Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.033792
Article

Network Intrusion Detection Model Using Fused Machine Learning Technique

Fahad Mazaed Alotaibi*

Faculty of Computing and Information Technology in Rabigh (FCITR), King Abdulaziz University, Jeddah, Saudi Arabia
*Corresponding Author: Fahad Mazaed Alotaibi. Email: fmmalotaibi@kau.edu.sa
Received: 28 June 2022; Accepted: 22 September 2022

Abstract: With the progress of advanced technology in the industrial revolution encompassing the Internet of Things (IoT) and cloud computing, cyberattacks have been increasing rapidly on a large scale. The rapid expansion of IoT and networks in many forms generates massive volumes of data, which are vulnerable to security risks. As a result, cyberattacks have become a prevalent and danger to society, including its infrastructures, economy, and citizens' privacy, and pose a national security risk worldwide. Therefore, cyber security has become an increasingly important issue across all levels and sectors. Continuous progress is being made in developing more sophisticated and efficient intrusion detection and defensive methods. As the scale of complexity of the cyber-universe is increasing, advanced machine learning methods are the most appropriate solutions for predicting cyber threats. In this study, a fused machine learning-based intelligent model is proposed to detect intrusion in the early stage and thus secure networks from harmful attacks. Simulation results confirm the effectiveness of the proposed intrusion detection model, with 0.909 accuracy and a miss rate of 0.091.

Keywords: Cyberattack; machine learning; prediction; solution; intrusion detection

1 Introduction

While increasing incorporation of the internet and social media has been transforming people's learning and work approach, it also poses increasingly serious security threats. Identifying various network attacks, particularly unseen attacks, is a critical issue that needs an urgent solution.

The upsurge in the confidence of information-age industry sectors, governments, and economies on cyberinfrastructure increases their vulnerability to cyberattacks. A cyberattack targets the most critical form of a country's enterprise, military, administration, or other infrastructure possessions and its citizens. Personally identifiable information containing credit card data, passwords, security numbers, and other complex information is at high risk of theft through cyberattacks. The volume and complexity of cyberattacks (including malicious hacking, cyber surveillance, and cyber warfare) are growing enormously, posing significant threats to the cyber domain.

Cyber security, often called electronic data security, safeguards computers, data centers, mobile devices, electrical components, networks, and data against malicious intrusions. Cyber security primarily aims to lower the risk of cyberattacks and protect against unauthorized system applications, networks, and technology. Defending systems, infrastructures, applications, equipment, and data from cyberattacks require technologies, processes, and policies.

Cyber security involves a set of techniques and practices to protect computers, networks, applications, data from attacks, and unauthorized admittance, modification, or devastation. Gateways, antivirus software, and intrusion detection schemes are examples of such cyber security systems. An intrusion detection system is a system to detect, determine, and identify unauthorized and malicious activities involved, such as consumption, copying, reconfiguration, and destruction of data. A network security platform is divided into a network security structure and a computer security structure.

Cyber security provides protection to both personal and commercial internet-connected gadgets, and it implements various precautionary measures to protect computer systems, cloud platforms, and online personal information from cyberattacks. A few types of cyber security are described below.

Application security protects sensitive information at the application level by developing and analyzing security measures within programs to prevent unauthorized access or modification threats. The security precautions are mostly implemented before the application's launch. Strategies such as demanding a secure password from the user may be used to secure an application.

Cloud security is the fortification of data stored online through cloud computing from attackers. It can be accomplished by implementing firewalls, ethical hacking, misdirection, tokenization, and virtual private networks as well as by preventing public internet connections. Cloud security involves buying and selling services enclosed in a data center. Most people use cloud storage services such as Google Drive, Microsoft OneDrive, and Apple iCloud. The vast amounts of data stored on such platforms must be highly secure.

Certain rules and network security settings are used for the software and hardware technologies to safeguard computer networks and data integrity, confidentiality, and accessibility. This type of security protects the computer from threats within and outside a network by employing several techniques to evade malicious files or other data breaches.

A firewall serves as a shield barrier between a network and an external, suspicious network, such as the internet, essentially protecting the network. A firewall may permit, or block network traffic based on security settings. A standard attack mitigation technique is cyberattacked detection that entails retorting to an unusual association to disclose the existence of an attack or outline in a network. Intrusion detection is one of the supreme effective techniques for detecting cyberattacks. According to [1], an intrusion detection method recognizes an intrusion signature in a persistent flow of associations.

Misuse detection in an intrusion detection system deliberates the signatures of attacks, thus aiding in detecting intrusions, whereas anomaly detection flags intrusions when the system perceives deviance from the profiles of ordinary network activities. A hybrid approach is developed by merging the outcomes of both methods [2].

A large amount of information regarding cyberattack detection strategies is available in the public domain. However, most of these strategies are ineffective in perceiving attacks and some require excessive computing resource. Moreover, most existing approaches are computationally infeasible although they can be considered conceptually classical methods. The subsequent section of this paper further discusses publicly available cyberattack detection approaches, highlighting the methodology, advantages, and weaknesses of each approach.

Machine learning (ML) techniques have gained popularity for cyberattack detection. ML algorithms use training data to classify and predict the occurrence of a learned example and use this information to perceive the consequence of specific measures centered on existing sample inputs. Then, based on the prediction data, a model is built to obtain accurate conclusions [3]. In the current cyber detection scenario, ML has dramatically improved the detection accuracy [4–6].

2 Literature Review

Extensive research has been conducted on cyber security and cyberattack detection. Teixeira et al. [7] developed a model for binary and multiclass classification and examined its efficiency. They also examined the effect of the number of neurons in the model and the learning rate on the model's performance. Furthermore, their model was compared with other ML techniques such as J48, artificial neural networks (ANNs), random forests (RFs), and support vector machines (SVMs) using a standard data set.

Pontes et al. [8] presented malware in machine code sequence data and clarified the malware using dynamic Bayesian networks (DBNs). They compared the performance of the DBN with that of three frequently used classification algorithms: SVM, decision trees (DT), and the k-nearest neighbor technique. The experiments demonstrated that the RNN-based intrusion detection system is suitable for building a high-accuracy classifier model and has better accuracy than the standard deep learning-based classification techniques for binary and multiclass classification. The detection accuracy of the DBN model is comparable to the best of the previous methods. When a higher amount of unlabeled data was used for DBN pre-training, it outperformed other classification methods considered for comparison. The DBNs also extract feature vectors from input data as an autoencoder.

Ladder networks, a semi-supervised technique, were used to analyze network data [9]. In this method, the autoencoder can precisely reflect the expected framework of the input data even with a fewer number of feature vectors. Two experiments were performed using the ladder network. In the first trial, where the number of classes and instances was varied, the semi-supervised ladder network performed better than the supervised classifiers in network data categorization. In the second trial, where the number of labeled samples was varied, the ladder network was able to attain an accuracy of over 90% with various labeled and unlabeled sample ratios.

Ingre et al. [10] proposed a proficient intrusion detection system for a vehicular network security center on a deep neural network. Using a pre-training technique for an unsupervised deep belief network, the DNN offers the likelihood of each class distinguishing from steady hacker packets, and the model can accurately recognize any malicious attack on the vehicle. Furthermore, the authors proposed a unique feature vector with its mode and value material detached from network packets and used it for training and testing. Experimental results proved that the suggested approach could detect attacks in real time with an accuracy of approximately 98% even with a relatively small number of convolution layers.

Najada et al. [11] proposed an Internet of Things (IoT) threat analysis using an ANN to detect potential risks [11]. A multi-level perceptron, a supervised ANN, was trained to utilize internet packet suggestions, and its capacity to detect distributed denial-of-service attacks was tested. The authors focused on classifying typical and harmful patterns on an IoT network and tested the proposed ANN approach on a simulated IoT network. Ullah et al. [12] developed a genetic algorithm-based intrusion detection system based on GA's proven success in detecting various intrusions competently. The GA parameters and the procedure of evolution were thoroughly investigated. The system's performance was tested by implementing it on the Defense Advanced Research Projects Agency (DARPA) 1998

dataset. The results indicated that some IP address classes were more vulnerable to breaches and attacks.

Khan et al. [13] discussed the design of a supervised control and data acquisition test platform for cyber security research. The method was tested for monitoring the water drainage process in a water tank. Advanced cyberattacks were initiated in contradiction to the tested. The performance of the proposed method was compared with that of five standard ML algorithms in perceiving the attacks: RF, DT, logistic regression, Naive Bayes, and KNN. In the tests, during the attacks, the network traffic was documented, and its characteristics were derived based on a training dataset and testing various ML techniques [14,15]. Moreover, the performance of ML models during training and testing was compared to the performance of the same models after they were deployed in the live network. The results show that ML models can identify threats in real time.

Khan et al. [16] applied various methods, namely DNNs, RF, voting, variation autoencoders, and stacking ML classifiers, for handling unfair datasets to develop a dynamic system using the most current intrusion detection dataset [17]. The efficiency of the sampling techniques was tested. The proposed method could detect attacks while dealing with excessive class dissemination with fewer samples, thereby producing more practical data fusion settings that target data classification.

In another study, the fine-grained channel state information (CSI) was used in Wi-Fi gadgets to develop and apply AR-Alarm, a robust human intrusion detection system [18]. AR-Alarm uses a robust feature and a self-adaptive learning engine to provide real-time intrusion detection in various scenarios deprived of calibration. In that study, a few unique approaches were proposed to detect actual human intrusion from normal item motion, such as object falling, curtain fluctuation, and dogs moving, to increase system robustness. AR-Alarm obtained a high detection rate and a low false alarm rate in the experiments. Feature selection increases the forecasting procedure of DT-based intrusion detection systems.

Saleem et al. [19] used the subset assessment approach for feature selection correlation. The performance of the method was tested for five classes in addition to binary class classification before and after feature selection. The result was compared with those of other existing methods. The dataset's binary class classification result was better than the five-class classification result, suggesting that the DT-based intrusion detection system has a high detection rate and accuracy.

Asif et al. [20] used significantly distorted real-world benchmark network traffic statistics of various types of attacks [20]. Their method adopted an oversampling approach to correct the class imbalance in the datasets. First, they created a unique prediction model for each attack and fine-tuned them for optimum accuracy. Next, they created a prediction model for all attacks based on deep learning and a minimum number of features, and then modified the model to accomplish the maximum accuracy. Their model precisely predicted the threat and type of attack.

In addition to the studies described above, the increasing importance of automated frameworks for worldwide company procedures in the industry 4.0 era has been analyzed from an academic and practical standpoint [21–23]. This research presented advances in ANNs, image processing, multi-purpose decision-making, and blurred linguistic variables. Furthermore, automated systems have been confirmed to improve the performance of supply chain administration systems and increase corporate performance [24–26]. It was also demonstrated that the growing function of automated arrangement necessitates capital reserves for R & D activities.

3 Methodology

The present study mainly aims to achieve reliable real-time prediction of cyberattacks by using a fused ML method and provide high-accuracy results intelligently. The proposed model is divided into training and validation phases, as shown in Fig. 1.

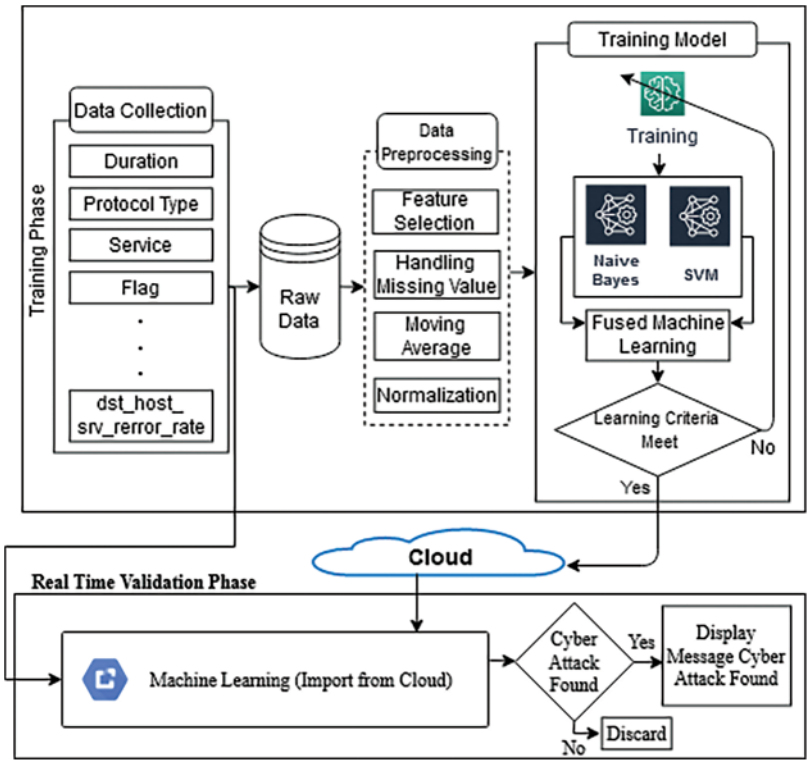

Figure 1: Proposed model of network intrusion detection using fused machine learning technique

The training phase comprises three steps. First, data collection is realized by sourcing data from input parameters and storing them in the database. Second, the stored data in the database are preprocessed to eliminate noise using feature selection and handle missing values, moving averages, and normalization. Finally, the processed data are forwarded to the training model through the Naïve Bayes and SVM algorithms.

The trained patterns are sent to the fused ML system, which combines the decision-level fusion method with ML to improve accuracy and decision-making. The fused ML method combines the predictions of both algorithms using a fuzzy inference system. Then, resulting prediction is checked to determine if the learning criteria are met; if it meets, then the trained output is stored on the cloud, and if not, it is updated.

Fig. 2 shows the graphical representation of the proposed model performance as good, satisfactory, and bad, indicated with yellow, green, and blue, respectively. Fig. 3 shows that if the Naïve Bayes and SVM outputs are “no”, intrusion detection is “no”. Fig. 4 shows that if Naïve Bayes and SVM outputs are “yes”, then intrusion detection is “yes”.

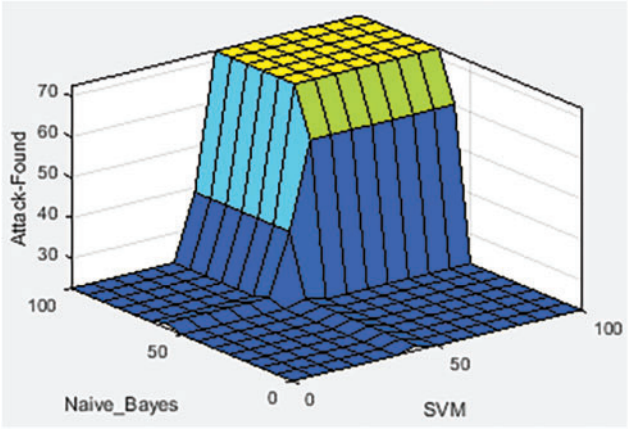

Figure 2: Rule surface of the proposed model

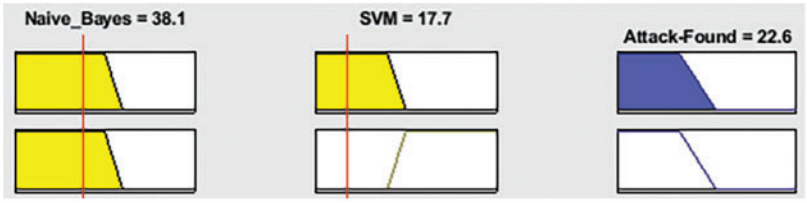

Figure 3: Illustration of the rule of the proposed model (No)

Figure 4: Illustration of the rule of the proposed model (Yes)

The trained patterns are imported from the cloud for prediction purposes in the validation phase. A message will be displayed if an intrusion is detected, while the process will be stopped in case intrusion is not found.

4 Simulation Results

The proposed smart system that uses a fused ML technique of the Naive Bayes and SVM algorithms was applied to 25192 cases of a UCI Machine Learning data repository dataset to forecast real-time cyberattacks. The dataset was divided into training and validation sets in a 7:3 ratio (training: 17634 samples; validation: 7558 samples). The performance of the method was evaluated in terms of

the statistical metrics of accuracy, sensitivity, specificity, miss rate, and precision, calculated as Eqs. (1)–(5), respectively.

$$Sensitivity = \frac{\sum TruePositive}{\sum ConditionPositive} \tag{1}$$

$$Specificity = \frac{\sum TrueNegative}{\sum ConditionNegative} \tag{2}$$

$$Accuracy = \frac{\sum TruePositive + \sum TruePositive}{\sum TotalPopulation} \tag{3}$$

$$Miss - Rate = \frac{\sum FalseNegative}{\sum ConditionPositive} \tag{4}$$

$$Fallout = \frac{\sum FalsePositive}{\sum ConditionNegative} \tag{5}$$

Further, the likelihood ratios and predictive values are calculated as follows:

$$LikelihoodPositiveRatio = \frac{\sum TruePositiveRatio}{\sum FalsePositiveRatio} \tag{6}$$

$$LikelihoodNegativeRatio = \frac{\sum TruePositiveRatio}{\sum FalsePositiveRatio} \tag{7}$$

$$PositivePredictiveValue = \frac{\sum TruePositive}{\sum PredictedConditionPositive} \tag{8}$$

$$NegativePredictiveValue = \frac{\sum TrueNegative}{\sum PredictedConditionNegative} \tag{9}$$

Table 1 shows the training results of the Naïve Bayes model.

Table 1: Training of the Naïve Bayes model

Input	Samples	Result (output)	
	Estimated output	Positive (Predicted)	Negative (Predicted)
		TP	FN
	8245 Positive	7000	1245
		FP	TN
	9389 Negative	392	8997

Of the 17634 samples, 8245 were positive and 9389 were negative samples, with positive indicating no intrusion and negative suggesting presence of intrusion. Of the actual positive cases, 7000 samples were correctly predicted as no intrusion (true positive (TP)), while 1245 were incorrectly predicted as an intrusion (false negative (FN)). Similarly, of the negative cases, 8997 samples were correctly detected

as an intrusion (true negative (TN)) and 392 samples were incorrectly predicted as no intrusion (false positive (FP)). Table 2 shows the validation results of the Naïve Bayes model.

Table 2: Validation results of the Naïve Bayes model

Input	Samples (7558)	Result (output)	
	Estimated output	Positive (Predicted)	Negative (Predicted)
		TP	FN
	3498 (Positive)	2890	608
		FP	TN
	4060 (Negative)	188	3872

Of the 7558 samples used in the validation process, 3498 were positive and 4060 were negative samples. Of the actual positive cases, 2890 samples were correctly predicted as no intrusion (TP), while 608 were incorrectly predicted as an intrusion (FN). Of the actual negative samples, 3872 samples were correctly predicted as an intrusion (TN) and 188 samples were incorrectly predicted as no intrusion despite the presence of intrusions (FP).

Tables 3 and 4 respectively show the training and validation results of the SVM model.

Table 3: Training results of the SVM

Input	Samples (17634)	Result (output)	
	Estimated output	Positive (Predicted)	Negative (Predicted)
		TP	FN
	8245 Positive	6745	1500
		FP	TN
	9389 Negative	527	8862

Table 4: Validation results of the SVM model

Input	Samples (7558)	Result (output)	
	Estimated output	Positive (Predicted)	Negative (Predicted)
		TP	FN
	3498 Positive	2730	768
		FP	TN
	4060 Negative	278	3782

Among the 17634 training samples, 8245 were positive and 9389 were negative samples. Of the actual positive cases, 6745 were correctly predicted as no intrusion (TP), while 1500 samples were incorrectly predicted as an intrusion (FN). Of the actual negative cases, 8862 samples were correctly

identified as an intrusion (TN), while 527 samples were incorrectly predicted as no intrusion despite the presence of intrusions (FP).

Among the 17634 training samples, 3498 were actual positive and 4060 were actual negative samples. Of the actual positive cases, 2730 were correctly predicted as no intrusion (TP), while 768 samples were incorrectly predicted as an intrusion (FN). Of the actual negative cases, 3782 samples were correctly identified as an intrusion (TN), while 278 samples were incorrectly predicted as no intrusion despite the presence of intrusions (FP).

Table 5 shows the performance of the Naïve Bayes model in terms of the five performance metrics.

Table 5: Performance of the proposed Naïve Bayes model in training and validation in terms of statistical measures

Naïve Bayes	Accuracy	Sensitivity TPR	Specificity TNR	Miss-rate	Fall-out FPR	LR+	LR-	PPV (Precision)	NPV
Training (NB)	0.907	0.849	0.958	0.093	0.041	20.70	0.097	0.947	0.878
Validation (NB)	0.894	0.826	0.953	0.106	0.046	17.95	0.111	0.938	0.864

The accuracy, sensitivity, specificity, miss rate, and precision of the Naïve Bayes model were, respectively, 0.907, 0.849, 0.958, 0.093, and 0.947 in the training, and 0.849, 0.836, 0.953, 0.106, and 0.938 in the validation. Furthermore, the fall-out likelihood positive ratio, positive and negative probability ratios, and positive and negative predictive values, respectively, were 0.041, 20.707, 0.097, 0.947, and 0.878 in the training and 0.046, 17.956, 0.111, 0.938, and 0.864 in the validation.

Table 6 shows the performance of the SVM model in terms of the five performance metrics.

Table 6: Performance of the proposed SVM model in training and validation in terms of statistical measures

SVM	Accuracy	Sensitivity TPR	Specificity TNR	Miss-Rate (%) FNR	Fall-out FPR	LR+	LR-	PPV (Precision)	NPV
Training	0.885	0.818	0.943	0.916	0.056	14.60	0.971	0.927	0.855
Validation	0.861	0.780	0.931	0.139	0.068	11.47	0.149	0.907	0.831

The accuracy, sensitivity, specificity, miss rate, and precision of the SVM model were, respectively, 0.885, 0.818, 0.943, 0.916, and 0.927 in the training and 0.861, 0.780, 0.931, 0.139, and 0.907 in the validation. Furthermore, the fall-out likelihood positive ratio, positive and negative probability ratios, and positive and negative predictive values, respectively, were 0.056, 14.607, 0.971, 0.927, and 0.855 in the training and 0.068, 11.470, 0.149, 0.907, and 0.831 in the validation.

Table 7 shows the results of the proposed fused ML-based intrusion detection model. Of the 11 tests conducted, only in one case, the proposed and expert-decision-based methods showed contradictory results. Table 8 shows the assessment of the performance of the proposed system in comparison with the Naïve Bayes and SVM methods alone. The accuracy and miss rate were 0.894

and 0.106 in the Naïve Bayes model and 0.861 and 0.139 in the SVM, respectively. Meanwhile, the proposed method had 0.909 accuracy and 0.091 miss rate. These results demonstrate the superior performance of the proposed fused ML-based approach.

Table 7: Results of the proposed fused ML-based intrusion detection model

Sr. No.	Naïve Bayes	SVM	Proposed intrusion detection model	Human expert decision of the intrusion detection model	Probability of correctness	Probability of errors
1	38.1 (No)	24.1 (No)	17.4 (No)	No	1	0
2	28.1 (No)	71.1 (Yes)	22.6 (No)	No	1	0
3	27.1 (No)	24.1 (No)	22.6 (No)	No	1	0
4	27.1 (No)	24.1 (No)	22.6 (No)	No	1	0
5	27.1 (No)	24.1 (No)	22.6 (No)	No	1	0
6	27.1 (No)	24.1 (No)	22.6 (No)	No	1	0
7	76.1 (Yes)	71.1 (Yes)	72.5 (Yes)	Yes	1	0
8	78.1 (Yes)	71.1 (Yes)	72.5 (Yes)	Yes	1	0
9	28.1 (No)	71.1 (Yes)	22.6 (No)	Yes	1	0
10	80.5 (Yes)	71.1 (Yes)	72.5 (Yes)	Yes	1	0
11	91.3 (Yes)	71.1 (Yes)	22.6 (No)	Yes	0	1

Table 8: Comparison of the proposed model with Naïve Bayes and SVM algorithms alone

Naïve Bayes	Accuracy	0.894
	Miss rate	0.106
SVM	Accuracy	0.861
	Miss rate	0.139
Proposed fused ML method	Accuracy	0.909
	Miss rate	0.091

5 Conclusion

With the drastic increase in cybercrimes and exploitation of the various vulnerabilities in the computing environment, ethical hackers are increasingly concerned with assessing security flaws and recommending mitigation strategies. Currently, there is an urgent need to develop effective cyber security systems. ML algorithms have been gaining popularity in intrusion detection systems owing to their ability to learn, adapt, and react appropriately without being explicitly programmed to execute specific tasks. This study proposed an intelligent model empowered with fused ML techniques such as the naïve Bayes and SVM to predict intrusion in a network. The simulation results confirmed that, compared with other approaches, the proposed system performs better, yielding an accuracy of 0.909 and miss rate of 0.091.

Acknowledgement: The author thanks his family and colleague for their moral support.

Funding Statement: This project was funded (grant no. G:432-611-1443) by the Deanship of Scientific Research (DSR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia.

Conflicts of Interest: The author declares that he has no conflicts of interest to report regarding the present study.

References

[1] C. Yin, Y. Zhu, J. Fei and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[2] S. Somasundaram, D. Kasthurirathna and L. Rupasinghe, "Mobile-based malware detection and classification using ensemble artificial intelligence," in *Int. Conf. on Advancements in Computing*, Sri Lanka, pp. 351–356, 2019.

[3] D. S. Berman, A. L. Buczak, J. S. Chavis and C. L. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 3, pp. 1–16, 2019.

[4] M. J. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *Plos One*, vol. 11, no. 2, pp. 1–13, 2016.

[5] M. S. Daoud, S. Aftab, M. Ahmad, M. A. Khan, A. Iqbal *et al.,* "Machine learning empowered software defect prediction system," *Intelligent Automation and Soft Computing*, vol. 31, no. 2, pp. 1287–1300, 2022.

[6] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, pp. 1–15, 2021.

[7] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin *et al.,* "Scada system tested for cybersecurity research using machine learning approach," *Future Internet*, vol. 10, no. 3, pp. 1–16, 2018.

[8] C. F. T. Pontes, M. M. C. Souza, J. J. C. Gondim, M. Bishop and M. A. Marotta, "A new method for flow-based network intrusion detection using the inverse potts model," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1125–1136, 2021.

[9] S. Li, X. Li, K. Niu, H. Wang, Y. Zhang *et al.,* "Ar-alarm: An adaptive and robust intrusion detection system leveraging CSI from commodity WiFi," *International Conference on Smart Homes and Health Telematics*, vol. 6, no. 1, pp. 211–223, 2017.

[10] B. Ingre, A. Yadav and A. K. Soni, "Decision tree-based intrusion detection system for NSL-KDD dataset," in *Int. Conf. on Information and Communication Technology for Intelligent Systems*, India, pp. 207–218, 2017.

[11] H. A. Najada, I. Mahgoub and I. Mohammed, "Cyber intrusion prediction and taxonomy system using deep learning and distributed big data processing," *IEEE Symposium Series on Computational Intelligence*, vol. 22, no. 4, pp. 631–638, 2018.

[12] M. A. Ullah, M. A. Khan, S. Abbas, A. Athar, S. S. Raza *et al.,* "Blind channel and data estimation using fuzzy logic-empowered opposite learning-based mutant particle swarm optimization," *Computational Intelligence and Neuroscience*, vol. 3, no. 1, pp. 1–18, 2018.

[13] F. Khan, M. A. Khan, S. Abbas, A. Athar, S. Y. Siddiqui *et al.,* "Cloud-based breast cancer prediction empowered with soft computing approaches," *Journal of Healthcare Engineering*, vol. 5, no. 4, pp. 1–16, 2020.

[14] A. Rehman, A. Athar, M. A. Khan, S. Abbas, A. Fatima *et al.,* "Modelling, simulation, and optimization of diabetes type II prediction using deep extreme learning machine," *Journal of Ambient Intelligence and Smart Environments*, vol. 12, no. 2, pp. 125–138, 2020.

[15] M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb *et al.,* "A machine learning approach for blockchain-based smart home networks security," *IEEE Network*, vol. 35, no. 3, pp. 223–229, 2020.

[16] M. A. Khan, S. Abbas, A. Atta, A. Ditta, H. Alquhayz *et al.,* "Intelligent cloud-based heart disease prediction system empowered with supervised machine learning," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 139–151, 2020.
[17] Z. Khan, S. Abbas, B. Umar, W. A. Khan and A. Sarwar, "Used car price evaluation using three different variants of linear regression," *International Journal of Computational and Innovative Sciences*, vol. 1, pp. 40–49, 2022.
[18] M. U. U. A. H. Muhammad, "Intelligent intrusion detection system for apache web server empowered with machine learning approaches," *International Journal of Computational and Innovative Sciences*, vol. 1, no. 1, pp. 16–25, 2022.
[19] M. Saleem, S. Abbas, T. M. Ghazal, M. A. Khan, N. Sahawneh *et al.,* "Smart cities: Fusion-based intelligent traffic congestion control system for vehicular networks using machine learning techniques," *Egyptian Informatics Journal*, vol. 8, no. 4, pp. 1–15, 2022.
[20] M. Asif, S. Abbas, M. A. Khan, A. Ftima, M. A. Khan *et al.,* "Mapreduce based intelligent model for intrusion detection using machine learning technique," *Journal of King Saud University-Computer and Information Sciences*, vol. 13, no. 3, pp. 14–28, 2021.
[21] T. Batool, S. Abbas, Y. Alhwaiti, M. Saleem, M. Ahmad *et al.,* "Intelligent model of ecosystem for smart cities using artificial neural networks," *Intelligent Automation and Soft Computing*, vol. 30, no. 3, pp. 513–525, 2021.
[22] R. Akmal, R. Iqbal and M. Saleem, "A novel method to improve the round robin CPU scheduling quantum time using arithmetic mean," *International Journal of Computational and Innovative Sciences*, vol. 1, no. 2, pp. 69–82, 2022.
[23] S. Fatima, "Integration of blockchain and edge computing to improve the scalability and latency," *International Journal of Advanced Sciences and Computing*, vol. 1, no. 1, pp. 23–32, 2022.
[24] A. Haider, M. A. Khan, A. Rehman, M. U. Rahman and H. Seok Kim, "A real-time sequential deep extreme learning machine cybersecurity intrusion detection system," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1785–1798, 2021.
[25] M. S. Farooq, S. Khan, A. Rehman, S. Abbas, M. A. Khan *et al.,* "Blockchain-based smart home networks security empowered with fused machine learning," *Sensors*, vol. 22, no. 12, pp. 4522–4535, 2022.
[26] M. A. Khan, A. Rehman, K. Masood Khan, M. A. Al Ghamdi and S. H. Almotiri, "Enhance intrusion detection in computer networks based on deep extreme learning machine," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 467–480, 2021.