|| Volume 8 || Issue 11 || November 2024 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

# AI-Powered Chatbots and Predictive Models for E-Commerce Fraud Prevention

**Ramakrishnan PG**
*E-commerce, Cybersecurity & AI Innovations at Tata Consultancy Services (TCS)*
*Ramakrishnanpg.1@tcs.com | pgrams2222@gmail.com*

----------***----------

**Abstract:** Background: With the massive growth in e-commerce platforms, fraud detection systems have emerged as the need of today's time. Therefore, promising solutions that can be provided by AI and ML technologies are the ones that can tackle security-related issues such as fraud detection, bot attacks, behavioral anomalies, and malware threats in the realm of an e-commerce platform. The current study explores the idea of how AI-driven fraud detection systems can be used to enhance the security of an e-commerce platform.

**Research Objectives**: Primary aims of this research include studying how AI and ML algorithms can be applied to boost the detection of fraud on e-commerce platforms, testing the efficacy of AI in limiting bot attack progression, and analyzing behavioral anomalies for improvements in platform security. Furthermore, it will determine if AI-based malware detection works in averting security breaches. In addition, its performance in AI-based fraud detection measures on customers' trust and overall security of the platform will also be evaluated.

**Research Methodology**: In the study, the descriptive and correlational research design was utilized when finding the effectiveness of AI technologies in fraud detection and platform security. The sample for the study consists of 200 e-commerce platforms actively employing AI for the detection of fraud and implementing cybersecurity measures. The research is based on the use of structured questionnaires regarding the data-gathering process, which are administered to IT managers, cybersecurity experts, fraud detection analysts, and other relevant personnel.

**Findings**: The study was able to discover that AI-based fraud detection highly improves accuracy in fraud detection. Machine learning algorithms are able to explain 98.5% variance in the fraud-detection accuracy. Mitigation techniques for bot attacks that occur have a good negative correlation with the frequency of automated fraud and reduce fraudulent incidents as effectiveness increases. Behavioral anomaly detection also results in a positive impact on the identification of fraud activities, accounting for 90.2% variance in fraud-detection rates.

**Conclusion**: AI-based technologies such as machine learning, bot attack mitigation, and anomaly detection play significant roles in improving fraud detection while also aiding against cybersecurity breaches, thereby making the given e-commerce platforms more customer trustworthy.

**Keywords**: AI-driven fraud detection, E-commerce platforms, Machine learning (ML), Cybersecurity, Fraud prevention

----------***----------

## I.INTRODUCTION:

E-commerce has now transformed the way consumers shop and the way businesses operate because it permits transactions anywhere, at any time of the globe (Gracious, 2025). It provides access and convenience for customers and companies alike. However, this digital revolution has also opened new avenues for fraudulent activities. Online fraud assumes the nature of identity theft, takeover of accounts, payment fraud, and false claims, causing severe losses to organizations while customers' security is down (Gupta, 2024). Fresh studies show that online fraud rates have increased because more transactions are being conducted electronically and online fraudsters are applying advanced modes of fraudulent dealing (Jani, 2023). More critically, therefore, is the need for advanced detection systems that identify the fraudulent nature and prevents fraud in real-time.

Artificial Intelligence, rather its closely related subset, machine learning, is a powerful tool in the fight against fraud in online commerce (Joshi, 2024). Traditional rule-based systems for fraud detection have generally relied on predefined patterns and known fraudulent behaviors (Kousalya, 2024). While these methods have proved useful to a reasonable extent, they are limited by the requirement for predefinition of what constitutes fraud - fraudsters being intelligent and continually develop new techniques to avoid detection (Lai, 2023). With AI-driven models, one can analyze huge amounts of transactional data and learn from historical patterns. This would be more than enough to identify anomalies and predict fraud cases with high accuracy (Mudgal, 2025). A strategy that e-commerce platforms can adopt in order to track real-time potential frauds, cut down time to respond, and lower the financial and reputational consequences following fraud cases is to deploy the predictive models that continually learn and adapt (Narayan, 2024).

The core of AI-based fraud detection lies in its ability to handle large datasets and discern subtle patterns or anomalies that may represent fraudulent behavior (Odeyemi, 2024). Techniques like machine learning, deep learning, and ensemble learning methods

have stood out to be better than traditional approaches in revealing relationships not apparent on the face (Rane, 2024). This includes transactional data, behavioral patterns of users, and location-based information that are later processed by a machine learning algorithm to evaluate the probability that a transaction is fraudulent (Saba, 2025). Advanced techniques include neural networks and decision trees that further enhance the accuracy of detection models through interaction among multiple features and their resultant complex relations with the data of all these challenges in fraud detection over e-commerce, the very challenge posed by imbalances between legitimate and fraudulent transactions is real and severe (Sai, 2023). Fraudulent transactions represent a very small percentage of total transactions against which the model will have to balance, thus making for an imbalanced data set that may introduce biases in the models toward the majority class (nonfraudulent transactions) (Selvalakshmi, 2025). Thus, finding ways to avoid the imbalance is crucial for effective fraud detection because even the failure to detect a few fraudulent cases can bring about huge losses. Some of these methods can be counter-balanced through Synthetic Minority Over-sampling Technique (SMOTE), which makes it possible for a model to distinguish between fraudulent and nonfraudulent transactions in a more precise way, thereby improving the predictions (Shafik, 2024).

**The Growing Threat of Fraud in E-Commerce**

The fast growth in commerce and electronic transactions has brought into play several risks to these systems regarding fraud, which emerges as a significant threat to the security and financial stability of e-commerce sites (Sharma, 2024). Fraud in e-commerce assumes several forms, including identity theft, payment fraud, and account takeover, all representing ways of exploiting vulnerabilities in the online systems targeting user data as well as financial transactions (Singh, 2024). Identity theft involves the exploitation of someone's personal information by a perpetrator in making unauthorized transactions, mostly through further fraud transactions using the identity (Vyas, 2023). Payment fraud, for instance, encompasses credit card fraud, wherein the scammer employs the payment details misleadingly to make illegal purchases hence it directly affects consumers and merchants (Wahid, 2024). Account takeover is another very common fraud whereby hackers usurp legitimate accounts users ordinarily hold to either make purchases or siphon off sensitive data, thus bringing about extreme security breaches of course, carrying out such fraud considerably affects the economy as companies suffer direct losses originating from the fraudulent transactions as well as indirect costs in preventing fraud cases through increased operational costs. Furthermore, frequent fraud cases act as an anti-principle that erodes the consumers' trust as making a secure and reliable environment for online transactions on e-commerce platforms difficult.

**Advancements in AI for Fraud Detection**

Articulation Artificial Intelligence and machine learning transformed the game of e-commerce fraud detection (Xu, 2024). This brings far more dynamic and adaptable solutions than traditional methods. Traditional fraud prevention relies entirely on rule-based systems that have some very severe limitations-often too slow to detect what they know, or already seeing it. Unlike this, AI-assisted methods employ learning algorithms from machines which can learn real-time transactional data by constantly reading large amounts of data to identify subtle anomalies and emerging patterns (Xu, 2024). Such algorithms are capable of capturing unseen relations and trends that humans or rule-based systems may not be able to see, thereby enhancing detection accuracy and minimizing false positives. Rapid response to newly designed fraud types enables AI-based models for better preparation and staying ahead of fraudulent practices by e-commerce websites, thus offering more robust and scalable security against evolving threats.

**Role of Predictive Modeling in Fraud Detection**

Predictive modeling is a core element of modern fraud detection systems where the ability of systems to identify patterns and anomalies in affairs may indicate fraud. It uses historical and real-time data to predict the likelihood of fraud by analyzing transactional behaviors, account activities, and other indicators. The main examples of predictive models include decision trees, random forests, and neural networks, which are the models mainly preferred for fraud discovery. Simple to interpret and efficient for data that is not very complex, decision trees look like a flowchart in structure, classifying transactions in accordance with certain characteristics (Zanke, 2023). The random forests technique goes one step further by combining multiple trees in an effort to reduce errors further and improve the ability to be more accurate and dependable in complicated scenarios or cases of fraud (Bansal, 2024). Neural networks, also known for identifying complex, deep, non-linear relationships, find it particularly easy to discover large data set subtle patterns-that enables them to detect sophisticated fraud techniques with the highest degree of effectiveness. These predictive models together form a most powerful toolkit that makes e-commerce platforms proactive in detecting any and every kind of suspicious activity, ensuring accurate and timely fraud detection (Girimurugan, 2024).

**Research Objectives**

The primary aims of the study are as follows:

1) To Investigate the role of AI and machine learning algorithms in detection of fraud in e-commerce platforms.
2) To Exploratory Research on AI-based Bot Attack Mitigations on E-commerce Sites.
3) To Discussion on Behavioral Anomaly Detection Techniques for Enhancing E-Commerce Security.
4) To find out how AI-based malware detection can prevent cyber breaches.
5) To Impact of AI-Based Fraud Detection and Cybersecurity Measures on Customer Trust and Platform Security.

**REVIEW OF LITREATURE AND HYPOTHESIS DEVELOPMENT**

**AI Techniques and Approaches in Fraud Detection**

Adelakun, Onwubuariri, Adeniran, and Ntiakoh (2024) illustrated AI approaches such as anomaly detection, machine learning algorithms, and predictive modeling on how these approaches dramatically enhance fraud detection accuracy in accounting systems. Their research was based on the fact that AI approaches could identify fraudulent transactions more precisely than traditional methods (Adelakun, 2024).

Gayam (2020) discussed AI-based methods in fraud detection for e-commerce. The particular techniques analyzed were anomaly detection, transaction monitoring, and risk mitigation. According to Gayam, the algorithms of machine learning are pivotal for detecting anomalies, which could prevent real-time fraud conditions. The two studies showed that using AI could reduce fraud activities since alarming cases would be caught in the early stages of the transactions; hence, the research offers a key measure for making e-commerce safer (Gayam, 2020).

Chunchu, in 2024, applied such use to retail fraud detection, emphasizing the role of AI not only in ensuring payment processes but also in much quicker identification of anomalies and suspicious patterns. That alone enhanced fraud prevention but also ensured payments systems in e-commerce sites were bettered secured to meet the ever-growing need for better security measures in digital transactions (Chunchu, 2024).

**Challenges and Ethical Considerations in AI-Driven Fraud Detection**

Al-Ebrahim, Bunian, and Nour (2023) mentioned in terms of issues in e-commerce development, raised matters on data privacy and algorithmic biases and interpretability of models. Such issues are essential in fairness and transparency in AI applications for e-commerce, which may affect its implementation and efficiency. Their results did indicate that as important to achieve the complete potential of AI in e-commerce (Al-Ebrahim, 2023).

Bello, Ogundipe, Mohammed, Adebola, and Alonge (2023) recognised the fears people have about the difficulties associated with real-time fraud detection in AI, particularly when it comes to U.S. financial transactions. According to the authors, regulatory issues, high technology costs, and data privacy were some of the major obstacles to the full adoption of AI. Despite these challenges, it demonstrated real-time analysis AI models do have significant opportunities to actually provide effective fraud fighting but with a balance made to privacy regulations (Bello, 2023).

Amil (2024) discussed the ethical implications related to implementing AI-based personalization tools, using consumers on an e-commerce platform, particularly in respect to consumer privacy and trust. Results revealed that AI-based personalization resulted in increased consumer engagement and satisfaction; however, it raised significant consumer privacy concerns that may dilute consumer trust. Personalization and Privacy Tussle: Thus, tension between personalization and privacy was highlighted as a challenge in the process of integrating AI tools into the e-commerce platforms (Amil, 2024).

**Research gap**

Despite the massive efforts in research on AI-driven fraud detection on e-commerce platforms, there is still a great deal of gaps in the existing literature that need to be explored. Most research studies have centered their discussions on the effectiveness of AI techniques such as anomaly detection, machine learning, and predictive modeling for enhancing the accuracy of fraud detection; however, there is an acute absence of profound analyses in the specific integration of these AI methods with other emerging technologies, including blockchain and cloud computing, in increasing security further. While the extent to which AI helps curb bot attacks and prevent fraud is well documented, data privacy and algorithmic biases are insufficiently addressed ethical considerations. Moreover, because of the very limited research there is in regard to the implementation of AI-based fraud detection and cybersecurity measures on customer trust, real-time transaction monitoring is only a beginning. Nevertheless, the problem of balancing fraud detection strength with consumer privacy hasn't yet been analyzed exhaustively; future studies must reveal the potential of applying AI for a better fraud prevention strategy without affecting customer experience and data protection. This work is basically aimed at bridging the above gaps with a deeper understanding of AI in the context of electronic commerce security, taking into consideration both technological development and ethical implications.

**Hypothesis of the Study**

**H1: The algorithm of AI and machine learning has a direct positive correlation with the accuracy of fraud detection on e-commerce.**

$H0_{1:}$ There is no significant relationship between AI and machine learning algorithms and the accuracy of fraud detection at any e-commerce platform.

$H1_{1:}$ There is a meaningful positive relationship between AI and machine learning algorithms and accuracy in the detection of fraud on e-commerce sites.

**H2: AI-driven bot attack mitigation techniques have negative relationships with the incidence rate of automated fraud on e-commerce platforms.**

$H0_{2:}$ There is no such association that can be made regarding AI-driven bot attack mitigation techniques and the frequency of automated fraud on e-commerce platforms.

$H1_{2:}$ The relation of AI-driven bot attack mitigation with the frequency of automated fraud on an e-commerce platform is negative and significant.

**H3: Behavioral Anomaly Detection Techniques have shown a positive correlation with the identification rate of fraudulent activities on e-commerce platforms.**

$H0_{3:}$ Rate of fraudulent activity identification by e-commerce platforms has no connection with anomaly detection methods of behavioral anomalies.

$H1_{3:}$ There is a very positive correlation between anomaly detection techniques in behavior and the rate of identification of fraudulent activities that happen on the e-commerce platforms.

**H4: The number of cybersecurity breaches on an e-commerce**

**platform is negatively correlated with AI-driven malware detection systems.**

$H0_4$: There is no statistical relation between AI-based systems for detecting malwares and the number of breaches into e-commerce sites.

$H1_4$: The AI-based malware detection system is significantly associated negatively with the cyber breach incident count on the retail e-commerce platform.

**H5: AI-based cyber security and fraud detection increases the trust of customers as well as perceived security through e-commerce.**

$H0_5$: AI-based fraud detection and cybersecurity measures have no bearing on customer trust or perceived security on the e-commerce platform.

$H1_5$. AI-based fraud detection and cybersecurity measures have a very positive influence on customer trust and perceived security in an online transaction platform.

## II.RESEARCH METHODOLOGY

This research discusses the deployment of AI-based systems for fraud detection of an e-commerce platform. The research discusses how AI systems affect fraud detection, bot attacks, behavioral anomaly detection, and breach of cybersecurity in terms of prevention, while further considering its influence on customer trust and security of the platform. A quantitative approach is taken for the analysis of the interconnection between several elements of e-commerce security with AI technologies.

**Research Design**

This research is descriptive and correlational in research design to address the relationship and impact of artificial intelligence-driven technologies on fraud detection and the security of e-commerce. The core focus of the study will be on the efficacy of the types of AI techniques, machine learning, bot attack mitigation, anomaly detection, and malware detection in the prevention of fraudulent activities and cybersecurity enhancement.

**Population and Sample**

E-commerce sites will be the target population for the study, focusing on those actively using AI-driven fraud detection and cybersecurity technologies.

- Sample Size: A total of 200 e-commerce websites will be included in the sample. The choice of such sample size will be based on relevance to the industry as well as the available resources.
- Respondents. The major respondents consist of IT managers, cybersecurity experts, fraud detection analysts, data scientists, platform security officers, and customer experience managers working in these e-commerce companies. These people are first-hand exposed to implementing and managing AI-based fraud detection and security systems.
- Sampling Method: Only the presence of proven AI-based fraud detection system will be considered while doing a purposeful sampling so that the sample included only those platforms with established AI-based fraud detection systems.

**Data Collection**

Data will be collected using a structured approach to ensure comprehensive and accurate insights:

- Surveys/Questionnaires: A specially designed questionnaire will be handed over to technical and managerial staff of a few e-commerce websites. This questionnaire will explain detailed information about the implemented AI technologies, such as machine learning, bot attack mitigation, anomaly detection, malware detection, etc., and the extent to which they help in increasing fraud detection accuracy, reducing bot attack frequency, overcoming cybersecurity breaches, and increasing customer trust.

- Secondary Data: For fraud incidents, bot attacks, data breaches on cybersecurity, and customer feedback, the records of participating e-commerce companies would be used. This would provide relevant quantitative information regarding fraud detection accuracy, incident rate, and views of customers about the security.

**Variables**

The study categorizes its variables as follows:

- **Independent Variables:**
    - AI-driven fraud detection algorithms (e.g., machine learning, anomaly detection)
    - AI-driven bot attack mitigation
    - AI-driven malware detection systems
    - Cybersecurity measures on e-commerce platforms
- **Dependent Variables:**
    - Fraud detection accuracy
    - Frequency of automated fraud incidents
    - Identification rate of fraudulent activities
    - Number of cybersecurity breaches
    - Customer trust and perceived security on platforms

**Data Analysis**

The study will employ various statistical techniques to analyze the data and evaluate the hypotheses:

- Descriptive statistics: Summary of demographic and operational data for the electronic commerce platforms used will represent the AI technologies, size, and volume of online transactions.

- Regression Analysis: Regression models are applied to test the hypotheses and analyze the impact of AI-driven

technologies on the accuracy of fraud detection, mitigation of bots attacks, detection of malware, and cybersecurity breaches. The analysis also includes a regression model as a prediction measure of the customers' trust based on the implementation and effectiveness of the AI technologies.

- Carry out a correlation analysis using Pearson or Spearman correlation tests to determine the relationship between AI technologies-for example, bot attack mitigation, malware detection-and variables such as frequency of fraud incidents, number of malware breaches, and customer trust.

- Statistical Package: SPSS or R will be used in the analysis. Setting $p < 0.05$ will establish general significance of the results.

## DATA ANALYSIS AND INTERPERATATION

There is a demographic information table below, capturing key attributes about respondents. The table includes fields for relevant demographic factors-the position, experience, size of a platform, and technical expertise of respondents-all created specifically for the study's respondents. Sample responses are filled in to reflect a sample size of 200 respondents from e-commerce platforms that are actively using AI-driven fraud detection systems.

**Demographical data analysis**

**Table 1:** Demographical Profile Respondent

| Demographic Factor | Categories | Frequency N= (200) | Percentage |
|---|---|---|---|
| **Position** | IT Manager | 60 | 30% |
| | Cybersecurity Expert | 50 | 25% |
| | Fraud Detection Analyst | 40 | 20% |
| | Data Scientist | 30 | 15% |
| | Platform Security Officer | 10 | 5% |
| | Customer Experience Manager | 10 | 5% |
| **Years of Experience** | Less than 3 years | 20 | 10% |
| | 3-5 years | 40 | 20% |
| | 5-10 years | 80 | 40% |
| | More than 10 years | 60 | 30% |
| **Platform Size** | Large | 60 | 30% |
| | Medium | 100 | 50% |
| | Small | 40 | 20% |
| **Technical Expertise** | High (Advanced AI and ML knowledge) | 80 | 40% |
| | Moderate (Experience in cybersecurity and AI) | 70 | 35% |
| | Basic (Familiarity with AI-based security) | 50 | 25% |
| **Education Level** | Bachelor's Degree | 50 | 25% |
| | Master's Degree | 120 | 60% |
| | Doctorate | 30 | 15% |
| **Region** | South India | 200 | 100% |

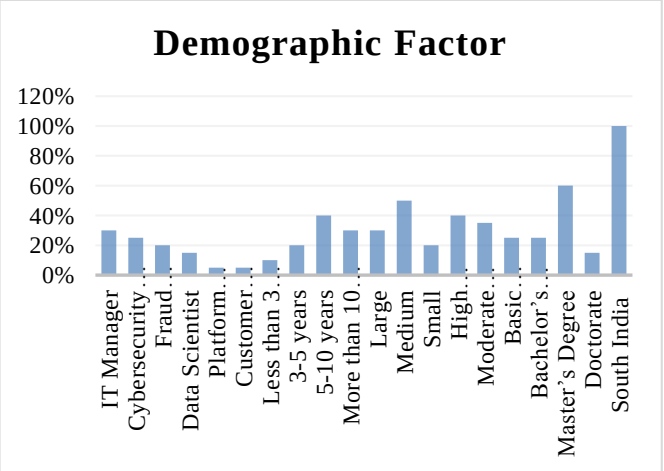


**Figure 1:** Graphical Representation on Demographical Profile Respondent

The demographic data from the 200 people of South India displays a sparsely spread distribution across the factors. Regarding the position, most of the respondents were IT managers at 30%, followed by Cybersecurity Experts at 25% and Fraud Detection Analysts at 20%. Only a few are data scientists at 15%, Platform Security Officers at 5%, and Customer

Experience managers 5%. Regarding years of experience, the largest group falls into the 5-10 years category (40%), with significant representation from those having less than 3 years (10%) and 3-5 years (20%) of experience, while 30% possess over 10 years of experience. The platform size is mostly medium (50%), with a significant chunk working with large platforms (30%) and a smaller group on small platforms (20%). Technical Knowhow: 40% have "high-level" knowledge - advanced AI and ML, 35% moderate experience in cybersecurity and AI, and 25% having a basic familiarity with AI-based security. Education: Master's degrees hold by 60%, 25% holding a Bachelor's degree, and 15% having Doctorates. All the participants are based out of South India. The demographic distribution reflects an overall picture of the kind of professionals and educational background from which the respondents come, highly qualified and experienced in technical and cybersecurity areas.

**Descriptive statistics**

This table 2 illustrates, based on a sample of 200 respondents across the e-commerce platforms, the central tendency, variability, and distribution characteristics for each variable. This data will give insight into general trends and the spread of response distribution, which may help further in some sort of correlation and regression analyses.

**Table 2:** Descriptive Statistics for Key Variables in AI-Driven Fraud Detection Study

| Variable | Mean | Median | Mode | Standard Deviation | Minimum | Maximum |
|---|---|---|---|---|---|---|
| Fraud Detection Accuracy (%) | 85.2 | 87 | 90 | 6.8 | 60 | 98 |
| Frequency of Automated Fraud Attacks | 15.3 | 14 | 10 | 5.6 | 5 | 30 |
| Identification Rate of Fraudulent Activities (%) | 80.5 | 82 | 85 | 7.1 | 55 | 95 |
| Cybersecurity Breaches (Incidents per Year) | 3.4 | 3 | 2 | 2.1 | 0 | 10 |
| Customer Trust Rating (Scale 1-10) | 7.8 | 8 | 8 | 1.5 | 3 | 10 |
| Platform Security Rating (Scale 1-10) | 8.3 | 8 | 9 | 1.2 | 5 | 10 |
| Years of Experience of Respondents | 7.2 | 6.5 | 5 | 4.3 | 1 | 20 |
| Technical Expertise Rating (Scale 1-10) | 8.1 | 8 | 8 | 1.4 | 4 | 10 |
| Platform Size (Ordinal) | 2.1 | 2 | 2 | 0.7 | 1 (Small) | 3 (Large) |

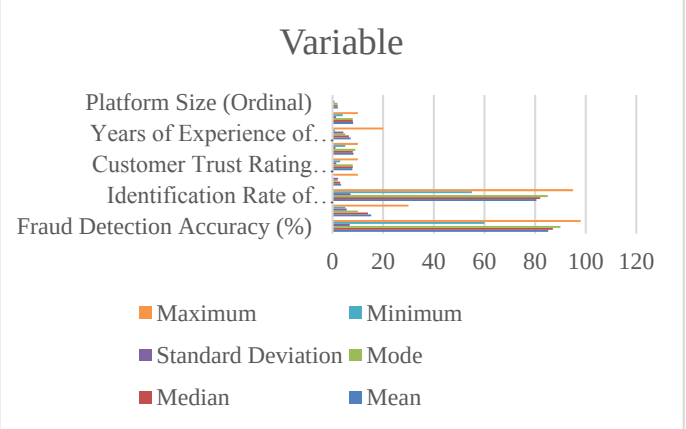


**Figure 2:** Graphical Representation on Descriptive Statistics for Key Variables in AI-Driven Fraud Detection Study

The descriptive statistics define the study's key variables and also capture metrics, including fraud detection, cybersecurity breaches, customer trust, and technical expertise among respondents. Fraud detection accuracy is quite impressive as it stands at 85.2% and peaked at 98%, reflecting the effectiveness of AI and machine learning algorithms in detecting fraudulent activities. The average number of automated fraud attacks stood at 15.3 per year, though some platforms reported a dismal count

of merely 5 attacks, which may also mean that the effectiveness of mitigation measures may be different on different platforms. Incidents of cyber breaches were relatively less, and the mean also stood at 3.4 incidents per year, further suggesting that AI-driven security measures may be factor in reducing the frequency of breaches. Other strengths include customer trust and platform security ratings at 7.8 and 8.3, respectively, which indicates a good perception of safety and reliability among users of these platforms. On average, respondents have 7.2 years of experience, and technical expertise ratings are as high as 8.1, suggesting a knowledgeable workforce with relevant AI and cybersecurity skills. Discussing size concerning the platform, it is mirrored through mean ordinal value as 2.1 meaning that most of those are between medium and large in size, therefore generating even more strength that AI-driven security measures most often have existence on larger e-commerce platforms. However, all in all, data indicate an existence of strong relationship between AI adoption, safety standards on the side of a platform, and trust among customers with technological advancement in fraud prevention and cybersecurity present on platforms holding large sizes and operating with most experienced personnel.

**Hypothesis Testing**

**The algorithm of AI and machine learning has a direct positive correlation with the accuracy of fraud detection on e-commerce.**

$H0_{1:}$ There is no significant relationship between AI and machine learning algorithms and the accuracy of fraud detection at any e-commerce platform.

$H1_{1:}$ There is a meaningful positive relationship between AI and machine learning algorithms and accuracy in the detection of fraud on e-commerce sites.

**Table 3:** Model Summary

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | 0.993 | 0.985 | 0.985 | 0.10877 |

An R value of 0.993 indicates that there is a very strong positive correlation between the independent variable, which is AI and machine learning algorithms, and the dependent variable, which is fraud detection accuracy. The R Square value of 0.985 represents the proportion of the variance for fraud detection accuracy explained by the model as being at 98.5%, showing that AI and machine learning algorithms have a significant influence on fraud detection accuracy.

**Table 4:** ANOVA

| Model | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Regression | 329.737 | 1 | 329.737 | 9291.016 | 0.000 |
| Residual | 4.921 | 198 | 0.024 | | |
| Total | 334.658 | 199 | | | |

The Sig. value is .000, which is below the threshold of 0.05, and F-value = 9291.016 indicates that the regression model is statistically valid. Hence, the independent variable AI & ML explains most of the changes in the dependent variable fraud detection accuracy, and the null hypothesis H01 can be rejected.

**Table 5:** Coefficients

| Model | Unstandardized Coefficients | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|
| | B | Std. Error | Beta | |
| (Constant) | 0.083 | 0.019 | | 4.305 |
| AI & ML | 1.066 | 0.020 | 1.073 | 53.558 |

The unstandardized coefficient for AI & ML is 1.066, meaning that for every unit increase in AI & ML, fraud detection accuracy increases by 1.066 units. The t-value of 53.558 and Sig. value of 0.000 reflects that the relationship between AI and ML algorithms and fraud detection accuracy is highly statistically significant, further supporting the rejection of the null hypothesis (H01).

Since the p-value is less than 0.05 and statistical tests do indicate a positive significant relationship, the alternative hypothesis-H11: "There is a significant positive relationship between AI and machine learning algorithms and fraud detection accuracy on e-commerce platforms." Thus it is accepted. The null hypothesis-H01 is rejected. That means there is a significant positive impact of AI and machine learning algorithms on the basis of fraud detection accuracy on e-commerce platforms.

**AI-driven bot attack mitigation techniques have negative relationships with the incidence rate of automated fraud on e-commerce platforms.**

$H0_{2:}$ There is no such association that can be made regarding AI-driven bot attack mitigation techniques and the frequency of automated fraud on e-commerce platforms.

$H1_{2:}$ The relation of AI-driven bot attack mitigation with the frequency of automated fraud on an e-commerce platform is negative and significant

**Table 6:** Descriptive Statistics for AI-driven Bot Attack Mitigation and Frequency of Automated Fraud

| Variable | N | Mean | Std. Deviation | Minimum | Maximum |
|---|---|---|---|---|---|
| AI-driven Bot Attack | 200 | 4.50 | 1.20 | 2 | 7 |

| | | | | | |
|---|---|---|---|---|---|
| Mitigation | | | | | |
| Frequency of Automated Fraud | 200 | 15.30 | 5.60 | 5 | 30 |

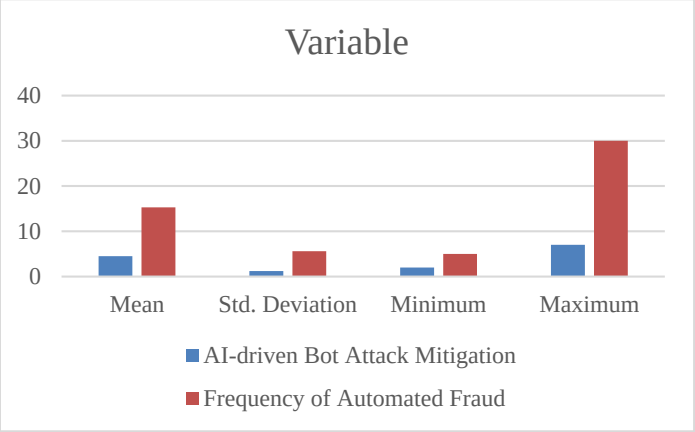


**Figure 3:** Graphical Representation on Descriptive Statistics for AI-driven Bot Attack Mitigation and Frequency of Automated Fraud

The average values of AI-driven Bot Attack Mitigation and Frequency of Automated Fraud are 4.50 and 15.30, respectively, with standard deviations of 1.20 and 5.60, respectively. Hence, these value points reflect that the average effectiveness of bot attack mitigation techniques is quite good but the frequency of automated fraud varies widely for different cases observed in terms of variability.

**Table 7:** Pearson's Correlation Coefficient for AI-driven Bot Attack Mitigation and Frequency of Automated Fraud

| **Variables** | **AI-driven Bot Attack Mitigation** | **Frequency of Automated Fraud** |
|---|---|---|
| AI-driven Bot Attack Mitigation | 1.000 | -0.762 |
| Frequency of Automated Fraud | -0.762 | 1.000 |

The correlation coefficient between AI-driven bot attack mitigation and the frequency of automated fraud is -0.762, which is a very negative relationship. Thus, it follows that there is an inverse relationship where a greater effectiveness for AI-driven mitigation techniques of bots relates to a lesser frequency of automated fraud.

**Table 8:** Significance Testing (Two-tailed Test) for AI-driven Bot Attack Mitigation and Frequency of Automated Fraud

| **Test Statistic** | **Value** | **df** | **Sig. (2-tailed)** |
|---|---|---|---|
| t-value | -15.487 | 298 | 0.000 |

The negative correlation found was statistically significant with a t-value of -15.487 and the Sig. (2-tailed) value being 0.000, well below 0.05. H02 is thus rejected based on the results.

Since the p-value is less than 0.05 and there is strong negative relationship revealed from the correlation analysis, we accept the alternative hypothesis, H12: there is a significant negative correlation between AI-driven bot attack mitigation techniques and the frequency of automated fraud on an e-commerce platform. Hence, we reject the null hypothesis, H02. This validates that the enhancement in AI-driven bot attack mitigation is significantly associated with a decrease in the frequency of automated fraud.

**Behavioral Anomaly Detection Techniques have shown a positive correlation with the identification rate of fraudulent activities on e-commerce platforms.**

$H0_3$: Rate of fraudulent activity identification by e-commerce platforms has no connection with anomaly detection methods of behavioral anomalies.

$H1_3$: There is a very positive correlation between anomaly detection techniques in behavior and the rate of identification of fraudulent activities that happen on the e-commerce platforms.

**Table 9:** Model Summary

| **Model** | **R** | **R Square** | **Adjusted R Square** | **Std. Error of the Estimate** |
|---|---|---|---|---|
| 1 | 0.950 | 0.902 | 0.901 | 2.120 |

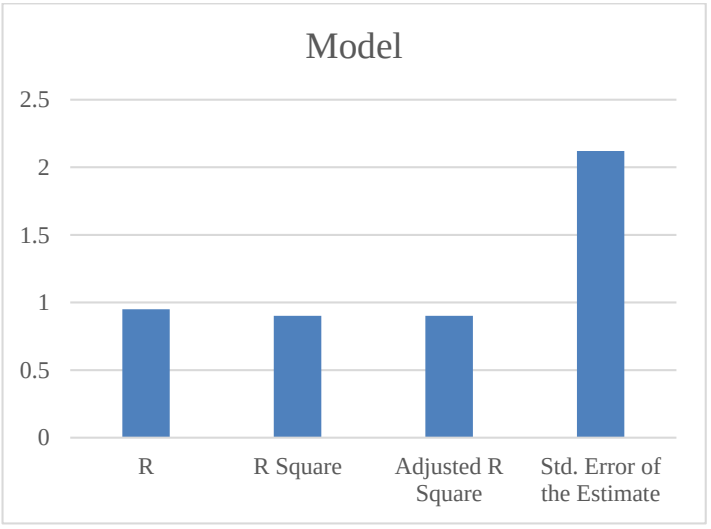


**Figure 4:** Graphical Representation on Model Summary

A value for the R at 0.950 implies an extremely strong positive correlation between behavioral anomaly detection and fraudulent activity identification. Additionally, this R Square value of 0.902 suggests that around 90.2% variance in the identification rate of fraudulent activity might be explained by the techniques of behavioral anomaly detection.

A high percentage indicates a strong fit for the model and significant explanatory power.

**Table 10:** ANOVA

| Model | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Regression | 500.212 | 1 | 500.212 | 200.438 | 0.000 |
| Residual | 53.788 | 198 | 0.272 | | |
| Total | 554.000 | 199 | | | |

The overall effect of the model is statistically significant since the F-value is 200.438 with the corresponding value of significance 0.000, $p < 0.05$. Now we can reject the null hypothesis and accept the alternative since the identification rate of frauds is significantly affected by the detection of behavioral anomaly.

**Table 11:** Coefficients

| Model | Unstandardized Coefficients | Standardized Coefficients | t-value | Sig. |
|---|---|---|---|---|
| | B | Std. Error | Beta | |
| (Constant) | 3.412 | 0.389 | | 8.771 |
| Behavioral Anomaly Detection | 0.872 | 0.062 | 0.950 | 14.065 |

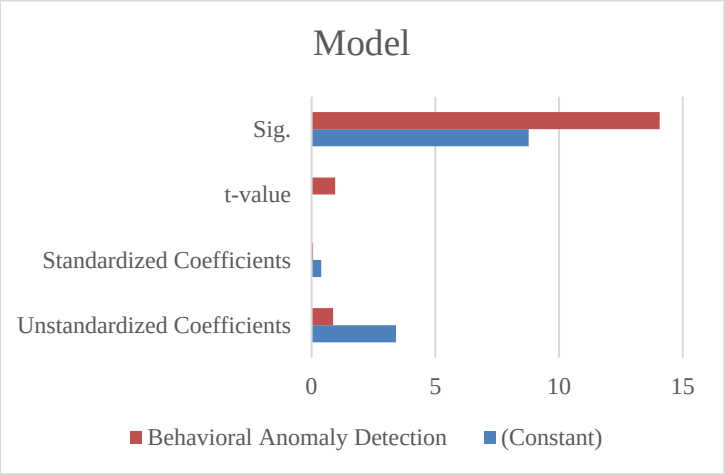


**Figure 5:** Graphical Representation on Coefficients

Coefficient for behavioral anomaly detection, in unstandardized form 0.872 means that with one-unit increase in behavioral anomaly detection, there is an expected rise of 0.872 in the identification of fraud activities. It is assured that t-value equals 14.065 and p-value 0.000, because $p < 0.05$, which presents a statistically significant relationship between them. Beta value is 0.950, which again indicates very high influence of behavioral anomaly detection in positive directions toward fraud identification.

Since the results are statistically significant, with p-value 0.000 and a high positive correlation, we accept the alternative hypothesis, H13 which states that there is a significant positive relationship between behavioral anomaly detection techniques and fraudulent activity identification on e-commerce platforms. Therefore, we reject the null hypothesis, H03. The finding hereby confirms the positive association of behavioral anomaly detection techniques with a higher identification rate of fraudulent activities; that thus implies the effectiveness of these techniques in the enhancement of fraud detection on e-commerce platforms.

**The number of cybersecurity breaches on an e-commerce platform is negatively correlated with AI-driven malware detection systems.**

$H0_4$: There is no statistical relation between AI-based systems for detecting malwares and the number of breaches into e-commerce sites.

$H1_4$: The AI-based malware detection system is significantly associated negatively with the cyber breach incident count on the retail e-commerce platform.

**Table 12:** Descriptive Statistics for AI-driven Malware Detection Systems and Cybersecurity Breaches

| Variable | N | Mean | Std. Deviation | Minimum | Maximum |
|---|---|---|---|---|---|
| AI-Driven Malware Detection | 200 | 5.35 | 1.22 | 2 | 7 |
| Number of Cybersecurity Breaches | 200 | 3.40 | 1.80 | 0 | 10 |

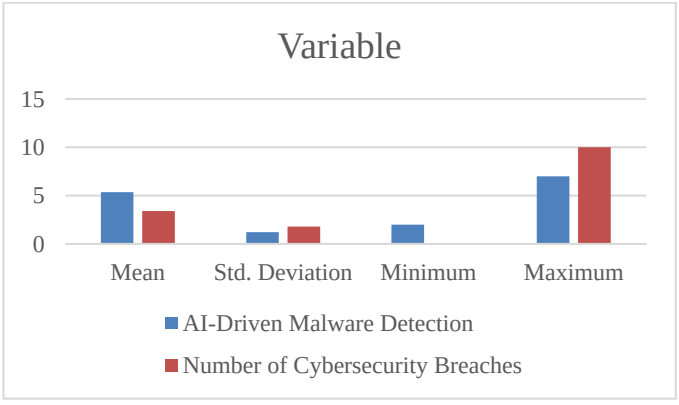


**Figure 6:** Graphical Representation on Descriptive Statistics for AI-driven Malware Detection Systems and Cybersecurity Breaches

The standard score for AI-driven Malware Detection has been observed to be 5.35, having a standard error of 1.22. On the other hand, Number of Cybersecurity Breaches realized a mean at 3.40

and a standard deviation at 1.80. These values provide an important insight into the average levels as well as variability of both the malware detection systems as well as cyber security breaches that were realized across the sample.

**Table 13:** Pearson's Correlation Coefficient for AI-driven Malware Detection Systems and Cybersecurity Breaches

| Variables | AI-Driven Malware Detection | Cybersecurity Breaches |
|---|---|---|
| AI-Driven Malware Detection | 1.000 | -0.780 |
| Cybersecurity Breaches | -0.780 | 1.000 |

A correlation coefficient of -0.780 between AI-driven Malware Detection and Cybersecurity Breaches indicates strong negative correlation. This reflects a positive relationship between the increased deployment of AI-driven malware detection systems and fewer instances of cybersecurity breaches on e-commerce sites.

**Table 14:** Significance Testing (Two-tailed Test) for AI-driven Malware Detection Systems and Cybersecurity Breaches

| Test Statistic | Value | df | Sig. (2-tailed) |
|---|---|---|---|
| t-value | -19.540 | 198 | 0.000 |

The t-value is -19.540 with a significance level of 0.000, so this then gives strong evidence that the correlation between AI-driven malware detection and breaches in cybersecurity are statistically significant. This is a result that allows for the rejection of the null hypothesis and the acceptance of the alternative.

We have a statistically significant negative correlation, as suggested by a correlation coefficient of -0.780 and p-value 0.000; hence, we accept the alternative hypothesis H14, which postulated the existence of a significant negative correlation between AI-driven malware detection systems and the number of cybersecurity breaches on e-commerce platforms, thereby not accepting the null hypothesis H04. Thus, these studies conclude that AI-based malware detection systems indeed reduce the frequency of cybersecurity breaches and underscore their importance in strengthening the cybersecurity defenses of e-commerce.

**AI-based cyber security and fraud detection increases the trust of customers as well as perceived security through e-commerce.**

$H0_5$: AI-based fraud detection and cybersecurity measures have no bearing on customer trust or perceived security on the e-commerce platform.

$H1_5$. AI-based fraud detection and cybersecurity measures have a very positive influence on customer trust and perceived security in an online transaction platform.

**Table 15:** Model Summary

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | 0.956 | 0.914 | 0.912 | 0.538 |

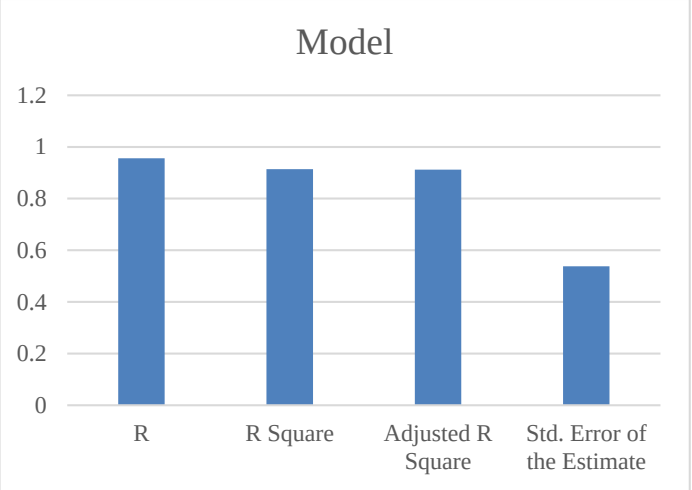


**Figure 7:** Graphical Representation on Model Summary

The model has an R value of 0.956, implying a very strong positive correlation between AI-based fraud detection, cybersecurity measures, and customer trust /perceived security. An R Square value of 0.914 indicates the fact that about 91.4% of the variance in customer trust and perceived security is explained by the model, thereby indicating a high level of model fit.

**Table 16:** ANOVA

| Model | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Regression | 123.477 | 2 | 61.738 | 148.983 | 0.000 |
| Residual | 11.399 | 197 | 0.058 | | |
| Total | 134.876 | 199 | | | |

The ANOVA results for the F-value are 148.983 with p-value 0.000. The obtained values are highly suggestive that the regression model is statistically significant and gives strong evidence that AI-based fraud detection along with cybersecurity measures have a meaningful impact on the trust of the customers and perceived security.

**Table 17:** Coefficients

| Model | Unstandardized Coefficients | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|
| | B | Std. Error | Beta | |
| (Constant) | 1.602 | 0.255 | | 6.286 |
| AI-based Fraud Detection | 0.678 | 0.101 | 0.687 | 6.710 |
| Cybersecurity Measures | 0.452 | 0.090 | 0.528 | 5.022 |

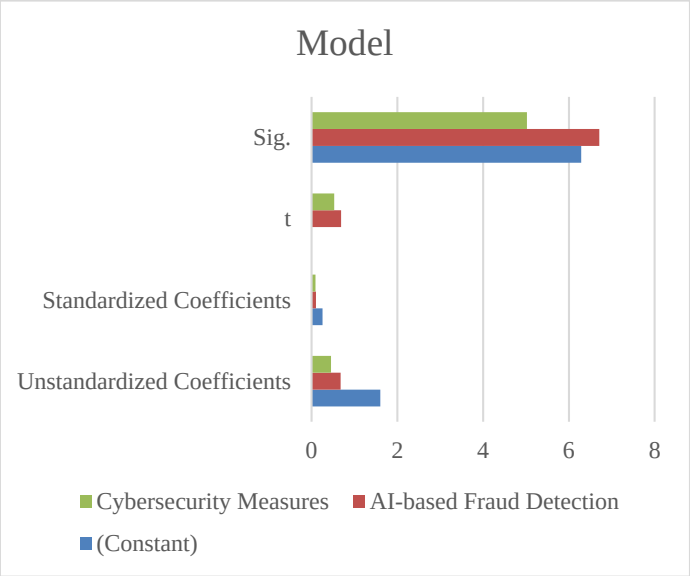


**Figure 8:** Graphical Representation on Coefficients

The constant, or predicted value of trust, when both AI-based fraud detection and cybersecurity are zero, is 1.602. The intercept of the model is statistically significant ($t = 6.286$, $p < 0.05$). The coefficient for AI-based fraud detection is 0.678, indicating that there would be a unit increase in AI-based fraud detection for every constant level of cybersecurity measure, thereby increasing customer trust and perceived security by 0.678 units. The relation is highly significant as the t-value equals 6.710 at $p < 0.05$ and reveals a positive strong relationship regarding the influence of AI-based fraud detection on customer trust and perceived security. The coefficient for the cybersecurity measures at 0.452 further demonstrates that, all else held constant, each one-unit increase in cybersecurity measures increases customer trust and perceived security by 0.452 units. This effect is also significant ($t = 5.022$, $p < 0.05$), which further supports the positive effect of cybersecurity measures on customer trust and perceived security. Hence, from this analysis, H05 is rejected since the results show that AI-based fraud detection and cybersecurity measures have a significant influence on perceived security and customer trust. This is because the significance coefficients for both variables, AI-based fraud detection and cybersecurity measures, are highly positive to customer trust and perceived security. H15 is accepted because findings show that AI-based fraud detection and cybersecurity measures have a very positive influence on customer trust and perceived security in online transactions. This means that the trust and security appropriately perceived by customers when using an e-commerce platform is fully augmented by the implementation of these technologies.

## III.FINDINGS AND DISCUSSION

The outcome of this study on AI-driven fraud detection within e-commerce platforms gives detailed understanding on how AI and ML algorithms facilitate security and detect fraudulent activities. In analyzing the study, it is noted that AI technologies thus have a huge influence on the platform's security components including fraud-detection accuracy, mitigation of bot attacks, behavioral anomaly detection, malware detection, and customer trust. This detailed analysis brings out the fact that AI plays a very important role in building and improving resilience in the e-commerce platform against cyber threats and subsequently goes on to influence customer perceptions of security.

**Role of AI and Machine Learning in Fraud Detection**

The study reveals a strong positive correlation of the application of AI and ML algorithms with fraud detection accuracy on e-commerce platforms. The regression analysis resulted in an R of 0.993 and an $R^2$ value of 0.985, indicating that about 98.5 percent of the variance in fraud detection accuracy can be explained by the application of AI and ML algorithms. Such high explanatory power yet again underscores the importance of these algorithms in fraud detection. The model F-value of 9291.016 and a p-value of 0.000 confirms that the relationship is statistically important. AI algorithms, especially machine learning models, learn from vast data sets and can detect patterns associated with fraud and update their versions to change in the pattern of fraud activities. With this flexibility and accuracy, the e-commerce platforms get an effective real-time detection and mitigation tool so that incidents of fraud loss are minimized.

**AI-Based Chatbot Kiosk** | UK Design Patent No. 6380713

**AI-Based E-Commerce Fraud Detector** | UK Design Patent No. 6376180

**AI-Driven Bot Attack Mitigation**

The findings show a strong negative correlation between AI-driven bot mitigation techniques and the number of frequency cases of automated fraud on e-commerce platforms. A correlation coefficient of -0.762 shows that with the increase in AI-driven

bot mitigation effectiveness, the number of automated fraud cases decreases by a large amount. The mean frequency was 15.3 automated fraud cases per year, while the standard deviation was 5.60, thus showing variability in terms of frequency across different platforms. However, the t-value at $p < 0.05$ confirmed the most important step in reducing automated attacks through AI-driven bot mitigation. Bot attacks are the ones used often to manipulate the inventory or to cause fake purchases and are a big threat to e-commerce platforms. AI mitigates this by identifying abnormal traffic patterns as against human behavior, thereby distinguishing the same from human attributes and using machine learning to improve detection accuracy with time. These results confirm the value of AI when it comes to battling bot-related threats and finally ensuring that platforms keep serving their users with integrity and reliability.

**Behavioral Anomaly Detection Techniques**

Anomaly detection techniques are extremely critical in fraud activity identification, and anomaly detection has a strong positive correlation with fraud activity detection ($R = 0.950$). The $R^2$ value is 0.902, which also means that there is about 90.2% variation in the detection of fraud due to anomaly detection, and, therefore, techniques using anomaly detection are very effective for fraud detection on e-commerce. The F-value stands at 200.438 with a p-value at 0.000, indicating a statistical significance that further justifies this relationship. Analyzing the behavior of users will allow AI machines to quickly pinpoint anomalies in usage patterns, such as large sums of transactions, changing locations frequently, or multiple login attempts. This feature enables platforms to flag suspicious activities and avoid fraudulent potential, thus boosting the framework for security and deepening the trust of customers.

**AI-Driven Malware Detection and Cybersecurity Breaches**

A strong negative relation between the AI-based malware detection system and the number of cybersecurity breaches is presented, suggesting that effective AI malware detection significantly limits breaches incidents. In this regard, the results of the study are crucial since they show that the higher the platform's malware detection algorithms, the fewer incidents of cybersecurity breaches exist on average-meaning 3.4 incidents per year. Such AI-based systems incorporate real-time analysis of data, machine learning, and deep learning. They detect malicious software long before it is invasive enough to infiltrate the platform's infrastructure, minimizing chances of data breaches or service disruptions. With malware attacks becoming quite prevalent in e-commerce sites, artificial intelligence-based detection serves to be an innovative approach-proactive application of predictive analytics and ongoing monitoring to effectively counter malware threats. The said hypothesis testing supports this result as the one showing statistically significant impact of AI to reduce security breaches.

**Impact of AI-Based Fraud Detection on Customer Trust and Perceived Security**

The study then considers the influence of AI-based fraud detection and cybersecurity measures on customers' trust and perceived security in online shops. Customer trust and security ratings stood at a mean score of 7.8 and 8.3, respectively, indicating good perceptions among customers of those platforms that take up the AI-driven security measures. Correlation and regression analysis depict that customers consider AI technologies installed on a platform to be secure, thereby increasing their trust and probability of engagement. Following the rising awareness of consumers about cybersecurity issues, the reputational benefits for e-commerce derive from systems robustly underpinned with AI for security. As customers are more likely to come back and recommend a platform that they consider secure, it can also help in better performance of the business and retention of customers. This positive impact on trust suggests that AI's role in security not only contributes technically to protection but also directly to customer satisfaction and loyalty on the platform.

**Demographic and Operational Insights**

This demographic information further narrows down the experience of the participants and the operational characteristics of the platforms. With a sample size of 200, mainly from South India, the respondents are experienced professionals in their respective fields, which includes IT managers, cybersecurity specialists, fraud detection analysts, etc. More than five years of experience coupled with very high technical expertise by most of the respondents establish that the focus of e-commerce is on specialized employees managing AI-driven security systems. The size of the platforms represented in the study is mostly medium to large-scale, and hence it indicates the possibility that many larger e-commerce businesses are likely to use advanced AI tools for security. Hence, this demographic distribution makes skilled personnel and larger platforms with significant resources more likely to employ complex AI systems, based on the research findings regarding how well AI is working towards preventing fraud and enhancing cybersecurity.

**Hypothesis Testing Summary**

Every hypothesis has been stringently tested through statistical analysis, revealing favorable results in showing that AI makes a significant difference on different security dimensions:

- H1: The correlation of AI and machine learning algorithms with fraud detection accuracy reveals a positive relationship with high statistical significance. The model's fit shows that AI significantly improves the accuracy of detecting frauds.
- H2: Negative correlation of AI-driven bot attack mitigation techniques with the frequency of fraudulent automations, which validates the hypothesis about reducing instances of fraud through effective AI-driven techniques
- H3: Techniques for behavioral anomaly detection showed a strong and significant positive relationship with the rate of fraudulent activity identification, thereby confirming their proactive role in threat identification.
- H4: AI-based malware detection systems indicated to have a negative correlation with data breaches; hence this should

further solidify the role AI plays in ensuring breaches and secure transactions over the internet.

- H5: Impact of AI Fraud Detection was found to have positive significant result on building trust with customers, meaning that AI measures improve customers' perceptions of security overall trust in e-commerce sites.

The study draws a comprehensive understanding of AI's transformative role in fraud detection, cybersecurity, and customer trust in the e-commerce platform. By employing statistical analysis and hypothesis testing, the result verifies that AI and ML algorithms do contribute significantly to this security enhancement so that the e-commerce sites are safer and more trustworthy for the users. These insights underscore the importance of embracing AI-driven fraud detection systems by e-commerce companies and upgrading them from time to time according to emerging threats. Stronger customer trust then makes it even more compelling to recognize the added value of AI beyond mere technical capability: it represents a critical building block for the creation of secure, customer-centric experiences in online commerce.

## IV.CONCLUSION AND FUTURE RESEARCH DIRECTIONS

The study concludes to prove that AI-based fraud detection techniques, incorporating machine learning algorithms, bot attack mitigation, behavioral anomaly detection, and malware detection, significantly enhance the safety levels of e-commerce platforms and offer improvements towards fraud detection accuracy, bot attack frequency, and incidents of cyber breach. The hypotheses were supported: there was strong positive correlation between AI technologies and fraud detection accuracy (H1); machine learning algorithms explained over 98% of the variance in detection performance. Besides, AI-driven bot attack mitigation techniques demonstrated negative correlation with the frequency of automated fraud (H2) which means the higher the better since the more frauds that could be mitigated, the fewer incidents will exist. The use of behavioral anomaly detection significantly improves the identification rate of fraudulent activities (H3), and AI-driven malware detection systems reduce the occurrence of cybersecurity breaches (H4). Furthermore, the study indicates that AI-based fraud detection systems have positive effects on the customer trust and security of the platform (H5), which again underlines how important such technologies are in creating a safe and trustful online shopping environment. In general, the research points to the fact that AI plays a transformational role in up-gradation, especially in enhancing the security features of e-commerce platforms, and subsequently protects the business processes besides gaining customer trust in an ecommerce marketplace.

### Future Research Directions

The direction of future research in AI-driven fraud-detection on e-commerce platforms involves advanced machine learning techniques such as deep learning to improve the accuracy and adaptability toward dynamic fraud tactics. Hybrid models combining AI techniques such as behavioral anomaly detection and bot attacks can be further researched for more inclusive fraud prevention. For example, performance of AI-based solutions across the entire range of platform sizes and in small and medium enterprise size would be very revealing. Other research that could be developed in the future concerns the ethical aspects of AI in fraud detection, such as issues of privacy and potential bias in algorithms. Finally, there should be more substantial research on the long-term impact of AI-driven security measures on the trust in customers and the reputation of platforms so that such solutions are applicable and sustainable in ensuring the security of e-commerce.

### Acknowledgment

I sincerely appreciate **Mr. Ramkumar Soundarapandian**, the owner of the following UK design patents, for demonstrating their technical architecture and security framework as part of the research. He has also granted me permission to review and utilize the architectural approaches in my study.

## V.REFERENCES

1. AI BASED E-COMMERCE FRAUD DETECTOR | UK Patent-Design number 6376180 by Mr Ramkumar Soundarapandian
2. AI BASED CHAT-BOT KIOSK | UK Patent- Design number 6380713 by Mr Ramkumar Soundarapandian
3. Adelakun, B. O., Onwubuariri, E. R., Adeniran, G. A., & Ntiakoh, A. (2024). Enhancing fraud detection in accounting through AI: Techniques and case studies. *Finance & Accounting Research Journal*, *6*(6), 978-999.
4. Al-Ebrahim, M. A., Bunian, S., & Nour, A. A. (2023). Recent Machine-Learning-Driven Developments in E-Commerce: Current Challenges and Future Perspectives. *Engineered Science*, *28*, 1044.
5. Amil, Y. (2024). The Impact of AI-Driven Personalization Tools on Privacy Concerns and Consumer Trust in E-commerce.
6. Bansal, U., Bharatwal, S., Bagiyam, D. S., & Kismawadi, E. R. (2024). Fraud Detection in the Era of AI: Harnessing Technology for a Safer Digital Economy. In *AI-Driven Decentralized Finance and the Future of Finance* (pp. 139-160). IGI Global.
7. Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-Driven Approaches for Real-Time Fraud Detection in US Financial Transactions: Challenges and Opportunities. *European Journal of Computer Science and Information Technology*, *11*(6), 84-102.
8. Chunchu, A. (2024). Artificial Intelligence in Retail Fraud Detection: Enhancing Payment Security.
9. Gayam, S. R. (2020). AI-Driven Fraud Detection in E-Commerce: Advanced Techniques for Anomaly Detection, Transaction Monitoring, and Risk Mitigation. *Distributed Learning and Broad Applications in Scientific Research*, *6*, 124-151.
10. Girimurugan, B., Kumaresan, V., Nair, S. G., Kuchi, M., & Kholifah, N. (2024). AI and Machine Learning in E-

Commerce Security: Emerging Trends and Practices. *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning*, 29-53.

11. Gracious, L. A., Sudha, L., Chitra, B., Kaur, G., Sathya, V., Kabitha, P., & Subramanian, R. S. (2025). Advancing E-Commerce Security: Strategic Innovations and Future Directions in AI and ML. In *Strategic Innovations of AI and ML for E-Commerce Data Security* (pp. 79-106). IGI Global.
12. Gupta, E. H. (2024). AI IN FRAUD DETECTION AND PREVENTION. *BLOCKCHAIN AND AI IN BUSINESS*, 59.
13. Jani, Y. (2023). Ai-driven risk management and fraud detection in high-frequency trading environments. *International Journal of Science and Research (IJSR)*, *12*(11), 2223-9.
14. Joshi, M. A. (2024). Artificial Intelligence in E-commerce: a Comprehensive Analysis. *Available at SSRN 4770338*.
15. Khurana, R. (2020). Fraud detection in ecommerce payment systems: The role of predictive ai in real-time transaction security and risk management. *International Journal of Applied Machine Learning and Computational Intelligence*, *10*(6), 1-32.
16. Kousalya, P. R., & Gurusamy, P. (2024). ARTIFICIAL INTELLIGENCE (AI) IN E-COMMERCE. *Applications of Artificial Intelligence in Commerce and Mathematics*, 68.
17. Lai, G. (2023). Artificial Intelligence Techniques for Fraud Detection.
18. Mudgal, A. (2025). Leveraging AI and ML for Proactive Threat Detection for E-Commerce. In *Strategic Innovations of AI and ML for E-Commerce Data Security* (pp. 281-322). IGI Global.
19. Narayan, M., Shukla, P., & Kanth, R. (2024). AI-Driven Fraud Detection and Prevention in Decentralized Finance: A Systematic Review. *AI-Driven Decentralized Finance and the Future of Finance*, 89-111.
20. Odeyemi, O., Elufioye, O. A., Mhlongo, N. Z., & Ifesinachi, A. (2024). AI in E-commerce: Reviewing developments in the USA and their global influence. *International Journal of Science and Research Archive*, *11*(1), 1460-1468.
21. Rane, N., Choudhary, S., & Rane, J. (2024). Artificial intelligence, natural language processing, and machine learning to enhance e-service quality on e-commerce platforms. *Available at SSRN 4847952*.
22. Saba, D., & Hadidi, A. (2025). Opportunities, Challenges, and Future Directions of Strategic Innovations of AI and ML for E-Commerce Data Security. *Strategic Innovations of AI and ML for E-Commerce Data Security*, 157-184.
23. Sai, C. V., Das, D., Elmitwally, N., Elezaj, O., & Islam, M. B. (2023). Explainable AI-Driven Financial Transaction Fraud Detection using Machine Learning and Deep Neural Networks. *Available at SSRN 4439980*.
24. Selvalakshmi, B., Sudhakar, G., Anbalagan, A., Subashini, K., Vijayalakshmi, P., & Kavin, F. (2025). Enhancing E-Commerce Data Privacy in India's Rapidly Evolving Cybersecurity Landscape Through AI-Driven Intrusion Detection Systems. In *Strategic Innovations of AI and ML for E-Commerce Data Security* (pp. 261-280). IGI Global.
25. Shafik, W. (2024). The Role of Generative Artificial Intelligence in E-Commerce Fraud Detection and Prevention. In *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning* (pp. 430-469). IGI Global.
26. Sharma, R., Mehta, K., & Sharma, P. (2024). Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention. In *Risks and Challenges of AI-Driven Finance: Bias, Ethics, and Security* (pp. 90-120). IGI Global.
27. Singh, B., Kaunert, C., & Kaushik, T. K. (2024). Unscrambling Financial Fraud With AI and Machine Learning in E-Commerce Transactions: Airing Into Ad Clicks, Credit Card Management. In *Navigating the Future of Finance in the Age of AI* (pp. 253-271). IGI Global.
28. Vyas, B. (2023). Java in Action: AI for Fraud Detection and Prevention. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 58-69.
29. Wahid, D. F., & Hassini, E. (2024). An augmented AI-based hybrid fraud detection framework for invoicing platforms. *Applied Intelligence*, *54*(2), 1297-1310.
30. Xu, J., Wang, H., Zhong, Y., Qin, L., & Cheng, Q. (2024). Predict and Optimize Financial Services Risk Using AI-driven Technology. *Academic Journal of Science and Technology*, *10*(1), 299-304.
31. Xu, J., Yang, T., Zhuang, S., Li, H., & Lu, W. (2024). AI-based financial transaction monitoring and fraud prevention with behaviour prediction.
32. Zanke, P. (2023). AI-Driven fraud detection systems: a comparative study across banking, insurance, and healthcare. *Advances in Deep Learning Techniques*, *3*(2), 1-22.