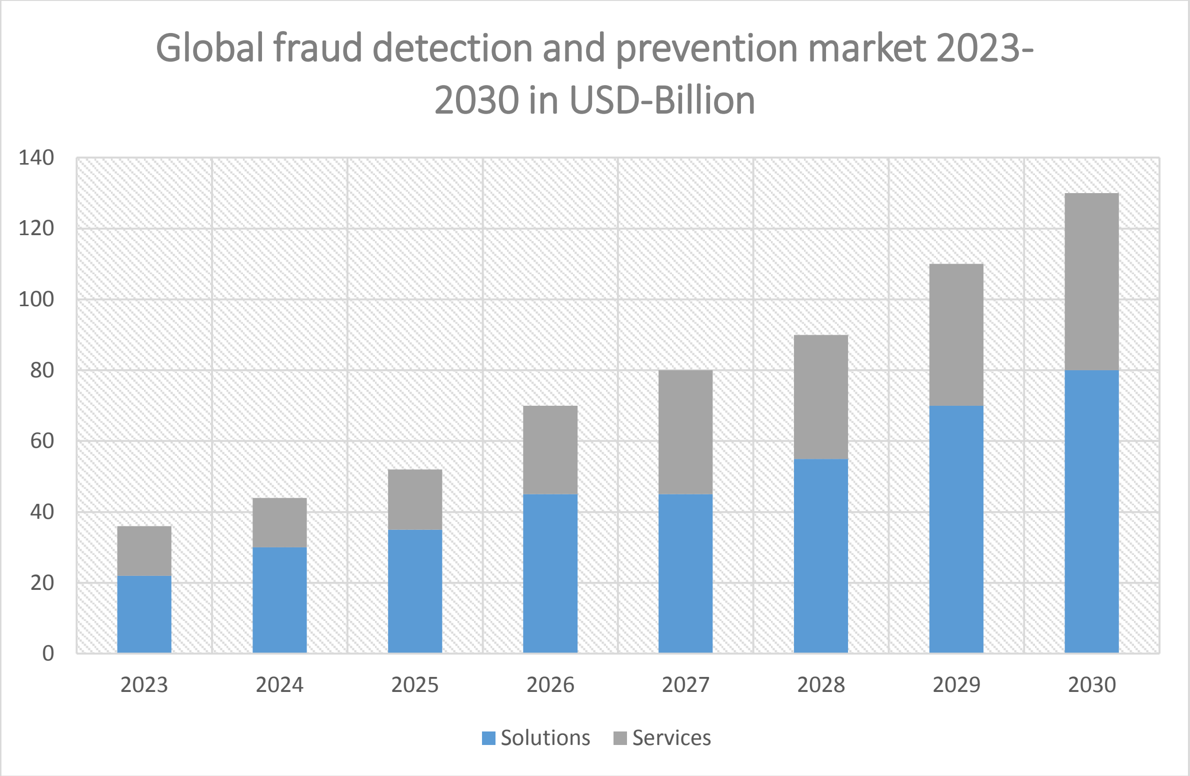

Figure 1: Global Fraud Detection and Prevention Market (2023-2030)

The Importance of Real-Time Monitoring: Real-time fraud detection has several uses as is explained below. First of all, fraudsters never sleep and are introducing even more advanced scams that facilitate the penetration of above mentioned security. Most fraud activities are completed in a second, that is why if banks cannot detect the fraud in real-time, they may face severe financial losses. For instance, misuse of credit cards, identity theft and other invasions into personal accounts only take a few minutes and responses that are delayed cannot suffice [13]. The customers' attitudes and the expectations are different as we witness today being in the electronic business age. Customers require more expeditious and ease of services and want security with no impairment of convenience. Real-time fraud detection helps to build credibility by letting clients know that fee, account and identity data is safe from fraudulent attempts and that any prohibited activity is promptly detected [14].

Traditional Fraud Detection vs. AI-Driven Approaches: Old security approaches to fraud detection were preprogrammed, using historical data and static detection rules that could identify only established threats. However, what AI based fraud detection systems do is quite a bit more than that as they employ machine learning techniques in order to analyze large volumes of real time transactional data. These algorithm can also recognize when there are new forms of fraud that have not been seen before and can point out other anomalies in traffic that could also indicate fraud [15]. They can perform thousands of transactions in one second; analyzing it, checking against similar types of fraud and, if necessary, learning new scenarios, automatically. For instance, an AI application that is purposely designed for a particular user may immediately note if there is an above-average-sized transaction, or if it is located in an unusual place or if it is made too frequently. It can also observe external cues, the device of the transaction, or even typing style and mouse movements because each person is exclusive to their pattern [16].

Benefits of Real-Time Fraud Detection: The subject of informative real- time fraud detection systems has significant advantages. In the first place, they allow enterprises to avoid considerable losses due to fraud detection beforehand. Also, real-time systems make customers more satisfied because customers can immediately know any undermining activity in their accounts, and take appropriate actions. However, these systems lessen the amounts of work attributed to banking employees to handle, especially when these involve isolating different cases of fraud from other pure alert noise that an AI model can handle [17]. Therefore, the presented real-time fraud detection using AI and machine learning can be considered as efficient and scalable solution to protect banking sector from constantly increasing fraud risks. The implementation of these technologies will make the banking arena safer for customers and their financial investment hence a more secure banking system [18].

BUSINESS INTELLIGENCE SYSTEMS AS A TOOL

The BI systems have been in use for many years in decision-making processes throughout industries such as the banking industries. These systems assist organizations to capture huge datasets to make information that can inform organizational improvement processes. When it comes to anti-fraud measures, BI systems are crucial since they allow banks to track the transaction information at the same time as notice fraud."

How BI Systems Integrate with Big Data and AI: BI systems are not a separate technology solution in the banking field; they are most efficient when implemented in parallel with Big Data as well as AI. Big Data offers the great volume of transactions and behavior data required to identify fraud, as well as the appropriate AI algorithms used to recognize patterns and make estimations regarding fraudulent actions [19]. BI systems play the role of an enabler where all these components come into existence to support the BI systems to collect and process data from a number of sources and further help in presenting it in the manner required. BI tools assist banks in analyzing and sorting large datasets and providing the necessary information in workable formats. For instance, dashboards and reports, created by BI systems, provides fraud analysts and decision-makers with the possibility to manage patterns, trends, and anomalies in the real time mode. But with Big Data integration, it enables more accurate detection of, say, fraud by using complicated machine learning models on Big Data, and then making the results in a format that can be easily consumed by human analysts [20].

Benefits of AI-Powered BI in Fraud Detection: In fraud detection, there are several benefits posit/s that can be provided by an AI-powered BI systems. First, they also improve the efficiency of the fraud detection by providing real-time analysis of transactional data. BI using traditional techniques of data analysis that involves physical audits and use of standard procedures cannot offer the same speed with accuracy as that of the automated BI system based on artificial intelligence. Intelligent BI systems use artificial intelligence to learn on their own as they carry out analysis on different data sets [21]. For instance, while it is easy for machine learning algorithms to learn fraud patterns and change the model specifications when new trends emerge, their predictive capabilities increase over time. Therefore fraud detection is not only reactive involved in describing fraud based on scenarios that have already happened but also proactive in that the techniques has to predict fraud scenarios before they happen. The other advantage that is apparent is that fewer false positive results are reported. Conventional models of fraud detection generally lead to high numbers of false positives where sound transactions are marked as complied with fraudulent intentions resulting in inconvenience to the customer. However, by using AI in BI systems more complex variables can be employed to distinguish between fraudulent and accurate transactions causing less numbers of false positives to be generated affecting the customer experience [22].

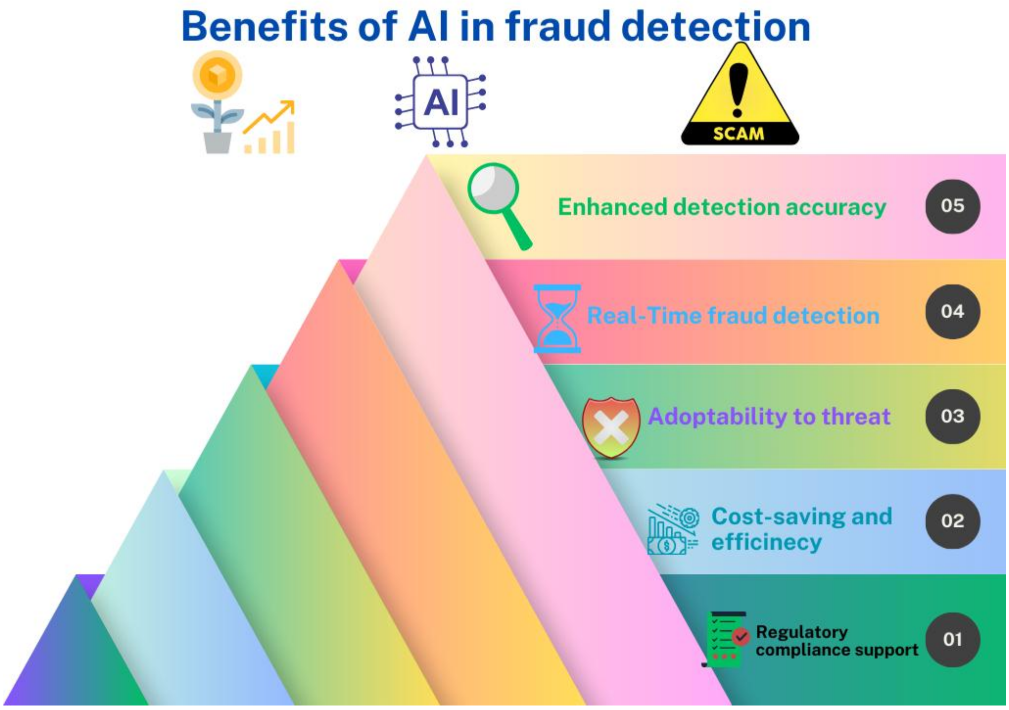
Benefits of AI in fraud detection
AI
SCAM
Enhanced detection accuracy
05
Real-Time fraud detection
04
Adoptability to threat
03
Cost-saving and efficiency
02
Regulatory compliance support
01

Figure: 2 showing benefits of AI in fraud detection

As a result, the role of applying AI in the construction of BI systems is Scalability. These systems on average have endless progress as far as the ability to handle larger volumes of transactions without any compromise. As for operations, it is possible to expand models through which the basic level of fraud detection is offered, without a proportionate relative increase in resource or infrastructural demand. BI systems are rudimentary in AI enhanced fraud detection in the banking sector [23]. When applying BI systems with Big Data and AI, the banking industry is capable of analyzing vast amounts of transactional data instantly, identifying such actions, and enhance the initial array of preventive measures against fraud incidences with the use of AI. These systems offer great optimality of speed, accuracy and scaling in combating more new threats that continue to emerge in financial fraud [24].

TECHNOLOGIES FOR THE IDENTIFICATION OF FRAUD

This paper therefore assesses the extent to which advanced technologies that exist in today's banking environment can detect fraud. Of these, Machine Learning, Predictive Analytics and Artificial Intelligence are the critical in formulating the advanced breed of fraud mitigation systems. These technologies help the banks to capture and manage large data volumes, or to reveal patterns that may lead to emergence of the fraud [25].

Machine Learning Algorithms in Fraud Prevention: Within the kernel of figure of AI, motivated fraud detection, there is machine learning. Whereas the first two methods involve pre-programmed rules indicating fictitious users in a program, machine learning identifies and concludes which one is defined by previous experience as fake accounts and other strange correlations thereto. In long-run such algorithms are better in distinguishing between actual genuine transaction from fake activities and transactions [26]. For better understanding, supervised learning as a machine learning technique is applied to model the training sets where the data points belong to features like for example, fraudulent transactions. Such models then go on to build the knowledge on new inputs of data and alert about fraud should there be in a real-time manner. When the data is presented and not pre-tagged, the system is capable of identifying new and unknown form of the fraudulent scheme since the data is format-free useful when new attacks and modifications occur to the existing one. Therefore, the machine learning models are always evolving in a dynamic environment just as it decides in real time and is less dependent on the current rigid rules [27].

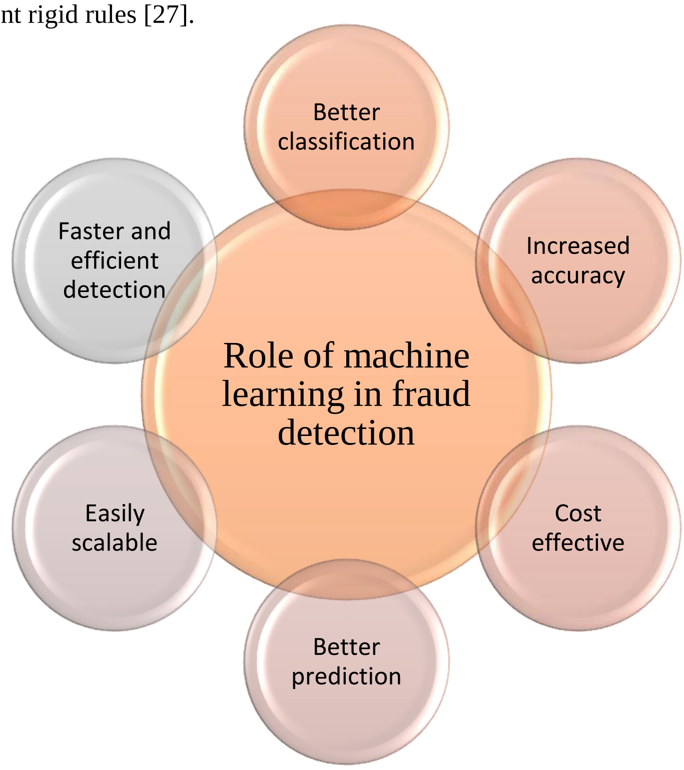

Figure: 3 showing role of machine learning in fraud detection

Predictive Analytics for Identifying Fraudulent Patterns: Predictive analytics may apply some statistics tools and models, and it use the concept of machine learning for making future forecast. In fraud detection, predictive analytics allow to define which transactions are potentially reckless even though they have not occurred yet. As fraud appears in some specific patterns in the beginning, an evaluation of the likelihood that definite purchases or actions are criminal enables banks to respond before they lose more money [28]. For example, analysis of spending could be made to be a predictor and when determining it, other factors such as geographical region or transaction density could also be included, afterwards, any transaction which deviates from the behavior baseline by distance could be checked. It is widely defined as online transaction monitoring which encompasses the efficient analysis of customer data bases for immediate detection of fraud projects as an additional layer of security [29].

The Role of AI in Fraud Detection: The typical AI and its categories, Natural language processing, and Deep learning enhance the techniques of the confrontation of fraud, and the fraud detection system is a set of technologies. Real time analysis of the transaction data is possible with the help of AI in order to bring out the suspicious activity as fraud. Due to the high speed of data processing, AI systems recognize such potentially unsafe actions that may remain unnoticed during regular monitoring, detection means. AI can also try to improve the fraudulent detection and this by trying to include behavioral biometrics for example, which aims at studying how a given customer may be engaging with the mobile application or the website [30]. These are typing speed, the movement of the mouse, force with which a touch pad or touch screen is clicked or tapped, and the speed at which it is clicked or tapped-they are parameters that are unique to the user and cannot in any way be imitated.. Therefore, by embedding behavioral biometrics in the security model, the banks overcome factors of fraud such as identity theft and account cloning. Machine, learning, analytics, and other advanced intelligence which are regarded in industries are also transforming the fraudulent detection in banking now. Using these tools, banks can analyze the continuous flow of transaction data, quickly detect large patterns of fraud, and construct credible models of further frauds. These technologies help the bank not to be on the receiving end by fraudsters as well as protect the customers [31].

PARTICULAR ILLUSTRATIONS AND APPLICATION IN PRACTICE

The articles provide useful examples of applying AI based fraud solutions in the banking industry to give insights on how various technologies such as AI are applied to tackle a emerging threats. Many commercial banks and other monetary institutions in the United States of America have adopted complex technologies for fraud detection by the proper application of Big Data, AI and Machine Learning. It is rather useful to mention some practical examples that reflect the efficiency of the described technologies and the result in combating fraud [32].

JPMorgan Chase: AI and machine learning have been employed in the United States' biggest bank, JPMorgan Chase as a weapon to fight fraudsters. The actual use of detailed AI algorithms involves procedures that help the bank detect suspicious transactions right on the instant and account behavior together with other elements. However, when adopting a deep learning technique, JPMorgan Chase is able to build right fraud maps and future plans. That means that the bank's system updates itself continually through learning from previous deals to boost its probabilities of detecting unlawful deals [33]. By far, JPMorgan Chase has achieved a milestone in fraud detection system in a way that the system differentiates the suspicious transactions from the original ones before the transactions are conducted. This is so because; artificial intelligence application in tracking fraudulent transaction on Real time transaction, will make the endangered bank save much time it usually used in detection of fraudulent transaction. This has not only dealt with cases of loss making, but has also made it possible for the bank to go on maintaining the trust of customers [34].

Bank of America: The bank has also incorporated artificial intelligence based Fraud Fighting solutions for the customer. This is has been applied at the bank by creating machine learning models to decide, develop and put into use models for processing large volumes of transactions to search for patterns of fraud. For instance, through machine learning, the bank had developed ways which assist the firm to identify ugly events like account takeover or fraudulent transactions using the usual pattern of the customer [35]. In addition, processes of Biometric authentication are integrated into the fraud detection services of the Bank of America. Through face recognition and fingerprint scanning the bank has enhanced the general efficiency of ascertaining customers and prosecution of cheating. In addition, it has helped the bank to reduce drastically the fraud rate and offered customers secure banking facilities [36].

Wells Fargo: More significantly, Wells Fargo has integrated some of its operations with the help of AI-based fraud detection especially working on credit card frauds. Machine learning is applied to process the transaction data in real-time, and identify suspicious grants of spending which may be fraudulent. Wells Fargo's system can alert it to a specific transaction if it seems out of the ordinary in relation to the spending pattern of the specific customer in question, including for instance, a large purchase, a purchase at a geographical location different from the usual. What is unique for Wells Fargo here is the active application of behavioral biometrics that focus on actions performed by customers with respect to their accounts [37]. This data is however incorporated with models for detecting frauds to improve on fraud prevention. Wells Fargo has indicated that it has enhanced the accuracy of identifying the fraud incident to increase separations between the falsely detected fraud and the true fraud to enable the actual transactions to happen as planned.

Success Stories and Lessons Learned: The use of cases and examples illustrated in these cases shows that the application of AI in fraud detection greatly minimizes fraudulent operations in different banking products. Worthy of note, nevertheless, are some practical effects which may be discussed as lessons learnt from the applications shown above. It is noteworthy that model training and adjustments are a priority of ongoing work in such a system [38]. The key issue here is that as fraud tactics change, AI models must be able to change too in order to address the new strategies. In all these cases the institutions spend a lot of resources in recalibrating their models for the new data that will help them resist new forms of fraud. The final important lesson that we can learn from this case is that mess is good for customer experience. Although preserving the antifraud infrastructure is the key task, it is highly important for the banks not to let their security measures interfere with the end-user experience. The key and the primary concern whether it be security and convenience can be a problem; however, the banks that are able to crack that nut well are in a better place to sustain the customer's trust while at the same time minimizing the fraud [39].

These case studies bring in the pragmatics of how AI, ML, and Big Data contribute towards the banking industry's anti-fraud activities. With the help of such technologies, a number of big level banks like JPMorgan Chase, Bank of America and Wells Fargo, has enhanced their fraud detection systems, which minimized the loss of bank as well as increase confidence level of customer. The above successful implementation of the model is proof that other financial institutions could make use of the present model to improve their fraud detection techniques [40].

CHALLENGES AND LIMITATIONS

Today, AI application for reducing fraud is the spring of banking industry, however its application is not without certain difficulties. Despite the prospects Big Data and AI technologies can show in terms of detecting fraudulent activities in real-time, there several challenges that financial institutions need to overcome to maximize the use of these technologies [41]. Some of these challenges include; Data protection Act, Algorithmic bias, Integration problems, and Monitoring and updated frequently.

Data Privacy and Security Concerns: However, AI-based anti-fraud systems are not completely devoid of drawbacks, and one of the largest drawbacks is the problems of data protection. Customers transmit their personal information, some of which can be sensitive, regularly to financial institutions, which then preserve all of their transaction records, details, and behaviors. However, such a data set is essential for detecting fraud, and AI systems require this data in real time which increases the involvement of the data being hacked [42]. Even though, banks commit lots of capital into protecting their data assets, the potential for cybercrimes, and data breaches does exist. Also, AI systems are designed to operate in one system or multiple systems of different organizations, and they use data sharing, which is also a problem of privacy [43]. For instance, information collected from third parties or information that is sold, swapped between credits or financial institutions may pose a great threat to the customer's privacy if not well regulated. Financial institutions have to uphold regulatory requirements such as the GDPR or CCPA to uphold the privacy of people's data and extend consumer loyalty.

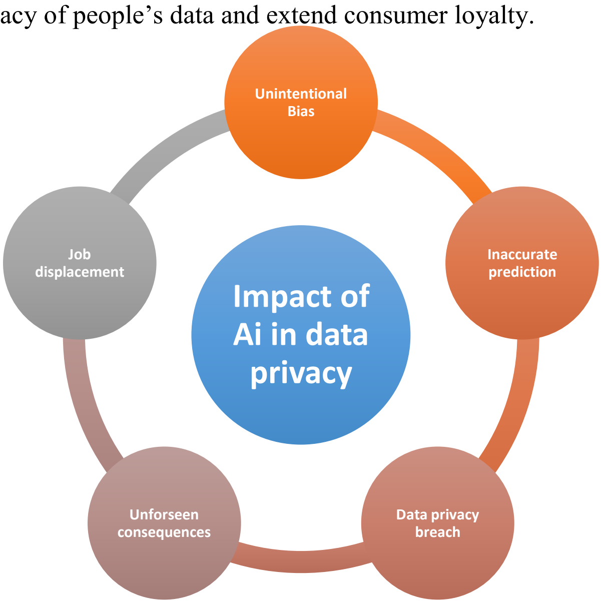

Figure: 4 showing impact of AI in data privacy

Algorithmic Bias and Accuracy: There is another difficulty for AI to combat fraud effectively – algorithmic bias. The machine learning models are based on a set of historical data and so occasionally the prediction may be biased if the input data set utilized to train the models was a partial or a less comprehensive data set. For example, if the training data-F contains two to three specific frauds (biases) then the system is going to be less efficient while recognizing the new fraud patterns [44]. This can sometimes lead to production of a false alarm, or in some circumstance a lack of alarm at all. Bias can also surface where the various demographics of a society are involved, and this is against the various demographics of a society. For instance, if the data that was used in training the fraud detection model does not contain adequate information regarding specific customer, tendencies of such a model are to label all transactions from certain region or customer group as fraudulent. The correct treatment of customers means that AI models must be trained on relevant and random datasets, and this data should be tested for bias regularly [45].

Integration with Legacy Systems: When implementing fraud detection systems based on artificial intelligence in banking organizations, it is necessary to connect them to existing classic systems, which often becomes a cumbersome process. This is a problem for many of today's banks because their infrastructures are legacy, and were not built for today's massively scaled, data-intensive fraud detection. Since AI models need to access large volumes of real-time data, it may be difficult for the supporting systems- legacy systems to support this topographical change without requiring too many enhancements or scrapping [46]. Similarly, costs and time to revamp or replace old-archetype systems may also pose significant challenges for small-scale channel-partner banks or other financial organizations having restricted capital and budget. Banks are trying to strike the balance between implementing the latest technological solutions to combat fraud and, at the same time, minimizing disruption to business continuity while upgrading legacy systems [47].

Continuous Monitoring and Model Updates: Perhaps, the secret to good AI models is that they are not "set-and-forget" kinds of things. These systems need to be, therefore monitored constantly and updated periodically to ensure that they remain useful in detecting cases of fraud. That's why fraud patterns change frequently, and AI models must be updated as often as possible to include new data. It may cause the performance of these systems to decreases if these systems are not fed with new patterns or optimized to improve for new fraud techniques. Supervised learning in monitoring means that adjustments are made constantly, so that an AI system is not drifting or getting false detections [48]. It is a requirement in the financial institutions to invest in resources that would make the fraud detection systems relevant no matter what the threats are at any given time.

Banks have already adopted AI-based FRAUD detection methods as very effective, but for these technologies to be utilized to their optimum several challenges need to be met. Chief among them is data privacy whose violations have resulted in huge penalties, there is a still a lack of full assurance that the algorithms used do not have bias, integration with the existing large systems employed in organizations, and the fact that they require frequent updates. It is therefore important to meet these challenges in order to improve on the efficiency of the AI fraud detection system, its fairness and security of the financial assets as well as the improvement of customer's experience [49].

FUTURE COMMON AND GLOBAL TRENDS AND INNOVATIONS IN FIGHTING FRAUD

The detection technology to fraud is on the advancement and seems to offer greater future to Banks and other financial institutions on how best to fight fraud. This may make it obvious why the banking sector will have undergo drastic changes because as fraudsters devises their strategies the banking sector will in turn devise better strategies. Some trends and innovations in the area of fraud detection are evident in the future they include the following; Block chain, Advanced biometrics, Quantum computing, Collaborative fraud detection [50].

Block chain Technology in Fraud Detection: In this paper has also realized that block chain in a capacity as the technology of the fast growing crypto currencies has much potential relative to enhancing fraud detection. It is in fact a decentralized ledger which allows to record actions that pass through different number of individuals and can be employed in order to avoid manipulations or cheating. It is possible to organize a block chain in the banking context in a manner that would check the transactions that cannot be easily tampered with and generate the record of transaction that cannot be changed [51]. Thanks to the block chain technology the banks can improve the protection from the double spending frauds in the context of the transaction control while at the same time increasing the data integrity for such purposes. In addition, security possibilities of block chain can significantly improve protection of customer information against Internet threats and penetration [52].

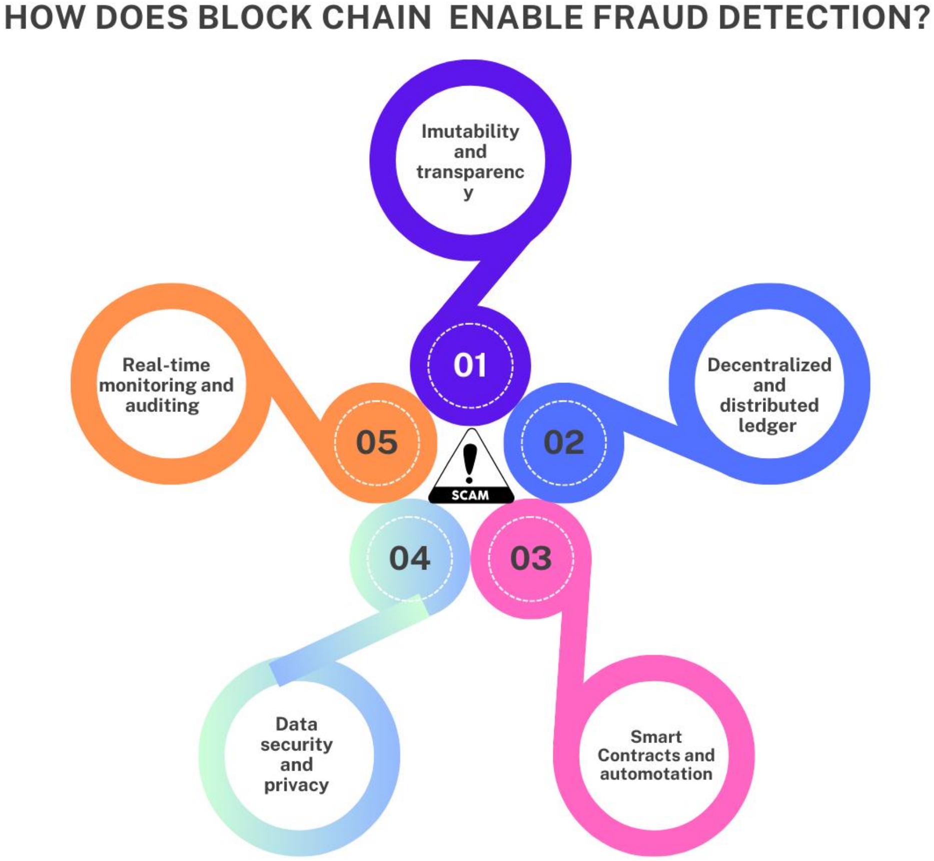
HOW DOES BLOCK CHAIN ENABLE FRAUD DETECTION?
01
Imutability and transparenc y
02
Decentralized and distributed ledger
03
Smart Contracts and automotation
04
Data security and privacy
05
Real-time monitoring and auditing
SCAM

Figure: 5 showing that how block chain enable fraud detection?

Advanced Biometrics for Identity Verification: Thus, there is another interesting update regarding anti-fraud: Biometric authentication in the process. The other basic type of securities for an example use of passwords and PINs are relatively easy to be stolen or hacked. However, biometric identification is mostly safe and increasingly more banks utilize fingerprints, face and voice recognition, even iris scanning to identify the buyer [53]. Biometrics can provide a more accurate and almost real time identification of the customers and the FID For instance, behavioral biometrics; typing behavior, movements of the mouse and contacts with the gadget can help to create a personnel profile. This layer the more an extra layer on the fraud since it is almost impossible for fraudsters to emulate such subtle unique features [54].

Quantum Computing's Role in Fraud Detection: In the next several years, quantum computing will be the future of fraud detection and will already be in its initial stages. Quantum computers are those private-compared PCs that can analyze large data in the shortest time possible and are more sophisticated than normal PCs. This means that they can locate complex patterns of fraud in real-time even in the most unfavorable environment. All sign point to the direction that quantum computing can enhance the applicability of cryptographic technologies, presenting much better encryption strategies that can least be vulnerable to hacking [55]. Furthermore, using the further performing of the quantum algorithms explainable, it is possible to calculate some kinds of fraud examples and determine the probably attacks afterwards with high accurate. Due to all these scenario, as quantum computing mature it is poised to be a key tool in identifying high risk frauds including those that are linked to deep fake or large scale cyber encroachment [56].

Collaborative Fraud Detection Networks: The next trend today is the trend to build networks of financial institutions for the purpose of fraudulent activities identification. Today bank and other financial organization are even exchanging data and canalization about fraud pattern in real time which has a broader view and understanding about the fraud within a bank. This is the case since on its own an organization can only achieve so much, but when they partner or fund an association, funds are pooled together, and intelligence can be more efficiently compiled towards the detection of cross-border or multi-channel fraud. It is also important as these collaborative networks can identify fraud patterns that specific institutions cannot access because of a shortage of funds and data. It will be easy to reduce the fraud risks and the protection measures as a whole if the banks voluntarily agree to do so [57].

AI and Machine Learning Advancements: As time goes on the advancement of AI, especially when combined with machine learning will render the way to beat fraud all the more concrete and predictable. One will be Explainable AI (XAI) which will involve the application of methods to AI for creating interpretable and transparent machine learning models. With this change of perspective, others who are in charge of making financial decisions will need to explain how the usage of AI tool got them to the final [58]. Which is true mainly because; XAI will help in dealing with issues such as; Overcome prior prejudices about the bias of the algorithm in the training phase and; improved understanding of how fraud detection models operate. Introducing deep learning into the systems used to implement the medium will enhance their capability to detect long and complex patterns from large datasets. This will help in identifying new types of fraud who hitherto would be difficult to classify as any of the other traditional type of fraud through normal means [59].

As useful as the concept of fraud detection has been over the years it has been marked by constant evolution and development in technology. From decentralized public transcription of databases where block chain security contention or uses of verification modalities such as fingerprints to face recognition systems use of increased computing power from quantum computers to solve the problems needing solution by the next generation of detection systems [60]. There is need and it is still crucial for financial institutions to remain relevant in being elastic as well as to remain vigilant in these tendencies where and when they exist in handling shifting fraud patterns. By adopting these innovative technologies, such banks will enhance value addition to the consumer when solving their credit problems, and prevent loss, thereby raising the consumers' confidence in the new technologies embracing the course's digital financial front.

CONCLUSION

The application of AI BI systems together with Big Data for fraud detection is a level up for the banking industry. Due to escalating risky incidents and as the risk bearer financial institutions experience more severe fraud plans, these technologies offer a strong strategy to detect the fraudulent transaction in less time and with better accuracy. By using machine learning and predictive analytical, and AI; banks as well as other financial institutions can perform analysis on systematic high volumes of transactional data and make relevant decisions much quicker. However, the problem exists in the implementation of these systems too. This has the problem that data privacy has to be accomplished first and then comes problems, like bias, integration with existing programs, and continual updating of the prescriptive models. Three challenges play an important role here: The efficacy of the methods as applied fairly and accurately, protection from fraud in the systems, and the customer protection of their data.

It is still considered that the future for the process of fraud detection is rather promising, given the essence of new technologies. Block chain solutions, biomimetic, and quantum computing fraud preventions applications are already here and set-up to quickly transform the capabilities of these applications. This is an indication that more connectivity of the financial institutions will strengthen the already emerging mechanism of shared cross-border fraud intelligence which makes it hard for fraudsters to exploit their vulnerable areas. AI and Big Data technologies embedded in fraud detection has potentially impacts the banking industry but as it turns to a new security concept. Much more can still be achieved and yet the progress towards the success of fraud detection implies a promising further development scenario. Banks and other financial institutions that implement such innovations and manage the appearing risks and losses will be prepared to protect the customers, save the monetary loses and maintain the customers' confidence in the digital finance form. When a trend begins to form and advance in the future there would be but the slight opportunity to significantly minimize fraud within the financial sector implying that any significant improvements in the fight against fraud can only occur incrementally

REFERENCES

1. Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. Applied Research in Artificial Intelligence and Cloud Computing, 6(8), 1-21.
2. Khan, I. (2023). Ai-powered Data Governance: Ensuring Integrity in Banking's Technological Frontier.
3. Khan, W. Z., Raza, M., & Imran, M. (2023). Quantum Cryptography a Real Threat to Classical Block chain: Requirements and Challenges. Authorea Preprints. 36. Khatri, M. R. (2023). Integration of natural language processing, self-service platforms, predictive maintenance, and prescriptive analytics for cost reduction, personalization, and real-time insights customer service and operational efficiency. International Journal of Information and Cybersecurity, 7(9), 1-30.
4. Lekota, F., & Coetzee, M. (2019). Cybersecurity incident response for the sub-saharan African aviation industry. In International Conference on Cyber Warfare and Security (pp. 536- XII). Academic Conferences International Limited.

5. Leo, P., Isik, Ö. & Muhly, F. (2022). The ransomware dilemma. MIT Sloan Management Review, 63(4), 13-15
6. Li, Y., Chen, K., Collignon, S., & Ivanov, D. (2021). Ripple effect in the supply chain network: Forward and backward disruption propagation, network health and firm vulnerability. European Journal of Operational Research, 291(3), 1117-1131
7. Luo, Y. (2022). A general framework of digitization risks in international business. Journal of international business studies, 53(2), 344-361.
8. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21(2), 1636-1675.
9. Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. ACM computing surveys (CSUR), 54(6), 1-35.
10. Mishra, A., Gupta, B. B., & Gupta, D. (2018). Identity Theft, Malware, and Social Engineering in Dealing with Cybercrime. In Computer and Cyber Security (pp. 627-648). Auerbach Publications.
11. Montesinos López, O. A., Montesinos López, A., & Crossa, J. (2022). Overfitting, model tuning, and evaluation of prediction performance. In Multivariate statistical machine learning methods for genomic prediction (pp. 109-139). Cham: Springer International Publishing.
12. Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. Journal of Artificial Intelligence and Machine Learning in Management, 5(1), 51-63.
13. Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). Machine learning for anomaly detection: A systematic review. Ieee Access, 9, 78658-78700.
14. Nembe, J.K., Atadoga, J.O., Adelakun, B.O., Odeyemi, O. and Oguejiofor, B.B., 2024. LEGAL IMPLICATIONS OF BLOCKCHAIN TECHNOLOGY FOR TAX COMPLIANCE AND FINANCIAL REGULATION. Finance & Accounting Research Journal, 6(2), pp.262- 270.
15. M. Thisarani and S. Fernando, “Artificial intelligence for futuristic banking,” 2021 IEEE International Conference, 2021.
16. S. Jahandari and A. Srivastava, “Adjusting for Unmeasured Confounding Variables in Dynamic Networks,” IEEE Control Systems Letters, vol. 7, pp. 1237– 1242, 2023.
17. T. Carpenter, “Revolutionising the consumer banking experience with artificial intelligence,” Journal of Digital Banking, vol. 4, no. 4, pp. 291–300, 2020.
18. Z. M. E. Kishada, N. A. Wahab, and A. Mustapha, “Customer loyalty assessment in Malaysian islamic banking using artificial intelligence,” J. Theor. Appl. Inf. Technol., 2016
19. H. I. Erdal and A. Ekinci, “A Comparison of Various Artificial Intelligence Methods in the Prediction of Bank Failures,” Comput. Econ., vol. 42, no. 2, pp. 199–215, Aug. 2013.
20. A. J. Albarakati et al., “Microgrid energy management and monitoring systems: A comprehensive review,” Frontiers in Energy Research, vol. 10, p. 1097858, 2022
21. B. Batiz-Lazo, L. Efthymiou, and K. Davies, “The Spread of Artificial Intelligence and Its Impact on Employment: Evidence from the Banking and Accounting Sectors,” in Business Advancement through Technology Volume II: The Changing Landscape of Industry and Employment, A. Thrassou, D. Vrontis, L. Efthymiou, Y. Weber, S. M. R. Shams, and E. Tsoukatos, Eds. Cham: Springer International Publishing, 2022, pp. 135–155.
22. S. P. S. Ho and M. Y. C. Chow, “The role of artificial intelligence in consumers’ brand preference for retail banks in Hong Kong,” Journal of Financial Services Marketing, 2023.
23. H. Fraisse and M. Laporte, “Return on investment on artificial intelligence: The case of bank capital requirement,” Journal of Banking & Finance, 2022.
24. Z. Bai, R. Yang, and Y. Liang, “Mental task classification using electroencephalogram signal,” arXiv preprint arXiv: 1910.03023, 2019.
25. H. Vijayakumar, “Revolutionizing Customer Experience with AI: A Path to Increase Revenue Growth Rate,” 2023, pp. 1–6.
26. S. Jahandari and D. Materassi, “How Can We Be Robust Against Graph Uncertainties?,” 2023, pp. 1946–1951.
27. M. S. Ali, I. A. Swiety, and M. H. Mansour, “Evaluating the Role of artificial intelligence in the automation of the banking services industry: Evidence from Jordan,” Philipp. Soc. Sci. Humanit. Rev., 2022.
28. T. Ravikumar, N. Murugan, and J. Suhashini, “Banking on artificial intelligence to bank the unbanked,” Annals of the, 2021.

29. L. F. Pau, C. Gianotti, L. F. Pau, and C. Gianotti, “Applications of artificial intelligence in banking, financial services and economics,” 1990.
30. G. Samata, P. Sudhakar, and G. Jyothsna, “In silico Analysis of Spike Protein Glycoprotein A of Omicron variant and identification of variant specific peptide based Vaccine,” Research Journal of Biotechnology Vol, vol. 18, p. 7, 2023.
31. M. Riikkinen, H. Saarijärvi, and P. Sarlin, “Using artificial intelligence to create value in insurance,” Journal of Bank …, 2018.
32. Charles E, Iseal S, Olusegun J, et al. Cloud computing for scalable financial data analytics. 2024.
33. Rehan H. AI-driven cloud security: the future of safeguarding sensitive data in the digital age. J Artifi Intell Gen Sci. 2024;1:132-51
34. Bello OA, Folorunso A, Onwuchekwa J, et al. A comprehensive framework for strengthening usa financial cybersecurity: integrating machine learning and ai in fraud detection systems. Eur J Comp Sci Inform Techn. 2023; 11:62-83.
35. Emehin O, Emeteveke I, Adeyeye OJ, et al. Securing artificial intelligence in data analytics: strategies for mitigating risks in cloud computing environments. Int Res J Modernization in Eng Tech Sci. 2024:6:1978-98
36. Bansal U, Bharatwal S, Bagiyam DS, et al. Fraud detection in the era of AI: harnessing technology for a safer digital economy. In: Irfan M, Gupta S, Elmogy M, et al (eds). AIDriven Decentralized Finance and the Future of Finance. IGI Global, Pennsylvania, United States. 2024; pp.139-60.
37. Sekar PK. The data-driven future of finance: advances in engineering for real-time analytics and decision making. Int J Res Comp Appli Inform Tech. 2024; 7:83-97.
38. Munagandla VB, Dandyala SS, Vadde BC. The future of data analytics: trends, challenges, and opportunities. J Artif Intell Med. 2022; 13:421-42.
39. Sohel A, Alam MA, Waliullah M, et al. Fraud detection in financial transactions through data science for real-time monitoring and prevention. Academ J Innov Eng Emerg Techn. 2024; 1:91-107.
40. Nimmagadda VS. Artificial intelligence and blockchain integration for enhanced security in insurance: techniques, models, and real-world applications. Afr J Artifi Intell Sustain Dev. 2021; 1:187-224.
41. Martin’s O, Fonkem B. Leveraging big data analytics to combat emerging financial fraud schemes in the USA: a literature review and practical implications. World J Adv Res Reviews. 2024; 24:17-43.
42. R. T. Stamler, H. J. Marschdorf, and M. Possamai, Fraud prevention and detection. London, England: Routledge, 2019.
43. M. R. Young, Financial fraud prevention and detection. Nashville, TN: John Wiley & Sons, 2014.
44. D. Njuguna, Fraud detection and prevention in organizations. Daniel Njuguna, 2023.
45. M. Krambia-Kapardis, Enhancing the auditor’s fraud detection ability. Pieterlen, Switzerland: Peter Lang AG, 2001.
46. J. Gesi, J. Li, and I. Ahmed, “An empirical examination of the impact of bias on just-in-time defect prediction,” in Proceedings of the 15th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), 2021, pp. 1–12.
47. M. Carey, A. K. Kashyap, R. Rajan, and R. M. Stulz, “Market institutions, financial market risks, and the financial crisis,” J. financ. econ., vol. 104, no. 3, pp. 421–424, Jun. 2012
48. A. Degas et al., “A Survey on Artificial Intelligence (AI) and eXplainable AI in Air Traffic Management: Current Trends and Development with Future Research Trajectory,” NATO Adv. Sci. Inst. Ser. E Appl. Sci., vol. 12, no. 3, p. 1295, Jan. 2022
49. H. Vijayakumar, “The Impact of AI-Innovations and Private AI-Investment on U.S. Economic Growth: An Empirical Analysis,” Reviews of Contemporary Business Analytics, vol. 4, no. 1, pp. 14–32, 2021.
50. F. Jirigesi, A. Truelove, and F. Yazdani, “Code Clone Detection Using Representation Learning,” 2019.
51. H. P. Kothandapani, “Applications of Robotic Process Automation in Quantitative Risk Assessment in Financial Institutions,” International Journal of Business Intelligence and Big Data Analytics, vol. 6, no. 1, pp. 40–52, 2023.
52. Jung, D., Dorner, V., Weinhardt, C., & Pusmaz, H. (2018). Designing a robo-advisor for risk-averse, low-budget consumers. Electronic Markets, 28(3), 367-380. https://doi.org/10.1007/s12525-017-0279-9
53. Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons, 62(1), 15-25. https://doi.org/10.1016/j.bushor.2018.08.004
54. Kshetri, N. (2021). Artificial intelligence in developing countries. IEEE Computer, 54(6), 84-88. https://doi.org/10.1109/MC.2021.3058503

55. Leo, M., Sharma, S., & Maddulety, K. (2019). Machine learning in banking risk management: A literature review. Risks, 7(1), 29. https://doi.org/10.3390/risks7010029
56. Mhlanga, D. (2021). Artificial intelligence in the industry 4.0, and its impact on poverty, innovation, infrastructure development, and the Sustainable Development Goals: Lessons from emerging economies? Sustainability, 13(11), 5788. https://doi.org/10.3390/su13115788
57. Obermeyer, Z., & Emanuel, E. J. (2016). Predicting the future—big data, machine learning, and clinical medicine. New England Journal of Medicine, 375(13), 1216-1219. https://doi.org/10.1056/NEJMp1606181
58. Palmatier, R. W., & Sridhar, S. (2021). Marketing strategy: Based on first principles and data analytics. Macmillan International Higher Education. https://www.macmillanihe.com/page/detail/MarketingStrategy/?K=9781352011074
59. Rust, R. T., & Huang, M. H. (2014). The service revolution and the transformation of marketing science. Marketing Science, 33(2), 206-221. https://doi.org/10.1287/mksc.2013.0836
60. Srivastava, U., & Gopalkrishnan, S. (2015). Impact of big data analytics on banking sector: Learning for Indian banks. Procedia Computer Science, 50, 643-652. https://doi.org/10.1016/j.procs.2015.04.098