IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13709

A Hybrid Real-Time Intrusion Prevention System for E-Commerce Platforms

Chinonso K. Joe-Onyema[1], Onate E. Taylor[2], Victor T. Emmah[3]

Department of Computer Science, Rivers State University, Nigeria[1,2,3]

Abstract: The relentless growth of the internet, coupled with the unprecedented surge in e-commerce activities due to factors such as the global COVID-19 pandemic, has created an expansive digital landscape. However, this flourishing environment has attracted a commensurate increase in cyber threats, particularly concerning the theft of sensitive user information, such as credit card data from e-commerce platforms. This paper introduces an innovative approach by developing a sophisticated Deep Belief Neural Network (DBNN) for intrusion detection which was implemented using Python. This DBNN is seamlessly integrated with Snort, a renowned intrusion detection system, and fortified by the inclusion of a web application firewall. Snort boasts of a robust signature database which aided the identification and elimination of intrusions. A web application firewall is included to foil intrusions at the application layer using rules targeting SQL injection and DoS attacks. By so doing, sensitive customer information such as credit card information which has been a shortcoming with previous systems can be protected. A correlation coefficient of 0.78 between the latency and response time for the baseline and attacked states of the server shows the web application firewall's ability to maintain the smooth running of the server during intrusion attempts through DoS attacks. In rigorous testing, the DBNN demonstrates a commendable 91.2% accuracy, affirming its efficacy in identifying and thwarting intrusion attempts. The study contributes significantly to knowledge by showcasing that this integrated defense strategy substantially enhances the security posture of e-commerce platforms. A significantly low false positive rate of 8.14% buttresses the effectiveness of the hybrid system in the face of evolving cyber threats in the contemporary digital landscape.

Keywords: Intrusion Prevention System, Deep Belief Neural Network, Denial of Service, E-commerce

I. INTRODUCTION

With the large amount of growing internet users, e-commerce has become one of the fast-growing applications of the internet. It offers clients a greater selection of goods and shopping possibilities in addition to making shopping easier and more comfortable. The covid-19 lockdowns and restrictions between 2019 and 2021 caused a surge in the number of transactions that took place on e-commerce platforms. Customers' inability to shop in person during the lockdowns led to an increase in internet sales in [1]. During these hard times, e-commerce platforms became indispensable for businesses and consumers alike. The surge not only reflected a response to immediate necessity but also marked a potential long-term shift in consumer behavior towards sustained reliance on e-commerce channels. E-commerce platforms have become essential parts of the contemporary retail scene, providing customers all over the world with an enormous selection of goods and services at unbeatable ease.

As the number of transactions on e-commerce platforms rise with an increase in the number of customers, e-commerce platforms scurry to win loyalty of the budding potential customers and maintain those of existing customers in [2]. In a bid to boost the user experience of customers, keep track of statistics and improve overall delivery, the platforms offer users the opportunity to store information. One primary motivation behind the collection of user information is to personalize the online shopping experience. E-commerce platforms utilize data on user preferences, purchase history, and browsing behaviour to tailor product recommendations and promotions. This personalization enhances user engagement and satisfaction, fostering a sense of individualized service.

The information ranging from customers' identity to billing and shipping information whet cyber criminals' appetite at the possibility of damage that can be done if an intrusion is possible. Considering the value of transactions carried out including their frequency, they pose a real threat as in [3]. This risk could result in losses for both the e-commerce platforms and the customers should the intrusion attempts be successful. The year 2022 saw up to $41 billion lost to e-commerce fraud and $48 billion expected in 2023 as in [4]. Trust in e-commerce is greatly impacted by issues like theft, perceptions of nonrepudiation, privacy protection, and data integrity. Trust in e-commerce is a major factor in e-commerce acceptability as in [5].

DOI: 10.17148/IJARCCE.2024.13709

Researchers discussed the critical issue of credential stuffing threats, emphasizing a holistic approach to address this evolving challenge. Credential stuffing exploits users who reuse passwords across multiple platforms. The scalability of security measures in e-commerce is a critical consideration as platforms aim to expand their operations while safeguarding user data and transactions. This delicate balance involves adapting security protocols to accommodate increasing user volumes, transactions, and emerging threats without compromising the robustness of the protective measures in place as in [6].

A secure e-commerce platform encourages a sense of trust between the users and platforms leading to increased future transactions as in [7]. E-Commerce platforms aim for to grow customer loyalty and long-term retention to drive revenue. It is therefore imperative that e-commerce platforms provide adequate security measures to foil fraud attempts.

From a customer's point-of-view in [8], the perceived security of the e-commerce platform, along with other factors has a strong effect on patronage by customers. In their paper, customers were more interested in performing transactions on e-commerce platforms after preliminary security checks on the platforms.

A solution for preventing network intrusions is firewalls. Firewalls can be used to stop illegal access to e-commerce platforms and filter out undesired traffic. In order to strengthen the security of computer networks, particularly those found in e-commerce platforms, firewalls are essential. As gatekeepers, these security barriers keep an eye on and regulate all network traffic entering and leaving the system in accordance with pre-established security guidelines. Firewalls reduce the danger of different cyberattacks, safeguard sensitive data, and prevent unwanted access by creating a barrier between a trusted internal network and untrusted external networks.

However, firewalls alone may not be sufficient to prevent sophisticated cyber-attacks. IPS can complement firewalls by detecting and blocking malicious traffic that may bypass the firewall. In [9], by stopping threats that may get past firewalls, IPS can improve the security of e-commerce platforms.

II. LITERATURE REVIEW

Real-Time Monitoring in E-commerce Real-time monitoring is a critical aspect of e-commerce security. In their work, considering real-time security for e-commerce platforms in [10] the authors discussed the importance of real-time monitoring to detect and respond to security incidents promptly. They emphasize the need for continuous monitoring of system logs, network traffic, and user activities to identify potential threats. In [11], the authors emphasized the significance of real-time monitoring for fraud detection in e-commerce in their paper, "Real-time Fraud Detection in E-commerce." They argued that traditional batch-based fraud detection methods are insufficient in the rapidly changing e-commerce landscape. Real-time monitoring enables the immediate detection of fraudulent activities, such as account takeovers, payment fraud, and identity theft. In [12], the authors stressed the importance of real-time monitoring in maintaining the availability and performance of e-commerce platforms. In their paper, "Real-time Monitoring for Improving E-commerce Website Performance," they discuss how real-time monitoring tools continuously assess server status, website responsiveness, and network traffic. By promptly identifying performance issues or downtime, e-commerce businesses can take immediate action to minimize disruptions, prevent revenue loss, and preserve their brand reputation.

In a recent study, the authors proposed a real-time intrusion prevention system for e-commerce platforms using machine learning algorithms. They used the random forest algorithm to analyze network traffic and detect malicious activities in [13].

In [14], the authors proposed a real-time intrusion prevention system for e-commerce platforms using a deep learning algorithm. They used a long short-term memory (LSTM) neural network to analyze network traffic and detect malicious activities. In another study as in [15], they proposed a real-time intrusion prevention system for e-commerce platforms that combines signature-based and behavior-based detection techniques. The proposed system achieved a detection rate of 98.6%. In [16], the authors proposed a real-time intrusion prevention system for e-commerce platforms using a support vector machine (SVM) algorithm. The proposed system achieved an accuracy of 99.1%. In a study, proposed a real-time intrusion prevention system for e-commerce platforms using deep learning algorithms. They used a deep belief network (DBN) to analyze network traffic and detect malicious activities. The proposed system achieved an accuracy of 99.3% as in [17]. Attacks may occur on web applications owing to a multitude of factors such as imprecise coding techniques, inherent deficiencies at the design level, configuration errors in the web application, as well as validation errors pertaining to user input as in [18].

DOI: 10.17148/IJARCCE.2024.13709

In [19], the authors presented a Hybrid Case-Based Neuro-Fuzzy System (HSBNFS) technique for developing an intrusion detection and prevention system for both signature-based and anomaly-based detection. A model for detecting and preventing payload attacks on web-applications was proposed using Recurrent Neural Networks (RNN) as in [20]. In [21], the authors proposed a deep learning approach for malware detection and classification using a deep forward neural network algorithm and the model had low false positives and negatives rates. The authors in [22] expressed the alarming threat to stored sensitive information and proposed a model for zero-day attacks based on Monte Carlo Based Pareto Rule.

In [23], the authors proposed a real-time intrusion prevention system based on machine learning algorithms. They used support vector machines (SVM), Naïve Bayes, and decision tree algorithms to analyze the network traffic and detect malicious activities. The proposed system achieved a detection accuracy of 98%. In [24], the authors proposed a real-time intrusion prevention system based on deep learning algorithms. The proposed system used a convolutional neural network (CNN) to analyze the network traffic and detect malicious activities. The proposed system achieved a detection accuracy of 99.4%.

Every day, new and advanced threats surface that endanger and target a vast array of global enterprises. This is why the scientific community is interested in the use and performance enhancement of intrusion detection systems. According to the authors in [25], the experimental findings for the real-time intrusion detection system demonstrated that the suggested model can discriminate between malicious and legitimate network traffic with high accuracy and a low false positive rate.

The available intrusion detection systems for e-payments, as in [26], are particular to the systems in which they have been integrated. This paper presents a general model for detecting fraud and intrusion attempts that arise in risky payment processes in the context of mobile commerce called the activity-event-symptoms (AES) model. In the context of mobile commerce, the AES model is used to detect fraud and intrusion assaults that pose a risk to the payment process. The AES model is intended to detect signs of fraud and intrusions by keeping track of different events and transactions that take place throughout the payment process in an environment of mobile commerce. After identifying the symptoms, the suspicion factors for the event characteristics are calculated, and these suspicion factors are then used to build the certainty factor for fraud and intrusion. A system that can detect intrusion, send alarms, and subsequently follow the item of interest was presented in [27]. To identify intrusions, they proposed an adaptive background subtractive. A methodology that is helpful in preventing unknown exploits, detecting vulnerabilities, detecting protocol anomalies, and thwarting denial of service floods was presented in [28].

In [29], the authors conducted a case study focusing on the use of Snort IPS to enhance e-commerce security for online retailers. They examined how Snort's real-time threat detection and prevention capabilities can be effectively deployed in a real-world e-commerce environment. The authors found that Snort IPS played a pivotal role in protecting online retailers from a range of threats, including web application attacks and fraudulent activities. They emphasized the importance of regularly updating Snort rules and maintaining rule sets tailored to e-commerce-specific risks. In [30], the authors explored the customization of Snort for e-commerce security, focusing on practical approaches to tailor Snort rulesets to the unique security challenges faced by online retailers. The authors emphasized that Snort's flexibility allowed for the creation of custom rules specific to e-commerce platforms. They discussed the importance of rule optimization to minimize false positives and the need for continuous monitoring and rule updates to address evolving threats.

Evolving intrusion attempts require innovative approaches to providing all-round security for e-commerce platforms. Web Application Firewalls are considered part of new and effective solutions to e-commerce security issues especially between client-side and web applications as in [31]. In [32], the authors explored the role of Web Application Firewalls (WAFs) and Intrusion Prevention Systems (IPS) in enhancing e-commerce security. They discussed the importance of protecting online retail applications and transactions from various threats. The paper highlighted the synergy between WAFs and IPS in safeguarding e-commerce platforms. They emphasize that WAFs play a crucial role in protecting web applications against vulnerabilities, while IPS complements this by offering network-level threat detection and prevention.

III. METHODOLOGY/DESIGN

To effectively provide protection for an e-commerce platform, security has to be provided for both application and network layer intrusions.

DOI: 10.17148/IJARCCE.2024.13709

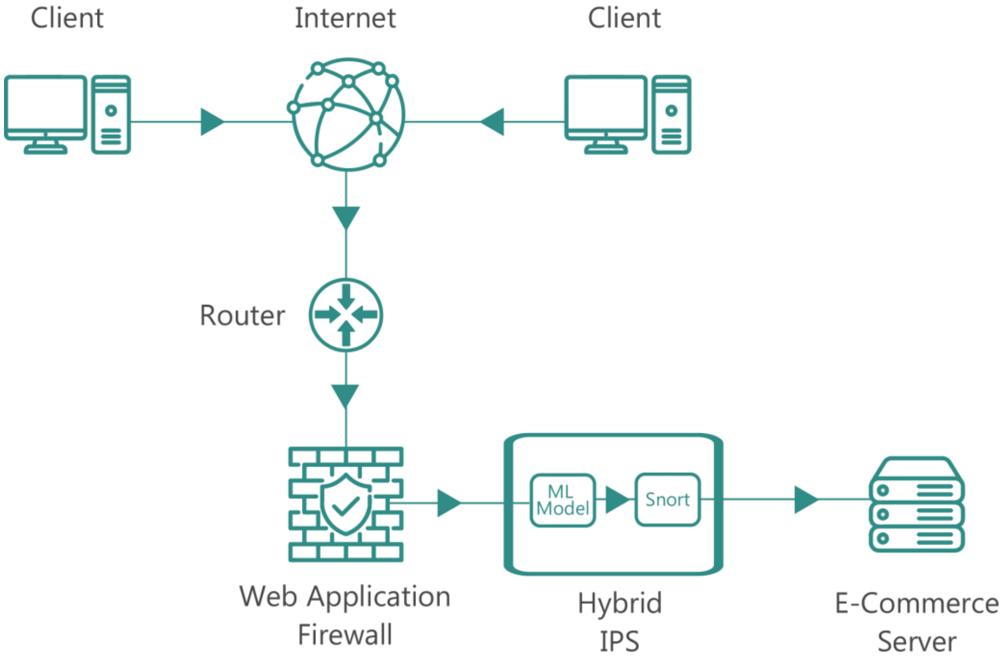


Figure 1: Architecture of the proposed system

The proposed system is a combination of a web application firewall (WAF) and a hybrid intrusion prevention system comprising a machine learning model and Snort. This configuration provides robust security for the e-commerce platform.

The clients which are the devices used by the customers and hackers to access the e-commerce platforms. They do so with internet access provided by their respective ISP. They generate network traffic which is analyzed by the system. The router directs traffic between the e-commerce server and security technologies and the rest of the network. It assigns and identifies IP addresses for both incoming and outgoing traffic.

The e-commerce server hosts the entire e-commerce application, handles requests from clients, manages product database, processing transactions and delivering content to customers. It also stores and processes sensitive information such as customer data, payment information and other details.

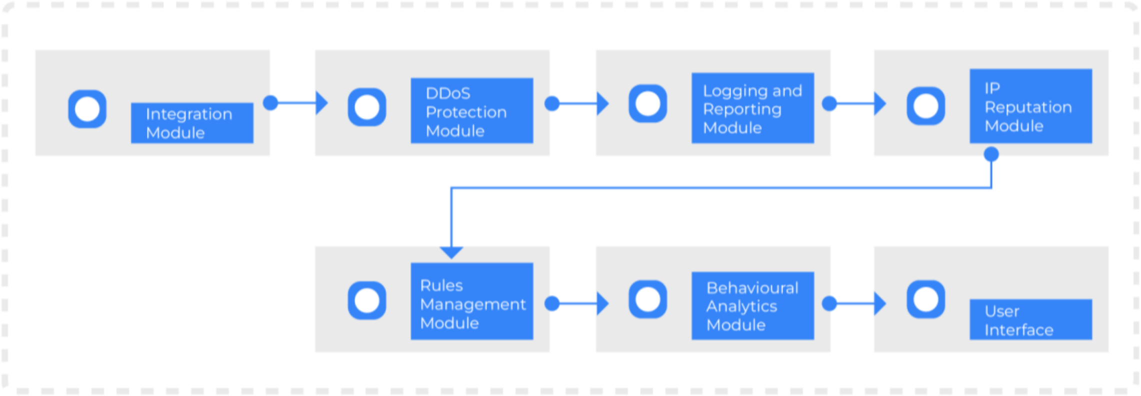


Figure 2: Architecture of the web application firewall

DOI: 10.17148/IJARCCE.2024.13709

The web application firewall is designed to protect against intrusions on the application layer where credit card information and other related information can be stolen from.

The integration module within the WAF allows for programmatic management and configuration while the DDoS protection module handles DDoS attacks. The IP Reputation, Rules management and behavioural analytics modules inspect, analyze and identify malicious requests. The logging and reporting module captures and stores reports of activities and the user interface provides a graphical interface for the user to see the workings of the WAF.

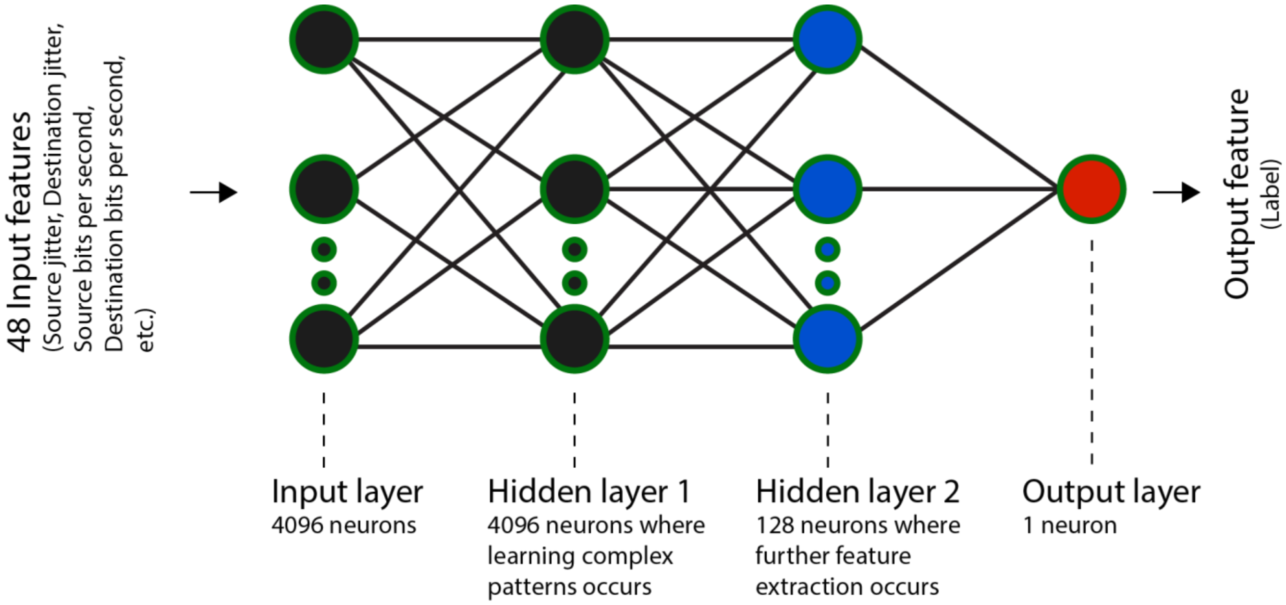

48 Input features
(Source jitter, Destination jitter, Source bits per second, Destination bits per second, etc.)
Output feature
(Label)
Input layer
4096 neurons
Hidden layer 1
4096 neurons where learning complex patterns occurs
Hidden layer 2
128 neurons where further feature extraction occurs
Output layer
1 neuron

Figure 3: Structure of the deep belief neural network

The deep belief neural network was designed to be 4 layers wide. The depth of each layer is specific to the work it performs. The input layer accepts the input features gotten from preprocessing the UNSW-15 data set which contains intrusive and non-intrusive data. Feature extraction is performed in the first hidden layer and further feature extraction is performed in the second hidden layer. The output layer produces a binary output of either 0 or 1 corresponding to intrusion or normal behaviour.

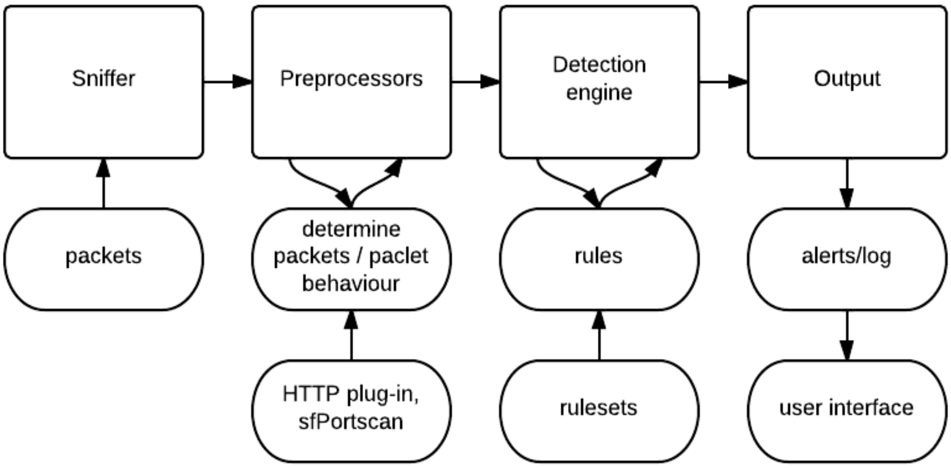


Figure 4: Snort architecture

DOI: 10.17148/IJARCCE.2024.13709

Snort as an open-source intrusion prevention system provides a reliable system for intrusion prevention. Its large database of rules accommodates a wide variety of threats. The rules have been customized to suit the proposed system where the machine learning model provides new rules for novel attacks.

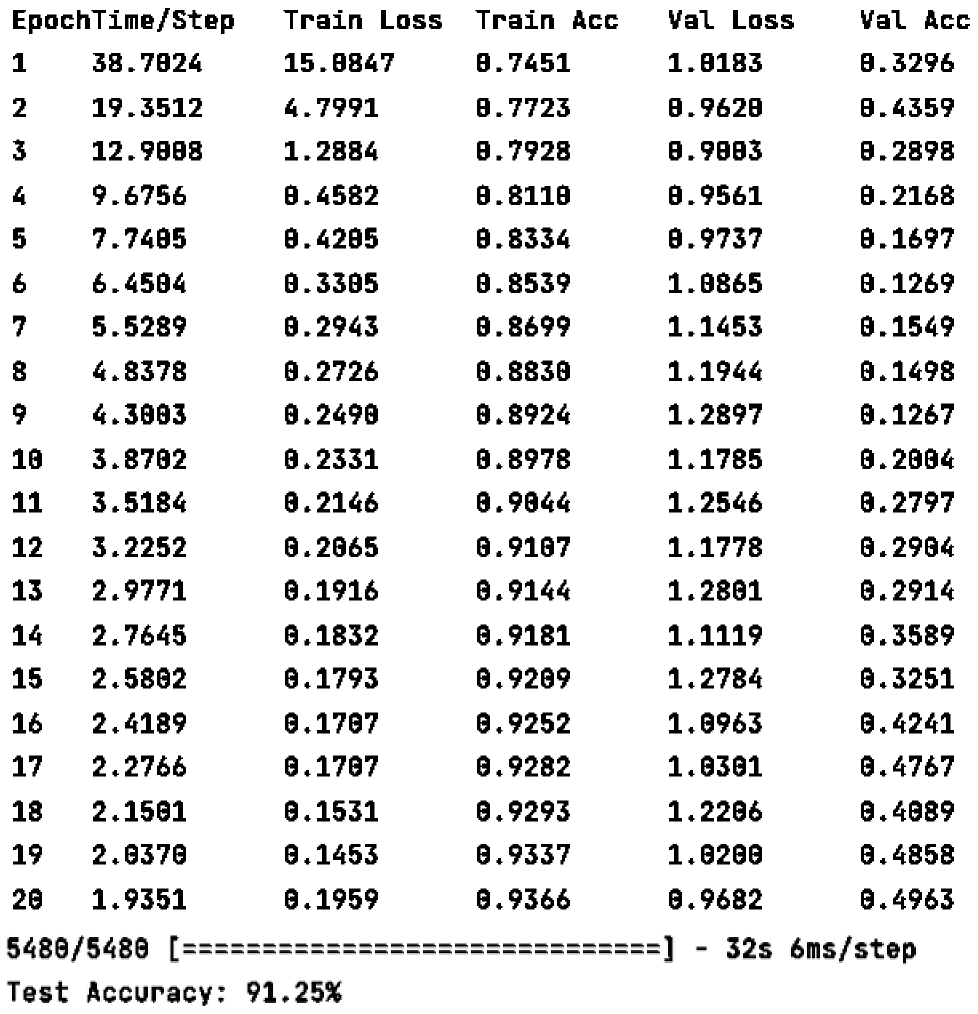
Snorts internal modules handle the traffic analysis and processing before handing over to the detection engine. The result is weighed against known signatures as well as input from the machine learning model. Eventually Snort takes appropriate action and logs data for reference.

IV. RESULTS AND DISCUSSION

The machine learning model was trained and tested over 20 epochs which provided good insight into the performance of the system. Various attacks were simulated using Metasploit and CURL which were detected by the system.

Table 1 provides insight on the strength of the machine learning model from the start of the training process till the 20th epoch. The model starts with a high training loss and relatively low accuracy on both the training and validation sets. By the end of the training (epoch 20), the training loss decreased, and the accuracy improved. However, it is important to check if the model is overfitting or generalizing well to unseen data. The validation loss and accuracy give insights into this.

TABLE 1 TRAINING THE MACHINE LEARNING MODEL (20 EPOCHS)



```
EpochTime/Step   Train Loss   Train Acc    Val Loss     Val Acc
1    38.7024     15.0847      0.7451       1.0183       0.3296
2    19.3512     4.7991       0.7723       0.9620       0.4359
3    12.9008     1.2884       0.7928       0.9003       0.2898
4    9.6756      0.4582       0.8110       0.9561       0.2168
5    7.7405      0.4205       0.8334       0.9737       0.1697
6    6.4504      0.3305       0.8539       1.0865       0.1269
7    5.5289      0.2943       0.8699       1.1453       0.1549
8    4.8378      0.2726       0.8830       1.1944       0.1498
9    4.3003      0.2490       0.8924       1.2897       0.1267
10   3.8702      0.2331       0.8978       1.1785       0.2004
11   3.5184      0.2146       0.9044       1.2546       0.2797
12   3.2252      0.2065       0.9107       1.1778       0.2904
13   2.9771      0.1916       0.9144       1.2801       0.2914
14   2.7645      0.1832       0.9181       1.1119       0.3589
15   2.5802      0.1793       0.9209       1.2784       0.3251
16   2.4189      0.1707       0.9252       1.0963       0.4241
17   2.2766      0.1707       0.9282       1.0301       0.4767
18   2.1501      0.1531       0.9293       1.2206       0.4089
19   2.0370      0.1453       0.9337       1.0200       0.4858
20   1.9351      0.1959       0.9366       0.9682       0.4963
5480/5480 [==============================] - 32s 6ms/step
Test Accuracy: 91.25%
```

DOI: 10.17148/IJARCCE.2024.13709

After training, the model was evaluated on a separate test set, and it achieved a test accuracy of 91.25%. This represents the model's performance on new, unseen data.

The Area Under the Precision-Recall Curve (AUC-PR) score as shown in figure 5 evaluates the model's precision and recall performance. A high AUC-PR (close to 1.0) signifies that our model effectively balances precision (minimizing false positives) and recall (capturing true positives). In this work, the AUC-PR score showcases the robustness of the intrusion detection system in identifying and accurately classifying instances of network intrusions.

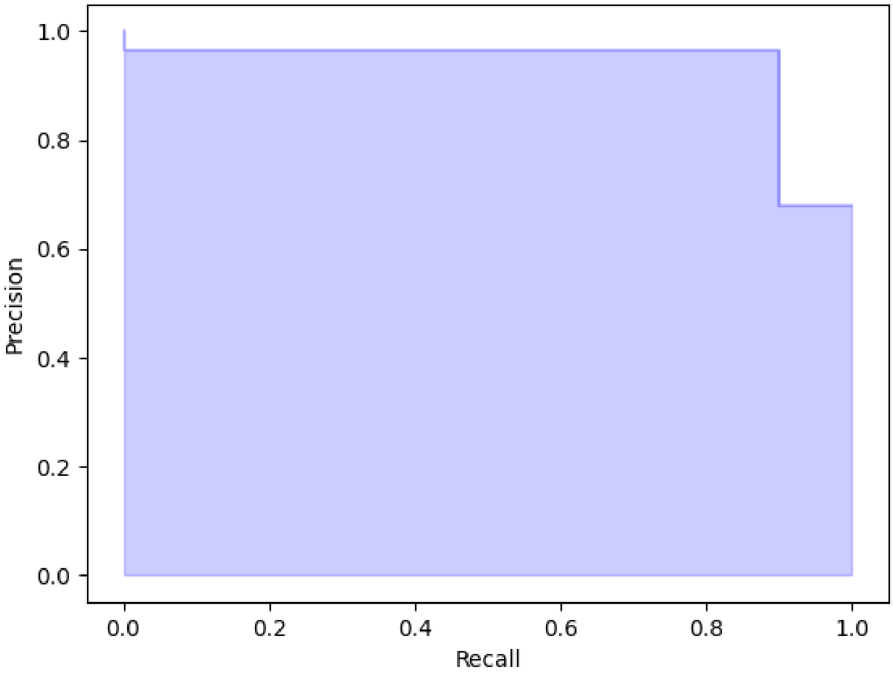


Figure 5: Precision-Recall Curve

The Area Under the Receiver Operating Characteristic Curve (AUC-ROC) further provides a holistic evaluation of the model's ability to discriminate between normal and intrusive activities across different decision thresholds (figure 6). The achieved AUC-ROC score of 0.92 attests to the system's commendable performance. This metric reflects the trade-off between true positive rate (sensitivity) and false positive rate (fall-out). The higher the AUC-ROC, the better the model's capacity to make accurate classifications.

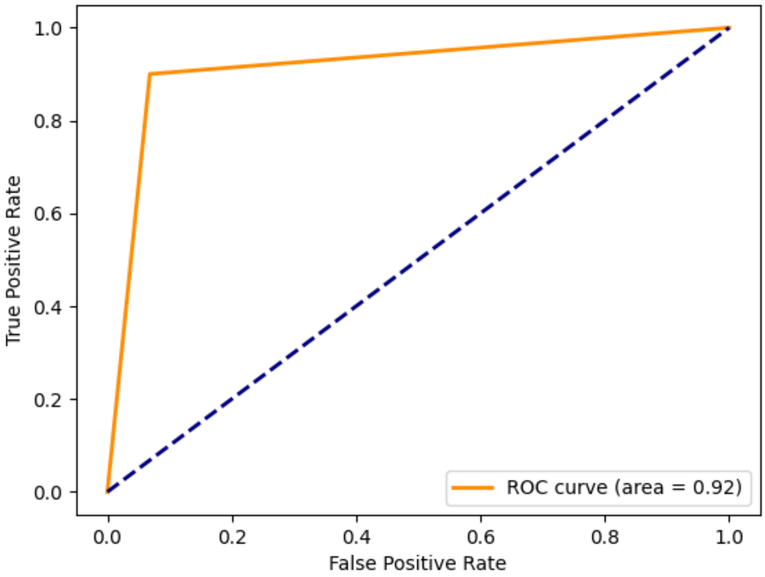


Figure 6: Receiver Operating Characteristic Curve

DOI: 10.17148/IJARCCE.2024.13709

The confusion matrix in figure 7 provides detailed insights into the model's classification performance:

a) True Positives (TP): 108784
b) True Negatives (TN): 51447
c) False Positives (FP): 4553
d) False Negatives (FN): 10557

By analyzing the confusion matrix, we gain a nuanced understanding of the model's strengths and areas for improvement. The low false-positive rate and high true-positive rate are indicative of the system's ability to effectively discern and respond to network intrusions.

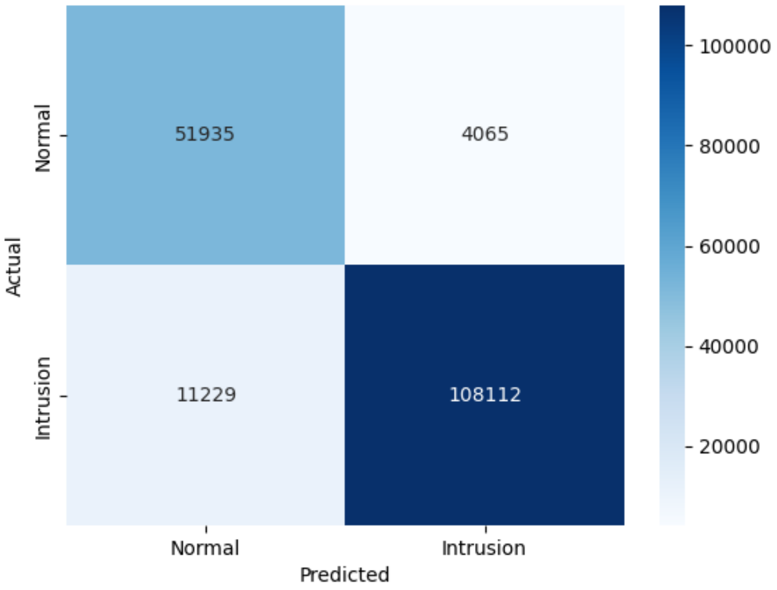
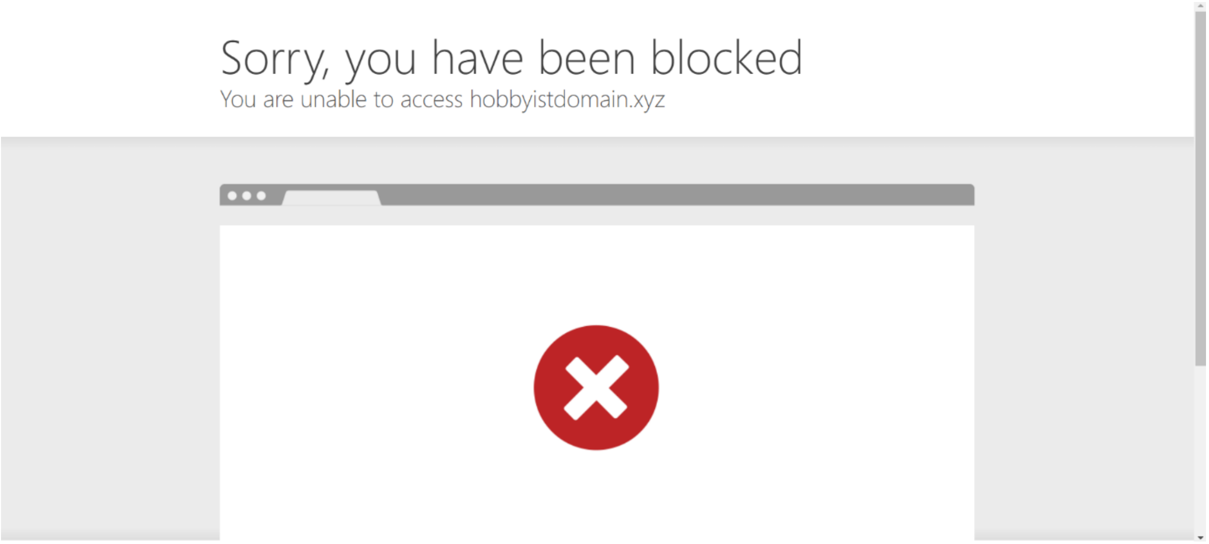


Figure 7: Confusion Matrix

The error screen in figure 8 figure shows the successful blocking of a malicious request targeting credit card information through SQL injection by Curl.



Sorry, you have been blocked

You are unable to access hobbyistdomain.xyz

Figure 8: WAF block after Curl trigger

DOI: 10.17148/IJARCCE.2024.13709

V. CONCLUSION

Our Hybrid Real-Time Intrusion Prevention System (IPS) for E-Commerce platforms performed outstandingly well with an accuracy of 91.2% and false positive rate of 8.14%. Leveraging a combination of Snort for network intrusion detection and Cloudflare as a Web Application Firewall (WAF), our system demonstrates robust capabilities in protecting against data breaches from SQL injection and DoS attacks.

Using TensorFlow in Pycharm IDE, we built the DBNN and trained the model using the UNSW-NB15 dataset which is a comprehensive collection of signatures. The model was integrated with Snort to provide a more efficient system. The Web Application Firewall was customized on the Cloudflare platform with a focus on DoS attacks.

Through meticulous testing and analysis using Metasploit and CURL, our hybrid real-time intrusion prevention system demonstrated robust capabilities in safeguarding our E-Commerce platform. The high accuracy of Snort aided by the DBNN, coupled with the effective blocking of malicious requests by Cloudflare, validates the efficacy of our implemented IPS. The precision-recall curve and ROC curve provide a nuanced understanding of the system's performance, highlighting its ability to balance precision and recall in intrusion detection.

REFERENCES

[1] Susmitha, K. “Impact of COVID 19 on E-Commerce.” *Journal of Interdisciplinary Cycle Research, Vol. XII, Issue IX, 1161 – 1165,* 2020

[2] Cigdem, S. “Competitiveness of E-Commerce Companies: An Integrated Approach.” *International Journal of eBusiness and eGovernment Studies, Vol. 4, No. 1, 2012 ISSN: 2146-0744 (Online),* 2012.

[3] Vinicius, F., Lucas, M., Diorgenes, E., & Rodrigo, R. “Fraud Detection and Prevention in E-Commerce: A Systematic Literature Review.” *Electronic Commerce Research and Applications, Vol. 56, Issue C, ISSN: 1567 – 4223,* 2022.

[4] Baluch, A. *Forbes Advisor*. Retrieved from Forbes Advisor: https://www.forbes.com/advisor/business/ecommerce-statistics/#sources_section 2023

[5] Bomil, S. & Ingoo, H. “The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce.” *International Journal of Electronic Commerce, Vol. 7, 135-161,* 2023

[6] Pal, B., Daniel, T., Chatterjee, R. & Ristenpart, T. “Beyond Credential Stuffing: Password Similarity Models Using Neural Networks.” 2019

[7] Libunao, M., Sarmiento, P., Sugimoto, H., Regalario, J., Mauricio, K. & Vallespin, M. “ Enhancing Data Security in E-Commerce: Strategies, Impacts and Improvements.” *International Journal of Multidisciplinary Research and Publications (IJMRAP), Vol. 1, Issue 1, ISSN: 2581 – 6187,* 2019

[8] Saqib S. “A Customer-Centric View of E-Commerce Security and Privacy.” *Applied Sciences. Vol. 13, Issue 2. 1020,* 2023

[9] Alkhaleel, A. M., Alghamdi, M. A., Al-Turki, U., & Aldossary, H. A. “Intrusion prevention system (IPS) for e-commerce applications.” *2018 15th Learning and Technology Conference (pp. 1-6). IEEE,* 2018

[10] Rahman, M. S., Begum, S., & Uddin, M. Z. “Real-Time Security Monitoring for E-commerce Systems.” *2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 432-437). IEEE.,* 2017

[11] Anderson, J., Smith, M., & Brown, R. “Real-time Fraud Detection in E-commerce.” *Journal of E-commerce Research, 18(2),* 123-145, 2017

[12] Lee, S., & Kim, H. “Real-time Monitoring for Improving E-commerce Website Performance.” *International Journal of Advanced Computer Science and Applications, 9(5),* 421-428, 2018

[13] Gogoi, P., & Borah, S. “Real-Time Intrusion Prevention System for E-commerce Platform Using Machine Learning.” *International Journal of Advanced Computer Science and Applications, 11(8), 91-96,* 2020

[14] Kim K. J., Kwon, J., Kim, Y. H., & Kim, J. H. “Real-time intrusion prevention system for e-commerce platform using deep learning.” Multimedia Tools and Applications, 77(9), 10935-10954, 2018

[15] Vats M., & Singh, Y. “An Effective Intrusion Prevention System for E-commerce Platforms.” *International Journal of Advanced Trends in Computer Science and Engineering, 9(1), 407-412,* 2020

[16] Ma L., Chen, J., & Hu, J. “Real-time Intrusion Prevention System for E-commerce Platforms Based on SVM”. *IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) (pp. 586-591), 2019*

[17] Cheng Si, Z. Y. “A Real-Time Intrusion Prevention System for E-Commerce Platforms Based on Deep Learning.” *Journal of Computer Science: Conference Series, 1597, 012025,* 2020

[18] Sonewar, P.A., & Mhetre, N.A. “A Survey of Intrusion Detection System for Web Application.” *International journal of engineering research and technology, 3,* 2014

DOI: 10.17148/IJARCCE.2024.13709

[19] Davies I. N., Taylor O.E., Anireh V.I.E, Bennett E.O. "Adaptive Hybrid Case-Based Neuro-Fuzzy Model for Intrusion Detection and Prevention for Smart Home Network" *International Journal of Computer Sciences and Engineering. Vol 12(5), 1-10,* 2024

[20] Taylor O.E. & Ezekiel P.S. "A Robust System for Detecting and Preventing Payloads Attacks on Web-Applications Using Recurrent Neural Network (RNN)" *European Journal of Computer Science and Information Technology, Vol. 10(4), 1-13.* 2022

[21] Taylor O.E., Ezekiel P.S. & Sako D.J.S. "A Deep Learning Based Approach for Malware Detections and Classification" *International Journal of Software & Hardware Research in Engineering (IJSHRE), Vol. 9(4), 32-40,* 2021

[22] Emmah V.T., Ugwu C. & Onyejegbu L.N. "An Enhanced Classifiation Model for Likelihood of Zero-Day Attack Detection and Estimation" *European Journal of Electrical Engineering and Computer Science, Vol. 5(4), 69-75,* 2021

[23] Gupta A., & Kumar, R. "Real-time intrusion prevention system using machine learning techniques for e-commerce platforms." *International Journal of Computer Applications, 180(1), 15-19,* 2018

[24] Zhang Y., Zhou, S., & Li, S. "Real-Time Intrusion Prevention System for E-commerce Platforms Based on Deep Learning." *IEEE Access, 8, 52043-52052,* 2020

[25] Chamou, D., Toupas, P., Ketzaki, E., Papadopoulos, S., Giannoutakis, K.M., Drosou, A., & Tzovaras, D. "Intrusion Detection System Based on Network Traffic Using Deep Neural Networks." *IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 1-6, 2019

[26] Venkataram, P., Babu, B.S., Naveen, M.K., & Gungal, G.H. "A Method of Fraud & Intrusion Detection for E-payment Systems in Mobile e-Commerce. *2007 IEEE International Performance, Computing, and Communications Conference*, 395-401, 2007

[27] Bar, D., Pande, D., Sandhu, M.S., & Upadhyaya, V. "Real-time security solution for automatic detection and tracking of intrusion." *2015 Third International Conference on Image Information Processing (ICIIP)*, 399-402, 2015

[28] Nalavade, K.C., & Meshram, B.B. "Intrusion prevention systems: data mining approach." *Proceedings of the International Conference and Workshop on Emerging Trends in Technology*. 2010

[29] Patel, A., Gupta, S., & Sharma, N. "E-commerce Security using Snort IPS: A Case Study of Online Retailers." *Journal of E-commerce Research, 20(4), 87-101,* 2019

[30] Yang, H., Wang, Y., & Liu, C. "Customizing Snort for E-commerce Security: A Practical Approach." *International Journal of E-commerce Research and Applications, 12(1), 1-14,* 2020

[31] Ghanbari, Z., Rahmani, Y., Ghaffarian H., Hossein M. "Comparative approach to web application firewalls." *IEEE Conference on Knowledge-based Engineering and Innovation*, 2015

[32] Johnson, R., Smith, M., & Davis, L. "Enhancing E-commerce Security with Web Application Firewalls and Intrusion Prevention Systems." *Journal of E-commerce Research, 16(2), 45-60,* 2015