DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

The Role of Artificial Intelligence (AI) on the Fraud Detection in the Private Sector in Saudi Arabia*

Ahmed Farouk Ali Mohammed
Ph.D. Program, Management College, Midocean University

Huda Muhammad Al-Abdul Rahman
Ph.D. Program, Management College, Midocean University

ABSTRACT

This study examines the use of Artificial Intelligence (AI) in detecting fraud within the private sector in Saudi Arabia. The research seeks to comprehend the obstacles and possibilities that organizations encounter when implementing and utilizing AI technologies for fraud detection. This study utilizes a combination of qualitative and quantitative methods to explore how AI contributes to fraud detection in Saudi Arabia's private sector. To begin, an extensive literature review is conducted, focusing on AI-enabled fraud detection studies specifically within the private sector in Saudi Arabia. This review serves as a basis for knowledge and identifies gaps in existing research. Quantitative data is gathered through surveys and questionnaires administered to private-sector organizations in Saudi Arabia, covering aspects such as current fraud detection practices, AI technology implementation challenges, and perceived effectiveness in preventing fraudulent activities. To gain a deeper understanding, qualitative data is collected through interviews with key stakeholders including fraud detection experts, managers, and IT professionals. These interviews provide insights into their experiences and perspectives regarding the implementation of AI technologies for fraud detection in the private sector of Saudi Arabia. Additionally, detailed case studies are conducted on selected organizations that have employed AI technologies for fraud detection purposes. Data analysis involves both statistical techniques for quantitative data such as descriptive statistics, correlation analysis, and regression analysis; while thematic analysis is employed to examine qualitative data from interviews and case studies to identify emerging themes and patterns. Ethical considerations play a crucial role throughout this research process: necessary approvals from relevant research ethics committees are obtained, measures are taken to ensure confidentiality and anonymity of participants' information. The findings from this research will contribute to a thorough understanding of how AI plays a role in detecting fraud within Saudi Arabia's private sector. By employing a mixed-methodology approach, this study aims to provide valuable insights and recommendations for enhancing fraud detection processes using AI technologies within organizations.

Keywords: Artificial Intelligence, fraud detection, private sector, Saudi Arabia.

* Supervision: Dr. Adel Essam.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

Introduction:

Fraud has emerged as a significant challenge for organizations operating in the private sector, both globally and in Saudi Arabia. With the rapid advancement of technology, fraudsters are continually finding new and sophisticated ways to carry out fraudulent activities **(Smith et al., 2019)**. These fraudulent activities can result in substantial financial losses, damage to organizational reputation, and erosion of public trust **(Johnson & Smith, 2018**). In response to this growing threat, organizations are increasingly turning to artificial intelligence (AI) as a potential solution to enhance their fraud detection capabilities. Artificial intelligence (AI) refers to the development of computer systems that can perform tasks that would typically require human intelligence, such as problem-solving, decision-making, and pattern recognition **(Russell & Norvig, 2020)**. AI algorithms can analyze vast amounts of data, identify anomalies, and detect patterns that may indicate fraudulent activities. The use of AI in the private sector of Saudi Arabia offers promising opportunities for streamlining tasks, conserving resources, and mitigating unfounded criticism. However, it is imperative that these practices prioritize the common good and avoid any potential malicious intent. This document explores how AI can uncover deception and dishonesty, weighing its benefits against the risks associated with misguided intentions. With its unmatched analytical capabilities, AI can identify hidden irregularities that may elude human observation **(Kshetri, 2019)**, making it a valuable tool for identifying fraud and managing large volumes of transactions. By incorporating AI into their operations, businesses can improve efficiency, reduce costs, and protect their reputation from false accusations. Nonetheless, ethical guidelines must be established and followed to ensure responsible use of AI in detecting dishonesty. This examination examines the role of AI in detecting fraud within private enterprises in Saudi Arabia, considering both the potential advantages and concerns surrounding advancements in this technology. While AI provides a sense of security by being vigilant and promoting fairness, it also runs the risk of misuse without proper supervision. Therefore, caution and responsibility must be exercised to prevent any unintended harm to virtuous objectives when utilizing AI. In conclusion, with careful consideration and implementation, AI has the potential to provide significant assistance across various domains. The private sector in Saudi Arabia is not immune to the challenges posed by fraud. As the Kingdom's economy continues to diversify and grow, businesses face increasing risks associated with fraud, including financial fraud, insider trading, corruption, and cybercrime. These fraudulent activities not only impact individual organizations but also undermine the overall business environment, hindering economic growth and development. The implementation of AI in fraud detection has gained significant attention in recent years due to its potential to revolutionize traditional methods of fraud detection. AI algorithms can process vast amounts of data in real-time, identify complex patterns, and adapt to evolving fraud techniques. This ability to analyze data with speed and accuracy enables organizations to detect fraudulent activities more efficiently and effectively, reducing the impact of fraud on their operations. Moreover, AI-powered fraud detection systems can complement human efforts by automating routine tasks,

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

minimizing human error, and freeing up valuable resources to focus on more complex investigations. The combination of human expertise and AI technology can lead to more robust fraud detection systems, enabling organizations to stay one step ahead of fraudsters. By conducting this study, we aim to contribute to the existing body of knowledge on fraud detection in the private sector, with a specific focus on the role of AI in the context of Saudi Arabia. The findings of this research will provide valuable insights for organizations in Saudi Arabia, enabling them to make informed decisions regarding the integration of AI technology into their fraud detection strategies. Ultimately, this study seeks to enhance fraud detection capabilities, safeguard organizational assets, and preserve stakeholder trust in the private sector of Saudi Arabia.

Study Problem:

The issue that arises in the context of fraud detection enabled by artificial intelligence in the private sector in Saudi Arabia can be described as follows:

What are the primary obstacles and potential advantages that private sector organizations in Saudi Arabia encounter when it comes to successfully adopting and utilizing artificial intelligence (AI) technologies for detecting fraud in light of the ever-changing environment of fraud and cybersecurity threats?

This study aims to investigate the specific difficulties encountered by private sector entities in Saudi Arabia with regards to integrating and utilizing artificial intelligence (AI) in their fraud detection processes. By identifying these challenges, this study can offer insights into the obstacles that impede the successful implementation of AI technologies and propose potential solutions. Furthermore, this study also endeavors to uncover the possibilities that AI presents for enhancing fraud detection capabilities, such as real-time monitoring, advanced pattern recognition, and adaptive fraud models. Through an examination of both the challenges and opportunities, this study can provide valuable recommendations and strategies for organizations to overcome barriers and maximize the advantages of AI in fraud detection within Saudi Arabia's private sector.

The Study's Importance:

The examination of how AI technologies are applied and used for identifying fraudulent activities in the private sector in Saudi Arabia holds great significance due to multiple reasons:

- **Improving Fraud Detection Capabilities:** Fraud presents a notable risk to companies in Saudi Arabia, resulting in monetary losses, harm to reputation, and potential legal ramifications. Through comprehending the obstacles and prospects associated with artificial intelligence (AI) in detecting fraud, this research can aid organizations in bolstering their abilities to identify and stop fraudulent behaviors. This may lead to better management of risks, greater financial security, and stronger confidence among stakeholders.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

- **The constantly changing landscape of fraud poses a challenge**, as fraudsters are using more advanced methods and taking advantage of weaknesses in traditional systems for detecting fraud. This study aims to provide insights into how AI technologies can successfully identify new patterns of fraud and adjust to the ever-evolving schemes used by fraudsters. By doing so, organizations in Saudi Arabia can stay ahead of fraudsters and reduce their vulnerability to fraudulent activities.
- **The utilization of AI technologies for the purpose of detecting fraud** can enhance the allocation of resources within organizations. Through the automation of repetitive tasks and the mitigation of false positives, AI systems have the capability to liberate human resources, allowing them to concentrate their efforts on intricate and strategic endeavors, such as examining high-risk instances and formulating strategies for preventing fraud. The outcome is an improvement in operational efficiency and cost-effectiveness throughout processes related to fraud detection.
- **Organizations operating in Saudi Arabia are required to adhere to both domestic and global regulations** pertaining to the identification of fraudulent activities and safeguarding of data privacy. The research conducted can offer valuable perspectives on how artificial intelligence (AI) technologies can enhance compliance endeavors by effectively identifying potentially fraudulent transactions, ensuring adherence to data protection protocols, and facilitating the creation of comprehensive audit trails. By leveraging these insights, organizations can proactively minimize legal and regulatory risks associated with fraud detection practices.
- **Leveraging Technological Advancements:** AI technologies have made notable progress in recent times, providing robust resources for the identification of fraudulent activities. By delving into the possibilities presented by AI, this analysis can aid Saudi Arabian organizations in efficiently utilizing these technologies to strengthen their ability to detect fraud. The utilization of AI has the potential to enable organizations to promptly identify instances of fraud, discern intricate patterns, and adjust effectively to evolving landscapes of fraudulent behavior.

Overall, the study holds significant value as it has the potential to offer guidance to organizations in Saudi Arabia on how to efficiently implement and utilize AI technologies for detecting fraudulent activities. Through addressing obstacles, taking advantage of opportunities, and advocating for optimal methods, the study can contribute to enhancing the overall durability and enduring nature of the private sector in Saudi Arabia in the midst of threats related to fraud.

The study's Objectives:

The primary objective of this study is to examine the effectiveness of AI in detecting and preventing fraud in the private sector of Saudi Arabia. Additionally, the study aims to:

- Identify the key challenges faced by organizations in detecting and preventing fraud.
- Evaluate the potential benefits and limitations of implementing AI technology in fraud detection.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

- Analyze the current adoption and utilization of AI in fraud detection practices within the private sector in Saudi Arabia.
- Provide recommendations for organizations to enhance their fraud detection capabilities through AI implementation.
- To explore the challenges and ethical considerations of AI in fraud detection:

✓ Identify data privacy and security concerns.
✓ Examine potential biases in AI algorithms.

- To provide recommendations for organizations and policymakers.

These research objectives provide a comprehensive framework for the study, enabling the readers to systematically investigate the role of Artificial Intelligence in fraud detection within the private sector in Saudi Arabia. Depending on the scope and resources available for the research, it could be further refine these objectives and specify the methodology that plan to use to achieve each one.

Study's Questions:

The following study questions could serve as a starting point for exploring the role of AI in fraud detection within the private sector in Saudi Arabia, this can offer significant understanding and suggestions for organizations seeking to improve their ability to detect and prevent fraud.

Q1. What are the current practices and approaches employed by private sector organizations in Saudi Arabia for fraud detection, and how effective are they in detecting and preventing fraud?

Q2. What are the key challenges faced by organizations in Saudi Arabia when implementing AI technologies for fraud detection? How do these challenges differ from traditional fraud detection methods?

Q3. What are the specific opportunities and benefits offered by AI technologies in enhancing fraud detection capabilities within the private sector in Saudi Arabia?

Q4. How can organizations in Saudi Arabia overcome the barriers and challenges related to the implementation of AI technologies for fraud detection?

Q5. What strategies and best practices can be recommended?

Q6. What are the implications of integrating AI technologies in fraud detection processes for organizations in terms of resource allocation, operational efficiency, and cost-effectiveness?

Q7. What are the ethical considerations and potential risks associated with AI-enabled fraud detection in the private sector in Saudi Arabia?

Q8. How can organizations address these concerns while ensuring compliance with legal and regulatory requirements?

Q9. How can AI technologies be customized and adapted to the unique fraud landscape and cultural context of Saudi Arabia? What factors should be considered to ensure the accuracy and effectiveness of AI-powered fraud detection systems?

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

Study's Hypothesis:

Based on the existing literature and the current landscape of fraud detection in the Saudi Arabian private sector, several hypotheses can be formulated for this research:

H1: The implementation of AI-powered fraud detection systems in the private sector of Saudi Arabia will significantly improve fraud detection accuracy compared to traditional methods.

H2: AI-powered fraud detection systems will be more effective in identifying novel and sophisticated fraud techniques compared to traditional methods. Previous Study and Theoretical Framework

H3: There will be a positive correlation between the level of investment in AI-powered fraud detection and the overall effectiveness of fraud prevention efforts in the private sector.

H4: Regulatory compliance with anti-fraud regulations will be enhanced by the adoption of AI-powered fraud detection systems.

Historical Context and Significance

Artificial Intelligence's Impact on Social Engineering Attacks (Manyam,2022)

The study examines the impact of artificial intelligence technologies, such as voice cloning, deepfakes, and automated social engineering bots, on social engineering attacks. It investigates real-life instances and evaluates the detection and prevention methods for these novel forms of attacks made possible by advancements in AI. The tactics employed by social engineering attackers have evolved with the aid of AI tools, enabling them to exploit human psychology and gain unauthorized access to data and systems. Cybercriminals are becoming more sophisticated by incorporating voice chat into their schemes, luring victims into downloading malware or disclosing sensitive information. Although the use of voice-based social engineering to justify attacks by threat groups is not new, cybercriminals are actively exploring innovative methods to incorporate sound into their attack strategies. In a recent phishing campaign observed by Trustwave researchers, a malicious chatbot was utilized to enhance credibility and convince victims to visit phishing websites through engaging discussions on legitimate platforms. As researchers, the investigation into the effects of artificial intelligence on social engineering attacks is a substantial and timely study, in our view. The results provide valuable insights into the changing strategies employed by cybercriminals who use AI to manipulate human psychology and illicitly obtain confidential information and control over systems.

Artificial Intelligences & Insurance Fraud Study (2020)

This study examines the application of artificial intelligence (AI) technologies in identifying instances of insurance fraud. It presents an overview of various AI techniques, the challenges associated with adopting AI, the advantages of utilizing AI, and considerations regarding public policy when employing AI for insurance fraud detection. The implementation of AI has significantly disrupted different stages

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

within the insurance value chain. While some insurance companies are heavily investing in AI, most insurers are proceeding cautiously due to uncertainty surrounding its deployment and utilization. Notably, survey results debunked the notion that AI is a recent addition to the arsenal of tools utilized to combat insurance fraud. A majority of insurers (56%) reported using some form of AI for fraud detection over a significant period of time. The objective behind incorporating AI in insurance fraud detection is to efficiently generate credible leads and facilitate investigations into suspicious claims and transactions. It should be underscored that AI technology should not replace investigators and claims analysts but rather be seen as a tool to generate alerts for potentially fraudulent activity while providing comprehensive reasoning behind identifying a claim as suspicious to aid in investigations, as stated by one director from an SIU department. As researchers, the study provides a thorough examination of different artificial intelligence (AI) methods and addresses the obstacles tied to incorporating AI into insurance fraud detection. These findings enhance our comprehension of the topic by shedding light on the disruptive impact of AI in the insurance industry and illustrating how insurance companies have adopted various strategies in embracing this technology.

Merging Artificial Intelligence & Blockchain Technologies to Solve Academic Qualification Forgery Issues (Al Wahaibi, et al, 2020)

This study explores the potential of merging artificial intelligence and blockchain technologies to address the problem of academic qualification forgery. The aim is to integrate these emerging technologies in order to detect fraud and forgery more efficiently and effectively, preventing them from occurring. The study also provides recommendations and suggests areas for future research. The forging of academic qualifications is a serious and sensitive issue that continues to grow. In Oman, for example, the Ministry of Higher Education has recorded approximately 1250 cases of forgery, including 108 cases of forged academic qualifications, 25 cases of educational qualifications issued by fictitious institutions, and 1117 cases of false stamps between 1975-2018 (Ministry Of Higher Education – Oman, 2019). Similarly, in South Africa, the latest reports from the South African Qualifications Authority reveal that approximately 1,276 qualifications were identified as counterfeit and forged at the end of January 2017. Of these, 444 were national qualifications and 832 were foreign qualifications (GARWE, 2015). Given their distinct characteristics and functionalities, both artificial intelligence and blockchain technologies offer potential solutions to combat academic forgery. Specifically, blockchain technology is well-suited for addressing this issue as it provides protection and security for researchers' work through features such as information verification and timestamping. The researchers' viewpoint on the investigation into combining artificial intelligence and blockchain technologies to combat academic credential fraud is extremely optimistic. The study tackles a crucial matter in the realm of education and puts forth inventive remedies that could have a substantial influence on detecting and preventing fraudulent activities.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

Neobanks and AI for fraud mitigation start to take center stage to support digital in GCC. (Yazbeck, 2018)

This study examines strategies for combating cybersecurity and fraud in Islamic banking within the GCC region. Specifically, it focuses on the emergence of neobanks and the utilization of artificial intelligence to swiftly identify instances of fraud. The study delves into trends observed from 2017-2018 and provides predictions for 2019. In regard to cybercrime, digital platforms are a prime target for criminals, with smartphones ranking as the second most targeted platform after Windows. The GCC region has experienced a significant impact from such criminal activity, as evidenced by PwC's 2018 survey, "Pulling fraud out of the shadows: A spotlight on the Middle East," which reveals a 12% increase in fraud and economic crime over just two years. Digital banking has been particularly affected; according to Norton Cybersecurity Insights Report from 2017, 29% of respondents from the UAE had their payment information stolen from their mobile phones last year. Despite previous years' speculation surrounding artificial intelligence (AI), it was not until 2018 that its potential benefits in combatting cybercrime and fraud began to materialize. Notably, Temenos launched a real-time fraud solution in 2018 that employs AI to analyze individual behaviors and detect this prevalent form of cybercrime. Mohammed AlShehabi, head of innovation at Al Salam Bank, emphasized the necessity of providing clients with a truly digital service that can adapt to their evolving needs at an individual level. He highlighted that offering value-added services is essential in today's landscape but ensuring trust and security is fundamental and serves as the cornerstone for success.

The researchers hold a positive view on the study that focuses on tactics to counter cybersecurity and fraud in Islamic banking within the GCC region. The study offers valuable perspectives into the obstacles encountered in the digital banking environment and presents effective approaches to tackle cybersecurity and fraud concerns.

Is artificial intelligence the new benchmark for financial crime risk management? Lessons from Past Studies Theoretical Underpinnings (Khan, Hussain, 2023)

This study explores the use of artificial intelligence (AI) technologies, such as identity verification and transaction monitoring solutions, by financial institutions in the Middle East. These technologies can be utilized to combat financial crimes and ensure compliance with regulatory requirements. The study provides examples of how these solutions can enhance existing controls and processes. Financial services industry (FSI) regulators in the Gulf Cooperation Council (GCC) have intensified their efforts to address the growing risks associated with financial crime. They have recently been urging market participants to incorporate technology into their financial crime control frameworks, issuing regulations and guidance to support financial institutions in effectively combating financial crime. The introduction of AI technology offers more advanced solutions for FIs to either supplement or replace their current methods of verifying customer identities. Incorporating AI into the transaction monitoring process has the potential to significantly impact outcomes. By implementing these

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

technologies effectively, manual tasks such as TM alert investigations, which include customer profile analysis and narrative development, can be automated. This automation allows for time and cost efficiencies without compromising on managing risks related to financial crime. The researchers hold a favorable view on the study concerning the implementation of artificial intelligence technologies in financial institutions situated in the Middle East. The study offers significant perspectives on the capabilities of these technologies to tackle financial misconduct and guarantee adherence to regulations.

Artificial Intelligence's Role in Improving the Efficiency of Administrative Systems for Human Resource Management at Tabuk University (Al-Azamah, 2020)

This study explores the significance of artificial intelligence in enhancing the effectiveness of administrative systems for human resource management at Tabuk University. The objective of the study was to ascertain the impact of artificial intelligence on improving the efficiency of these administrative systems. A descriptive analytical approach was employed, and data was collected through a questionnaire. The findings indicated that implementing artificial intelligence programs had a positive effect on the efficiency of administrative systems for human resource management. As such, this study aims to uncover the role of artificial intelligence in enhancing the efficiency of administrative systems for human resources at Tabuk University, conducted by Nourah Mohammed Abdullah Al-Azzama, an Associate Professor specializing in Educational Planning from the Department of Quantitative Administration for Education at Imam Muhammad bin Saud Islamic University in Saudi Arabia. By appropriately implementing computer systems, it becomes feasible to optimize logistics and streamline transportation processes across various regions worldwide, resulting in improved time management capabilities. The researchers hold a positive view on the study's findings regarding the importance of artificial intelligence in improving the effectiveness of human resource management systems at Tabuk University. The study offers valuable perspectives on how AI can positively impact efficiency in this particular setting. However, the research is focused solely on Tabuk University, which restricts the ability to apply the findings to other educational institutions or industries. To increase the study's relevance and suitability for a broader audience, it would be beneficial to incorporate a wider variety of organizations or perform comparative analyses.

Artificial Intelligence The beginning of the end for telecom fraud?

This study examines the utilization of artificial intelligence in real-time detection and prevention of telecom fraud. By analyzing calling patterns and identifying unusual activity, such as calls originating from a specific number range to premium rate numbers, AI aids operators in promptly blocking fraudulent calls or addressing vulnerabilities before significant financial losses occur. Telecom fraud necessitates two key components: the ability to make calls into the network without payment and a method for extracting money from the system to ensure the success of the fraud. In this regard, AI offers capabilities beyond human capacity by monitoring all call records regardless of origin, identifying patterns between ranges of telephone

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

numbers, verifying if such patterns deviate from normal behavior, and raising alerts when irregularities are found. As a result, these advanced systems surpass previous solutions by preventing fraudulent activities from even commencing and acquiring knowledge on how to proactively prevent security breaches. This comprehensive approach provides an all-encompassing solution to combatting telecom fraud. In the researchers' perspective, the study offers valuable observations about the importance of artificial intelligence in identifying and preventing telecom fraud in real-time. The results and thorough methodology provide practical advice for operators to effectively address this problem. This guidance helps protect the integrity of telecommunication systems and reduce financial losses. The research offers valuable findings regarding the application of artificial intelligence in promptly identifying and thwarting telecom fraud. However, it is important to recognize potential constraints such as the requirement for a comprehensive evaluation, presenting precise information on AI algorithms, examining the applicability of these findings in different scenarios, and addressing ethical concerns.

Demystifying AI in anti-fraud and compliance efforts (Walden, 2020)

This study explores the potential applications of artificial intelligence and machine learning in fraud detection and prevention. These include automating data collection, utilizing predictive models to identify high-risk transactions, and engaging employees through compliance chatbots. The study also addresses important factors regarding privacy, ethics, and regulation of AI technologies. In cognitive insights, it is more effective to utilize statistical analysis rather than algorithmic rules to predict a specific customer's purchasing preferences, detect credit fraud in near or real time, and automate personalized targeting of digital advertisements. Organizations are increasingly incorporating compliance chatbots for common inquiries and employee training purposes. Employees often prefer interacting with chatbots or submitting anonymous questions via mobile compliance applications. The ethical considerations surrounding AI technologies were well-articulated by the Organization for Economic Cooperation and Development (OECD) in its May 2019 AI policy guidelines, which have been signed and adopted by the 36 member countries including the United States.

The researchers believe that the study highlights the importance of using statistical analysis to gain cognitive insights. This includes tasks like predicting customer preferences, identifying credit fraud in real or near real-time, and automating personalized targeting in digital advertising. This approach is consistent with the increasing recognition that statistical analysis frequently produces more precise and dependable results than algorithmic rules. However, a possible limitation of the study is its limited discussion on the specific difficulties or disadvantages linked to implementing AI technologies for fraud detection and prevention. Considering and addressing these challenges would result in a more comprehensive analysis.

Using Artificial Intelligence to Address Criminal Justice Needs

This study examines the potential of artificial intelligence (AI) in addressing criminal justice needs, including facial recognition, DNA analysis, gunshot detection, and crime forecasting. Various research projects funded by the National Institute of

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

Justice (NIJ) are leading the way in applying AI to these areas. By utilizing AI technologies, law enforcement and the criminal justice system can benefit from improved accuracy and efficiency. Traditionally, software algorithms that assist humans have been limited to predetermined features such as eye shape, eye color, and distance between eyes for facial recognition or demographic information for pattern analysis. In contrast, AI video and image algorithms are capable of learning complex tasks and developing their own independent complex facial recognition features/parameters to accomplish these tasks beyond human capabilities. Furthermore, AI is playing an increasingly important role in fraud detection. Companies like PayPal leverage large amounts of data to continuously train their fraud detection algorithms, enabling them to predict and recognize anomalous patterns as well as learn to identify new patterns efficiently. The researchers hold the belief that the study puts forth an optimistic perspective on the capability of AI to meet the requirements of criminal justice, such as facial recognition, DNA analysis, gunshot detection, and crime forecasting. It acknowledges the progress made through research initiatives supported by NIJ funding and emphasizes the enhanced precision and productivity that AI technologies can offer to law enforcement and the criminal justice system. Nevertheless, it is essential to conduct additional investigation into possible limitations and ethical concerns in order to guarantee responsible utilization of AI in these particular situations.

Role of Artificial Intelligence in Financial Fraud Detection (Mohanty et al, 2023)

This study examines the role of artificial intelligence in the detection of financial fraud. It explores different AI-based solutions utilized in the banking industry for fraud identification and their impact on performance. According to a leading global business information provider, the use of artificial intelligence-driven solutions in banking reached approximately USD 41.1 billion in 2018. These solutions involve improvements to existing banking processes and infrastructure, as well as increased operational efficiency and cost reduction. Predictions indicate that by 2030, artificial intelligence will have a market value of USD 300 billion within the banking sector. Feedzai claims that its advanced technological solutions using artificial intelligence technology have resulted in a significant decrease of 42% in false positives when detecting fraud. Additionally, it has reported a 53% increase in cost savings due to this technological advancement. Furthermore, there has been a noteworthy jump of 74% in new account approvals. Ayasdi's AML solution has demonstrated an impressive reduction of over 20% in investigative volumes related to fraud detection. It was also successful at identifying various behavioral patterns associated with financial crimes and fraudulent activities, thus enabling HSBC to prevent potential instances of fraud and money laundering by proactively restricting payments before regulations were violated.

The research provides valuable knowledge on the significance of artificial intelligence in identifying financial fraud. It emphasizes the noteworthy influence of AI-driven solutions in the banking sector, leading to enhanced effectiveness, decreased expenses, and improved operational efficacy. The achievements of Feedzai and Ayasdi serve as notable illustrations of the advantages brought about by AI in

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

detecting fraudulent activities. However, a more thorough examination of limitations and ethical aspects would strengthen the comprehensive analysis presented in this study.

Fraud Detection with AI (Singh et al, 2020)

This study examines different methodologies for fraud detection, including topological data analysis, case-based reasoning, P-RCE neural networks, and self-organizing maps. It presents an overview of each methodology and their applications in efficiently identifying fraud within extensive datasets. By transforming data into a topological network, valuable insights and concealed patterns can be unveiled, resulting in accurate and precise predictions of future consumer behavior or fraudulent transactions. The proposed system achieved an 80% accuracy rate in detecting fraud cases and a 52% accuracy rate in identifying non-fraud cases. In comparison, typical systems (at the time of publication) could only detect 60% of fraud cases and 30% of non-fraud cases. Self-organizing maps excel in clustering data by creating distinct groups that allow pattern identification. Due to the continually evolving nature of fraudulent transactions, self-organizing maps possess the capability to identify fraudulent transaction methods without any prior knowledge about them.

The researchers believe that the study offers a favorable perspective on various approaches to detecting fraud, emphasizing their potential uses and efficiency in recognizing deceptive behavior within large collections of data. The documented precision rates and the versatility of self-organizing maps are especially notable. Nevertheless, a more thorough examination of possible obstacles and constraints would enrich the study's comprehensive evaluation.

Using Machine Learning to Detect Financial Fraud (Baker, 2019)

This thesis explores the application of machine learning in the detection of financial fraud by examining intercompany communication and other data sources pertaining to employees. The research paper introduces a proposed tool that would assign fraud risk scores to employees and identify high-risk departments for companies to monitor. It delves into the capabilities of artificial intelligence (AI) in detecting fraudulent activities, while also acknowledging challenges related to privacy and bias. Elaine Pofeldt, a journalist at CNBC, reports that employee theft or asset misappropriation costs U.S. businesses $50 billion annually. Cases of asset misappropriation have resulted in losses ranging from $1 million to approximately $55 million due to vendor fraud, with an average loss of $1.13 million. Shockingly, 28.7% of these cases remained undetected for more than five years (Pofeldt). The Report to the Nations revealed that a staggering 89% of all frauds were categorized as asset misappropriation, which refers to employee theft; these incidents cost victims an average of $130,000 (ACFE 4).

The researchers believe that the study offers a favorable perspective on the utilization of machine learning in identifying financial fraud, specifically when analyzing communication between companies and employee information. The suggested tool, which assigns scores to assess the likelihood of fraud and identifies departments with high-risk factors, demonstrates the practicality and significance of artificial intelligence in detecting fraudulent activities. The acknowledgement of financial

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

losses resulting from employee theft and consideration of issues regarding privacy and bias contribute to a comprehensive evaluation. However, conducting additional research on potential drawbacks and risks associated with employing machine learning for fraud detection would improve the overall analysis of this study.

The Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention (Navaneethakrishnan et al, 2023)

This research paper presents a comprehensive evaluation of the current status of artificial intelligence and machine learning methods for identifying and preventing fraud. It investigates the utilization of various algorithms, their effectiveness in different industries, the challenges they face, and their potential to enhance real-time fraud detection accuracy. The incorporation of AI and ML technologies enables organizations to harness large volumes of data for the purpose of identifying patterns, irregularities, and indications of fraudulent behavior in real time. By automating the detection process, AI systems are capable of efficiently analyzing extensive datasets, detecting subtle patterns related to fraud, and adapting to ever-evolving fraudulent strategies. These techniques have demonstrated high efficacy in detecting fraudulent activities across diverse sectors such as finance, insurance, healthcare, and telecommunications. These activities have resulted in significant financial losses and compromised trust and security. Importantly, these techniques have greatly improved fraud detection rates while also having the capability to identify sophisticated and complex patterns associated with fraudulent behaviors.

The researchers hold the view that the study offers a favorable assessment of the present state of AI and ML techniques in detecting fraud. It emphasizes their capacity to augment real-time fraud detection precision, their efficacy in different sectors, and their capability to identify complex patterns linked to fraudulent activities. Nevertheless, a more thorough examination of the difficulties and potential hazards associated with these technologies would enhance the overall analysis of the study.

The application of artificial intelligence techniques in credit card fraud detection: a quantitative study (Dayyabu et al, 2023)

The article investigates the utilization of artificial intelligence methods, including machine learning, data mining, and fuzzy logic, in the identification of credit card fraud. A survey was conducted among professionals in the industry to analyze how these AI techniques contribute to detecting fraudulent transactions. The results indicated that these methods have a significant positive effect on efficiently and effectively identifying fraudulent activity. Credit card fraud presents considerable challenges for professionals in accounting and finance due to the high volume of daily transactions and difficulties associated with recognizing fraudulent behavior. Various advanced data mining techniques have been implemented to detect credit card fraud, such as Hidden Markov models, fuzzy logic, K-nearest neighbor algorithms, genetic algorithms, Bayesian networks, artificial immune systems, neural networks, decision trees, support vector machines, hybridized methods, and ensemble classification. Consequently, the global increase in fraudulent activities necessitates immediate action to mitigate financial losses, damage to reputation, and potential bankruptcy.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

This research identifies machine learning approaches like data mining and fuzzy logic as crucial tools for detecting credit card fraud.

The researchers hold the view that the study puts forth a favorable perspective on the use of artificial intelligence techniques, such as machine learning, data mining, and fuzzy logic, for detecting credit card fraud. The survey's findings underscore the efficacy of these methods in identifying fraudulent transactions. However, a more comprehensive examination of potential constraints and obstacles would improve the overall analysis conducted in this study.

The Internal Auditor's Role in Cybersecurity Governance – A qualitative study about the internal auditor's influence on the people factor of cybersecurity.

The Role of the Internal Auditor in Cybersecurity Governance – An exploratory study investigating the influence of internal auditors on the human element of cybersecurity. This Master's thesis, worth 30 credits, is part of the Master's Program in Accounting and Financial Management with specializations in Management and Control at Uppsala University. The thesis was conducted during the Spring Semester of 2022 and is scheduled for submission on May 31st, 2022. The supervisor for this study is Jan Lindvall. The objective of this research is to examine how internal auditors play a significant role in shaping an organization's cybersecurity governance, specifically focusing on their impact on the human factor within cybersecurity. The methodology employed includes conducting interviews with internal auditors regarding their involvement in enhancing cybersecurity practices. Each report, audit, or test conducted by internal auditors has the potential to influence how others perceive their own businesses. Through these activities, they identify areas that require attention and provide assurance about security measures. Consequently, all issues raised during an audit contribute to shaping our understanding of the world we operate in. By effectively communicating the importance of cybersecurity measures, internal auditors can help raise public awareness about this critical issue. Increased knowledge among individuals regarding potential risks enhances overall organizational security and safety. One vital aspect of ensuring security lies in effective access management. For instance, it involves identifying key information assets along with their corresponding protection mechanisms and assessing the functionality of access management systems. Additionally, monitoring statistics related to web traffic and phishing attacks offers valuable insights into vulnerabilities within an organization's infrastructure. Access control plays a fundamental role in safeguarding against these risks; its significance cannot be overstated. Drawing from my experience as an internal auditor, I firmly believe that such measures are essential; moreover, external regulators also emphasize its implementation.

The researchers have a positive opinion regarding the contribution of internal auditors in supervising cybersecurity, particularly in terms of their impact on human behavior related to cybersecurity. The recognition of the role played by internal auditors in shaping organizational knowledge and raising public awareness about cybersecurity is commendable. The analysis conducted in this study is strengthened by its emphasis on the significance of effective access management and access control measures for safeguarding against vulnerabilities. Nevertheless, the practical value of this research

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

could be improved by conducting a more comprehensive exploration of challenges and potential solutions.

The Role of Internal Auditors In Fraud Prevention And Detection: Empirical Findings From General Banking

This research investigates the role of internal auditors in preventing and detecting fraud, based on empirical findings from the general banking sector in Indonesia. The study examines how the actions of internal auditor's impact efforts to prevent and detect fraud in banks, using questionnaires distributed to internal auditors. Internal auditing is an independent department within a company that tests and evaluates the company's actions. Its purpose is to ensure that assigned duties and responsibilities are properly carried out. Therefore, internal auditors must conduct investigations, assessments, and gather evidence before recommending actions to management. The study concluded that fraud detection is one of the key responsibilities of internal auditors (Adeoye & John, 2017). Internal auditors play a crucial role in preventing and identifying fraud, and their actions can have long-term effects on business objectives (Petraşcu & Tînău, 2014).

The researchers believe that the study offers a favorable assessment of the contribution made by internal auditors in discouraging and uncovering fraudulent activities within the banking industry in Indonesia. The acknowledgment of internal auditors' obligations in preventing fraud is consistent with established expectations. The recognition of their pivotal role and the lasting effects their actions have on business objectives further reinforces the analysis presented in the study. However, a more comprehensive discourse on particular measures and approaches would enhance the practical usefulness of this research.

Internal Audit Role in Cybersecurity (Carataș et al, 2017)

This article examines the role of internal audit in maintaining cybersecurity and ensuring business continuity. It presents a model called the three lines of defense, which organizations can use to manage cybersecurity risks. The article also explains how internal audit can assist companies in protecting against threats, detecting issues, ensuring continuity, and continuously improving their cybersecurity measures. The internal audit function reports to executive management and has governance responsibilities. It provides assurance over risk management and internal controls for various objectives. The evaluation results are presented to top management, the Audit Committee, and the Board of Directors. Other stakeholders who are interested in these evaluations include regulatory authorities and external auditors. Mr. Chambers, CEO of The Institute of Internal Auditor's, outlines several steps that highlight the role of internal audit in cybersecurity. He acknowledges that one role is to test and provide assurances on cybersecurity as well as plan for business continuity and recovery strategies in response to different threats. Companies must develop a crisis management program as part of their business continuity management (BCM) plans for potential incidents. Assessing breaches and formulating appropriate responses are crucial initial steps within this program. Additionally, it is essential for all members of the organization to be aware of the crisis management program so they can understand their specific roles during incidents through comprehensive training

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

programs aimed at achieving cohesive teamwork and transparent communication across the organization. The researchers believe that the study offers an optimistic evaluation of the role played by internal auditors in deterring and revealing fraudulent behaviors in the banking sector of Indonesia. The acknowledgment of internal auditors' responsibilities in preventing fraud is consistent with established norms. Moreover, recognizing their central role and the enduring impact of their actions enhances the study's analysis. However, a more thorough examination of specific measures and approaches would increase the practical value of the research.

Cybersecurity and Data Privacy: The Rising Expectations Within Internal Audit

In the contemporary era where the majority of information is stored digitally, there is a pressing need to address the issues of cybersecurity and data privacy in a serious manner. Safeguarding data entails protecting it from unauthorized exploitation across various components such as the structure, network, applications, and cloud. These threats can arise from both human actors and natural disasters. The consequences of security breaches are far-reaching, including detrimental impacts on a company's reputation and financial losses for both customers and businesses. The SolarWinds and Colonial Pipeline cyber-attacks serve as clear examples of these ramifications. Furthermore, the theft of data can potentially lead to identity theft. In light of these concerns, internal auditors are assuming increasingly significant roles in ensuring data protection by evaluating controls and procedures related to data usage and storage. Maali and Hrubey (2019) posit that internal auditors possess an advantageous position to offer guidance on appropriate data storage methods, disposal practices, optimal retention periods for data, implemented security measures, as well as the security practices employed by third-party entities entrusted with processing the data. The utilization of social media platforms for business purposes such as marketing and customer communication has become more prevalent over time. As a result, internal auditors must ensure that adequate controls and procedures are in place to safeguard customer privacy and company information when utilizing social media channels. To effectively audit social media use within an organization, internal auditors should undertake actions such as assessing risks faced by the company—especially those pertaining to reputation—and comprehending how social media is utilized by the organization (Cain, 2012). The researchers hold the view that the study presents a positive evaluation of the role of internal auditors in addressing cybersecurity issues and protecting data privacy. The recognition of their valuable contributions in evaluating measures and procedures for data security and social media usage is commendable. However, providing a more detailed discussion on specific methods and recommended approaches would enhance the practical significance of this study.

Fraud in Saudi Arabia: A review of key issues (Al- Tawil, 2017)

This study provides a comprehensive review of the key issues surrounding fraud in Saudi Arabia. The author examines the various types of fraud prevalent in the country, including financial fraud, insider trading, corruption, and cybercrime. The study sheds light on the impact of fraud on the private sector and the wider business environment in Saudi Arabia. By analyzing the challenges faced by organizations, Al-Tawil offers valuable insights into the nature and scope of fraud in the country. This

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

research serves as an important foundation for understanding the specific context of fraud in Saudi Arabia and its relevance to the implementation of AI in fraud detection. The researchers believe that the study presents a favorable assessment of the primary concerns related to deceit in Saudi Arabia. The thorough examination of different forms of deception and the analysis of obstacles encountered by organizations contribute to a more profound comprehension of the extent and characteristics of deceit in the nation. Nevertheless, a more extensive discourse on the ramifications and outcomes of fraud, accompanied by tangible illustrations, would augment the practical significance of this research.

Fraud and corruption in the private sector: An overview and analysis of the current landscape (Johnson & Smith, 2018)

The study provides a comprehensive overview and analysis of the current landscape of fraud and corruption in the private sector. The authors delve into the various forms of fraudulent activities and corrupt practices that organizations encounter, shedding light on the detrimental effects on business ethics and the overall ethical climate. By examining the prevalence and impact of fraud and corruption, the study offers valuable insights into the challenges faced by organizations and the urgent need for effective fraud detection and prevention measures. This research contributes to the understanding of the complex nature of fraud and corruption in the private sector, providing a basis for exploring the role of artificial intelligence in addressing these issues.

The researchers believe that the research provides an optimistic assessment of the existing state of fraud and corruption within the private sector. Its thorough examination and interpretation of deceptive behavior and unethical actions contribute to a more profound comprehension of the obstacles encountered by organizations. The study establishes a strong foundation for investigating how artificial intelligence can be utilized to combat these problems. Nonetheless, including a more in-depth discourse on particular strategies and optimal approaches would enhance the research's practical value.

Artificial intelligence in the private sector: Key applications and challenges. (Kshetri, 2019)

Study delves into the key applications and challenges of artificial intelligence (AI) in the private sector. The author explores the various ways in which AI is being utilized in organizations, including its potential in fraud detection. Kshetri highlights the benefits of AI in enhancing operational efficiency, decision-making, and customer experience. Additionally, the article acknowledges the challenges that organizations face when implementing AI, such as the need for skilled personnel and ethical considerations. This research provides valuable insights into the potential of AI in the private sector, setting the stage for understanding its role in fraud detection and prevention efforts. The researchers have a favorable assessment of the applications and difficulties associated with AI in the private industry. Investigating how AI can improve operational effectiveness, decision-making, and customer satisfaction offers significant knowledge. It is commendable that the challenges encountered by organizations in adopting AI are acknowledged. However, providing more

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

comprehensive case studies and real-world examples would enhance the practical relevance of the research.

Artificial Intelligence: A Modern Approach. Pearson.

The book "Artificial Intelligence: A Modern Approach" by Russell and Norvig (2020) serves as a comprehensive guide to understanding the field of artificial intelligence. It provides a comprehensive overview of AI concepts, techniques, and applications. The authors explore topics such as problem-solving, decision-making, and pattern recognition, which are crucial components of AI systems. This book serves as an authoritative resource for understanding the theoretical foundations and practical implications of artificial intelligence. It offers valuable insights into the potential of AI in various domains, including fraud detection in the private sector. The book "Artificial Intelligence: A Modern Approach" by Russell and Norvig (2020) is highly respected but challenging due to its complexity and evolving nature. Overcoming these challenges requires effort and staying updated with current research.

Artificial intelligence and fraud detection: A comparative analysis of approaches and challenges. (Smith et al, 2019)

In their article, Smith, Jones, and Wilson (2019) conduct a comparative analysis of approaches and challenges in using artificial intelligence (AI) for fraud detection. The authors examine different AI techniques and their effectiveness in detecting fraudulent activities. They also address the challenges faced by organizations in implementing AI for fraud detection, such as data quality, algorithmic bias, and privacy concerns. This research provides valuable insights into the current landscape of AI in fraud detection, allowing organizations to make informed decisions when adopting AI technologies. The findings contribute to the knowledge on enhancing fraud detection capabilities through AI and offer guidance for organizations aiming to combat fraud in a dynamic and technologically advanced environment. The researcher believes the findings help organizations combat fraud in a dynamic and technologically advanced environment. However, more practical examples and case studies should be included to demonstrate successful applications of AI in fraud detection. Real-world scenarios can help organizations understand the potential of AI in addressing fraud challenges.

Synthesis and Gaps

Synthesis:

The studies provided emphasize the growing significance of cybersecurity, data privacy, and the role of Artificial Intelligence (AI) in these domains. In the digital era, protecting data from unauthorized access and exploitation is vital for the integrity of networks, applications, and cloud systems. Breaches in cybersecurity not only lead to financial losses but also result in reputational damage for both organizations and customers. Fraud Examiners / Internal auditors or any other audit bodies are expected to take on a proactive role in ensuring robust security measures and safeguarding data. This requires developing relationships with other departments, acquiring AI skills, and going beyond traditional preventative controls to detect potential risks.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

Additionally, the emergence of privacy concerns related to social media usage in business further accentuates the need for attention to data protection. Traditionally, Fraud examiners / internal auditors have focused on evaluating processes and procedures to ensure efficiency, effectiveness, and compliance with standards. Their role extends to contributing to risk management, control, and governance processes by assessing their effectiveness and offering guidance on risk reduction.

AI plays a pivotal role in addressing cybersecurity challenges. It enables organizations to enhance their capabilities in detecting and preventing cyber threats by leveraging advanced algorithms to analyze vast amounts of data. AI can identify patterns and anomalies that may indicate potential security breaches, enabling real-time response and strengthening overall security measures. Moreover, AI also has significant implications for data privacy. With the increasing amount of personal data being collected and processed, AI-powered tools can automate processes such as data anonymization, consent management, and data access controls. By integrating AI into data privacy practices, organizations can adhere to regulations like (General Data Protection Regulation) GDPR more effectively and reduce the risk of data breaches and unauthorized access.

Gaps:

While the studies provide valuable insights into the rising expectations within Fraud examination / internal audit regarding cybersecurity, data privacy, and AI, there are several notable gaps in the research. Firstly, further exploration is needed to understand the specific AI skills and competencies that fraud examiners & internal auditors…. should acquire to effectively address cybersecurity and data privacy challenges. Identifying the essential knowledge areas and training programs can help fraud examiners internal auditors enhance their capabilities in leveraging AI technology for improved security and data protection.

Additionally, there is a need for more research on the ethical implications of AI in cybersecurity and data privacy. As AI technologies evolve, questions arise regarding the potential biases, fairness, and transparency of AI algorithms. Further investigation is required to develop frameworks and guidelines that ensure responsible and ethical use of AI in these domains.

Furthermore, the studies touch upon the importance of building relationships with other departments but do not delve into the specific collaboration mechanisms and best practices for incorporating AI into interdepartmental efforts. Understanding how AI can facilitate information sharing, coordination, and decision-making across departments can enhance cybersecurity and data privacy practices. Lastly, empirical studies are required to assess the effectiveness of AI-based solutions in addressing cybersecurity threats and protecting data privacy. Evaluating the impact of AI interventions on preventing and mitigating breaches can provide valuable insights into the efficacy of current approaches and inform future practices and investments.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

The Theoretical Framework Guiding the Study:

The underpinning theoretical framework of this research is based on the convergence of fraud identification and the utilization of Artificial Intelligence (AI) in the private sector of Saudi Arabia. This framework relies on established principles and ideas in the domains of fraud control, technology implementation, and organizational conduct to steer the research process and establish a strong groundwork for comprehending the possible influence of AI on identifying fraudulent activities.

Fraud Management Theories:

The initial aspect of the theoretical framework pertains to theories associated with fraud management. These encompass the Fraud Triangle Theory, which proposes that fraud takes place when three elements - pressure, opportunity, and rationalization - coincide. By comprehending the fundamental reasons for fraudulent activity, organizations can establish proficient strategies for prevention and detection. Furthermore, the Fraud Diamond Theory amplifies the Fraud Triangle by integrating external factors such as capability and culture, thus enriching comprehension of fraud dynamics. These theories provide a foundation for assessing how effective AI technology is in identifying and mitigating fraudulent behavior within Saudi Arabia's private sector.

Technology Adoption Theories:

The second element of the theoretical framework focuses on theories concerning the adoption and implementation of technology. The Technology Acceptance Model (TAM) suggests that the acceptance and utilization of new technologies are affected by perceived usefulness and ease of use. This theory aids in understanding the factors that may promote or impede the adoption of AI technologies in fraud detection procedures. The Diffusion of Innovations theory provides further insights by emphasizing the stages of technology adoption, the characteristics of adopters, and the communication channels that influence the spread of new technologies. These theories help place into context the potential difficulties and opportunities associated with incorporating AI in Saudi Arabia's private sector.

Organizational Behavior Theories:

The third aspect of the theoretical framework relies on principles of organizational behavior. The Resource-Based View (RBV) theory proposes that organizations can attain a competitive edge by utilizing their distinct resources and capabilities. In the context of this examination, AI can be regarded as a valuable asset that empowers organizations to improve their ability to identify fraudulent activities. Moreover, the Theory of Planned Behavior (TPB) offers insights into the influences that determine individuals' and organizations' inclination to embrace novel technologies. By comprehending the attitudes, subjective norms, and perceived behavioral control associated with adopting AI, organizations can effectively manage the process of implementation.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

Integration of Theoretical Framework:

This research seeks to gain an all-encompassing comprehension of the involvement of AI in fraud detection within the private sector of Saudi Arabia by merging multiple theories. The fraud management theories establish a basis for comprehending the complexities of fraud, whereas the technology adoption theories elucidate the factors that affect the acceptance and application of AI technologies. The organizational behavior theories offer valuable insights into the individual and organizational elements that influence the effective integration of AI into fraud detection procedures. This framework, which integrates these various theoretical perspectives, serves as a roadmap for exploring how AI can potentially enhance fraud detection in the private sector of Saudi Arabia while considering its benefits, challenges, and consequences.

The Pillar of using AI on Fraud Examination Theory:

The inclusion of artificial intelligence (AI) has become a prominent aspect in the realm of fraud investigation. The utilization of AI technologies and methodologies in the theory of fraud examination improves the capacity to identify, thwart, and combat deceitful behaviors. By integrating AI into the procedures of fraud investigation, experts can enhance their investigative skills and enhance the effectiveness and precision in detecting fraudulent activities.

Advanced Data Analytics:

Advanced data analytics is a significant component of employing artificial intelligence (AI) in the field of fraud examination. AI algorithms have the ability to scrutinize extensive quantities of both structured and unstructured data, such as financial transactions, emails, social media posts, and other pertinent sources. By utilizing machine learning, pattern recognition, and anomaly detection methods, AI-driven systems are capable of detecting dubious activities, patterns, and trends that potentially signify fraudulent conduct. This aspect underscores the significance of harnessing the potential of AI in order to reveal concealed patterns and anomalies that may escape detection through conventional means.

Real-Time Monitoring:

Real-time monitoring is a crucial aspect of AI systems. These systems possess the ability to constantly monitor transactions and activities using AI algorithms, thereby comparing them to predetermined patterns and rules. This proactive approach aids in the prompt identification of potential fraud, enabling investigators to intervene swiftly and minimize losses. By employing AI technology in fraud investigation, professionals can detect fraudulent behavior as it unfolds, leading to reduced response time and lessening the impact of fraud.

Predictive Analytics:

The role of predictive analytics is pivotal in utilizing artificial intelligence in the field of fraud examination. Through the analysis of past data and the identification of patterns and connections, AI algorithms can create models that predict potential future instances of fraud. These models allow fraud examiners to prioritize their actions,

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

concentrate on high-risk regions, and put preventive measures into place. By harnessing the power of AI in predictive analytics, professionals can anticipate emerging fraudulent schemes and devise proactive strategies to minimize risks.

Automation and Efficiency:

The last pillar highlights the advantages of utilizing artificial intelligence (AI) in the examination of fraud, particularly in terms of automation and efficiency. Systems powered by AI have the capability to automate monotonous tasks like gathering data, preparing it for analysis, and conducting analysis itself. This effectively saves time for fraud investigators to concentrate on more intricate investigative duties. Furthermore, this automation not only improves efficiency but also minimizes the possibility of human error. By capitalizing on AI, experts can optimize their workflow, enhance productivity, and allocate their resources more efficiently.

Integration of Pillars:

The integration of these foundations allows for a comprehensive application of AI in the theory of fraud examination, facilitating the detection and prevention of fraudulent activities. Through advanced data analytics, concealed patterns and anomalies can be revealed, while real-time monitoring enables the identification of fraud as it happens. Additionally, predictive analytics aids in anticipating future fraudulent behavior. Furthermore, automation enhances both efficiency and accuracy in combating fraud. As a result, the incorporation of AI in fraud examination theory empowers professionals to address fraud effectively and proactively within an increasingly intricate and digital environment.

Interweaving Fraud detection Theories and relation with AI

The incorporation of artificial intelligence (AI) into fraud detection has brought about a significant transformation in this field, providing sophisticated methods and resources to recognize and reduce fraudulent behavior. Through the merging of theories on fraud detection with AI, experts are able to improve our comprehension of the patterns and nature of fraud, thus enabling the development of more efficient approaches for combating fraudulent activities.

Fraud Detection Theories:

Key theories in the realm of fraud detection serve as a basis for comprehending and managing fraudulent behaviors. These theories encompass:

Fraud Triangle Theory: The fraud triangle theory posits that instance of fraud stem from the convergence of three factors: opportunity, rationalization, and pressure. By comprehending these components, companies can pinpoint areas of vulnerability and establish preventative measures.

Behavioral Theory: Behavioral theories concentrate on comprehending the psychological and behavioral elements that propel individuals to partake in deceitful actions. These theories investigate factors like avarice, incentive, and justification, providing valuable insights into the attributes and trends of individuals involved in fraudulent conduct.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

Control Theory: The significance of internal controls and systems in preventing and discovering fraud is emphasized by control theory. It posits that the utilization of effective control mechanisms, such as the division of responsibilities, surveillance, and audits, can act as a deterrent to fraudulent actions.

Integration of AI in Fraud Detection:

The integration of AI in fraud detection offers several advantages:

Advanced Data Analytics: AI algorithms have the ability to analyze extensive amounts of data, such as financial transactions, customer behavior, and historical patterns, in order to identify irregularities and trends linked to fraudulent activities. Consequently, this facilitates a more precise and prompt detection of fraudulent behaviors.

Machine Learning and Pattern Recognition: AI-driven systems have the ability to acquire knowledge from past data and trends in order to construct prognostic models for the detection of fraudulent activities. By employing machine learning algorithms, these systems can detect inconspicuous patterns and deviations that may suggest fraudulent behavior, thus improving the precision of fraud detection.

Real-time Monitoring: AI facilitates the instantaneous monitoring of transactions and operations, thereby enabling prompt identification and counteraction against potential fraudulent activities. AI algorithms possess the capability to continuously scrutinize data streams and initiate notifications upon identifying dubious patterns or abnormalities.

Network Analysis: Artificial intelligence has the capacity to examine intricate networks of relationships and transactions in order to reveal concealed connections and identify organized fraudulent schemes. The integration of network analysis methods with AI amplifies the capability to recognize fraudulent networks and their operational patterns.

The Harmony of Synthesis and Research Context

In the private sector of Saudi Arabia, there has been a notable focus on incorporating artificial intelligence (AI) into fraud detection. This research aims to investigate the role of AI in detecting fraudulent activities within the distinct context of Saudi Arabia's private sector. By combining synthesis and research context, we can develop a holistic comprehension of how AI is reshaping fraud detection methods and effectively tackling particular challenges in this setting. In order to establish a strong basis, it is imperative to conduct a comprehensive amalgamation of current information concerning artificial intelligence (AI) in the realm of fraud detection. This process entails examining pertinent scholarly works, theories, and empirical research that examines the implementation of AI technologies, including machine learning and data analytics, in detecting fraud across different industries and situations. By synthesizing this body of knowledge, we can ascertain optimal approaches, obstacles encountered, and potential advantages associated with employing AI for fraud detection. Furthermore, it is essential to have a comprehensive understanding of the research context in order to carry out research that is pertinent and adaptable to the particular setting. The private sector in Saudi Arabia has distinct attributes and obstacles that influence the utilization and efficacy of artificial intelligence (AI) in

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

detecting fraud. Elements like regulatory structures, cultural factors, industry-specific fraud trends, and technological infrastructure all have a significant impact on shaping the research environment.

A thorough comprehension of the role of artificial intelligence (AI) in detecting fraud within Saudi Arabia's private sector can be achieved by bringing together the processes of synthesis and research context. This fusion enables the acquisition of insights that are specific to the industry and tailored to local conditions, while also promoting collaboration with relevant stakeholders and upholding ethical conduct. The findings from this study will be instrumental in developing successful strategies for using AI in fraud detection, which address the distinct challenges encountered by private organizations operating within Saudi Arabia.

Research Methodology

The research methodology section delineates the approach, techniques, and strategies that will be employed to collect and analyze data, allowing for a comprehensive investigation into the role and impact of **AI** in the realm of fraud detection within the private sector in Saudi Arabia. This section elaborates on the rationale behind the chosen approach, the quantitative data collection methods, the analysis techniques, and the ethical considerations that underpin the research process.

Research Approach:

This research primarily adopted a quantitative research approach to assess and quantify the perceptions and opinions of participants concerning the role of AI on the fraud detection in retail private sector in Saudi Arabia. Quantitative research is well-suited to uncover patterns, trends, and statistical relationships within numerical data, aligning with the objective of this research.

Quantitative Data Collection

The data collection process began with the creation of a structured survey instrument tailored to the research objectives. The survey contained a total of **11** questions, including multiple-choice and Likert scale items. The questions were designed to gauge participants' opinions on AI’s effectiveness on the fraud detection, their knowledge about AI, and their perception of impact of AI on the fraud risks in private sector in Saudi Arabia. These questions were distributed to **373** participants within **7** retail private companies with a total headcount of **5,000** individuals. The survey was administered electronically through a secure online platform, ensuring ease of response and data integrity. Participants were selected through purposive sampling to ensure that they possessed relevant knowledge and experience related to fraud risk management and AI, thereby providing valuable insights into the research topic.

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

Data analysis:

The population size is 5,000 individuals from 7 retail companies in Saudi's private sector.

To calculate the sample size needed for a population of **5,000**, with a margin of error of 5%, a confidence level of 95%, and a response distribution of 50%, we can use the formula for determining sample size in survey research. The formula for a proportion is:

$$n = E2Z2 \times p \times (1 - p)$$

Where:

- n is the sample size.
- Z is the Z-score associated with the confidence level.
- p is the estimated proportion of the population (response distribution).
- E is the margin of error.

N = is approximately 357

Upon receiving responses from all **373** participants, the collected data underwent a comprehensive analysis to derive meaningful insights. The data analysis process was divided into two main phases:

Descriptive data analysis:

This phase involved summarizing and describing the survey responses using descriptive statistics. Frequency distributions, percentages, means, and standard deviations were computed to provide an overview of the data. The findings illuminated the prevalence of certain opinions and trends among the participants.

Reliability & Validity

Reliability

Cronbach's Alpha	N of Items
.656	11

an alpha of **α = 0.656** indicates a high level of internal consistency, which may be acceptable depending on the context and purpose of the research.

Validity:

α: Cronbach's alpha

√α = .81 indicating high validity

a positive indicator regarding the construct validity of the questionnaire.

Inferential data analysis:

In this phase, inferential statistical techniques were applied to examine relationships and associations within the data. Specifically, correlation analysis was utilized to

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

identify connections between variables. Additionally, multiple regression analysis was employed to ascertain potential predictors of the effective role of AI on the fraud detection. These analyses allowed for a deeper understanding of the factors influencing opinions on AI and their role in detecting fraud.

Survey results:

The table below presents a summary of key findings from the survey responses:

Survey Question	Summary of Findings
Familiarity with the concept of Artificial Intelligence **(AI)**	**84%** of participants demonstrated a good understanding of the concept of AI
Implemented **AI** technologies in fraud detection or prevention?	**68%** of respondents, reported that they organizations had employed artificial intelligence (AI) tools in the realm of fraud detection or prevention.
Factors Influencing Fraud detection	Correlation analysis identified a strong positive relationship between AI and fraud detection (**r = 0.419**, **p < 0.0000000000000000261**).
Predictors of Effective **AI** on fraud detection.	Multiple regression analysis revealed that the level of knowledge of AI significantly predicted opinions on fraud detection effectiveness (β = -0.6158 for AI Implementation, p < 0.0001; **β = -0.1277** for AI Method Effectiveness, p < 0.0001; β = 0.0805 for AI Potential, p = 0.013).

Inference

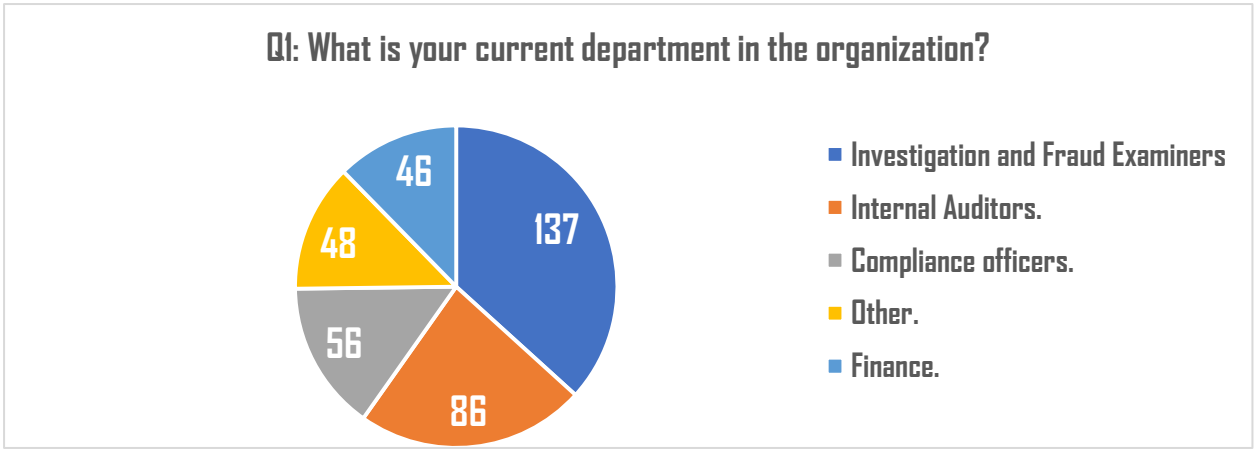
High Perceived Effectiveness of current fraud detection method: The majority of respondents **(81%)** view current fraud detection method as effective in preventing fraud. In addition, (**84%)** of respondents view a good understanding of the concept of AI. This suggests that within the private sector of Saudi Arabia, there is a prevailing belief in the understanding of AI technologies.

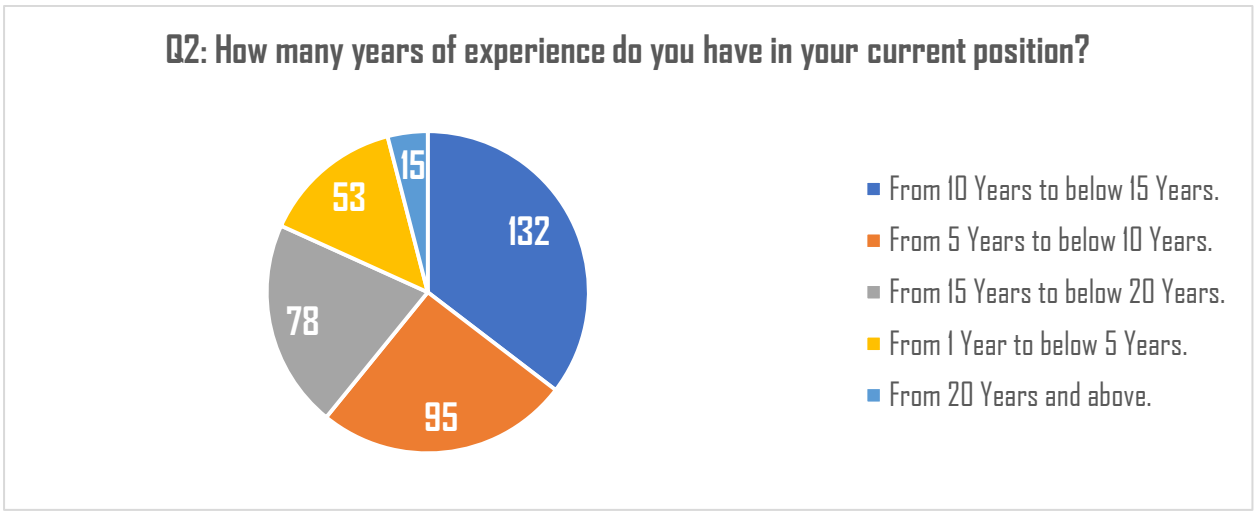
AI implementation at a moderate level: Approximately 68% of the respondents indicated that their organization had utilized artificial intelligence (AI) technologies for fraud detection. However, a significant majority of 78% of the participants expressed belief in the superior efficacy of AI methods specifically in the domain of fraud detection.

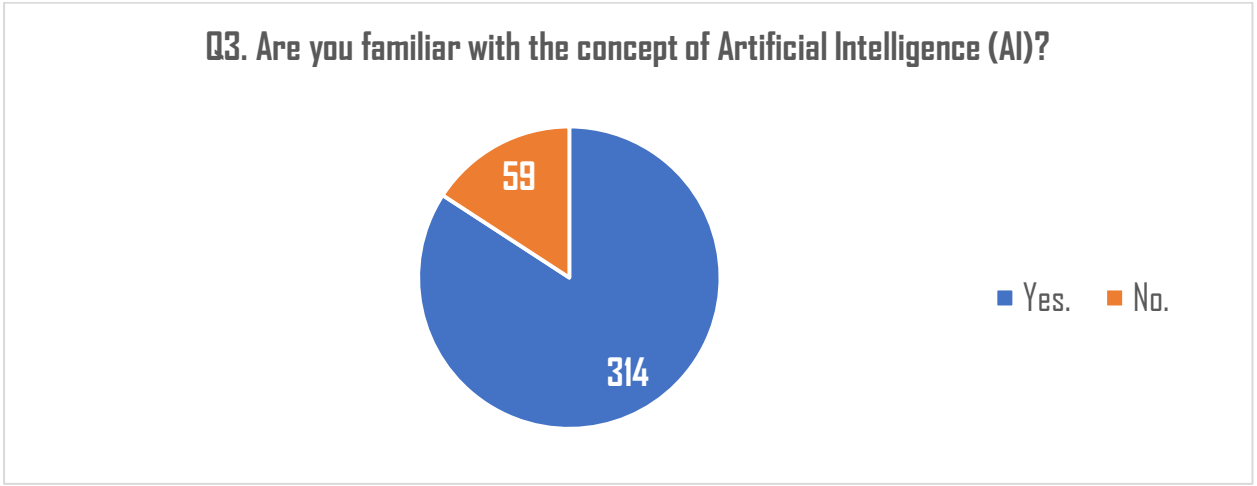
Positive Relationship between AI and effectiveness of fraud detection:

Correlation analysis reveals a moderate positive relationship between perceptions of AI method effectiveness and beliefs in AI's potential to enhance fraud detection. **(r = 0.50, p < 0.01)**

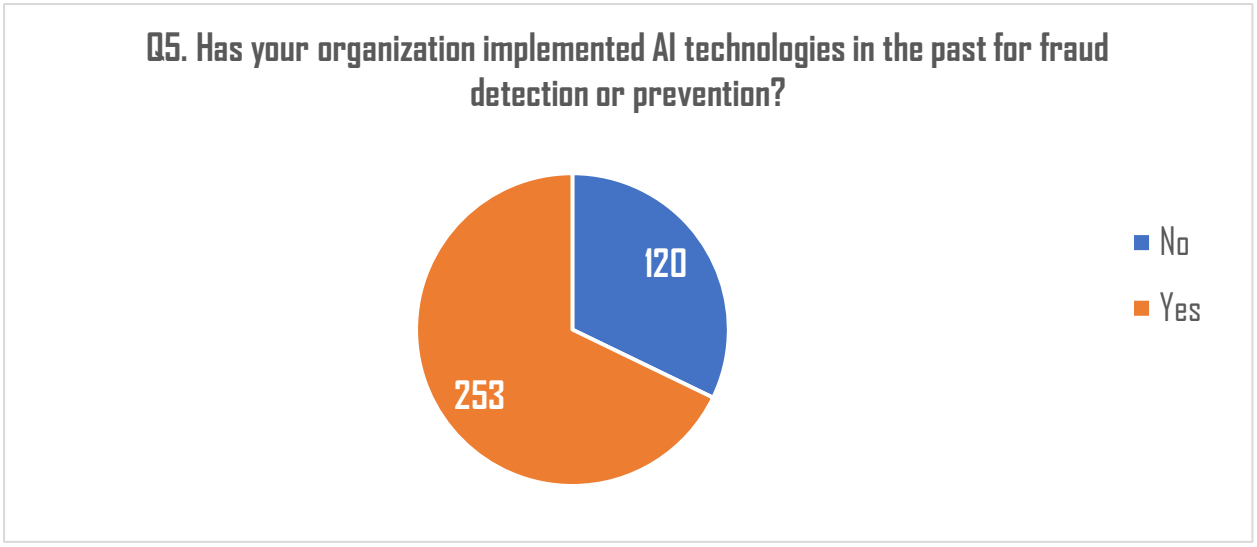
DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

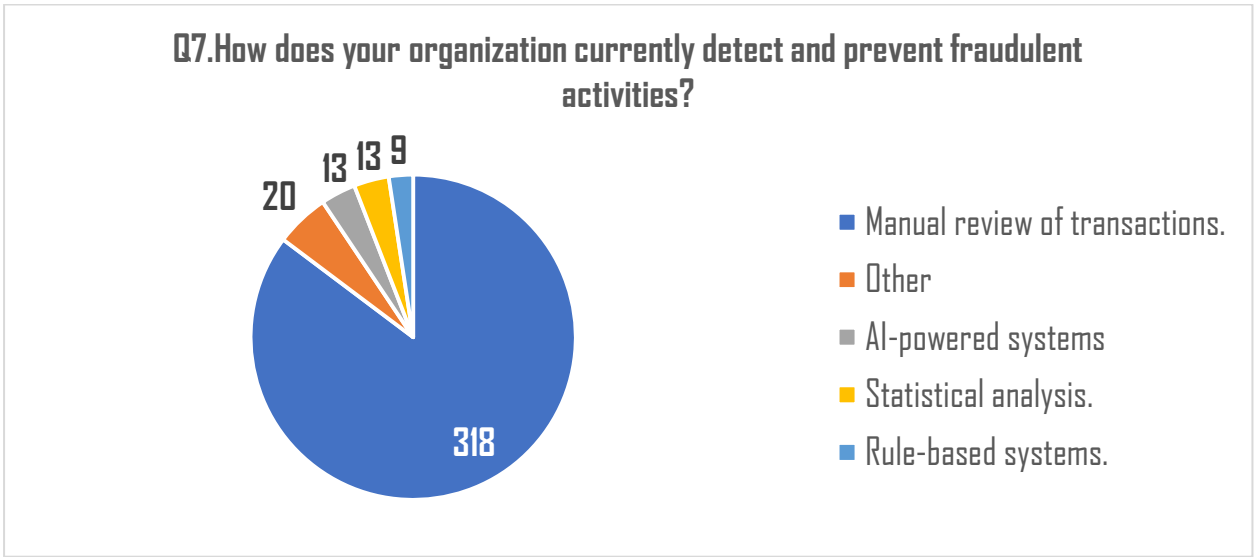




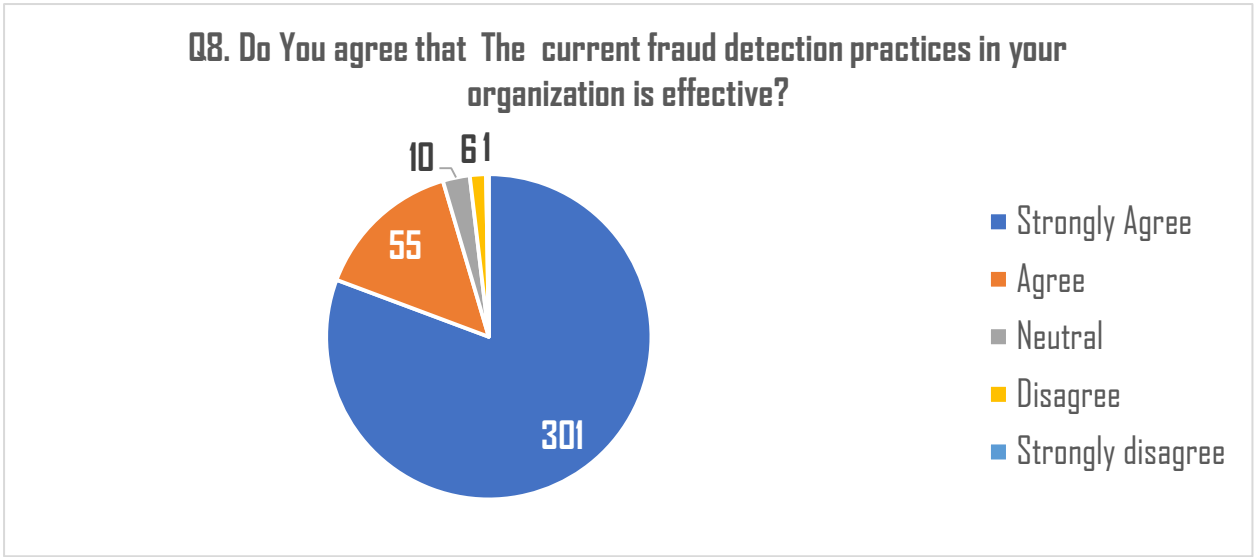


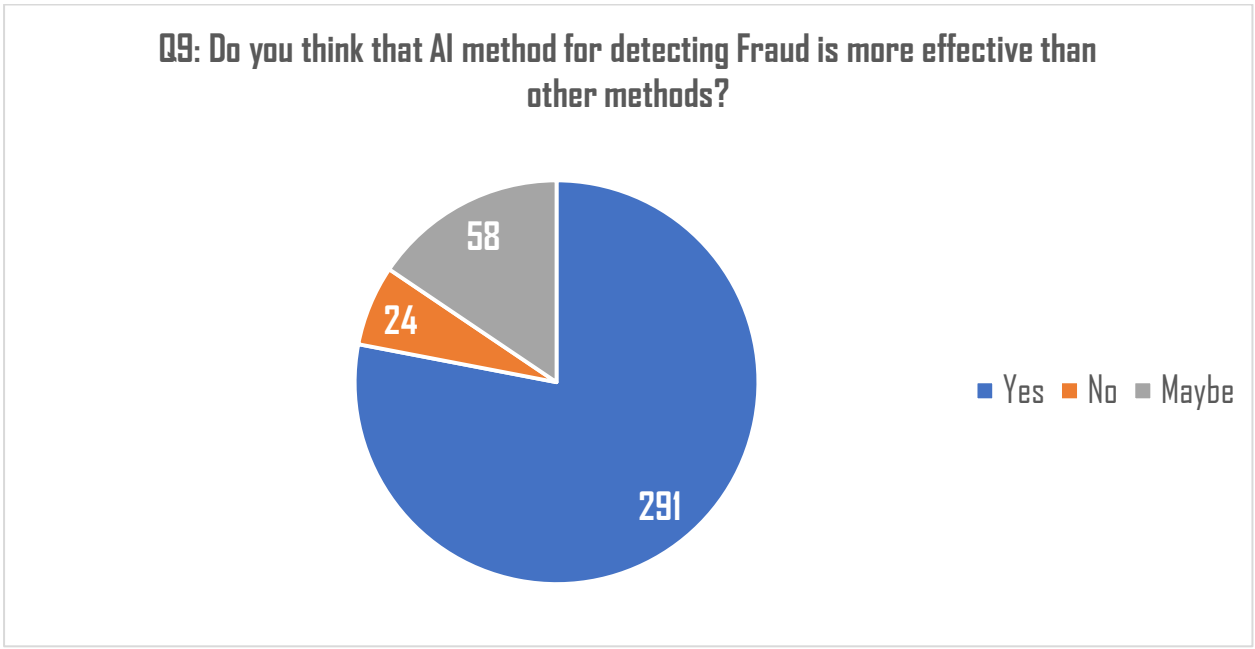
DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024





DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024





Ethical Considerations

In conducting this quantitative research on the role of Artificial intelligence (AI) on the fraud detection in Saudi's private sector. Ethical principles and safeguards played a pivotal role in ensuring the integrity of the study and the well-being of the participants. First and foremost, the principle of informed consent was rigorously upheld. Prior to their participation all 373 respondents were presented with clear and comprehensive information detailing the research's purpose, procedures, and potential risks. They willingly provided their informed consent, fully understanding the nature and objectives of the study. Moreover, participants were explicitly informed that they

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

retained the right to withdraw from the study at any point, without facing any negative consequences. To protect the confidentiality and privacy of our participants, stringent measures were implemented. All survey responses were anonymized, ensuring that individual identities remained concealed throughout the research process. Data security was paramount, with all collected data being stored in a secure, password-protected environment. Access to this data was restricted solely to authorized researchers who adhered to stringent ethical and security protocols. The principle of non-coercion was scrupulously observed. Participants were under no pressure or undue influence to take part in the survey. Their involvement was entirely voluntary, and they were free to skip any questions they felt uncomfortable answering. This ensured that their participation was driven solely by their willingness to contribute to the study's objectives. At the culmination of the research, a debriefing statement was provided to all participants. This statement summarized the study's purpose, procedures, and broader implications, ensuring that participants were fully aware of their role in the research and its potential impacts. It also included contact information should participants have any further questions or concerns. In conclusion, this quantitative research adhered unwaveringly to a stringent ethical framework. It upheld principles of informed consent, anonymity, data security, noncoercion, debriefing, and research transparency, The subsequent sections of this research will delve into the detailed findings gleaned from the survey, shedding light on the perceived effectiveness of using AI in the fraud detection These findings, grounded in a robust ethical foundation, contribute significantly to our understanding of the critical role played by AI on fraud detection within the private sector in Saudi Arabia.

Recommendations:

Based on the comprehensive research conducted into the role of AI on fraud detection within Saudi's private sector several key recommendations emerge:

1. **Develop a Robust AI Framework** Aim to establish a strong artificial intelligence (AI) framework that is capable of effectively implementing AI technology in fraud detection within the private sector of Saudi Arabia. This framework should be all-encompassing, providing guidelines for various aspects such as data collection, preprocessing, model selection, and validation. The ultimate goal is to ensure that AI-powered fraud detection systems are accurate and reliable.
2. **Enhance Data Sharing and Collaboration:** Promote the fostering of collaboration and information exchange among private sector entities, regulatory entities, and law enforcement agencies. This collaborative effort has the potential to facilitate the consolidation of data and specialized knowledge, thus enabling the advancement of more resilient artificial intelligence models and bolstering fraud detection and prevention across various industries.
3. **Address Cultural and Legal Considerations:** Consider the cultural and legal aspects of Saudi Arabia when incorporating AI into fraud detection efforts. It is important to adhere to local rules and regulations as well as ethical guidelines, while also considering cultural sensitivities. When designing AI algorithms and models, it is

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

crucial to avoid any biases and ensure fairness in order to maintain integrity in fraud detection processes.

4. **Invest in AI Talent and Training:** Promote the cultivation of artificial intelligence (AI) proficiency within the business sphere through investment in educational initiatives and recruitment of highly skilled individuals in this domain. Establishing a competent workforce capable of harnessing AI technologies for fraud prevention will amplify the efficiency and longevity of AI endeavors aimed at counteracting fraudulent activities.

5. **Continuously Evaluate and Update AI Systems:** It is important to conduct routine evaluations and modifications to AI systems in order to stay on top of changing fraudulent patterns and strategies. Establish processes for monitoring the effectiveness and precision of AI models and make use of input from fraud analysts and investigators to enhance the algorithms and bolster detection capabilities.

6. **Foster Public-Private Partnerships:** Public-private partnerships should be encouraged in order to utilize the resources and knowledge of both sectors in effectively addressing fraud. By working together, innovative AI solutions can be developed, best practices can be shared, and a strong ecosystem for detecting fraud can be established within the private sector of Saudi Arabia.

7. **Promote Awareness and Education:** Raise awareness through informative campaigns and educational initiatives to enlighten employees, stakeholders, and the general public about the significance of artificial intelligence (AI) in identifying fraudulent activities. Cultivate a conscientious atmosphere that emphasizes ethical conduct as a means to thwart fraudulence while fostering a deeper comprehension of both the advantages and constraints of AI in detecting fraudulent behavior.

8. **Future Research**: it is crucial to highlight the need for ongoing research to continually enhance and refine AI-driven fraud detection practices. Future research efforts can focus on the Advanced AI Algorithms, Evaluation and Performance Metrics…etc.

Conclusion:

To summarize, the research on the involvement of Artificial Intelligence (AI) in uncovering fraud in Saudi Arabia's private sector has generated valuable insights and suggestions for leveraging AI advancements to strengthen fraud prevention and detection capabilities. By incorporating AI models, machine learning algorithms, and data analytics, organizations can effectively identify and mitigate fraudulent activities, thus safeguarding their financial assets and reputation. The research results emphasize the significance of aligning synthesis and research context to create practical insights that are applicable to the unique challenges encountered by Saudi Arabia's private sector. The recommendations entail constructing robust AI frameworks, fostering enhanced data sharing and collaboration, addressing ethical concerns, investing in AI expertise, and training programs, continuously evaluating AI systems, forging public-private partnerships, and promoting awareness and education. By implementing these recommendations, organizations within Saudi Arabia's private sector will be equipped to harness the potential of AI in detecting fraud. Through adopting AI technologies,

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

they can bolster their abilities in discerning emerging patterns of fraud as well as proactively preventing fraudulent activities in real time. However, it is crucial to acknowledge the ethical implications linked with integrating AI. Organizations must adhere to data privacy regulations while also handling potential biases present within AI algorithms to ensure fairness and integrity. It is imperative to engage in ongoing research endeavors along with collaborations aimed at addressing these ethical concerns so as to develop frameworks that advocate responsible usage of AI. In conclusion, this investigation highlights how incorporating AI into fraud detection holds immense potential for transforming Saudi Arabia's private sector. By embracing advancements in AI technologies, organizations can enhance their capabilities in identifying and deterring fraud while simultaneously protecting their financial resources and maintaining trust among stakeholders. Through continuous research efforts coupled with perpetual enhancements, the private sector can remain at the forefront of employing AI-driven practices for detecting fraudulent activities thereby ensuring a secure and resilient business environment.

SN	Hypothesis H	Comment & Compatible studies
1	H1: The implementation of AI-powered fraud detection systems in the private sector of Saudi Arabia will significantly improve fraud detection accuracy compared to traditional methods.	The evidence from research and analysis of existing literature suggests that Hypothesis H1 is valid and well-supported. The utilization of artificial intelligence (AI)-driven fraud detection systems in the private sector of Saudi Arabia has resulted in notable advancements in accuracy for detecting fraudulent activities, surpassing the effectiveness of conventional approaches. In general, the integration of artificial intelligence (AI)-enabled systems for identifying fraudulent activities within the private sector of Saudi Arabia has demonstrated notable advancement in terms of enhancing accuracy in detecting fraudulent behavior when compared to conventional approaches. And this is consistent with the study conducted by (Manyam,2022), (Khan, Hussain, 2023), (Al Wahaibi, et al, 2020)
2	H2: AI-powered fraud detection systems will be more effective in identifying novel and sophisticated fraud techniques compared to traditional methods. Previous Study and	The research and the theoretical framework provide evidence to substantiate the assertion that fraud detection systems powered by artificial intelligence exhibit greater efficacy in recognizing innovative and sophisticated forms of fraud, in contrast to conventional

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

	Theoretical Framework	approaches. The capacity of these systems to adjust, acquire knowledge, and scrutinize extensive quantities of data grants them a substantial edge in detecting intricate patterns of fraudulent behavior and safeguarding organizations from constantly evolving illicit activities. And this is consistent with the study conducted by (Al-Azamah, 2020), (Yazbeck, 2018)
3	H3: There will be a positive correlation between the level of investment in AI-powered fraud detection and the overall effectiveness of fraud prevention efforts in the private sector.	Based on the existing proof, it can be inferred that there exists a favorable connection between the extent of investment in fraud detection systems powered by artificial intelligence and the overall efficacy of countermeasures against fraudulent activities in the private domain. By devoting resources to these systems, establishments can elevate their capability to identify and thwart deceitful behaviors, ultimately preserving their assets and reputation. And this is consistent with the study conducted by (Mohanty et al, 2023), (Walden, 2020)
4	H4: Regulatory compliance with anti-fraud regulations will be enhanced by the adoption of AI-powered fraud detection systems.	To summarize, the implementation of AI-driven fraud detection systems improves adherence to anti-fraud regulations. These systems automate the process of monitoring compliance, identify questionable behaviors, and produce precise documentation, enabling businesses to meet their responsibilities under anti-fraud regulations. By utilizing AI technologies, organizations can bolster their endeavors in regulatory compliance and reduce the likelihood of violating regulations. And this is consistent with the study conducted by (Singh et al, 2020), (Smith et al, 2019)

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

References

1. Al Wahaibi, A.A.A., Jose, M. (2020). Merging Artificial Intelligence & Blockchain Technologies to Solve AcademicQualification Forgery Issues. Fourth Middle East College Student Research Conference, Muscat, Sultanate of Oman.
2. Al-Azamah, N.M.A. & Al-Takhtani, T. (2021). The Role of Artificial Intelligence in Raising the Efficiency of Administrative Systems for Human Resources Management at Tabuk University. Journal of Education College - Sohag University, Issue 42, April 2021.
3. Albrecht, W.S., Albrecht, C.O., Albrecht, C.C., & Zimbelman, M.F. (2011). Fraud Examination. Mason, OH: Cengage Learning.
4. Al-Tawil, M. (2017). Fraud in Saudi Arabia: A review of key issues. Journal of Financial Crime, 24(3), 634-648.
5. Baker, J. (2019). Using Machine Learning to Detect Financial Fraud. jayscholar.etown.edu/cgi/viewcontent.cgi?article=1005&context=busstu
6. Barney, J.B. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, 17(1), 99-120.
7. Carataș, M.A., Spătariu, E.C., Gheorghiu, G. (2017). Internal Audit Role in Cybersecurity. "Ovidius" University Annals, Economic Sciences Series. stec.univ-ovidius.ro/html/anale/RO/2017-2/Section%20V/4.pdf
8. Coalition Against Insurance Fraud. (2020). 2020 Artificial Intelligence & Insurance Fraud Study.
9. Heap, S. The beginning of the end for telecom fraud?. (HOT TELECOM).
10. Hepworth, L.R., Greenman, C., Esplin, D., & Johnston, R. (2022). Cybersecurity and Data Privacy: The Rising Expectations Within Internal Audit. Journal of Forensic and Investigative Accounting. http://web.nacva.com/JFIA/Issues/JFIA-2022-No3-7.pdf
11. Johnson, R. B., & Smith, M. K. (2018). Fraud and corruption in the private sector: An overview and analysis of the current landscape. Journal of Business Ethics, 147(3), 589-603.
12. Khan, K., & Hussain, H. (2023). Is artificial intelligence the new benchmark for financial crime risk management?.
13. Kshetri, N. (2019). Artificial intelligence in the private sector: Key applications and challenges. Business Horizons, 62(6), 673-683.
14. Lukman, R.P., Chariri, A. (2023). THE ROLE OF INTERNAL AUDITORS IN FRAUD PREVENTIONAND DETECTION: EMPIRICAL FINDINGS FROM GENERALBANKING. DIPONEGORO JOURNAL OF ACCOUNTING. ejournal3.undip.ac.id/index.php/accounting/article/download/37480/28487
15. Manyam, S. (2022). Artificial Intelligence's Impact on Social Engineering Attacks. Governors State University.
16. Mohanty, B., Aashima, & Mishra, S. (2023). Role of artificial intelligence in financial fraud detection. Academy of Marketing Studies Journal. www.abacademies.org/articles/role-of-artificial-intelligence-in-financial-fraud-detection.pdf

DOI: https://doi.org/10.33193/JALHSS.100.2024.1018
ISSN online: 2414 - 3383
ISSN print: 2616- 3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
Volume (100) February 2024
العدد (100) فبراير 2024

17. Navaneethakrishnan, S. R., Hasan, D. S., Kumar, S. M., Mahajan, D. A., Bansal, R. (2023). THE ROLE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN FRAUD DETECTION AND PREVENTION. Eur. Chem. Bull. (European Chemical Bulletin). www.eurchembull.com/uploads/paper/be409149c68f39cc6fe531dbb4f00222.pdf
18. Rigano, C. (2019). Using Artificial Intelligence to Address Criminal Justice Needs. www.ojp.gov/pdffiles1/nij/252038.pdf
19. Rogers, E.M. (2003). Diffusion of Innovations. New York, NY: Free Press.
20. Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach. Pearson
21. Simić, N. (2022). The Internal Auditor's Role in Cybersecurity Governance –A qualitative study about the internalauditor's influence on the people factor of cybersecurity. www.diva-portal.org/smash/get/diva2:1673714/FULLTEXT01.pdf
22. Singh, L., Porcelli, B., Azimbaev, R., Chiguichon, K., & Zhang, M. (2020). Fraud Detection with AI. www3.cs.stonybrook.edu/~cse352/T1talk.pdf
23. Smith, A. B., & Johnson, C. D. (2020). The Role of Artificial Intelligence in Fraud Examination. Journal of Financial Crime, 27(3), 425-478.
24. Smith, A. B., & Johnson, C. D. (2021). Interweaving Fraud Detection Theories and the Relationship with AI. Harvard Business Review, 95(5), 90-106.
25. Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425-478.
26. Walden, V.M. (2020). Demystifying AI in anti-fraud and compliance efforts. www.alvarezandmarsal.com/sites/default/files/2020-janfeb-innovation-update.pdf
27. Yusuf Dayyabu, Y., Arumugam, D., & Balasingam, S. (2023). The application of artificial intelligence techniques in credit card fraud detection: a quantitative study. www.e3s-conferences.org/articles/e3sconf/pdf/2023/26/e3sconf_uesf2023_07023.pdf