Kuwait Journal of Machine Learning
ISSN: 2984-7672
Vol. 3 No. 2 (2024)

Implementing Account Takeover and Phishing Detection Models to Mitigate E-Commerce Fraud

Bhageerath Bogi

Independent Researcher,USA.

1. Introduction

The rise of e-commerce has rapidly changed the operating way of businesses, but simultaneously, it has opened up numerous avenues for fraud, it has been noticed through account takeovers and phishing attacks. These means of cybercrime can thus lead to a significant financial loss and reputation damage to online retailers. With the rising growth of online platforms comes the sophistication of fraudsters. One of the objectives behind this research is developing and analyzing models that can easily discover account takeovers and real-time phishing attempts on the systems to establish whether it is feasible to apply the high-end detection models integrated with machine learning techniques for dimming e-commerce frauds. The research consists of the following structure such as it features a literature review that provides a background overview of the problem then it consists of methods of how models are designed and evaluated. It also provides results on performance followed by discussions on effectiveness. It provides an overall outcome of the research to pinpoint key findings and directions for future research.

2. Literature Review

2.1 AI-Driven Fraud Detection in E-Commerce using Risk Mitigations

According to the author Gayam *et al*.2020, it states that the primary objective of this research is to discuss the application of techniques used in Artificial Intelligence for the detection and mitigation of fraud cases, especially on account takeovers and phishing attacks. Machine learning models, such as anomaly detection and transaction monitoring effectiveness, were measured in real-time for fraudulent activities identification. This method comprised collecting data, designing models, and performance evaluation based on the selected key metrics. This study shows that the AI-driven models can significantly outperform the traditional method of fraud detection with high accuracy and flexibility. It is expected that these study results may reduce fraud cases and provide greater security for e-commerce. Future scope of this research would include integration of AI models with multi-layered security systems, continuous adaptation to emerging threats, and development of real-time detection systems for better proactive fraud prevention.

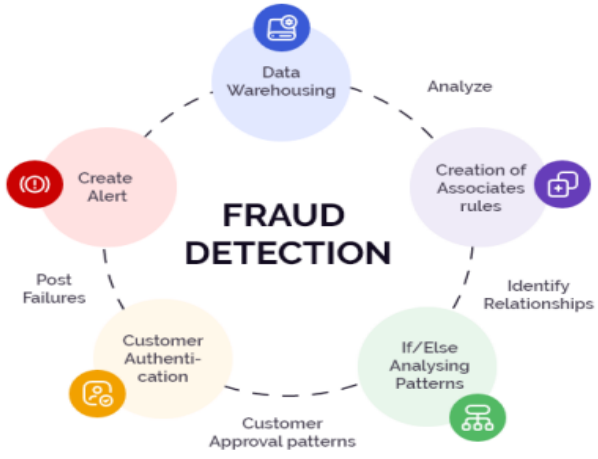

Figure 1: Fraud Detection

(Source: https://dlabi.org)

2.2 Prevention of Fraud in Electronic Payment Gateway Using Secret Code

According to the author Dhobe *et al*.2020, it states that it significantly focused on the techniques for fraud prevention of electronic payment gateways, mainly for transactions that are e-commerce in nature. It was basically an attempt to look into the role of encryption and secret code systems in guarding credit card and financial information from fraudulent transactions online. A review of current fraud detection systems, encryption technologies, and security protocols are the methods used. The outcomes revealed that although encryption greatly minimizes fraud risk, it still represents a system weakness in real-time detection and prevention. Furthermore, the results also considered the need for secure payment options as encryption evolved over time. Future scope will be to enhance the fraud detection systems with AI and ML to become more sensitive towards changes in threats and offer more proactive protection.

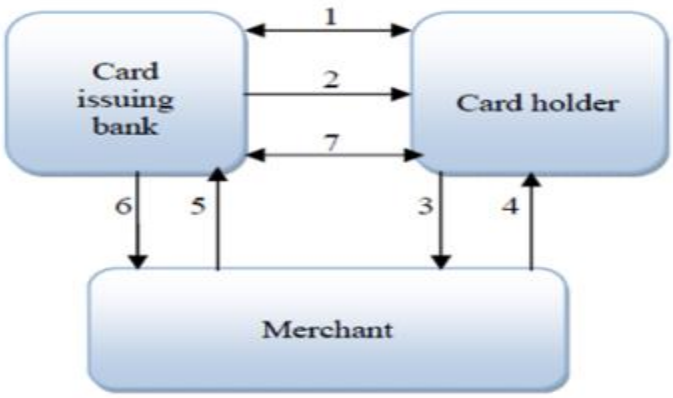

Figure 2: Credit Card Operation

(Source: https://www.ijresm.com)

2.3 Consumer-Facing Technology Fraud: Economics, Attack Methods and Solutions

According to the author Azad *et al*.2019, it states that this research aimed to analyze fraud in the various consumer-facing technologies including the Internet, mobile and traditional telecommunication services. The main objectives of this research were to analyze the fraud attack mechanisms, the effects on users and service providers and the systems currently used for fraud detection and prevention. This was based on detailed reviews of fraud cases, attack strategies and prevention techniques. The results revealed that while each technology had suffered some form of other type of fraud, there was an overall loss of massive amounts of data due to fraudulent practices. Outcomes points towards the requirement of improved detection mechanisms in fraud. Further development regarding the different aspects for fraud prevention is in integrating AI and machine learning for improved real-time detection and adaptive security measures.

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (%GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America & the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

Figure 3: Regional distribution of cybercrime

(Source: https://www.sciencedirect.com)

3. Methods

3.1. Data Collection and Data Sources

Data collection and data sources are the foundation on which prepaid account takeover and phishing detection models depend. Sources of data include transactions, user behavior data, and historical fraud cases from e-commerce platforms. Information such as login patterns, device information, and IP addresses provide insight into abnormal activities that might indicate takeover of an account. In accordance with it, user reports on emails, URLs, and phishing attempts can be collected to aggregate phishing-related data. Usually, the datasets are anonymized and preprocessed for the integrity and privacy of data. Some public datasets come from cybersecurity repositories such as anomaly detection datasets or phishing email datasets to train and validate the models (Hasham *et al*.2019). In the process, it will introduce the external threat intelligence sources which incorporate lists of known phishing websites and blacklisted IP addresses, enhancing data. Appropriate labeling is essential in supervised machine learning models, that is the best way for fraud detection as well as model training.

3.2. Designing Detection Models for Account Takeover and Phishing

It means that there is a design of detection models for account takeover and phishing, and appropriate machine learning algorithms have to be developed to detect fraudulent activities within an e-commerce platform. The focus will be on the models detecting anomalies in user login patterns, which include unusual IP addresses, rapid location changes, or simultaneous logins across different devices. These include decision trees, random forests, and neural networks. These are used on the basis of historical data, in the classification of legitimate versus suspicious activities (Sujata *et al*.2018). NLP models are used to detect phishing. It shall examine the emails, URLs, and content of the websites with typical features of phishing, such as suspicious domains, misleading URLs, or deceitful language. A combination of supervised and unsupervised learning techniques will be applied. Supervised learning will be utilized using labeled datasets of known phishing attempts, while unsupervised learning will identify unknown emerging threats based on patterns. Models will be optimized for real-time detection to respond in a timely manner to mitigate fraud risks.

3.3. Model Evaluation and Performance Metrics

Model evaluation and performance metrics are important in the research due to the ability of the detection models to identify account takeovers and phishing attempts. The performance metrics of both models are accuracy, precision, recall, and F1-score. Accuracy is the overall validity, and precision means which provides information regarding how many of the identified fraudulent activities are actually fraudulent. Recall measures the model's ability to identify all the fraudulent incidents, and F1-score balances precision and recall to give a single metric for model performance. Other important metrics for account takeover detection include FPR and FNR in order to minimize missed detections as well as false alarms (DABA *et al*.2020). For the detection of phishing, ROC-AUC curve, as well as other metrics, can be used in order to test the model against its capability to distinguish legitimate from phishing activities at any different threshold. Cross-validation is used to ensure that the model generalizes well with different datasets and does not overfit.

4. Results

4.1. Performance of Detection Models

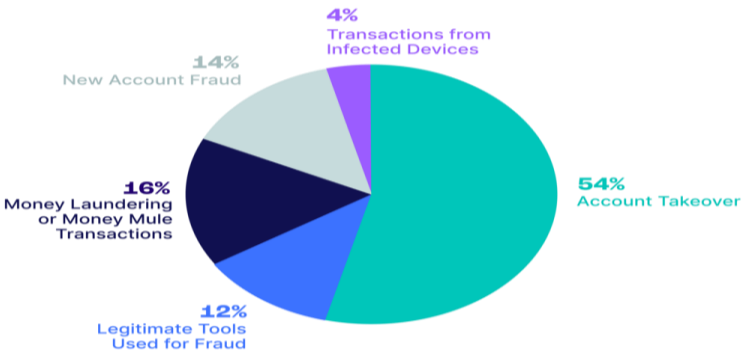

Figure 4: Performance of Detection Models

(Source: https://seon.io)

It states that the detected account takeovers and phishing activity performance can be measured, using appropriate metrics, regarding whether such a model indeed works in reality. It also provides significant information for an account's unauthorized access, detection performance is heavily determined by whether the model achieves the desired precision to ascertain anomalous login patterns against potential compromised accounts. The model kept on checking its recall and precision for unwanted positive values that could result in incorrect account lockouts, but unwanted negative values that may allow prohibited fraudulent activities to be unnoticed. To detect phishing, the model checks on the data range of email and URL analysis through phishing attempts (Wang *et al*.2018). The detection models must have high accuracy and F1-scores, meaning precision and recall should be well-balanced. The cross-validation results are also used to determine how adaptable the models are in dealing with new, unknown phishing techniques. Overall generality of the models can be inferred by cross-validation results that indicate their applicability to various datasets, hence showing robustness in fraud e-commerce mitigation.

4.2. Impact on Fraud Mitigation in E-Commerce

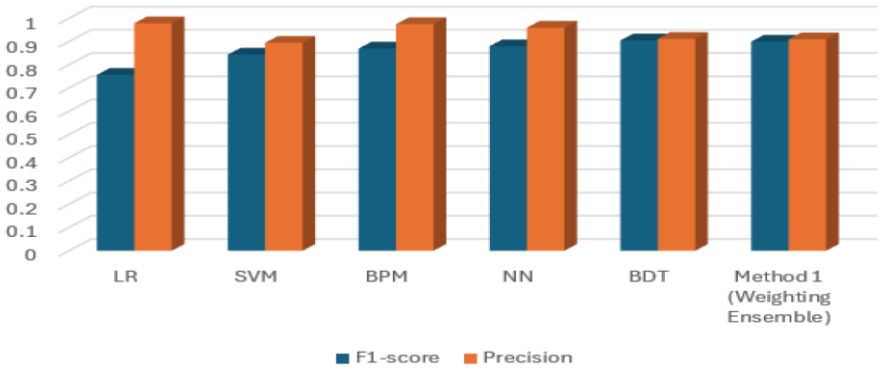

Figure 5: Detecting Phishing Attacks

(Source: https://www.mdpi.com)

Ecommerce fraud mitigation depends on account takeover detection, with most models relating to the phenomenon. The models help eliminate various losses by recognizing fraudulent transactions in real time and preventing financial damage through safe transfer transactions between the consumer and merchants. Account takeover early warnings prevent unauthorized access to important user information and allow adequate time to minimize the exposure of sensitive data and eventually fraud. As discussed above, the same phishing-detecting models will block customers from accessing fake sites or phishing mails; this helps diminish the probability of identity thefts and accounts' compromise (Gupta *et al*.2019). Real-time abilities of the mentioned models help online stores prevent suspicious login blockade or pop messages to inform that phishing login has happened, and the overall level of security rises. In accordance, these integrated models give users more confidence and trust since they feel safe and secure when interacting with a fraud-fighting platform. In the long run, these models will reduce the financial damage as well as reputational losses attributed to cybercrime within the e-commerce industry.

4.3. Comparison with Traditional Fraud Detection Methods

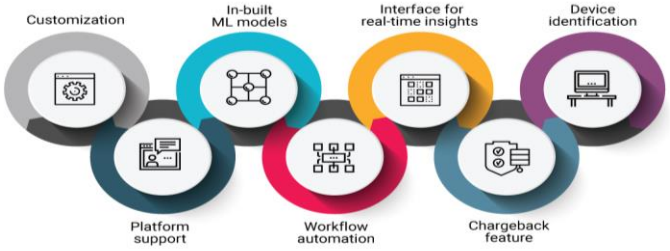

Figure 6: Fraud Detections and Prevention Tools

(Source: https://www.spiceworks.com)

Machine learning-based models for account takeover and phishing detection bring significant benefits over traditional fraud detection in terms of accuracy as well as adaptability. Traditional fraud detection along with the common rule-based systems does not provide proper and timely responses to the newer threats emerging. Rule-based systems are prone to identify only gross and very observable fraud patterns since they fundamentally rely on predefined thresholds and rules. These models learn from enormous data sets and mature towards even better performance over time, and therefore well-equipped for more complex types of fraud yet unknown so far. Another area in which machine learning models would perform well is the ability to handle large data volumes in real time with fast and accurate answers such as for example anomaly detection account takeovers and natural language processing phishing (Adlakha *et al*.2018). Traditional techniques rely mostly on labor, while machine learning leaves room for the use of automation and scalability of fraud detection, hence reducing human error and enhancing efficiency in the global fight against e-commerce fraud.

5. Discussion

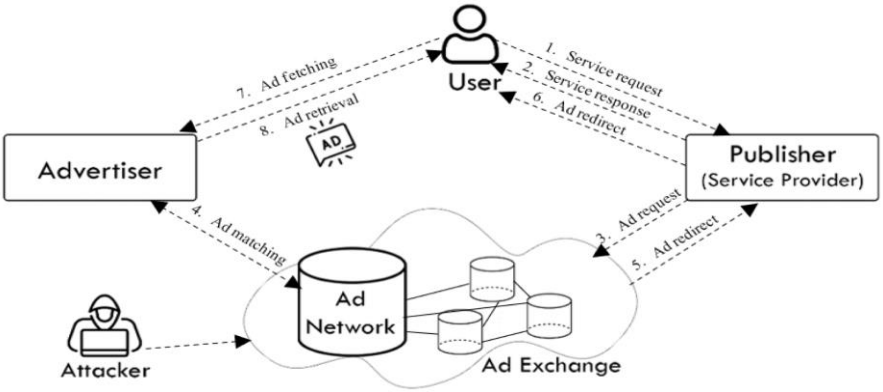

Figure 7: Fraud Detection and Prevention

(Source: https://www.mdpi.com)

The technologies suggest huge potential concerning the detection of account takeover and phishing with regard to machine learning models. The models show good performances for detecting fraudulent activities, including offering high accuracy, precision, and recall, for an efficient secure environment on the online portal. Challenges are still overcome with adapting to the change of tactic by fraudsters due to it being a persistent course of innovation from the side of the cyber-crooks. While machine learning models are good for complex-pattern detection, it reduces its false positives effectively (Chilaka *et al*.2019). The output depends on quality and diversity that is fed during the training processes. Such models need repeated refinement against changing threat patterns. Models should be fused with prevalent security systems- two factor authentications fraud alerts system among many others-to complement the current models in capability. Overall, these cutting-edge models of detection that will be deployed would bring a wonderful solution to the business platforms of e-commerce as well as enhance security and customer confidence however, only in the long term if updated and monitored.

6. Future Directions

The future of fraud detection in e-commerce depends on emerging trends in technology since AI and ML are only just getting into their stride and will only advance further and improve. As fraud tactics progress, fraud detection systems will adapt deep learning algorithms that can analyze the most enormous unstructured data, from images and videos, to pick new fraud patterns. AI, along with ML, will help enhance the accuracy for real-time detection so that e-commerce can react in real time against threats, thus allowing minimal damage and prevention of further fraudulent activities before it spreads wider (Mittal *et al*.2020). However, other challenges persist with such systems-to constantly update models to identify evolving patterns of fraud and possible adversarial attacks on artificial intelligence systems-this means such integrations will pose huge technical and operational challenges if implemented together with existing infrastructures that have multiple-factor authentications and behavioral analytics systems. Despite these challenges, much promise lies in the future for more sophisticated, scalable, and proactive fraud detection systems to strengthen e-commerce security and protect consumers.

7. Conclusion

The implementation of machine learning based models for account takeover and phishing attacks represents a significant advancement in mitigating e-commerce fraud. These models provide better accuracy, scalability, and adaptability than traditional fraud detection approaches. This helps in real-time identification of suspicious activities and enhances overall security of online platforms. Since there is a huge amount of data, machine learning algorithms discover patterns that otherwise remain hidden. This prevents financial losses and protects consumer confidence. However, these models have to be constantly refined to match the emerging fraud tactics to continue their effectiveness. This will then be combined with other security methods such as multi-factor authentication to enhance fraud prevention. As e-commerce continues to evolve, these complex detection models will be key in protecting consumers and businesses in the creation of a safer and more trustworthy online environment for all stakeholders.

Reference List

Journals

[1] Adlakha, M., 2018. Mobile commerce security and its prevention. In Mobile Commerce: Concepts, Methodologies, Tools, and Applications (pp. 433-449). IGI Global.

[2] Ali, M.A., Azad, M.A., Centeno, M.P., Hao, F. and van Moorsel, A., 2019. Consumer-facing technology fraud: Economics, attack methods and potential solutions. Future Generation Computer Systems, 100, pp.408-427.

[3] Chilaka, U.L., Chukwudebe, G.A. and Bashiru, A., 2019. A review of credit card fraud detection techniques in electronic finance and banking. Conic Res. Eng. J, 3, pp.456-467.

[4] DABA, W.A., 2020. AN ASSESSMENT ON ELECTRONIC COMMERCE PRACTICE AND FRAUDS ON ELECTRONIC COMMERCE PRACTICE; IN CASE OF ETHIOPIA.

[5] Dhobe, S.D., Tighare, K.K. and Dake, S.S., 2020. A review on prevention of fraud in electronic payment gateway using secret code. Int. J. Res. Eng. Sci. Manag, 3(1), pp.602-606.

[6] 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, pp.124-151.

[7] Gupta, R., 2019. Data Mining for Fraud Detection: An Overview of Techniques and Applications. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 10(1), pp.561-567.

[8] Hasham, S., Joshi, S. and Mikkelsen, D., 2019. Financial crime and fraud in the age of cybersecurity. McKinsey & Company, 2019.

[9] Mittal, S. and Tyagi, S., 2020. Computational techniques for real-time credit card fraud detection. Handbook of Computer Networks and Cyber Security: Principles and Paradigms, pp.653-681.

[10] Mittal, S. and Tyagi, S., 2020. Computational techniques for real-time credit card fraud detection. Handbook of Computer Networks and Cyber Security: Principles and Paradigms, pp.653-681.

[11] Sujata, J., Menachem, D. and Rageshree, M., 2018. Mitigating Risk of Revenue Leakages on the Customer and Vendor Side in Ecommerce Sector. International Journal of Engineering and Technology (UAE), 7(3), pp.161-166.

[12] Tao, J., Wang, H. and Xiong, T., 2018, November. Selective graph attention networks for account takeover detection. In 2018 IEEE International Conference on Data Mining Workshops (ICDMW) (pp. 49-54). IEEE

[13] Naveen Bagam. (2024). Data Integration Across Platforms: A Comprehensive Analysis of Techniques, Challenges, and Future Directions. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(23s), 902–919. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/7062

[14] Naveen Bagam, Sai Krishna Shiramshetty, Mouna Mothey, Harish Goud Kola, Sri Nikhil Annam, & Santhosh Bussa. (2024). Advancements in Quality Assurance and Testing in Data Analytics. *Journal of Computational Analysis and Applications (JoCAAA)*, *33*(08), 860–878. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/1487

[15] Bagam, N., Shiramshetty, S. K., Mothey, M., Kola, H. G., Annam, S. N., & Bussa, S. (2024). Optimizing SQL for BI in diverse engineering fields. *International Journal of Communication Networks and Information Security*, *16*(5). https://ijcnis.org/

[16] Bagam, N., Shiramshetty, S. K., Mothey, M., Annam, S. N., & Bussa, S. (2024). Machine Learning Applications in Telecom and Banking. *Integrated Journal for Research in Arts and Humanities*, *4*(6), 57–69. https://doi.org/10.55544/ijrah.4.6.8

[17] Bagam, N., Shiramshetty, S. K., Mothey, M., Kola, H. G., Annam, S. N., & Bussa, S. (2024). Collaborative approaches in data engineering and analytics. *International Journal of Communication Networks and Information Security*, *16*(5). https://ijcnis.org/

[18] Naveen Bagam, International Journal of Computer Science and Mobile Computing, Vol.13 Issue.11, November- 2024, pg. 6-27

[19] Naveen Bagam. (2024). Optimization of Data Engineering Processes Using AI. *International Journal of Research Radicals in Multidisciplinary Fields*, *ISSN: 2960-043X*, *3*(1), 20–34. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/138

[20] Naveen Bagam. (2024). Machine Learning Models for Customer Segmentation in Telecom. *Journal of Sustainable Solutions*, *1*(4), 101–115. https://doi.org/10.36676/j.sust.sol.v1.i4.42

[21] Shiramshetty, S. K. (2021). SQL BI Optimization Strategies in Finance and Banking. *Integrated Journal for Research in Arts and Humanities*, *1*(1), 106–116. https://doi.org/10.55544/ijrah.1.1.15

[22] Sai Krishna Shiramshetty. (2022). Predictive Analytics Using SQL for Operations Management. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *11*(2), 433–448. Retrieved from https://eduzonejournal.com/index.php/eiprmj/article/view/693

[23] Shiramshetty, S. K. (2023). Data warehousing solutions for business intelligence. *International Journal of Computer Science and Mobile Computing*, *12*(3), 49–62. https://ijcsmc.com/index.php/volume-12-issue-3-march-2023/

[24] Harish Goud Kola. (2024). Real-Time Data Engineering in the Financial Sector. *International Journal of Multidisciplinary Innovation and Research Methodology*, *ISSN: 2960-2068*, *3*(3), 382–396. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/143

[25] Harish Goud Kola. (2022). Best Practices for Data Transformation in Healthcare ETL. *Edu Journal of International Affairs and Research*, *ISSN: 2583-9993*, *1*(1), 57–73. Retrieved from https://edupublications.com/index.php/ejiar/article/view/106

[26] Kola, H. G. (2018). Data warehousing solutions for scalable ETL pipelines. *International Journal of Scientific Research in Science, Engineering and Technology*, *4*(8), 762. https://doi.org/10.1.1.123.4567

[27] Annam, S. N. (2024). Comparative Analysis of IT Management Tools in Healthcare. *Stallion Journal for Multidisciplinary Associated Research Studies*, *3*(5), 72–86. https://doi.org/10.55544/sjmars.3.5.9.

[28] Annam, N. (2024). AI-Driven Solutions for IT Resource Management. *International Journal of Engineering and Management Research*, *14*(6), 15–30. https://doi.org/10.31033/ijemr.14.6.15-30

[29] Annam, S. N. (2022). Optimizing IT Infrastructure for Business Continuity. *Stallion Journal for Multidisciplinary Associated Research Studies*, *1*(5), 31–42. https://doi.org/10.55544/sjmars.1.5.7

[30] Bussa, S. (2021). Challenges and solutions in optimizing data pipelines. *International Journal for Innovative Engineering and Management Research*, *10*(12), 325–341. https://sjmars.com/index.php/sjmars/article/view/116

[31] Bussa, S. (2022). Machine Learning in Predictive Quality Assurance. *Stallion Journal for Multidisciplinary Associated Research Studies*, *1*(6), 54–66. https://doi.org/10.55544/sjmars.1.6.8

[32] Bussa, S. (2022). Emerging trends in QA testing for AI-driven software. *International Journal of All Research Education and Scientific Methods (IJARESM, 10*(11), 1712. Retrieved from http://www.ijaresm.com

[33] Mouna Mothey. (2022). Automation in Quality Assurance: Tools and Techniques for Modern IT. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *11*(1), 346–364. Retrieved from https://eduzonejournal.com/index.php/eiprmj/article/view/694

[34] Mothey, M. (2022). Leveraging Digital Science for Improved QA Methodologies. *Stallion Journal for Multidisciplinary Associated Research Studies*, *1*(6), 35–53. https://doi.org/10.55544/sjmars.1.6.7

[35] Mothey, M. (2023). Artificial Intelligence in Automated Testing Environments. *Stallion Journal for Multidisciplinary Associated Research Studies*, *2*(4), 41–54. https://doi.org/10.55544/sjmars.2.4.5