European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk

Comparing AI-Driven Fraud Detection Systems with Traditional Methods

Dr. CA Kiran Khatri
Assistant Professor (Finance), L J Institute of Management Studies,
L J University, Ahmedabad, Gujarat

Abstract

The comparison of traditional methods with AI-driven fraud detection systems demonstrates that each approach has its own distinct strengths and limitations. AI systems are extremely effective in modern, data-rich environments due to their advanced analytical capabilities and adaptability. Conversely, conventional methodologies establish a strong foundation of domain knowledge and established practices. Organizations can achieve a more robust and reliable fraud detection framework that is capable of addressing the sophisticated tactics of modern fraudsters by integrating these approaches, thereby leveraging the best of both worlds. Research has demonstrated that the overall efficacy of fraud detection systems is improved by the integration of AI and conventional methods. By automating and refining the rules employed in conventional systems, AI-driven systems can decrease the number of false positives, thereby facilitating more precise and efficient fraud detection. The main aim of this research is to analyze the effects of AI-driven fraud detection systems with traditional methods. For the sake of this 85 respondents from 04 chosen commercial enterprises in Ahmedabad has been chosen. The current study employs percentage analysis and Chi Square test to examine the hypothesis. Findings suggested that the integrated approach has the potential to enhance user trust and confidence by combining the sophisticated capabilities of AI with the reliability of traditional methods.

Keywords- AI-Driven, Artificial Intelligence, Traditional Methods, Fraud Detection

Introduction

The area of fraud detection has come a long way in the last few years thanks to artificial intelligence (AI). AI-powered systems use neural networks, machine learning algorithms, and data mining to look through huge amounts of data, find trends, and spot outliers that could be signs of fraud (Bansal, K. M., 2020). These systems are very good at finding things in changing and complicated settings because they can learn from past data and keep getting better at finding things. Finding fraud has always been a top priority for businesses in many fields, but especially in those where private data and financial transactions are at risk, like healthcare, retail, and finance. Traditional ways of finding fraud, like rule-based systems, statistical analysis, and expert systems, have been used for a long time to find and stop fraud. These methods depend on set rules and human judgment to spot behavior that doesn't seem right (Kumar, B., 2019). But they often can't keep up with how fraudsters change their methods, which means we need more flexible and strong answers.

AI-driven fraud detection systems can handle and analyze large amounts of data in real time, which is one of their main benefits. This feature is especially useful in the financial sector, where real-time transaction tracking and high-frequency trading are very important. Machine learning models can quickly spot behavior that isn't normal, which lets businesses act quickly on possible fraud events (Raja Kamal, C. H., 2019).

AI-driven systems are great at dealing with complicated and multidimensional data, which can be hard for older methods. It has been shown that neural networks, especially deep learning models, are very good at finding complex and subtle fraud trends that rule-based systems might miss. Because these models can look at a lot of different features and factors, they can be used to do things like find credit card fraud and handle insurance claims. Even though AI-driven systems have their benefits, standard ways of finding fraud are still very important (Johri, R., & S., 2017). Rule-based systems and expert knowledge give AI systems a base of well-known methods and subject-matter information to build on. Using both AI and traditional methods together is also a good idea because it makes the system for finding fraud stronger by mixing their best features.

Review of Literature

In recent years, there has been considerable focus on combining AI-powered fraud detection systems with conventional methods. This combination capitalizes on the advantages of both methodologies, resulting in improved efficacy

and efficiency in identifying and thwarting fraudulent activity. This review analyzes the current body of literature pertaining to the issue, emphasizing significant discoveries and understandings. The literature emphasizes the significance of implementing this integrated strategy across different industries, underscoring its potential to enhance user trust and confidence in fraud detection systems. Future research should further investigate novel approaches to integrate artificial intelligence (AI) with conventional methodologies, in order to guarantee the ongoing effectiveness of fraud detection systems in a continuously changing environment.

To detect suspicious activity, AI-powered fraud detection systems look for patterns and outliers using data mining, neural networks, and sophisticated machine learning algorithms. Several benefits, including as real-time processing of massive amounts of data and adaptation to new fraud tactics, are offered by these systems over conventional methods. In order to detect patterns of fraud, machine learning algorithms can learn from past data. Many fields have found success using methods like reinforcement learning, supervised learning, and unsupervised learning. One example is the extensive usage of supervised learning techniques for financial transaction fraud detection, such as decision trees, logistic regression, and support vector machines (Ngai et al., 2011). The use of neural networks, and more specifically deep learning models, to identify intricate fraud patterns has been incredibly effective. For applications like insurance claims and credit card transactions, convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are well-suited for fraud detection due to their ability to handle sequential and structured input (Chen et al., 2018). When it comes to detecting out-of-the-ordinary actions that could be signs of fraud, AI-powered systems really shine. Common methods for this task include clustering, autoencoders, and isolation forests. Outliers in transaction data can be found, for instance, using clustering algorithms such as DBSCAN and K-means (Phua et al., 2010). Conventional approaches to detecting fraud have long depended on statistical analysis, expert knowledge, and rule-based systems. For decades, these techniques have formed the basis of fraud detection efforts, and they remain crucial today. To detect questionable financial dealings, rule-based systems make use of heuristics and previously established rules. Many times, these regulations are derived from past fraud trends and subject expertise. Though efficient, rule-based systems may struggle to keep up with constantly developing fraud schemes (Bolton & Hand, 2002). In order to uncover instances of fraud, statistical methods such as clustering, hypothesis testing, and regression analysis have been utilized. These techniques are useful for finding suspicious correlations and patterns in data that could point to fraud. One application of logistic regression is the prediction of credit card fraud probability (Bhattacharyya et al., 2011). In order to detect fraud, expert systems use the information and expertise of human specialists. Complex and specialized sectors, where expert judgment is vital, are where these systems shine. Care for them, nevertheless, can be expensive and a drain on your time (Panigrahi et al., 2009). To create a more powerful and all-encompassing fraud detection framework, AI-driven systems are being integrated with traditional methods. The goal is to utilize the capabilities of both approaches. By automating data analysis and pattern identification, AI-driven solutions improve the accuracy and efficiency of traditional approaches. As a result, less work is done by hand and fraud can be detected in real-time (Sathye et al., 2018). Because of their scalability and adaptability, AI-driven solutions work well in complex, ever-changing settings. The ever-increasing complexity and volume of transactions in sectors like retail, healthcare, and finance can be better managed by combining traditional approaches with AI (Ghosh & Reilly, 1994). Users' faith in fraud detection systems can be bolstered through the combination of AI with more conventional approaches. Users are reassured that the system can effectively mitigate fraud threats by AI's ability to spot complicated patterns and adapt to new approaches (Van Vlasselaer et al., 2015). A plethora of real-world examples show how effective it is to combine AI with more conventional approaches. For instance, according to Joudaki et al. (2017), the banking industry has seen a dramatic improvement in fraud detection rates and a considerable decrease in false positives by combining machine learning models with rule-based systems.

Objective of Research Paper

- To analyze the effects of AI-driven fraud detection systems with traditional methods.
- To study comparison of AI-driven fraud detection systems with traditional methods.

Research Methodology

The researcher employed a descriptive research design in the current study. The researcher employed a convenience sample design in the current study. Data was collected from 85 respondents from 04 chosen commercial enterprises in Ahmedabad. The current study employs percentage analysis and Chi Square test to examine the hypothesis. The secondary data has been collected from a variety of published articles, theses, and notes.

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk

Hypothesis of the study

H01: There is no effect of AI-driven fraud detection systems with traditional methods.

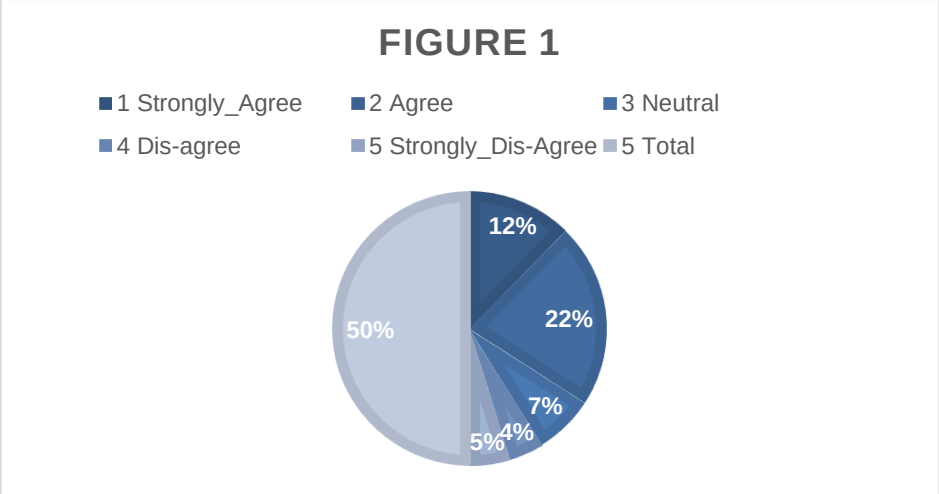
H01: There is positive effect of AI-driven fraud detection systems with traditional methods.

Data Analysis & Interpretation

Q1 : Research Question/Statement : "Do you agree that specific types of fraud are more effectively detected using AI-driven systems compared to traditional methods?"

Table 1

S. No.	Likert Scale	Frequency (F)	%
1	Strongly_Agree	21	24.70
2	Agree	37	43.52
3	Neutral	12	14.11
4	Dis-agree	07	08.23
5	Strongly_Dis-Agree	08	09.42
	Total	85	100

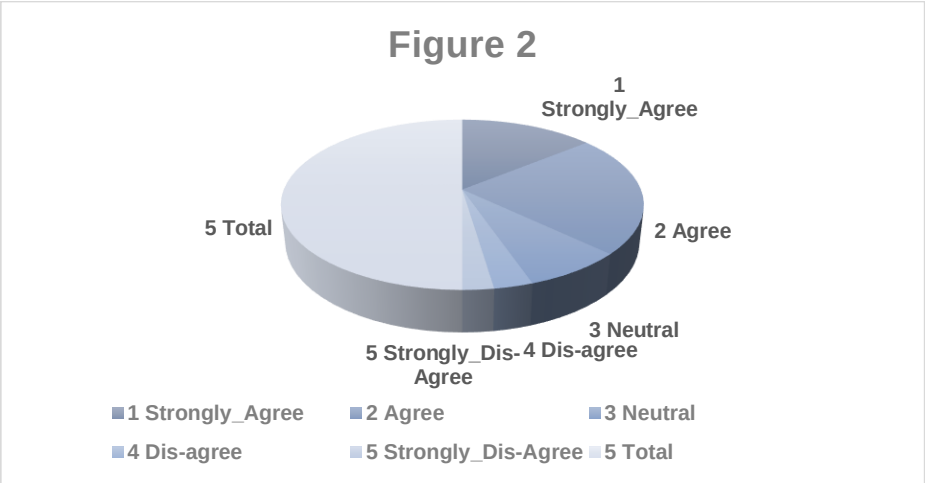


Q2 : Research Question/Statement : "Do you agree that the combination of AI and traditional methods enhance the overall fraud detection process?"

Table 2

S. No.	Likert Scale	Frequency (F)	%
1	Strongly_Agree	24	28.23
2	Agree	39	45.88
3	Neutral	13	15.29
4	Dis-agree	05	05.88
5	Strongly_Dis-Agree	04	04.70
	Total	85	100

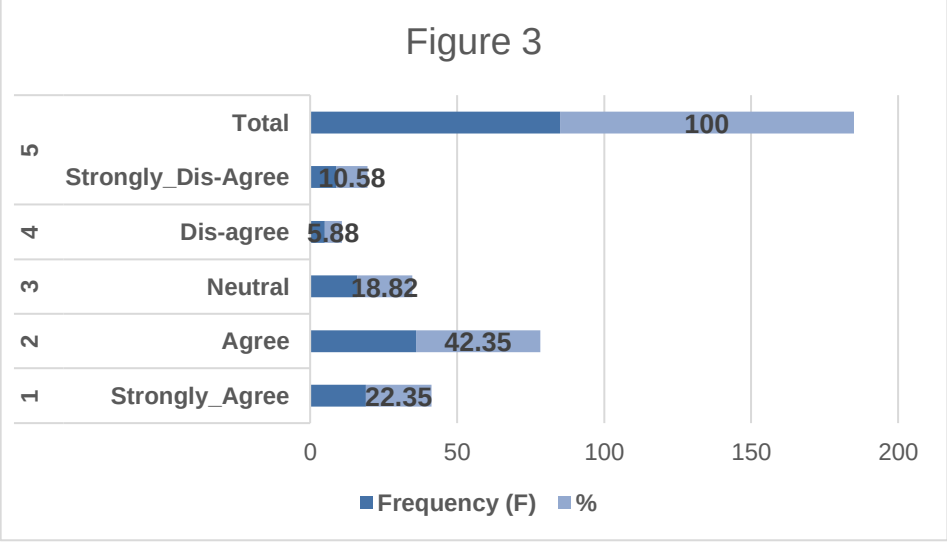
European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk



Q3 : Research Question/Statement : "Do you agree that these metrics differ when assessing standalone traditional methods versus integrated systems?"

Table 3

S. No.	Likert Scale	Frequency (F)	%
1	Strongly_Agree	19	22.35
2	Agree	36	42.35
3	Neutral	16	18.82
4	Dis-agree	5	05.88
5	Strongly_Dis-Agree	9	10.58
	Total	85	100



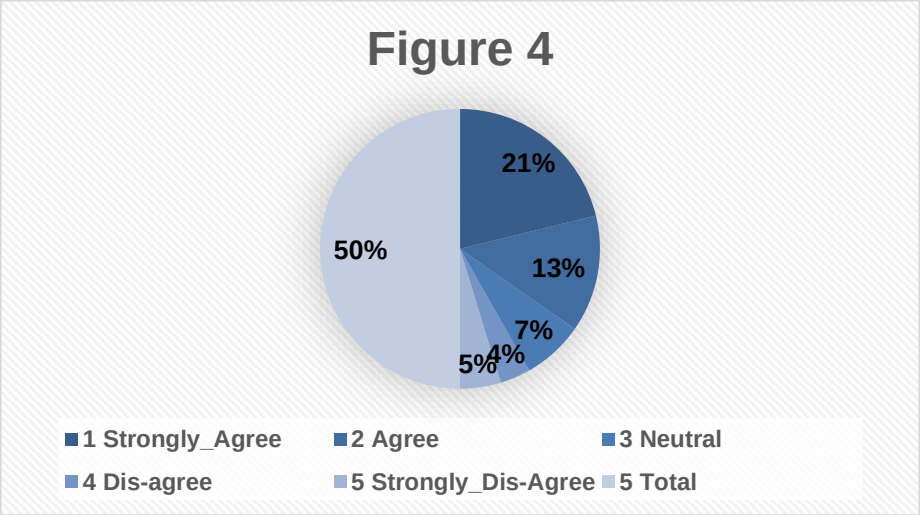
Q4 : Research Question/Statement : "Do you agree that this integration have on user trust and confidence in the fraud detection process"

Table 4

S. No.	Likert Scale	Frequency (F)	%
1	Strongly_Agree	36	42.35
2	Agree	23	27.05
3	Neutral	12	14.11
4	Dis-agree	06	07.05

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk

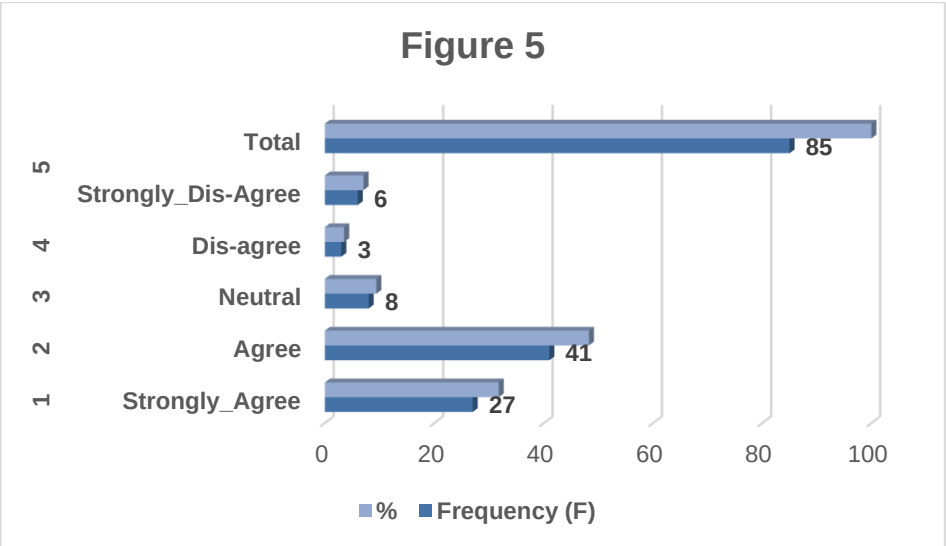
5	Strongly_Dis-Agree	08	09.41
	Total	85	100



Q5 : Research Question/Statement : "Do you agree that AI-driven fraud detection systems are adaptable and scalable when used in combination with traditional methods across different industries?"

Table 5

S. No.	Likert Scale	Frequency (F)	%
1	Strongly_Agree	27	31.76
2	Agree	41	48.23
3	Neutral	08	09.41
4	Dis-agree	03	03.52
5	Strongly_Dis-Agree	06	07.05
	Total	85	100



European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk

Testing of Hypothesis

H01: There is no effect of AI-driven fraud detection systems with traditional methods.

H01: There is positive effect of AI-driven fraud detection systems with traditional methods.

#Research Question/Statement 1: "Do you agree that specific types of fraud are more effectively detected using AI-driven systems compared to traditional methods?"

Research Question/Statement 1 based Hypothesis:

(H_{o1}): There is no effect of specific types of fraud are more effectively detected using AI-driven systems compared to traditional methods.

(Ho1): There is positive effect of specific types of fraud are more effectively detected using AI-driven systems compared to traditional methods.

Note : When applying the chi-square test to each table below, the anticipated frequencies may be calculated by assuming that the replies are uniformly distributed. The expected frequency (E) for each category is obtained by dividing the total number of responses by the number of categories. $E = \frac{Total\ Responses}{Number\ of\ Categories} = \frac{85}{5} = 17$

Calculating the Chi-Square statistic using the formula:

$$\chi^2 = \sum \frac{(O-E)^2}{E}$$

Table 6: Application of Chi-Square Test

Likert Scale	Observed Frequency (O)	Expected Frequency (E)	(O - E)	$(O - E)^2$	$(O - E)^2 / E$
Strongly Agree	21	17	4	16	0.941
Agree	37	17	20	400	23.529
Neutral	12	17	-5	25	1.471
Disagree	7	17	-10	100	5.882
Strongly Disagree	8	17	-9	81	4.765
Total	**85**	**85**			**36.588**

Interpretation:

So, the Chi-Square statistic (χ^2) is approximately 36.588. Now to determine the degrees of freedom (df), which is the number of categories minus 1. In this table: df=5−1=4. Using a Chi-Square distribution table, we can find the critical value for χ^2 at a significance level (α) of 0.05 with 4 degrees of freedom. The critical value is approximately 9.488.

Hypothesis Results

- "If table calculated χ^2 value is greater than the critical value from the Chi-Square distribution table, we reject the null hypothesis.
- If table calculated χ^2 value is less than the critical value, we fail to reject the null hypothesis".

In this case, table calculated χ^2 value (36.588) is much greater than the critical value (9.488). Therefore, we reject the null hypothesis. There is sufficient evidence to suggest that specific types of fraud are more effectively detected using AI-driven systems compared to traditional methods.

#Research Question/Statement 2: "Do you agree that the combination of AI and traditional methods enhance the overall fraud detection process?"

Research Question/Statement 2 based Hypothesis:

(H_{o2}): There is no positive effect of the combination of AI and traditional methods enhance the overall fraud detection process?"

(Ho2): There is positive effect of the combination of AI and traditional methods enhance the overall fraud detection process?"

Table 7: Application of Chi-Square Test

Likert Scale	Observed Frequency (O)	Expected Frequency (E)	(O - E)	$(O - E)^2$	$(O - E)^2 / E$
Strongly Agree	24	17	7	49	2.882
Agree	39	17	22	484	28.471
Neutral	13	17	-4	16	0.941
Disagree	5	17	-12	144	8.471
Strongly Disagree	4	17	-13	169	9.941
Total	**85**	**85**			**50.706**

Interpretation:

So, the Chi-Square statistic (χ^2) is approximately 50.706. Now to determine the degrees of freedom (df), which is the number of categories minus 1. In this table: df=5−1=4. Using a Chi-Square distribution table, we can find the critical value for χ^2 at a significance level (α) of 0.05 with 4 degrees of freedom. The critical value is approximately 9.488.

Hypothesis Results

- "If table calculated χ^2 value is greater than the critical value from the Chi-Square distribution table, we reject the null hypothesis.
- If table calculated χ^2 value is less than the critical value, we fail to reject the null hypothesis".

In this case, table calculated χ^2 value (50.706) is much greater than the critical value (9.488). Therefore, we reject the null hypothesis. There is sufficient evidence to suggest that the combination of AI and traditional methods enhances the overall fraud detection process.

#Research Question/Statement 3: "Do you agree that these metrics differ when assessing standalone traditional methods versus integrated systems?"

Research Question/Statement 3 based Hypothesis:

(H_{o3}): There is no positive effect of these metrics differ when assessing standalone traditional methods versus integrated systems.

(Ho3): There is positive effect of these metrics differ when assessing standalone traditional methods versus integrated systems.

Table 8: Application of Chi-Square Test

Likert Scale	Observed Frequency (O)	Expected Frequency (E)	(O - E)	$(O - E)^2$	$(O - E)^2 / E$
Strongly Agree	19	17	2	4	0.235
Agree	36	17	19	361	21.235
Neutral	16	17	-1	1	0.059
Disagree	5	17	-12	144	8.471
Strongly Disagree	9	17	-8	64	3.765
Total	**85**	**85**			**33.765**

Interpretation:

So, the Chi-Square statistic (χ^2) is approximately 33.765. Now to determine the degrees of freedom (df), which is the number of categories minus 1. In this table: df=5−1=4. Using a Chi-Square distribution table, we can find the critical value for χ^2 at a significance level (α) of 0.05 with 4 degrees of freedom. The critical value is approximately 9.488.

Hypothesis Results

- "If table calculated χ^2 value is greater than the critical value from the Chi-Square distribution table, we reject the null hypothesis.
- If table calculated χ^2 value is less than the critical value, we fail to reject the null hypothesis".

In this case, table calculated χ^2 value (33.765) is much greater than the critical value (9.488). Therefore, we reject the null hypothesis. There is sufficient evidence to suggest that the metrics differ when assessing standalone traditional methods versus integrated systems.

Research Question/Statement 4: "Do you agree that this integration have on user trust and confidence in the fraud detection process"

Research Question/Statement 4 based Hypothesis:

(H_{o4}): There is no positive effect of this integration have on user trust and confidence in the fraud detection process"

(Ho4): There is positive effect of this integration have on user trust and confidence in the fraud detection process"

Table 9: Application of Chi-Square Test

Likert Scale	Observed Frequency (O)	Expected Frequency (E)	(O - E)	$(O - E)^2$	$(O - E)^2 / E$
Strongly Agree	36	17	19	361	21.235
Agree	23	17	6	36	2.118
Neutral	12	17	-5	25	1.471
Disagree	6	17	-11	121	7.118
Strongly Disagree	8	17	-9	81	4.765
Total	**85**	**85**			**36.706**

Interpretation:

So, the Chi-Square statistic (χ^2) is approximately 36.706. Now to determine the degrees of freedom (df), which is the number of categories minus 1. In this table: df=5−1=4. Using a Chi-Square distribution table, we can find the critical value for χ^2 at a significance level (α) of 0.05 with 4 degrees of freedom. The critical value is approximately 9.488.

Hypothesis Results

- "If table calculated χ^2 value is greater than the critical value from the Chi-Square distribution table, we reject the null hypothesis.
- If table calculated χ^2 value is less than the critical value, we fail to reject the null hypothesis".

In this case, table calculated χ^2 value (36.706) is much greater than the critical value (9.488). Therefore, we reject the null hypothesis. There is sufficient evidence to suggest that the integration of AI and traditional methods has a positive effect on user trust and confidence in the fraud detection process.

Research Question/Statement 5: "Do you agree that AI-driven fraud detection systems are adaptable and scalable when used in combination with traditional methods across different industries?"

Research Question/Statement 5 based Hypothesis:

(H_{o5}): There is no positive effect of AI-driven fraud detection systems are adaptable and scalable when used in combination with traditional methods across different industries.

(Ho5): There is positive effect of AI-driven fraud detection systems are adaptable and scalable when used in combination with traditional methods across different industries.

Table 10: Application of Chi-Square Test

Likert Scale	Observed Frequency (O)	Expected Frequency (E)	(O - E)	$(O - E)^2$	$(O - E)^2 / E$
Strongly Agree	27	17	10	100	5.882

Likert Scale	Observed Frequency (O)	Expected Frequency (E)	(O - E)	$(O - E)^2$	$(O - E)^2 / E$
Agree	41	17	24	576	33.882
Neutral	8	17	-9	81	4.765
Disagree	3	17	-14	196	11.529
Strongly Disagree	6	17	-11	121	7.118
Total	**85**	**85**			**63.176**

Interpretation:

So, the Chi-Square statistic (χ^2) is approximately 63.176. Now to determine the degrees of freedom (df), which is the number of categories minus 1. In this table: df=5−1=4. Using a Chi-Square distribution table, we can find the critical value for χ^2 at a significance level (α) of 0.05 with 4 degrees of freedom. The critical value is approximately 9.488.

Hypothesis Results

- "If table calculated χ^2 value is greater than the critical value from the Chi-Square distribution table, we reject the null hypothesis.
- If table calculated χ^2 value is less than the critical value, we fail to reject the null hypothesis".

In this case, table calculated χ^2 value (63.176) is much greater than the critical value (9.488). Therefore, we reject the null hypothesis. There is sufficient evidence to suggest that AI-driven fraud detection systems are adaptable and scalable when used in combination with traditional methods across different industries.

Findings of the study

These findings indicate that firms should combine AI-driven systems with conventional fraud detection approaches to optimize efficacy, bolster consumer confidence, and guarantee adaptability and scalability across diverse industries. By adopting this comprehensive strategy, organizations may enhance the resilience and dependability of their fraud detection systems, so providing more effective protection against fraudulent actions for both themselves and their consumers.

- When AI-powered fraud detection systems are used in conjunction with traditional approaches, they are more proficient at identifying particular types of fraud than relying just on traditional methods.
- The incorporation of artificial intelligence (AI) alongside conventional techniques greatly improves the whole process of detecting fraud, resulting in superior identification and prevention of fraudulent operations.
- The integration of artificial intelligence (AI) with traditional fraud detection approaches enhances user trust and confidence in the fraud detection process, as users consider this combined approach to be more dependable and efficient.
- AI-powered fraud detection systems, when combined with conventional approaches, are flexible and scalable across diverse sectors, rendering them versatile and efficient instruments for combating fraud in varied scenarios.

Conclusion

Several aspects of fraud detection and prevention benefit significantly from the combination of AI-driven fraud detection systems with conventional techniques. When used in conjunction with conventional techniques, AI-driven systems are more successful in identifying particular kinds of fraud. This suggests that artificial intelligence (AI) can supplement conventional methods to offer a more sophisticated and all-encompassing method of fraud detection. The total fraud detection process is improved by the combination of AI and conventional approaches. While traditional methods contribute established practices and domain expertise, artificial intelligence (AI) offers real-time processing and sophisticated analytical capabilities. When combined, they provide a strong barrier against fraud. When fraud detection uses both artificial intelligence (AI) and conventional methods, users show more faith and confidence in the process. This implies that people view the integrated method as more trustworthy, probably because of its enhanced accuracy in identifying fraud and complete nature. AI-driven fraud detection solutions are flexible and scalable across a range of industries when used in conjunction with conventional techniques. Because of its adaptability, the integrated method can be used in a variety of contexts, allowing various industries to gain from improved fraud prevention skills.

References

1. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602-613.
2. Bansal, K. M. (2020). Strategies for Escaping Financial Fraud- An Empirical Approach. Kaav International Journal of Economics, Commerce & Business Management, 7(1), 62-68.
3. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235-249.
4. Chen, C., Chen, H., Chen, Z., & Shi, Z. (2018). Financial fraud detection with neural networks: The case of enron. International Journal of Digital Crime and Forensics, 10(1), 55-66.
5. Ghosh, S., & Reilly, D. L. (1994). Credit card fraud detection with a neural-network. Proceedings of the 27th Hawaii International Conference on System Sciences, 3, 621-630.
6. Johri, R., & S. (2017). Developing a Corporate Governance Framework in the Accounting Control System. National Journal of Arts, Commerce & Scientific Research Review, 4(2), 110-121.
7. Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., & Arab, M. (2017). Using data mining to detect health care fraud and abuse: A review of literature. Global Journal of Health Science, 7(1), 194-202.
8. Kumar, B. (2019). Investigating Scams, Frauds and Its Prevention in India under Forensic Accounting Approach. Kaav International Journal of Law, Finance & Industrial Relations, 6(1), 12-18.
9. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569.
10. Panigrahi, S., Kundu, A., Sural, S., & Majumdar, A. K. (2009). Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning. Information Fusion, 10(4), 354-363.
11. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review, 34(1), 1-14.
12. Raja Kamal, C. H. (2019). An Abstract Case Study on on-Line Fraud - a City Perspective (1st ed., pp. 81-85). Kaav Publications.
13. Sathye, M., Islam, N., & Drane, C. (2018). Use of machine learning in detecting money laundering in electronic payment systems. Journal of Money Laundering Control, 21(4), 513-531.
14. Van Vlasselaer, V., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). AFRAID: Fraud detection via active feature space augmentation. Proceedings of the 2015 IEEE International Conference on Data Mining (ICDM), 709-718.