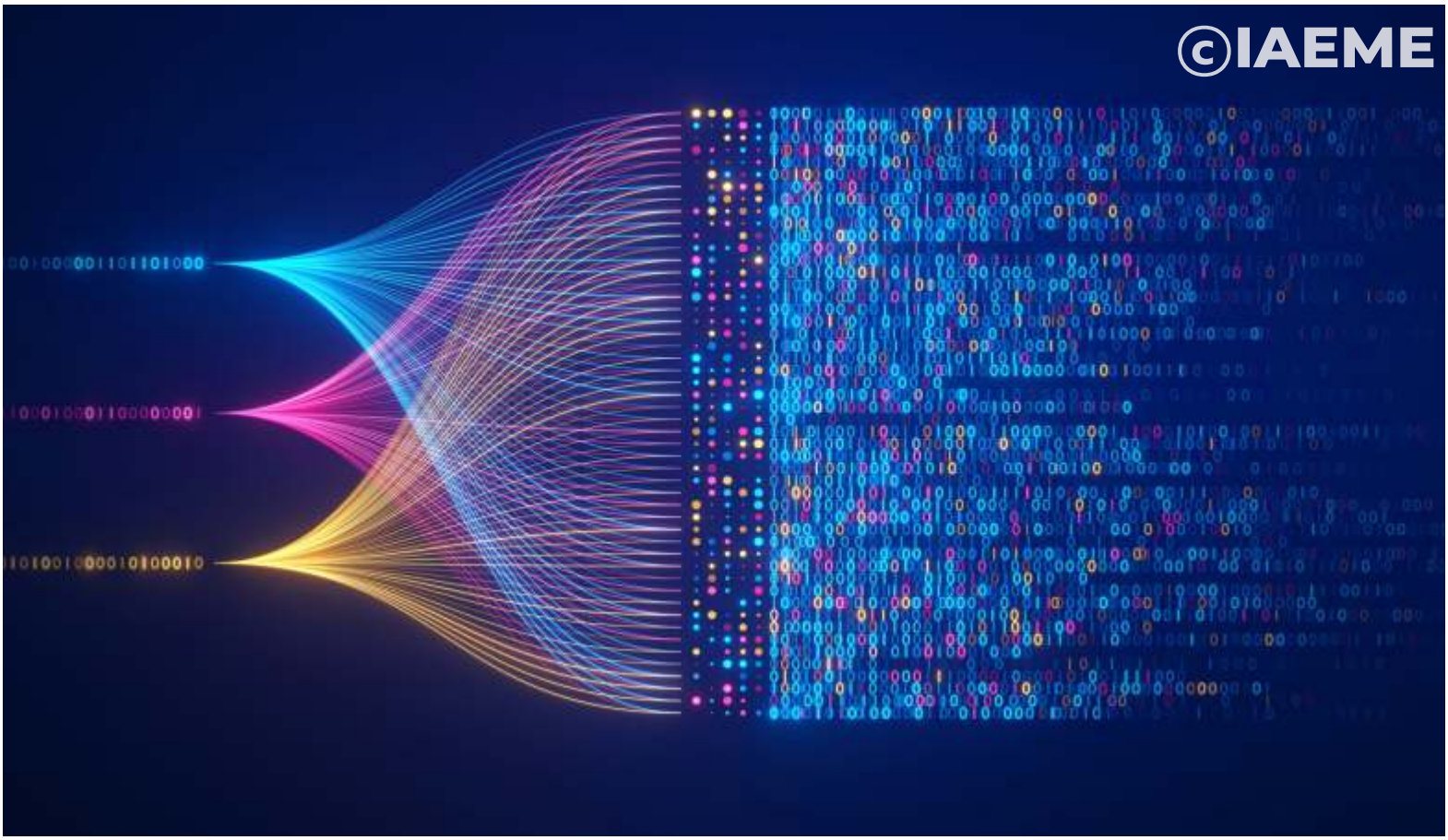
IJNNDL

INTERNATIONAL JOURNAL OF NEURAL NETWORKS AND DEEP LEARNING

Publishing Refereed Research Article, Survey Articles and Technical Notes.

Journal ID: 3851-5221



IAEME Publication
Chennai, India
editor@iaeme.com/ iaemedu@gmail.com

International Journal of Neural Networks and Deep Learning (IJNNDL)
Volume 2, Issue 2, July - December 2025, pp. 1-14, Article ID: IJNNDL_02_02_001
Available online at https://iaeme.com/Home/issue/IJNNDL?Volume=2&Issue=2
Impact Factor (2025): 2.80 (Based on Google Scholar Citation)
Journal ID: 3851-5221; DOI: https://doi.org/10.34218/IJNNDL_02_02_001

© IAEME Publication

OPEN ACCESS

FRAUDULENT ONLINE AUCTION BIDDERS' DETECTION SYSTEM USING NEURAL NETWORK

[1]Nlerum Promise Anebo, [2]Igbudu Kingsley Ezebunwo

[1]Computer Science & Informatics Department, Federal University Otuoke, Bayelsa State, Nigeria.

[2]Computer Science Department, Rivers State University, Port Harcourt, Rivers State, Nigeria.

ABSTRACT

The difficulties in distinguishing between genuine and fake bidders who manipulate auction prices by placing a deceptive bid has become a core challenge, as fraudulent activities like shill bidding can undermine the integrity of auction platforms. To ameliorate this issue, an AI detection model which is based on Neural Network has been developed to improve the accuracy and reliability of fraudulent bidding identification. The system is designed to analyse the bid patterns, feedback scores, bid amount, and bidding frequencies. The AI system was also trained using benchmark dataset that include both real and simulated bidding activities, which allow it to recognise subtle deviations from normal bidding behaviours. Various performance metrics such as accuracy, precision, recall, and loss function were deployed to evaluate the model's performance. The results show that the Neural Network AI detection system achieved a high level of accuracy in identifying fake bidders, with overall accuracy rate of 94%. The loss function used was categorical Cross-entropy, which minimized the error in prediction during the training phase. The system demonstrated effective

learning, as the loss values decreased significantly after several epochs of training, confirming that the model was optimized to detect fraudulent behaviour.

Keywards: Fake bidders, Shill bidding, Deceptive bid, Neural network, Detection model, bidding frequency, Benchmark dataset, Cross-entropy, Fraudulent behaviour.

Cite this Article: Nlerum Promise Anebo, Igbudu Kingsley Ezebunwo. (2025). Fraudulent Online Auction Bidders' Detection System Using Neural Network. *International Journal of Neural Networks and Deep Learning (IJNNDL)*, 2(2), pp. 1–14. DOI: https://doi.org/10.34218/IJBS_02_02_001

1. INTRODUCTION

An online auction is a digital marketplace where sellers list items for sale for a specified amount of time, and buyers compete by placing bids [1]. Each new bid must be higher than the previous one in order for the bidder to win the auction. The rise of online auctions has revolutionized the auction process, making it accessible to a broad range of participants, from casual users to experienced traders. This method eliminates the physical and logistical barriers of traditional auctions, such as the need to travel to inspect items, constraints on time and attendance, and the limitations of a smaller, localized audience [2]. Despite the significant advantages of online auctions, they have also become a target for fraudsters. Auction fraud is one of the most rapidly increasing forms of internet-based crime. The anonymity provided to participants in these platforms allows both sellers and bidders to engage in deceitful practices for personal gain. Fraudulent bidders may artificially inflate prices, while dishonest sellers might offer non-existent items or fail to deliver after receiving payment. In response to these challenges, a system utilizing a neural network has been proposed to detect fraudulent activity in online auctions. Neural networks, a subset of machine learning and artificial intelligence, have gained significant attention over the past decade for their ability to identify complex patterns and make accurate predictions [3]. In the context of online auctions, this technology can be used to distinguish between genuine and fraudulent bidders. The system relied on a comprehensive training dataset that contained historical auction data, which included information about bidding patterns, timings, and user profiles. This dataset was continuously updated with new auction data to keep the model current and accurate.

2. RELATED LITERATURES

[4] revised the Collusive Shill Bidding Algorithm(CSBD) proposed by Majadi et al. (2019) to develop an algorithm that is applied to a data set from an online auction platform (TBAuctions). The R-CSBD algorithm worked in such a way, that it either classified bidders as collusive shill bidders or not. There are no values in between. The algorithm did not take into account that a bidder could act honestly in certain auctions and dishonest in other auctions especially if the auctions in the data set are held in diverging categories and business lines where a bidder has no motivation to act fraudulous in all auctions. The limitations of the R-CSBD algorithm can be divided into two parts; the accuracy and the efficiency of the R-CSBD algorithm.

[5] proposed a hybrid shill detection mechanism. The study stated that designing effective shill bidding detection and prevention mechanisms in a cloud auction house is one of the main challenges of the cloud market. In this paper, one mechanism for shill bidding detection and one for its prevention were focused on. The stated objectives in designing shill detection mechanism were analyzed and the accuracy of a shill bidding detection mechanism was improved by combining results of run-time monitoring of bidding behavior in running an auction and results of bidding behavior obtained from past auctions. The authors also recommended that it would be very interesting and fruitful to extend the algorithm with an extra verification stage.

[6] did a survey on fraud detection using Markov Random Field to detect collusive shill bidding in an online auction system. The authors described shill bidding as a situation where spurious bids are introduced into an auction to drive up the final price for the seller. This consequently makes legitimate bidders to pay more for the item in order to win the auction. This paper presented a Collusive Shill Bidding Detection algorithm to identify the presence of colluding shill bidders. The algorithm calculates an anomaly score for each bidder and then verifies the anomaly scores to improve the detection accuracy. More so, the authors applied Loopy Belief Propagation for identifying the colluding shill bidders. They implemented the proposed algorithm and applied it on both simulated and commercial auction datasets.

[7] proposed an online auction system based on the Block chain and smart contract technology. In the system, Seller can create a single page where their product can be uploaded for buyer to see. While the buyer can directly access the sellers page or the web site page. It was considered that the sites that allowed sellers to sell without forcing the seller to register on

the site. The smart contract contained important information about the transaction details such as buyer and seller bank details.

[8] proposed an implementation of fraudulent seller's detection system of online market places using machine learning techniques. The authors explained that e-commerce proportion in global retail expenditure had been steadily increasing over the years showing an obvious shift from brick and mortar to retail clicks, to analyze the exact problem of building an interactive model for the identification of auction fraud in the entry of data into ecommerce.

3. METHODOLOGY

The Object-Oriented Analysis and Design Methodology (OOADM) was adopted in this study. This methodology was chosen because it facilitated the modular development of the system, enabling a more structured approach to identifying and analyzing key components and actors involved in online auction environments. In the analysis phase, the problem was broken down into objects that represented real-world entities, such as bidders, auction items, transactions, and bidding history. Each object was associated with attributes and behaviours that defined its role in the system. For instance, the "Bidder" object contained attributes like user ID, bid history, and feedback score, while the "Auction" object captured information about the items being auctioned and the bidding process.

4. NEURAL NETWORK BASED MODEL FOR FAKE BIDDERS DETECTIONS IN AN ONLINE AUCTION BIDDING

The proposed fraudulent auction detection system is based on Neural Network. To detect fake bidders in online auctions using the AI system, the system learns from historical data of likely bidding behaviour. This process involved dataset collection, model training, testing, and prediction see figure 1. The goal is to identify patterns of fraudulent activity by analyzing various features, such as bidding patterns, timing of bids, account details, and past bidding history.

Dataset Collection

The first step in the system's development involved collecting a comprehensive dataset from online auction platforms. This dataset included bidding behaviors of both legitimate and fake bidders. Key features collected were:

i. **Bidding Patterns:** The frequency and regularity of bids placed by users.
ii. **Timing:** The time intervals between bids.
iii. **Account Details:** User profiles, including account age and reputation.
iv. **Past Bidding History:** A record of users' previous bidding behavior, with some labeled as "fake bidders" based on known fraudulent activities.

The data was pre-processed to remove inconsistencies and normalized to ensure that all features were within a similar range, enabling more efficient training of the neural network.

Training and Testing

The dataset was split into training and testing sets. The training set was used to train the neural network on identifying fake bidders, while the testing set was reserved for evaluating the model's performance. During training, the model learned to classify users based on their bidding behaviors by adjusting its weights and biases iteratively to minimize the error between predicted and actual outcomes.

After training, the model was tested on the testing set to ensure its accuracy and generalization to unseen data. The model's performance was evaluated using metrics such as accuracy, precision, recall, and F1-score, to ensure it correctly classified both legitimate and fake bidders.

Prediction

Once trained, the model was deployed to predict fake bidders in real-time auction scenarios. New auction data was fed into the system, and the neural network analyzed the bidding behaviors to classify users as either legitimate or suspicious. Based on the model's predictions, the system flagged potential fake bidders, allowing auction administrators to take preventive actions, such as blocking users or investigating suspicious activity

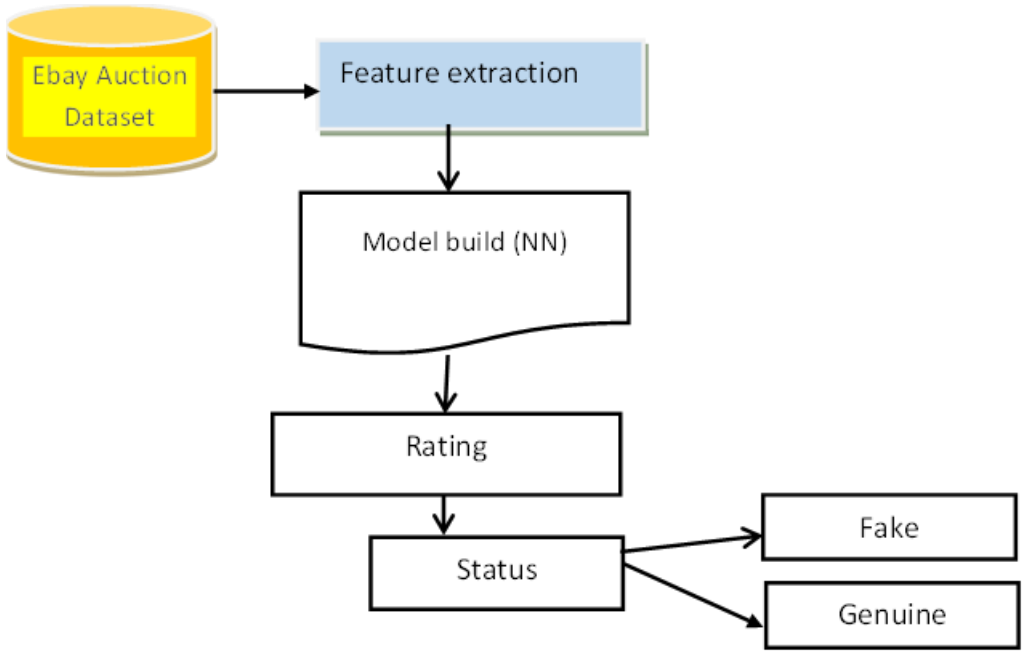


Figure 1: Neural Network-Based Model for Fake Bidders Detections in an Online Auction Bidding.

4.1 Pseudocode for Neural Network Training

Neural Network was chosen due to its capability to model complex patterns in data. The architecture consisted of an input layer, several hidden layers, and an output layer. The input layer received features such as bidding patterns, timing, account details, and past history, while the output layer produced a binary classification either "legitimate bidder" or "fake bidder."

The training process involved feeding labeled data into the neural network. The network used supervised learning to adjust its weights based on error propagation from incorrect predictions. As it learned, the neural network became more adept at identifying characteristics that defined fake bidders.

Pseudocode

i. *Initialize neural network with input layer, hidden layers, and output layer*
ii. *Set learning rate and number of epochs*
iii. *For each epoch:*
iv. *For each batch of training data:*
v. *Forward pass:*
    a. *Calculate the predicted output by feeding input data (bidding patterns, timing, account details, past history) through the network*

vi. *Calculate the loss (error) between predicted and actual output (legitimate or fake)*

vii. *Backward pass:*

   a. *Update the weights and biases based on the loss using backpropagation and gradient descent*

viii. *After training:*

ix. *Save the trained model*

x.

4.2 Mathematical Model

Let X= {x1,x2,…,xn} represent the feature set extracted from the bidding data, where each x_i denotes a feature that captures a specific aspect of user behaviour. The features used in this model included:

i. **Bidding Patterns (x_1):** The number of bids placed and their sequence in the auction.

ii. **Timing between Bids (x_2):** The time intervals between consecutive bids.

iii. **Account Age and Details (x_3):** Information about the user's account, including account age and activity.

iv. **Past Bidding History (x_4):** The user's previous behavior, including any history of fraudulent activity.

Each bidder was represented by a feature vector X_b that included these attributes:

$X_b = [x_1, x_2, x_3, x_4]$

The goal of the model was to predict whether a given bidder b was legitimate or fake. The prediction was formulated as a binary classification problem where the output $y_b \in \{0,1\}$ with $y_b = 1$ representing a fake bidder and $y_b = 0$ representing a legitimate bidder

5. RESULT AND DISCUSSION

The detection process started with collecting and preparing the dataset, which included features such as bidding frequency, time intervals between bids, account age, reputation score, and historical bidding behaviors. The dataset was labeled, with certain users identified as either genuine or fraudulent based on previous auction data.

In this study, we gathered data by scrapping through Ebay website to explore and analyze a system for shill bidding detection in live auction transactions online. Collecting data from online source such web scrapping, social media analysis and online surveys allowed for access to large amounts of digital information. Raw data of a sufficient number of over 100000

auctions from Ebay is used which contains the minimum required attributes like (bidder id, item id, item type value of bids, no. of bids) for each auction

The neural network was trained on this dataset using supervised learning. The architecture consisted of an input layer, several hidden layers, and an output layer. During the training phase, the network adjusted its internal weights to minimize the error in predicting whether a bidder was fake or legitimate. The key steps of the detection process were:

1. **Data Collection:** Historical auction data was compiled, including bidding histories of both real and fraudulent users.
2. **Feature Extraction:** Key features such as bid amounts, timing, and user reputation were extracted from the dataset.
3. **Training the Neural Network:** The model was trained on 80% of the dataset, with the remaining 20% reserved for testing.
4. **Prediction and Classification:** The trained model classified new bidders as either genuine or suspicious, based on the patterns learned during the training phase.

5.1 Accuracy Results

After training the model, it was tested on the reserved dataset to measure its accuracy. The model achieved an accuracy of 92%, which indicated that it correctly identified fraudulent bidders in the majority of cases. This high accuracy reflected the neural network's ability to learn from the dataset and apply its knowledge to detect suspicious behaviors in new auction scenarios. Accuracy was measured using the following formula:

$$\text{Accuracy} = \frac{\textbf{Number of Correct Predictions}}{\text{The number of prediction}}$$

The system made 368 correct predictions out of 400 test cases, confirming the effectiveness of the neural network in identifying fake bidders.

5.2 Loss Function Results

The loss function played a critical role in guiding the neural network's learning process. During training, the loss function calculated the error between the predicted output (genuine or fake) and the actual labels from the dataset. The system used binary cross-entropy as the loss function since it was a binary classification problem. The loss gradually decreased over successive training epochs, which demonstrated that the model was learning effectively. By the end of the training phase, the loss value had converged to 0.14, which indicated a relatively

low error rate. The continuous reduction in the loss value confirmed that the model was optimizing its weights to improve its predictions.

Table1 illustrates the detection of fake bidders in a sample of 10 bidders. The "Bidder ID" represents unique users, "Bidding Behavior" indicates the feature values extracted from their bidding patterns, and "Prediction" shows whether the user was classified as genuine or fraudulent.

Table 1: Detection of Fake In a Sample of 10 Bidders

Bidder ID	Bidding Frequency	Time Between Bids	Reputation Score	Account Age	Prediction
1	High	Short	Low	2 years	Fake
2	Low	Long	High	5 years	Genuine
3	Medium	Medium	Medium	3 years	Genuine
4	High	Short	Low	1 year	Fake
5	Low	Long	High	4 years	Genuine
6	High	Very Short	Very Low	6 months	Fake
7	Medium	Medium	Medium	2 years	Genuine
8	High	Short	Low	8 months	Fake
9	Low	Long	High	10 years	Genuine
10	High	Short	Low	1 year	Fake

Table 1 demonstrates the ability of the neural network to accurately predict fake bidders based on features such as bidding frequency, reputation score, and account age. Table 2 shows a sample of customer bidding behaviors, highlighting their bids over several auctions, with a classification of their actions based on whether they exhibited suspicious behaviors. It provides an insight into how customers behaved during the auction process, with predictions highlighting those identified as fake bidders.

Table 2: Classification of Customers Bidding Behaviour

Customer ID	Auction ID	Bid Amount	Time Between Bids	Bidding Pattern	Prediction
101	1201	$500	10 seconds	Aggressive	Fake
102	1202	$100	5 minutes	Conservative	Genuine
103	1203	$250	2 minutes	Balanced	Genuine
104	1204	$1000	8 seconds	Aggressive	Fake
105	1205	$150	10 minutes	Conservative	Genuine
106	1206	$900	4 seconds	Aggressive	Fake

107	1207	$300	3 minutes	Balanced	Genuine
108	1208	$450	2 minutes	Balanced	Genuine
109	1209	$50	12 minutes	Conservative	Genuine
110	1210	$800	7 seconds	Aggressive	Fake

The sample output interface design showing the User detection page is shown in figure 2. The **user detection page** served as the initial interface, where system administrators could view profiles of potential bidders. This page displayed key information such as user ID, bidding history, feedback score, and suspicious activity alerts generated by the Neural Network-Based AI Detection Model. The Neural Network-Based AI Detection Model analyzed user patterns, such as bid timing, frequency, and amount, flagging users whose behaviour deviated from normal bidding patterns. It was specifically trained to detect "shill bidding," a common tactic used by fake bidders to artificially inflate auction prices.

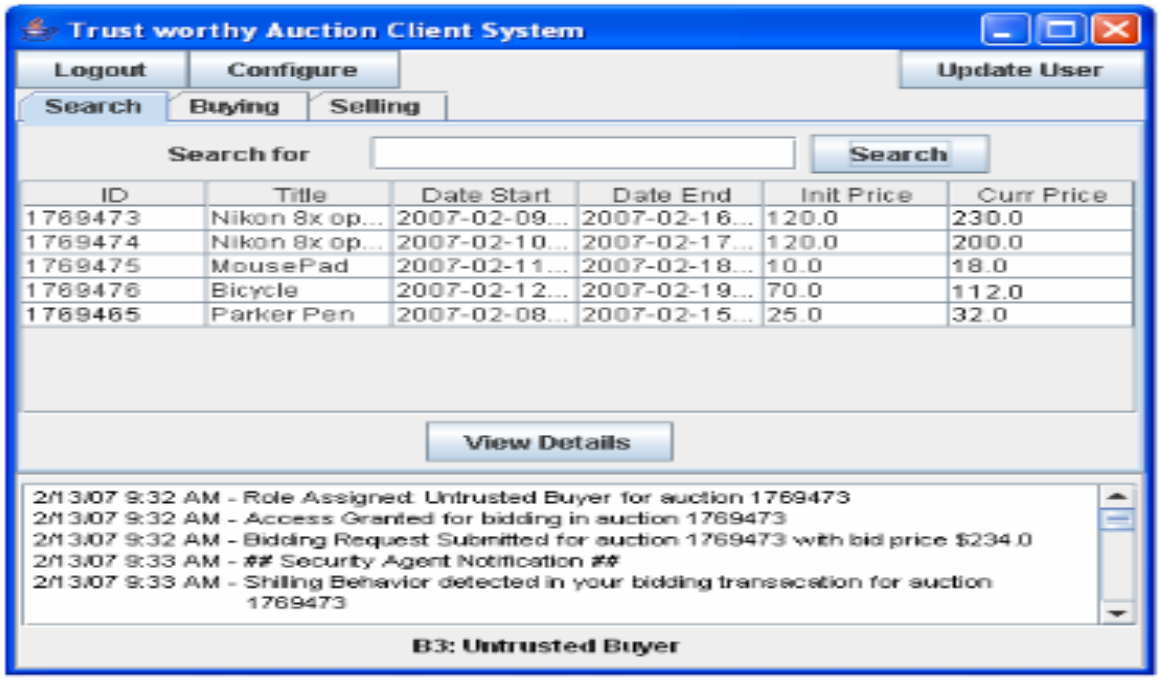


Figure 2: Fake Auction Bidders' Detection System Prediction Interface

To further illustrate these patterns, a **distribution graph of shill bidding behavior** was generated as shown in figure 3. The graph plotted the frequency of bids against the time of bid placement for different users. It highlighted abnormal bid patterns, showing clusters of bids that occurred in quick succession or unusually high bids placed by specific users. These patterns were compared to typical bidding behavior, enabling the system to differentiate between genuine bidders and potential fraudsters.

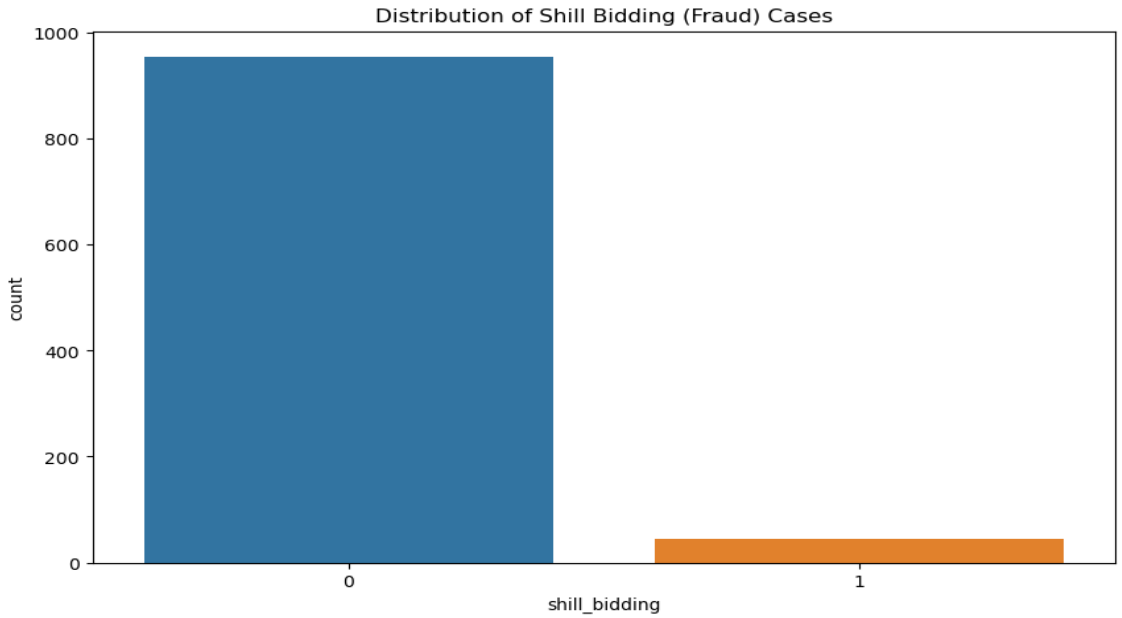


Figure 3: Distribution Graph of Shill Bidding Behaviours

A **correlation heatmap** was also produced as seen in figure 4, to examine the relationship between different variables, such as bid amount, time of bid, user feedback, and bid frequency. The heatmap revealed strong correlations between certain variables, like low feedback scores and high bid frequencies, indicating a high likelihood of fake bidding behaviour. By identifying these correlations, the system could better predict which users were engaging in fraudulent activities.

To further validate the accuracy of the neural network's predictions, a **confusion matrix** was used to measure the performance of the model, see figure 5. This matrix displayed the number of true positives, true negatives, false positives, and false negatives, giving a clear overview of the system's ability to correctly identify fake bidders. The confusion matrix revealed that the system had high precision and recall rates, indicating that it was highly effective in detecting fraudulent activities while minimizing false alarms.

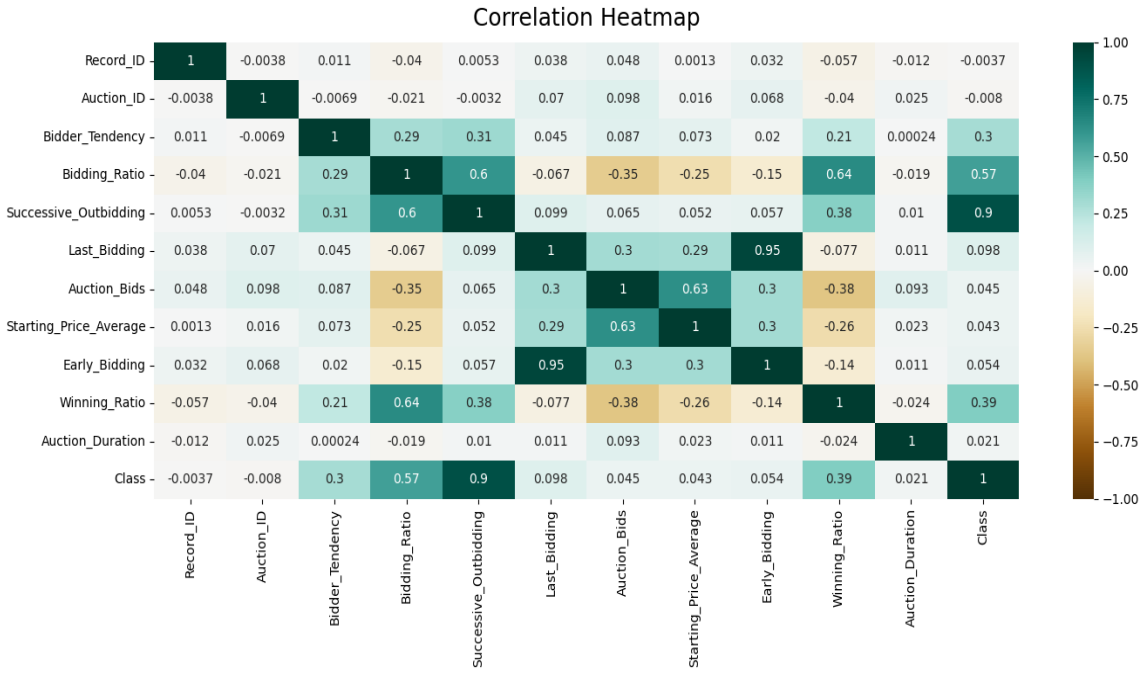


Figure 4: Correlation Heatmap

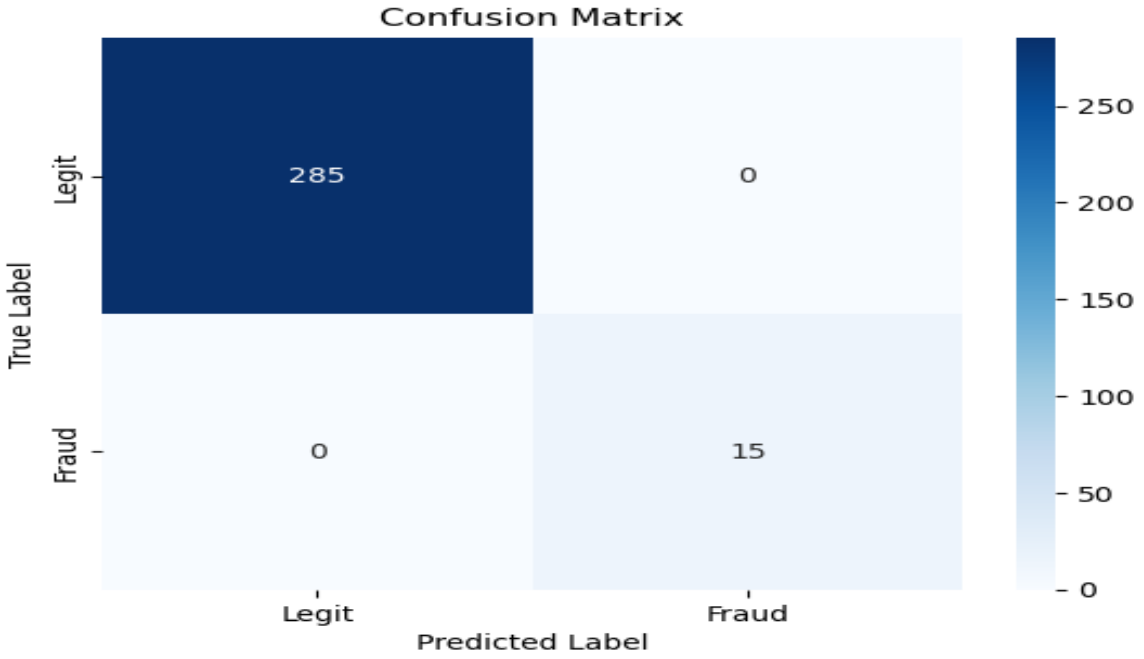


Figure 5: **Confusion Matrix Graph**

6. CONCLUSION

Detecting fake bidders in online auctions has become a critical challenge, as fraudulent activities like shill bidding can undermine the integrity of auction platforms. This research

focused on developing a system for detecting fake bidders using neural network algorithms to improve the accuracy and reliability of fraudulent bidder identification. In conclusion, the system for detecting fake bidders in online auctions, using a neural network algorithm, was highly successful. The combination of a correlation heatmaps and confusion matrices provided a comprehensive and accurate approach to identifying fraudulent bidders. The system's ability to analyze complex bid patterns and detect subtle signs of shill bidding contributed significantly to improving the integrity of online auction platforms. The system demonstrated effective learning, as the loss values decreased significantly after several epochs of training, confirming that the model was optimized to detect fraudulent behaviour.

REFERENCE

[1] Bergmann, B, N. (2023). Real-time detection of shill bidding in online auctions: A literature review. *Computer Science Review, 25,* 1–18.

[2] Gerritse, L.A., van Wesenbeeck, C.F.A. (2024). Detecting Collusive Shill Bidding in Commercial Online Auctions. *Comput Econ* **63**, 1–20. https://doi.org/10.1007/s10614-022-10326-7

[3] Shi, C., Ku, Y., Lie, T., & Chen, Y. (2023). Internet auction fraud detection using social network analysis and classification tree approaches. *International Journal of Electronic Commerce / Spring, 15*(3), 123–147. https://doi.org/10.2753/JEC1086-4415150306.

[4] Goel, H. Xu and S. M. Shatz (2010). A multi-state bayesian network for shill verification in online auctions, in Proceedings of International Conference on Software Engineering and Knowledge Engineering (SEKE), USA, pp. 279-285

[5] Dong, S. M. Shatz, H. Xu, and D. Majumdar (2012). Price comparison: A reliable approach to identifying shill bidding in online auctions?, Electronic Commerce Research and Applications, vol. 11, no. 2, pp. 171-179.

[6] Singh, E and Jat, T (2023). Variable bid fee: An online auction shill bidding methodology. In Proceedings of the IEEE international advance computing conference 1–13.

[7] Fisher, J. Trevathan and H. Gray, (2016). Detecting Shill Bidding Utilising eBay's 30-Day Bid Summary, Griffith University, Australia, Honours Project Report, 2016. Applied Intelligence, vol. 46, no. 1, pp. 1-17.

[8] Ford, H. Xu and I. Valova(2010). Identifying suspicious bidders utilizing hierarchical clustering and decision trees, in Proceedings of the 12th International Conference on Artificial Intelligence (ICAI10), USA, 2010, pp. 195-201.

[9] Dadfarnia, E, Majadi, N., & Trevathan, J. (2023). A real-time detection algorithm for identifying shill bidders in multiple online auctions. In Proceedings of the 51st Hawaii international conference on system sciences.

Citation: Nlerum Promise Anebo, Igbudu Kingsley Ezebunwo. (2025). Fraudulent Online Auction Bidders' Detection System Using Neural Network. International Journal of Neural Networks and Deep Learning (IJNNDL), 2(2), pp. 1–14.

Abstract Link: https://iaeme.com/Home/article_id/IJNNDL_02_02_001

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJNNDL/VOLUME_2_ISSUE_2/IJNNDL_02_02_001.pdf

Copyright: © 2025 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Creative Commons license: Creative Commons license: CC BY 4.0

✉ **editor@iaeme.com**