BULLET: Jurnal Multidisiplin Ilmu
Volume 3, No. 05, Oktober-November (2024)
ISSN 2829-2049 (media online)
Hal 673-684

Advancing Healthcare, Petroleum, Chatgpt, Fraud Detection, and Cybersecurity: The Transformative Role of Artificial Intelligence

Mohammad Ali

Independent Researcher Iraq

m.ali.m2000m@gmail.com

Abstract: The results found are that AI is quickly changing the industries with increasing prominence in areas such as health, petroleum fraud identification and cybersecurity. In healthcare, AI to lift the accuracy of diagnosis, of treatment plans and of drug development, directly enhancing patients' quality and outcomes. AI is set to reform the way petroleum's sector identifies frauds and prevents them by detecting fraud cases, ensuring transparency and integrating with other technologies such as block chain. Likewise, AI is taking a more strategic stance within cybersecurity as threats are detected, analyzed and projected, wherein its use presents organizations with powerful preventative solutions for their data and structures. Nevertheless, with the growing use of AI in these sectors there arises important ethical questions that need to be answered. Such include issues to do with privacy, security of data, fairness of algorithms and the inherent requirement of human supervision. Health care related artificial intelligence systems should respect patient rights to privacy and avoid compromise of such rights as well as ensure that it does not have pre – coded biases affecting operations of vulnerable patients. Surveillance, accountability and transparency themes hence play major roles in analyzing fraud detection in the petroleum sector for a secure fair process. In cybersecurity, there is a problem of proportioning privacy with the accessibility of security; another challenge is controlling adversarial attacks on the AI systems; or maintaining human supervision in the decision-making processes dominated by AI. Chatgpt sophisticated natural language processing skills are making it a flexible AI tool that is revolutionizing a number of industries and spurring innovation. All these industries – healthcare, petroleum and cybersecurity – handle large amounts of data that is sensitive that must be collected, stored, and processed in real time to make decisions. By extension and as AI continues to mature, there is still much that AI can do for these industries, but the key to this is going to be the establishment of more concrete and measurable ethics and rules of operation. In this abstract, the prospect of using Artificial Intelligence in healthcare, petroleum fraud, and cybersecurity is presented, along with the focus on the ethical issues in this process for proper and fair AI implementation.

Key words: Artificial intelligence, healthcare sector, petroleum sector, cybersecurity, precision medicine, big data analytics and 'data privacy, algorithmic fairness, Chatgpt, security, privacy, distributed ledger technology, fraud detection and prevention, dashboard analytics and 'transparency, threat intelligence and 'smart threat detection, artificial intelligence conceptual and practical issues in ethical implications of AI.

INTRODUCTION

Artificial Intelligence (AI) has been the greatest innovation that has found its way into many organizations in this 21st century to automate services, decision processes, and increase productivity. Actually, in such fields as healthcare, petroleum, and cybersecurity, AI has emerged as one of the critical technologies with enormous potential to enhance value propositions, solve the existing problems, and co-build the future of these industries [1]. While these fields may appear unrelated; however, all of them have one obvious requirement – development of efficient, smart, and data-guided solutions resulting in improved and more secure performance. The presence of AI in all these different areas further establishes its applications and uses in solving boundary-less issues.

And for instance, the healthcare system is experiencing a rising necessity for individualized precise and timely services and procedures. Given this world economic dilemma, increasing health costs, rising population, and demands for a rapid way of diagnosing diseases; AI is proving its worth. The technologies which have gained latest prominence include machine learning algorithms, natural language processing, and predatory analytics for enhanced patient assessment and diagnosis [2]. The other problem of heath care is poor health resource base, this is also tackled by the use of Artificial intelligence technologies as they allow healthcare professionals to arrive at better decisions faster thus improving the patient's condition. Also, in telemedicine, algorithms are crucial in processing large amounts of data in order to track the patient's conditions, identify the disease and possibly forecast the risks of becoming severe.

Nevertheless, the most apparent problem in the sector, especially the petroleum industry, is fraud and theft, which thwart profit-making goals, erode organizational reputations, and compromise supply routes. The use of AI is

becoming fashionable as fraud fighting tools to identify, eradicate, and prevent fraud related schemes in the oil and gas industry, including transaction monitoring, supply chain and compliance. AI helps reduce embezzlement instances to a bearable level because; through AI, a company can in real time identify signs of fraudulent activities. It is necessary to use advanced technologies, including machine-based fraud detection systems to detect, for instance, irregular behavior of certain commodity traders, false estimates of production capabilities or faked documents which should make it more transparent [3]. This innovative use of AI also increases the efficiency of compliance, which is extremely important in the oil and gas industry that is well regulated and very responsive to environmental and geopolitical challenges. At the same time, cybersecurity as a field continues to expand as the attack techniques become increasingly convoluted and frequent. The growth of digital solutions and the proliferation of smart connected devices have provided unauthorized hackers with a larger attack area that violates the traditional security approach [4]. Cybersecurity workers are now employing Artificial Intelligence to improve threat identification, response initiation, and prognosis of an attack. Machine learning-based AI models can take up the challenge to analyze the vast traffic within networks, discover new threats and weaknesses inherent in a network. AI can also shave the required time to provide responses to the incidents, as the system may be capable of applying pre-scripted security mechanisms in case of intrusion, which may Defense the attack before a human interjection is ever made possible [5].

By increasing automation, strengthening decision-making, and streamlining communication, Chatgpt AI is transforming industries. In cancer, it helps with the analysis of medical data for treatment planning, while in healthcare, it facilitates patient engagement and diagnostic procedures. AI is used in the petroleum sector to forecast equipment faults and improve operations. By examining trends and spotting irregularities, Chatgpt is also playing a significant part in fraud detection. It also helps in cybersecurity by automating reactions and identifying threats. Chatgpt sophisticated natural language processing skills are making it a flexible AI tool that is revolutionizing a number of industries and spurring innovation. All these industries – healthcare, petroleum and cybersecurity – handle large amounts of data that is sensitive that must be collected, stored, and processed in real time to make decisions. Another aspect essential in these contexts is the capacity of AI to analyze and make meaningful patterns out of huge volumes of information in these fields as a lever towards optimizing the operational performance, enhancing security, and encouraging new levels of inventive expansion. However, the convergence has led to the new opportunity to cooperate between these industries [6].

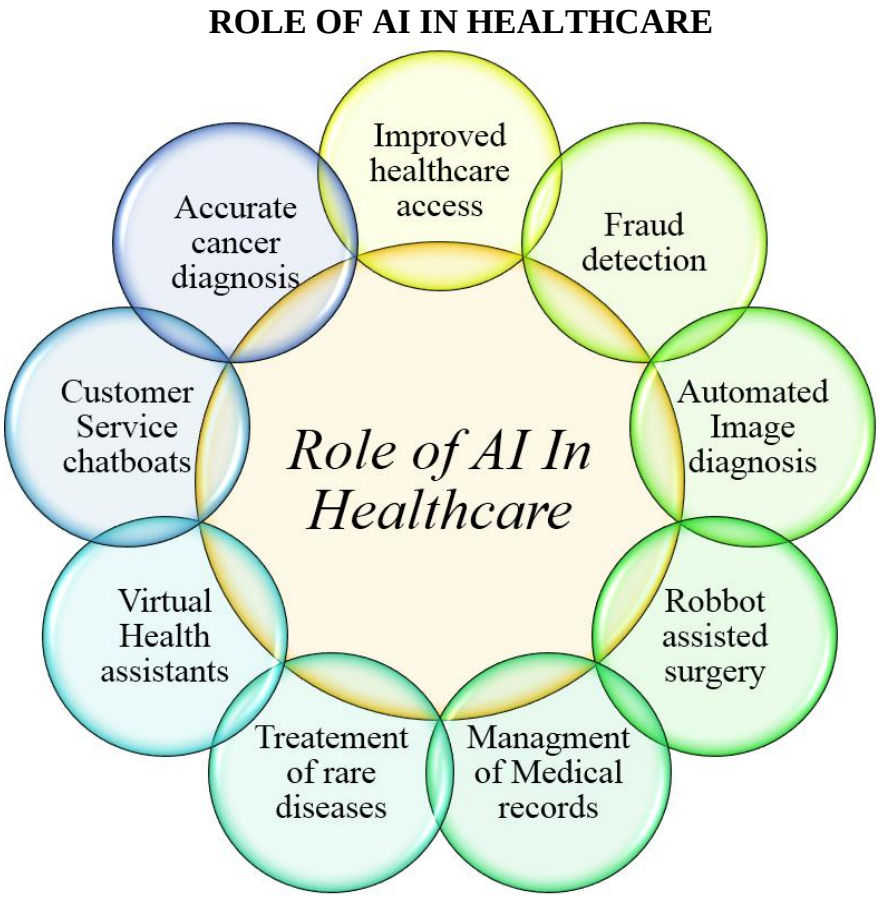

Figure: 1 showing role of AI in healthcare

BULLET: Jurnal Multidisiplin Ilmu
Volume 3, No. 05, Oktober-November (2024)
ISSN 2829-2049 (media online)
Hal 673-684

AI IN THE HEALTHCARE SERVICES

Artificial Intelligence or AI, is gradually becoming integrated in the healthcare delivery systems around the global as it offers solutions that can enhance patients' experiences, make work easier for the medical practitioners and most importantly maintain low costs. AI has become the key driver in how healthcare providers are able to deliver care that is better, faster and more precise. Incorporation of artificial intelligence systems in the medical field has gone to transform the system hence improving diagnostic abilities and probable treatment, monitoring of patients, and administrative responsibilities. This section is focused on the uses of AI in healthcare; the advantages, and the disadvantages; as well as the potential for the future of this technology in enhancing the global healthcare system. The usage of AI in healthcare is probably most notable in the sphere of medical diagnosis [7]. AI computation models particularly, ML and DL can efficiently look into huge clinical data such as images, genes, patient records and analyses for better and faster diagnosis of ailments as compared to conventional techniques. For instance, the AI systems like those used in radiology can diagnose medical images like X-ray, MRI or CT scan to look for symptoms of diseases like cancer, pneumonia or cardiac disease. These AI models can classify images often times better than human eyes, improving the feasibility time of diagnoses hence early intervention which is very vital for a patient. Moreover, it leverages links between massive databases to seek and find diseases that are not so often encountered thus being used to diagnose diseases which otherwise would have been diagnosed after a very long time.

AI is also proving to be very useful for something called precision medicine; that's medicine that is customized based on the patient's unique attributes [8]. This paper shows how a patient's genomic data, clinical records, and other biomarkers can be leveraged by AI for developing a more personalized therapy that is less likely to produce adverse reactions. For example, an AI-based solution can determine the specific reaction of patient to the certain medication and calculate an individual dose. This individualization is even important in management of chronic illnesses such as cancer where therapies can be designed according to the genetic marker on the tumor. One more quite prominent trend present within AI industry is the use of the technology for the purposes of predictive analysis and health issues prevention. ; Using EHRs and other patient information, AI algorithms can then estimate the probability of the patient being at risk for the development of some conditions in future [9]. For instance, AI can help predict cases of diabetes, heart or stroke through early warning on risks associated with individuals' lifestyle, the genetic makeup and their clinical history. Predictive models should therefore allow the healthcare professionals to act before the appearance of these diseases which in some cases may be prevented from fully manifesting after an earlier intervention has occurred. Real time data analysis also means that health care providers can act quickly in the event of changes in a patient's status, thus improving the management of chronic diseases, and minimizing use of emergency interventions.

AI in healthcare administration has also been transformative mostly in areas of increasing efficiency in the operations. AI can be applied in organization of appointment schedules, claims management and administrative duties in relation to patient's records which reduces the involvement of the health care professionals thereby increasing their efficiency of attending to the patients. AI chatbots and virtual assistants are also being incorporated into communicating with patients, for example to answer questions, to remind about a medication or to help sort patients' inquiries, which decrease response time and increase patients' satisfaction. In addition, AI applications continue to support various aspects of organizing hospitals, such as forecasting demand for admissions or staff and equipment distribution, so that the functioning of healthcare institutions is more efficient [10].

In medical, AI helps upend the process of discovering new things at a faster pace. Clinical trials, research papers and patients' recorded results are massive, but AI can take days, or even weeks, to discover what could take years for human beings. AI systems are not only capable of suggesting the future drugs, estimating clinical trial results, and creating molecules that have the potential of being tried out for various diseases. In the context of the recent COVID-19 pandemic, the AI models were used for predicting the virus spread, finding the potential treatment and helping to develop the vaccines' rapidly [11]. The capability of what is currently able to process and analyze data at an unprecedented scale has the potential to reform the approach to drug development and medical research, offering quicker and better treatment.

But let's discuss the primary issues that may appear on the way to the full implementation of AI in healthcare. Security is still crucial, especially when it comes to personal data as patient information is personal and its leakage is impermissible. Secondly, creation of AI models requires large quantities of high quality data; thus, variations in data quality may result in increased incorrect predictions, or biased decisions. Another problem is that AI algorithms contain prejudice [12]. When training models on the data available, there is a tendency for the models

to replicate the existing bias and hence provide prejudiced results in terms of health care treatment for specific subgroups such as the minority or the underrepresented. These risks are why it is vital AI systems are trained on balance datasets and contain the demographics of the society. They also suggest that ethical issues are at the heart of AI uptake. Issues concerning the responsibility of the technology, the intelligibility of recommendations made by the algorithms, and its implications for the relationship between the physician and the patient have to be answered. It is therefore important that the human oversight occurs in the process a AI becomes more integrated into the decision making system, so that care providers remain responsible for the overall care of the patients. There is a great future growth of AI in connected to healthcare [13]. Therefore the use of AI technologies as applied in the healthcare sector is expected to advance further and widening over the years. Further, better diagnostic capabilities, individual care, and forecasting tools will enable care givers to deliver superior care to patients that is cheaper, better, and patient-sensitive. Further advancement in application of artificial intelligence will also assist in solving the problem of shortage of workforce in healthcare departments since Artificial intelligence will assist in enhancing the ability and capacity of the human health care workers. Altogether it is entirely possible for AI to improve healthcare delivery, patient outcomes and transform systems of healthcare globally [14].

ARTIFICIAL INTELLIGENCE FOR PETROLEUM FRAUD MANAGEMENT

Petroleum is among the biggest and indispensable industries all over the world, but it is not exempted from different types of fraud, which result to more losses, noncompliance with laws and regulations and adverse impacts on the image of firms involved. Emerging research issues in the petroleum sector include fraud which may include exaggerated production figures, understating fuel consumption, cheating in the pricing structure, and outright fraud in supply chains. The global petroleum market is quite a complicated one and as such most of the time it is not very transparent which makes it hard for companies, or even regulatory authorities, to easily pin down fraudsters this way [15]. Nonetheless, the modern phenomenon of Artificial Intelligence (AI) is extending a new lease of life in the fight against fraud in the petroleum industry through the enhancement of new techniques that assist in identification, prevention, and minimization of fraud before it contributes to the advancement of enormous losses.

Another of the most visible ways in which AI is being applied in petroleum fraud detection is by use of Anomaly detection. Types of methods being able to learn from a large amount of transactional data, reports of productions, and movements of market prices to develop unexpected patterns that reveal fraud. For example, as a result of built-in algorithms, the AI systems can alert the management to suspected fuel inventory discrepancies, frequent and unexpected plate-audio changes, or deviation in production reports, which are apparent distortions in most cases. By creating patterns from historical data, AI can identify and compare real-world activities to normal trends in real-time allowing for deviation alerts to investigators or systems to further scrutinize. Such ability to provide timely indications of any irregularities potentially transform the campaign against fraud in the petroleum sector as well as enhance transparency in the sector's business transactions [16].

AI also has a massive impact on the monitoring of transactions within the petroleum industry. Unscrupulous business practices, related to corruption, oil laxity and forgery of documents are some of the typical issues. AI models which use natural language processing can look for minuscule cues that indicate manipulation in contracts, emails and records of transactions. By developing an inference system at the application level, the software can look for inconsistencies in contract terms, delivery logs or financial data that an auditor cannot easily detect due to limitations to human cognition [17]. Moreover, AI systems are capable of performing cross-referencing in real-time of many data points from global commodity prices, shipment records, and financial transactions, for example, in order to detect discrepancies or violations in time. This efficiency makes it possible for businesses to dissipate huge capacities of divergent data, thus intensifying the surveillance of transactions and minimizing fraud despite occasioning desist from cumbersome audits.

Another field in which AI is a valuable tool is being able to monitor supply chains. Supply chain networks have different elements which make the petroleum industry's supply chains to become large and have many linkages with suppliers, distributors, carriers and other government agencies. Such dishonest actions as staking and shipment of products together with the false declarations of the fuel quantities are almost impossible to detect when there is no a comprehensive and updated record of all the transactions and shipments [18]. When integrated with block chain technology, it can improve supply chain management control to improve supply chain transparency through a record of any steps in the creation and distribution process of the product. Some of these are as follows:
- AI algorithms can keep watching this block chain and look for examples of malice, theft, or other aberrance. Based on the results obtained in real time it is also possible to forecast potential threats or weak points in the chain, which allows companies to take preventive actions and minimize the probability of fraudulent activity in the chain.

Another is, intelligence utilization of applying artificial intelligence in the regulation of the petroleum industry in its fight against fraud is also another factor [19]. The anti-trust laws, immigration laws and other political policies require compliance in the petroleum sector and failure to adhere leads to fines, sanction and legal action. AI applies in ensuring that the organizations meet various compliance levels concerning specific regulations by offering notification solutions for such compliance status. Existing AI tools are designed to read the rules and regulations, hence comparing them with the working of any business and it's every function to check on all aspects of it to ensure that it is compliant. For example, environmental emissions from the extraction and refining of petroleum can be monitored and verified by AI which are in most cases highly regulated by governments. This means that with the involvement of AI in the processes mentioned above, human influence in terms of negative impact on the result, and delays due to non-compliance with regulations, is eliminated [20].

Another example of AI used in detecting petroleum frauds is applied in the analysis of predictive analytics. AI systems can capture enhanced data from different segments of the petroleum value creation cycle of the exploration and production, the refining, and distribution segments to build models that can predict future trends or fraudulent procedures. Through the possible risks in the system, AI aids in preventing the risks from arising through enhancing surveillance in risky regions or readjusting operational strategies in the regions prone to fraud. By fore casting the impacts of fraud, this is especially useful particularly when fraud occurs in large, high risk areas of organization [21]. For instance, using predictive AI models, organizations may see that there are tendencies in the pricing manipulations or investigate the high degree of likelihood of fraudulent underreporting in the oil quantity, or something like that, and companies can act accordingly.

However there is potential risk involved in the use of AI for deficiency detection of fraud in the petroleum sector. The major issue one is likely to experience when working with such datasets is Data Quality. AI models in development depend much on the quality of the inputs and data used in their development to make meaningful forecasts and discover oddities [22]. Problem: In the scenario of the petroleum industry, where supply chain data may be scattered, incompatible among regions and systems, or incompatible among processes, the challenge of maintaining data integrity and quality for AI analysis can be significant. In addition, the performance of AI systems depends upon the algorithms that form their rudimentary base. That is why models or biases within the data can lead to poor results – making fraud go unnoticed or genuine transactions appear suspicious.

The second difficulty is implementation. The implementation of artificial-intelligence based fraud detection system involve high capital investment with regards to the technology infrastructure and the human resource. The enterprises have embraced the idea of artificial intelligence and data science to develop, implement and support these systems, hence it is crucial for organizations to have relevant talent to support the process [23]. Moreover, such algorithms require constant updating as the fraudsters try to create new, and sophisticated schemes, therefore, the process involves high investment and the need for specialists. All in all, thanks to AI application, the detection and prevention of fraud in the petroleum sector is being significantly shifted towards the enhanced voluminous data analysis, activities monitoring and compliance with the regulatory requirements. Thus, the incorporation of AI in the petroleum industry will help this industry enhance its transparency and minimize losses arising out of fraud and potentially increase its efficiency of transacting business through improved and enhanced supply chain integrity, transaction monitoring and predictive analysis. Over time, more and more uses of the technology will be seen in mitigating fraud threats in the petroleum sector, delivering even better and efficient instruments to businesses for preventing fraud in real time. But to fully unlock the benefits of AI in this critical area, addressing the issues like data quality, data bias, and integration issues are again fundamental to success here [24].

ENHANCE CYBERSECURITY WITH THE HELP OF ARTIFICIAL INTELLIGENCE

In a relatively short period of time, the necessity and urgency of the maintenance of security in cyberspace have become one of the most essential topics in the world. Despite the rise in volume and complexity of threats in the cyber domain, traditional security practices are having a hard time coping. In response to this, Artificial Intelligence (AI) is beginning to be seen as a force multiplier for cybersecurity. Thanks to the processing capacity and cutting edge pattern recognition, AI is revolutionizing cybersecurity detection, prevention and response in the real time. This section examines how AI is enhancing cybersecurity, the issues arising from it, and opportunity of transforming the security domain [25].

Artificial intelligence in Threat Identification and Mitigation: Perhaps the most valuable use of AI in cybersecurity is the identification of threats with higher speed and accuracy than manual methods offer. Cyber threats such as the malware, phishing, and ransom ware are hard to decipher and easy to penetrate traditional security provisions like firewall, anti-virus amongst others. Software, especially the ML software is very capable

of detecting and dealing with these threats immediately since it involves data from network traffic, user activities, and feeds from outside the network [26]. Machine learning algorithms learn patterns of normal and abnormal behavior typical for the system, using the system's history data. Once trained, an AI model can continuously observe activities within a network such as; traffic patterns, logs, and users' activities in search of negative patterns that may indicate a security breakdown. For instance, if a system identifies high traffic data activity, or an attempt to enter a password protected site or area, or large variation from normal patterns of employees' functioning, the AI alerts these as suspicious and may either notify the administrators or respond automatically. Indeed, the ability to spot even a micro-deviation is a significant strength of AI since the rule-based system is often unable to identify new risks.

AI in Malware Detection: AI is also bringing a radical change in malware identification. It was mentioned earlier that traditional methods for detecting malware depend on known databases of malware signatures; these are highly effective in detecting threats only if the latter are already recognized. Such obfuscation is ineffective against unknown or zero day attack types – those for which no known exploits exist [27]. AI based on the other hand, utilizes machine learning to discover similar new malware through behavior but not signatures. What makes AI great here is that it can detect suspicious activity based on the actions that files and programs perform in a system, and even brand new malware will not go unnoticed? This proactive approach also means that cybersecurity frameworks already capture threats and neutralize them before they can do much harm.

For instance, AI in the systems can track this behavior like a change in files on the system, connection to external servers or servers, and running unknown processes to name a few. As a behavior-based detection approach, has been found to be quite effective in detecting APTs as well as any other sophisticated malware that most of the other systems do not detect. It also worth to notice that one more advantage of AI application in the cybersecurity field is its capacity for providing automatic reaction on appeared threats [28]. Usually, attacks happen quickly and waiting for the human interaction delays the analysis of the consequences significantly. This is because AI can quickly analyses and act on threats as they start to emerge, without needing to alert human control. For example, once an AI system has identified an intrusion or other malicious activity, it will be able to shut down a compromised system, black list the identified IP address, or trigger one of a number of pre definable protection measures without requiring human intervention [29].

Other associated and automatic incident response systems are also advancing, allowing analysts to prioritize and examine more strategic information, while regular or recurring motions are executed by the AI. Malware can be 'healed' automatically, the firewall can be updated, or the countermeasures can be enacted such as containing ransom ware. Outsourcing such tasks to AI, organizations can minimize response time, the overall damage caused by cyber-attacks, and shift their cybersecurity specialists' attention to more extensive threats. Another way in which AI proves its value is through the massive volume of data it can also analyze in order to improve threat intelligence and predictive security [30]. Through accessing and processing the information circulating within networks, logs, security descriptions, social networks, the dark net, and other threat intelligence systems, AI can determine where threats will probably occur next. Automated analyzing of data is capable to detect IOCs, malware trends and TTPs with the help of analyzing capabilities of machine learning algorithms. This results in this predictive capability to enable cybersecurity teams to be ready when certain attacks are likely to happen.

For instance, AI systems enable identification of pre-cursors to the cyber-attack such as a sharp rise in scanning activities or diffusion of certain types of malware to prevent an attack [31]. When it comes to the power of predictive models, they are also capable of detecting initial weaknesses in a system to be targeted by the attacker; the weaknesses can then be sealed off and therefore minimize chances of the attack succeeding. Thus, there is nothing peculiar about strengthening the role of AI in cybersecurity coming with certain hurdles. The major challenge that was outlined to me is data quality. AI function is based on ability to learn machine learning algorithms from the large volume of data and detecting threats depends on the quality of data set. That is the reason why if training data for the AI models contains bias, some missing values, or noises, it will result in false positives, meaning it will flag normal activity as malicious, or false negatives meaning that it will not detect actual threats [32].

The last challenge is unpredictability where the nature of cyberattacks keeps changing but the solutions do not. Hackers never sleep and this is why artificial intelligence systems will always need to update so they can be ahead of hackers. This is done by continuous update of the machine learning models which at time may need additional power and some considerations of difficulty. Furthermore, injected attacks from hackers who try to deceive the AI security measures deliberately are another challenge to AI security measures [33]. Currently, there has been efforts made by researchers to ensure that AI models are more resistant to such kinds of attacks.

BULLET: Jurnal Multidisiplin Ilmu
Volume 3, No. 05, Oktober-November (2024)
ISSN 2829-2049 (media online)
Hal 673-684

TOPICS INCLUDED ARE THE FUTURE OF AI IN HEALTHCARE, PETROLEUM FRAUD DETECTION, AND CYBERSECURITY

AI has been on the spotlight in recent years and is being implemented throughout different industries; with huge benefits projected in health care, petroleum fraud detection and cyber security. This establishes the current and future development of AI in these domains where growing industries complement advanced AI technologies, to respond to current and future issues in these industries, will witness further positive changes in efficiency, accuracy and security of these industries. In this section, the future developments of AI in these significant areas are discussed based on emerging technologies, challenges, trends, the impact on fields, and society. AI in Healthcare: Now we are witnessing a revolution in the forms of personalized and predictive medicine. AI holds much potential and many opportunities in health care, and there are likely to be constant improvements in press personalized medicine, diagnosis and online predictive analysis in the future [34]. With advancement in AI solution, the AI systems' accuracy increases and capability of handling large complex data, for instance, genomics data, patients' data, and the streaming health data from wearable's and IoT.

In the sphere of Precision Medicine AI is going to contribute to the development of individual treatment that takes into account the person's genetics, their health history, and many other things. Such patient sensitive personalization could enhance delivery of therapies and timing of medications while lowering the risk of side effects and enhancing the quality of care. For instance, one may think about how algorithms might advance in their capacities to identify how certain patients will react to given therapies and how this might change chronic illness such as cancer, diabetes, or heart disease [35]. They also stated that advancement in AI's predictions may also result in mass adoption of precision medicine, which is accurate to the specific patient's needs will make the health sector more efficient.

The use of chance profiling technology in medical care is also up for dramatic expansion also. Using AI artificial cases will have to be built around each patient to assess the probability of potential disease, emergency, for instance heart attack, stroke, or even mental disorder. With this concept of early warning system in one's health, healthcare givers could be in a position to act early enough, eliminating the major health dangers and avoiding lot of emergency measures. In addition, AI will likely be used in the process of drug discovery and clinical trials in a more extensive way to prescribe the likely success of different potentially healing and curing agents as well as to define populations most in need of new drugs. However, the issue of data privacy, the problematic of bias in AI algorithms and the question of the Ethical use of AI decision-making remain open questions [36]. It then becomes the duty of the health care systems to guarantee that the AI structures are developed in a way that they do not infringe patient's right to privacy, extreme caution has to be observed in the type of data fed into the systems to avoid bias incidences and lastly the system's decision making must be easily explainable.

AI IN PETROLEUM FRAUD DETECTION: IMPROVING ENVIRONMENT – INCREASE TRANSPARENCY AND SECURITY

Real-time AI application in petroleum fraud will be influenced by future technological developments such as one stop integration of AI with block chain technology for effectiveness, transparency, and security for the petroleum sectors in the international market. Since fraud in the petroleum industry is on the incipient stage of elevation AI assistance in the fight against fraudulent activities will be central for checking financial and operational malfeasance. Advanced anomaly detection systems are set to become an area for innovation by refining the means, extent, and effectiveness of recognizing disarray in the supply chain, costs, and production reports [37]. Then, based on extensive data coming from contracts, history of transactions, and current market factors, AI will detect fraud much earlier in the case, potentially even prophylactically, because more and more technologies will be able to predict certain fraud-related events. This should increase efficiency by helping to eliminate such fraud as under-reporting, wrong pricing and thefts thus; with the integration of block chain, artificial intelligence could offer a better and more secure pedigree of tracks in the petroleum transactions.

Further, as the AI recognizes the fraud patterns more accurately in the future, it can take a form of predictive model where AI models the likelihood of the fraud and the risk to be expected in the future and hence ease the emergence of threats and preventions [38]. Such level of advancement will greatly limit financial losses, enhance the confidence of stakeholders besides ensuring that the industries operating in the respective countries adhere to the standards set by the laws of the land. But it is beyond the scope of this study to discuss the limitations of data quality and the global nature of the oil and gas industry that must be resolved to fully unlock the potential of AI.

AI in Cybersecurity: Advancing Defense Mechanisms: AI is poised to play a more critical part in cybersecurity as cyber threats become more complex, commonplace, and expensive. In more details, the future of AI in cybersecurity is all about developing better and more advanced force multipliers capable of preventing attacks before they happen. This will be done by upkeeps of machine learning, deep learning and natural language processing that are used to assist the AI system to detect the advanced and unknown risks as well as responding to them in the current real time. They predict that in the following years AI systems will be able to manage even more extensive and intricate information flow of cyber incidents and evolve based on previous occurrences. These AI models will not only respond to breach incidents as seen by the models but also prevent them before they occur. ABEL, Arise; the use of pattern recognition from various information streams like flow, user activity, and threat intelligence across the globe will enable accreditation of emergent trends of cyber assaults including the phishing cons, ransom ware, and APTs and timely intervention [39].

AI will control automated response systems to perform mundane cybersecurity tasks including patching of vulnerabilities, quarantining affected systems, and blacklisting anomalous IP addresses. This automation will decrease the response time rapidly, which in return will improve security operations, increase efficiency in security and allow the professional cyber security staff to concentrate on other important activities. AI could improve the IAM systems, by analyzing biometric data and the behavior of the actors that attempt to access the systems with the objective of detecting potential illegitimate accesses and protecting data. However, when advanced AI is adopted, it is likely that AI cyber attackers may also employ higher levels of AI to attack deep learning systems; often referred to as adversarial machine learning. Such a high attrition rate of security professionals against ruthless cybercriminals means that AI updates will constant and constantly refined. Privacy and ethical concerns as well as the gathering and analyses of huge amounts of data are also an issue at the moment [40].

CONCLUSION

The possible of future look good of AI in healthcare industries, petroleum industries for lessing fraudulence issues and in cybersecurity. The point here is that as the AI technologies continue to develop they will be used more extensively in these industries as solutions to problems that have been known for a long time. Across such critical areas of human endeavors, AI can offer greater efficiency and rise to build safer and more efficient system in healthcare, Cybersecurity, and Petroleum sectors against patient harm, cyber threats, and fraudulent practices respectively. However, these potentiates' realization requires overcoming data quality issues, linking different systems, privacy, and ethical issues. However, as we progress into the future, artificial intelligence will inevitably remain as one of the defining forces of these industries and their further development, alongside generating new business perspectives, it is already a subject to sophisticated analyses to its societal consequences.

Healthcare sector is among the major industries that has been impacted by integration of Artificial intelligence in their operations. But as a concept, it presents certain unprecedented ethical challenges based on issues to do with privacy and security of information. AI systems in healthcare operate based on significant amounts of clients' sensitive personal health information, medical history, genetic information, and lifestyle information. This data, if not well analyzed will lead to some issues regarding privacy of the patients and may lead to information breaches. Any AI systems that are established must adhere to data protection measures such as the Health Insurance Portability and Accountability Act (HIPAA) for the US, and as the technology for AI continues to improve, the difficulty of data protection increases. The reports show that the revelation of precious patient data present a challenge, which require best practices to guide the anonymization of the data, storage and usage to those that have authorization.

This paper focuses on two large areas of ethically contentious healthcare AI: opacity and bias. Machine learning, which forms a basis for many AI systems, are inherently capable of reproducing the bias found in their data; clinical judgment are often trained on historical patient data. If the data used to create the model contained some inherent bias such as racism or sexism, the AI system will feed on that bias and make more prejudicial decisions. This can lead to discrimination of some patient groups especially those from relegated or unpopular groups all in an attempt to augment their profits. For example, an AI system can be trained using a dataset with fewer minority patients; in diagnosing diseases in minorities, the AI will not be very accurate, and determines health disparities. To counter this there is a need for developers in AI to utilize dataset that are inclusive of various minorities and to perform a regular check on the algorithms to determine their level of bias. Moreover, there is an ethical question of whether human supervision comes into play in AI healthcare services. But it is also important to understand that machine learning solutions make recommendations and generate opinions. Healthcare decisions should remain a team's affair where artificial intelligence works hand in hand with the professionals in the field. However, when the AI makes mistakes or supplies incorrect or insufficient information, often a situation happens that a patient's life might be at risk, the final decision is to remain in the hands of a doctor.

Relative to petroleum fraud investigations, AI deployment can strengthen accountability, fairness, and rectification of undeclared, manipulated and fraudulent transactions. But the use of AI in this sector has some ethics that are considered as pros and cons such as surveillance and, responsibility. Fraud detection using AI techniques can encompass the analysis of massive data coming from different areas such as the Record of Transactions, Supply Chain Management and Production Control. Still, these systems can have issues regarding detecting irregularities and perpetual fraud but can also spur privacy and data rights issues. In some cases, such observation of corporate transaction and operation may violate the rights of privacy of the employment, contractors and even consumers due to collection of personal or sensitive information. Any corporation that opts for adopting surveillance powered by technology must guarantee that its tracking processes do not encroach, are adopted with adequate permission, clear disclosure, and monitoring.

Another essential ethical concern is; who is to blame when the much-touted system of fraud detection fails to work as expected? In the case when AI systems classified some legal transaction as fraud, or did not classify some fraud cases at all, then, the question about responsibility can appear. Should the organization or the specific persons who developed and implemented this artificial intelligence system be liable for such results? That is still a grey area: who takes the blame if a large-scale fraud is not detected by the system or if an innocent party is hurt by operations of the system? Such questions raise questions of who is at law for AI mishaps and who is to blame when these AI technologies are used malevolently? There is the question of deciding on algorithmic opacity. Deployed AI models on the production of fraud are sophisticated and rather operate in a 'black-box' philosophy whereby it is not easy to comprehend the decision making process. This is because it becomes extremely difficult or rather near to impossible to explain things especially in situations where the accused business people or individuals involve fraud related offenses. If we want AI to be open and fair, then it has to be transparent, and thus explainable and auditable.

REFERENCES

1. Autor, D. H. (2015). Why Are There Still So Many Jobs? The History and Future of Workplace Automation. Journal of Economic Perspectives, 29(3), 3-30. https://doi.org/10.1257/jep.29.3.3
2. Susskind, R. (2020). Online Courts and the Future of Justice. Oxford University Press.
3. Uzzaman, A., Jim, M. M. I., Nishat, N., & Nahar, J. (2024). Optimizing SQL databases for big data workloads: techniques and best practices. *Academic Journal on Business Administration, Innovation & Sustainability*, *4*(3), 15-29.
4. Rahman, M. A., & Jim, M. M. I. (2024). Addressing Privacy and Ethical Considerations In Health Information Management Systems (IMS). *International Journal of Health and Medical*, *1*(2), 1-13.
5. Jeni, F. A., Mutsuddi, P., & Das, S. (2020). The impact of rewards on employee performance: a study of commercial banks in Noakhali Region. *Journal of Economics, Management and Trade*, *26*(9), 28-43.
6. Valli, L. N., Sujatha, N., Mech, M., & Lokesh, V. S. (2024). Accelerate IT and IoT with AIOps and observability. In *E3S Web of Conferences* (Vol. 491, p. 04021). EDP Sciences.
7. Khan, A. H., Zainab, H., Khan, R., & Hussain, H. K. (2024). Implications of AI on Cardiovascular Patients' Routine Monitoring and Telemedicine. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(5), 621-637.Panhwar, M., Keerio, M. I., Soomro, N., Jamali, A. R., & Lashari, Z. (2017). The role of presoaking in hydrogen peroxide and their involvement in salt tolerance in wheat genotypes.
8. Arif, A., Khan, M. I., & Khan, A. R. A. (2024). An overview of cyber threats generated by AI. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 67-76.
9. Sircar, A., Yadav, K., Rayavarapu, K., Bist, N., & Oza, H. (2021). Application of machine learning and artificial intelligence in oil and gas industry. *Petroleum Research*, *6*(4), 379-391.
10. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI's Revolutionary Role in Cyber Defense and Social Engineering. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 57-66.
11. Choudhary, V., Patel, K., Niaz, M., Panwala, M., Mehta, A., & Choudhary, K. (2024, March). Implementation of Next-Gen IoT to Facilitate Strategic Inventory Management System and Achieve Logistics Excellence. In *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies* (pp. 1-6). IEEE.
12. Khan, M. A. A., Hussain, M., Lodhi, S. K., Zazoum, B., Asad, M., & Afzal, A. (2022). Green metalworking fluids for sustainable machining operations and other sustainable systems: a review. *Metals*, *12*(9), 1466.
13. Jiang, Y., Zheng, G., Li, T., & Lu, S. (2021). AI-assisted medical documentation and diagnosis: A narrative review. Journal of Artificial Intelligence in Medicine, 116, 102074.
14. Leins, K., Lau, J., & Pearce, D. (2020). All the Queen's MEs: Automated Extraction of Definitionsfor Comparative Legal Linguistics. Journal of International Legal and Comparative Law, 2(2), 183-202. https://doi.org/10.1007/s12027-020-00627-w

15. Valli, L. N. (2024). A succinct synopsis of predictive analysis applications in the contemporary period. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 26-36.
16. Zainab, H., Khan, A. H., Khan, R., & Hussain, H. K. (2024). Integration of AI and Wearable Devices for Continuous Cardiac Health Monitoring. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 123-139.
17. Mehta, A., & Choudhary, V. (2023). COVID-19 as a Catalyst for Innovation: Pharmaceutical Industry Manufacturing Techniques and Management of Endemic Diseases. *International Journal of Multidisciplinary Sciences and Arts*, *2*(4), 242-251
18. Samad, A., & Jamal, A. (2024). Transformative Applications of ChatGPT: A Comprehensive Review of Its Impact across Industries. *Global Journal of Multidisciplinary Sciences and Arts*, *1*, 26-48.
19. Valli, L. N., & Sujatha, N. (2024, April). Predictive Modeling and Decision-Making in Data Science: A Comparative Study. In *2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)* (pp. 603-608). IEEE.
20. Lalji, S. M., Ali, S. I., Hussain, S., Ali, S. M., & Lashari, Z. A. (2023). Variations in cold flow and physical properties of Northern Pakistan gas condensate oil after interacting with different polymeric drilling mud systems. *Arabian Journal of Geosciences*, *16*(8), 477.
21. Lodhi, S. K., Hussain, H. K., & Gill, A. Y. (2024). Renewable Energy Technologies: Present Patterns and Upcoming Paths in Ecological Power Production. *Global Journal of Universal Studies*, *1*(1), 108-131.
22. Rauf, M. A., Jim, M. M. I., Rahman, M. M., & Tariquzzaman, M. (2024). AI-POWERED PREDICTIVE ANALYTICS FOR INTELLECTUAL PROPERTY RISK MANAGEMENT IN SUPPLY CHAIN OPERATIONS: A BIG DATA APPROACH. *International Journal of Science and Engineering*, *1*(04), 32-46.
23. Khan, M. A. A., Hussain, M., Lodhi, S. K., Zazoum, B., Asad, M., & Afzal, A. (2022). *Green Metalworking Fluids and Other Sustainable Systems: A Review. Metals 2022, 12, 1466*.
24. Valli, L. N., & Sujatha, N. (2024, April). Predictive Modeling and Decision-Making in Data Science: A Comparative Study. In *2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)* (pp. 603-608). IEEE.
25. Jeni, F. A., & Al-Amin, M. (2021). The impact of training and development on employee performance and productivity: An Empirical Study on Private Bank of Noakhali Region in Bangladesh. *South Asian Journal of Social Studies and Economics*, *9*(2), 1-18.
26. Lodhi, S. K., Gill, A. Y., & Hussain, I. (2024). 3D Printing Techniques: Transforming Manufacturing with Precision and Sustainability. *International Journal of Multidisciplinary Sciences and Arts*, *3*(3), 129-138.
27. Rahman, A., Ashrafuzzaman, M., Jim, M. M. I., & Sultana, R. (2024). Cloud Security Posture Management Automating Risk Identification and Response in Cloud Infrastructures. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 151-162.
28. Mehta, A., Patel, N., & Joshi, R. (2024). Method Development and Validation for Simultaneous Estimation of Trace Level Ions in Purified Water by Ion Chromatography. *Journal of Pharmaceutical and Medicinal Chemistry*, *10*(1).
29. Nasir, S., Zainab, H., & Hussain, H. K. (2024). Artificial-Intelligence Aerodynamics for Efficient Energy Systems: The Focus on Wind Turbines. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(5), 648-659.
30. MEHTA, A., CHOUDHARY, V., NIAZ, M., & NWAGWU, U. (2023). Artificial Intelligence Chatbots and Sustainable Supply Chain Optimization in Manufacturing: Examining the Role of Transparency, Innovativeness, and Industry 4.0 Advancements.
31. Jim, M. M. I., Hasan, M., Sultana, R., & Rahman, M. M. (2024). Machine Learning Techniques for Automated Query Optimization in Relational Databases. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 514-529.
32. Khan, R., Zainab, H., Khan, A. H., & Hussain, H. K. (2024). Advances in Predictive Modeling: The Role of Artificial Intelligence in Monitoring Blood Lactate Levels Post-Cardiac Surgery. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 140-151
33. SHARMA, G., & BOKORO, P. N. Blockchain and AI-empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects.
34. Li, J., & Cui, L. (2021). A survey of AI-driven approaches for K-12 education. International Journal of Information Management, 56, 102233. https://doi.org/10.1016/j.ijinfomgt.2021.102233
35. , S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 610-623.
36. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity. *BIN: Bulletin Of Informatics*, *2*(2), 248-261.

37. World Economic Forum. (2020). the Future of Jobs Report 2020. Retrieved from https://www.weforum.org/reports/the-future-of-jobs-report-2020
38. Arif, A., Khan, A., & Khan, M. I. (2024). Role of AI in Predicting and Mitigating Threats: A Comprehensive Review. *JURIHUM: Jurnal Inovasi dan Humaniora*, *2*(3), 297-311.
39. Valli, L. N. (2024). Predictive Analytics Applications for Risk Mitigation across Industries; A review. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(4), 542-553.
40. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(4), 566-578.