www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Evaluation of Network Security Grade Protection for Intrusion Detection

[1]I.Tavya Sri
Assistant Professor, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd.
email: tavyasri@gmail.com

[2]T.Laxmi
UG Student, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd.
email: thallapallilaxmi39@gmail.com

[3]D.Sri Ragni
UG Student, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd.
email: dasarisriragni@gmail.com

[4]Y.Shanthi
UG Student, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd.
email: shanthiyerra82@gmail.com

***Abstract*— Using deep learning models, we predict information system security indicators and obtain corresponding security evaluation scores. The scores of these predicted security evaluation are used as the input data of regression tree model, and the security grade protection evaluation system is constructed. The model training process involves four different models: VGG19, ResNet-50, XceptionNet, and EfficientNet. Based on the training results, we find that the EfficientNet model consumes fewer computational resources in single detection while achieves a detection accuracy of 99.93%. Subsequently, we apply the CART regression tree to assess the network security posture of 14 commercial systems. The test results of the model show that the mean absolute percentage error (MAPE) is 0.029 and the correlation coefficient is 0.9. These empirical results strongly support the performance of the proposed model and show its significant potential in improving security assessments. With these training results, we gain preliminary insights into the performance of each model and select the EfficientNet model with the best performance for the generation of subsequent security posture evaluation data. Ultimately, the developed security grade protection assessment system provides a reliable and efficient evaluation means for the network security.**

Keywords: **Anomaly detection, Cyber Security, Cyber Threat Intelligence, False Positives, Intrusion Detection System, Network Attack Detection, Neural Networks, Supervised Learning, Unsupervised Learning.**

I.INTRODUCTION

The issues of safeguarding our systems and society from changing threats are growing more complex as our society grows more interconnected and technologically advanced. Cybersecurity is the use of a variety of techniques to shield systems from threats and weaknesses while effectively offering users the right services. Due to human evaluations, traditional graded protection assessment techniques are inconsistent, subjective, and poorly adaptive, which reduces their efficacy in quickly changing danger scenarios. There is currently little deep learning integration in security assessments, which means that complicated data patterns are not being fully utilized. Our study responds by using deep learning to provide an accurate, scalable, and instantaneous network security assessment solution. Our method improves accuracy, adjusts to changing networks, and offers useful information for effective security risk management.

This study aims to bridge this gap by integrating deep learning techniques into a grade protection framework, ensuring accurate and efficient risk assessment for network security. According to the comprehensive multiplication method, we evaluate the relative levels of assets, threats and vulnerabilities by considering the key parts of security risk assessment, threats, vulnerability severity and their related factors, such as likelihood of threat occurrence, likelihood of threat success, and vulnerability severity of assets. Then, the relative value of the risk is calculated by multiplying these values, and the risk level is determined based on the range of the risk level. In the process of network situational awareness, it is necessary to model the complex networks, analyze the network security situations, and provide the quantitative results for network situational awareness . To achieve this process, it is necessary for the situational awareness model to have a powerful knowledge base that can quickly detect and match the network situations, and perform inference to provide reliable situational awareness results. In recent years, with the impressive performance of artificial intelligence algorithms in feature extraction, many researchers have studied and developed solutions for network security situational assessment based on artificial intelligence. Yang et. al. proposed a new calculating security indexes method based on

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

CNNs . Yuan et al. proposed a ML-based method for malware detection that utilizes more than 200 features extracted from both static and dynamic analysis of Android app. The issues of safeguarding our systems and society from changing threats are growing more complex as our society grows more interconnected and technologically advanced. Cybersecurity is the use of a variety of techniques to shield systems from threats and weaknesses while effectively offering users the right services. Due to human evaluations, traditional graded protection assessment techniques are inconsistent, subjective, and poorly adaptive, which reduces their efficacy in quickly changing danger scenarios. There is currently little deep learning integration in security assessments, which means that complicated data patterns are not being fully utilized. Our study responds by using deep learning to provide an accurate, scalable, and instantaneous network security assessment solution. Our method improves accuracy, adjusts to changing networks, and offers useful information for effective security risk management. Cyber threats are becoming increasingly sophisticated, making traditional security evaluation methods insufficient.

II. LITERATURE REVIEW

Network Security Grade Protection (NSGP), particularly in the context of China's Classified Protection of Cybersecurity (CPCS), has been extensively studied. Early foundational work by Hu and Lv [1] proposed a fuzzy neural network-based risk assessment method under classified security protection frameworks, enabling adaptive responses to dynamic threats. Cai [2] emphasized protection strategies for e-government external networks, laying down practical challenges in public sector cyber defense. Further development in NSGP implementation was detailed by Sun and Wang [3], who proposed a concrete design methodology to support security classification across different protection levels. Integrating analytic models, Zhi et al. [4] used a combination of the Fuzzy Comprehensive Evaluation Method and the Analytic Hierarchy Process (AHP) for more objective evaluation of security levels. As cyber threats became more sophisticated, machine learning and deep learning approaches emerged to enhance intrusion detection systems (IDS). Kim et al. [5] leveraged LSTM networks, which excel at identifying sequential and time-series data anomalies, to build a robust IDS. Yin et al. [7] echoed this approach by using RNNs, which achieved high accuracy in differentiating between normal and malicious traffic patterns. Kang and Kang [6] targeted the in-vehicle network context using deep neural networks, a noteworthy expansion of IDS to embedded systems. More advanced hybrid techniques were introduced by Al-Qatf et al. [8], combining sparse autoencoders for unsupervised feature extraction with SVMs for classification, thus improving both detection rate and precision. Vinayakumar et al. [11][12] extended these methods using deep CNN architectures tailored for cybersecurity data, and Ferrag et al. [9] provided a comparative study of various deep learning models and datasets for IDS, establishing baseline metrics for model performance in cyber defense. Moving beyond detection, situational awareness and intelligent monitoring systems were developed. Bao et al. [10] proposed an AI-based information security awareness system built on big data analytics, which can help in real-time decision-making and predictive threat intelligence. Decision trees remain a fundamental classification technique for intrusion detection. Sathyadevan and Nair [14] compared ID3, C4.5, and Random Forest, revealing strengths in tree ensemble models. Further optimization through pruning strategies was examined by Esposito et al. [15], crucial for reducing overfitting and increasing efficiency in tree-based models. While not directly related to intrusion detection, Lin et al. [13] developed a segmentation algorithm for damage detection in vehicles. This kind of visual deep learning model contributes to the broader ecosystem of AI in security, showing cross-domain adaptability of learning techniques.

III. Methodology

To further optimize the security assessment system of the information systems, we adopt an assessment strategy that 130992 focuses on network intrusion security indicators. As the intrusion detection system is the main source of security elements in situation awareness, its accuracy directly affects the assessment of network security. It can detect the maliciousness without compromising the security of hosts and networks [32]. This article further combines network intrusion security with security factors, such as devices and applications, to construct a multifactor fusion network security situation assessment scheme, further improving the effectiveness and accuracy of security situation assessment.

A. INTRUSION DETECTION ALGORITHM BASED ON DEEP LEARNING In terms of improving the network security grade of the system, the traditional network security protection system mainly focuses on the protection of the boundary, such as controlling the corresponding gate switch or defining the fire wall to directly reject the attack. It also uses various physical isolation or network protection methods to prevent the attack from penetrating the network. The traditional model for handling abnormal network traffic tends to be defensive, and thus there will be hidden threats. Once the defense is breached, it is easy to be further invaded. As the new network attacks become increasingly complex and diverse, the traditional method has many problems, such as difficulty in data feature extraction, low accuracy, high false alarm rate, and high operating costs. In order to solve the above problems, we built an efficient network intrusion detection system based on deep learning [33], [34]. This system can detect various types of attacks, including PortScan, Web Attack, DOS, DDoS, Brute Force and Bot, achieving the monitoring and perception of network traffic intrusion and improving the security grade of the service platform.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

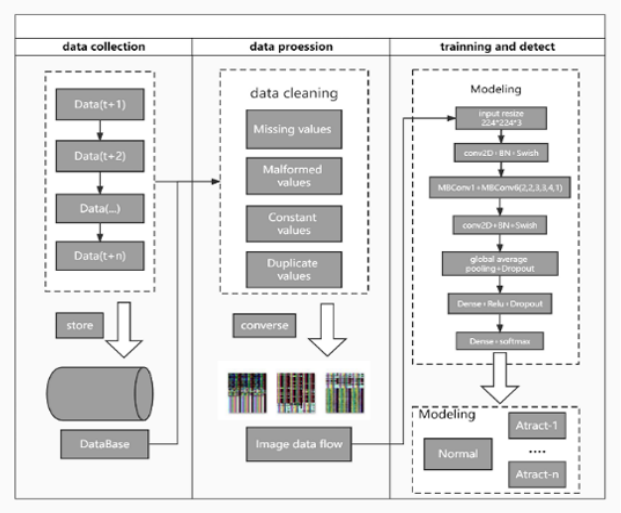

FIGURE-1:Steps involved in intrusion detection

B. THE CALCULATION OF INTRUSION SECURITY INDICATORS: The evaluation results of intrusion security indicators are determined by the severity and impact of threats on network security. The severity of threats is determined by the number of occurrences of various attacks, as well as the severity fac tors of various attacks. Therefore, we use an efficient neural network to detect the current security status of the network, and identify the types and quantities of possible network attacks. The impact of threats is calculated by referring to the evaluation table of attack impact for the common vulnerability scoring system. The scores for confidentiality (C), integrity (I), and availability (A) are shown in Table 1.

TABLE 1. The evaluation results of attack impact.

Indicators	Impact Degree	Impact Value
C	None/Low/Hight	0/0.22/0.56
I	None/Low/Hight	0/0.22/0.56
A	None/Low/Hight	0/0.22/0.56

UsingTable1,wecalculate the threat impact of each attack as follows: Pi = Ci + Ii +Ai (3) The calculation method of intrusion security index is shown in Formula (4). Ci = 1 N −Mn n−1 t=1 Ti ×Pi (4) where N represents the total number of network traffic data samples collected by the system platform, n represents the number of identifiable network attack types(n = 6), Mn represents the number of occurrences of normal data, and P represents the threat impact score. We obtained the scores for confidentiality, integrity, and availability of the information system through the deep learning model. Based on these scores, we calculated the threat impact of each attack. Then, according to these security indicators, we classify the security grade of the information system into three aspects: network intrusion security, device and computing security, and application and computing security. This comprehensive evaluation enables us to assess the overall security performance of the information system application and computing security indicators. The secondary indicators of equipment and computing security, as well as application and computing security indicators, have determined at least five indicator values of control points. The security grade indicators of the evaluated information system can be finally represented as C = {C1,C2,C3}, where C1 represents the network intrusion security indicators, C2 represents the device and computing security, and C3 represents the application and computing security indicators. The indicators of device-and computing security and application-and-computing security are respectively C2 = {C21,C22,C23,C24,C25,C26} and C3 = {C31,C32,C33,C34,C35,C36,C37}.

C. CONSTRUCTION OF SECURITY INDICATORS: Because the evaluation conclusion of the security grade protection object is influenced by the scores of multiple security control points, we adopt three different types of security factors as evaluation indicators, including net work intrusion security, device and computing security, and

From the security classification in the statistical list of information security measurement indicators and the analysis of the basic indicator points in Table 2, it can be seen that information security measurement consists of several security grade measurement indicators and security control frequency indicators. Fuzzy set theory can play a decisive role in network assessment ,which essentially uses conceptual fuzzy theory to study the undetermined things and quantifies them into information that can be displayed by a computer through a matrix model. In this research, the fuzzy comprehensive judgmental decision-making method is used for information system measurement in the grade assessment conclusions. The grade assessment conclusions are ‘‘Excellent’’,‘ ‘Good’’, ‘‘Fair’’ and ‘‘Poor’’. We calculate the score as follows: 100− p k=1 m(k) i=1 non-conformity assessment item weight p k=1 m(k) i=1 assessment item weight(Wi) ×100 (5) where p is the total number of items measured by the number of subjects, and m(k) is the number of corresponding subjects. The determination and comprehensive calculation models are shown inTable3

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Other Security Indicators	
Security Grade Indicators	Security Control Point Indicators
Network Intrusion Security C_1	Network Intrusion Security C_{11}
Device and Computing Security C_2	Identification C_{21}
	Access Control C_{22}
	Security Audit C_{23}
	Malicious Code Prevention C_{24}
	Resource Control C_{25}
	Remaining Information Protection C_{26}
Application and Computing Security C_3	Identification C_{31}
	Access Control C_{32}
	Security Audit C_{33}
	Communication Integrity C_{34}
	Communication Confidentiality C_{35}
	Software Fault Tolerance C_{36}
	Resource Control C_{37}

TABLE-2: The evaluation of security indicators

System Architecture:

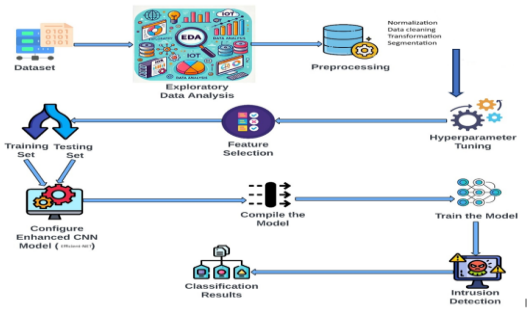

FIGURE-2:System Architecture of Intrusion Detection

IV. RESULTS AND ANALYSIS

A. MODEL TRAINING RESULTS: In this study, we trained four different models, namely VGG19,ResNet-50,XceptionNet,andEfficientNet,andthen selected the model with the best performance. We used three Tesla V100 GPUs to conduct the training, and set the batch size as 32 to obtain pre-trained weights. The dataset was divided into three sets with a ratio of 7:1.5:1.5, resulting in 11,900 samples for the training set, 2,850 samples for the validation set, and 2,850 samples for the test set. The input images were resized to 224∗224 with 3 channels. The learning rate for training was set to 0.001, and the Adam optimization algorithm was used, where the weight of first-order moment estimate is 0.9 (i.e., gradient's first moment) and the second-order one is 0.999 (i.e., gradient's second moment)..During the training process, the ''early stop'' technique was employed. The model's performance on the validation set was continuously monitored, and if there was no improvement within a specified number of epochs, the training process would be terminated early, and the model with the best performance on the validation set would be saved. This approach prevents over fitting and excessive training of the model on the training data, ensuring better generalization performance.As shown in Fig.3, the number of training steps of VGG19 model is 930, with an accuracy of 0.803; the number of training steps of ResNet-50 model is 558, with an accuracy of 0.987; the number of training steps of XceptionNet model is 1116, with an accuracy of 0.988; and the number of training steps of EfficientNet model is 744, with an accuracy of 0.999. As shown in Fig.4, the number of training steps of VGG19 model is 930, and the minimum training gradient value is 0.01806. The number of training steps of ResNet-50 model is 558, and the minimum training gradient value is 0.00875.The number of training steps of XceptionNet model is 1116 and the minimum training gradient value is 0.00003.The number of training steps of EfficientNet model is 744 and the minimum training gradient value is 0.00044. According to the training results, ResNet-50 and XceptionNet models perform well, with the accuracy reaching 98.7% and 98.8%respectively.However,theperformanceof VGG19model is relatively poor, the accuracy of which is only 80.3%. Efficient Net model performs best on the training set ,with an accuracy of close to 100% and a small training gradient. It is the top-performing model. Through these training results , we can have a preliminary understanding of the performance of each model and select the best performing model for the generation of security situational assessment data.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

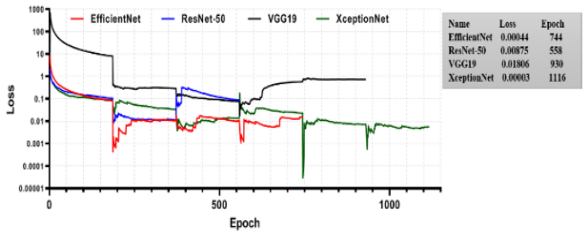

FIGURE 3. Comparison of training accuracy for four models.

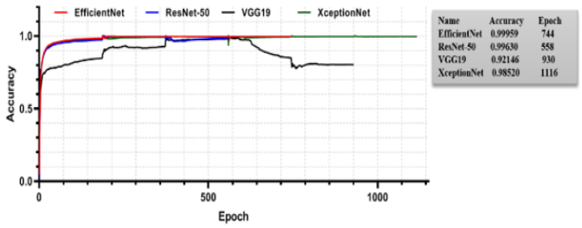

FIGURE 4. Comparison of training gradients for four models.

B. SECURITY SITUATION ASSESSMENT RESULTS: The security grade protection evaluation model fully con siders the influence of each security control point on the evaluation conclusion and controls the size of the regression tree through dimensionality reduction and pruning ,ensuring the efficiency of the prediction process .Experiments show that this model can effectively predict the security evaluation conclusion scores of information systems. The results can provide quantitative indicators for the security evaluation of security control points in related business systems. The scores of security control points and comprehensive scores of14 business systems are shown in Table4

System Number	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	Overall Score
1	4.95	14.09	3.64	-6.31	-6.49	-0.47	-3.32	-4.59	-2.77	1.86	70.23
2	-13.1	-3.25	-3.72	5.33	-5.67	3.32	-1.52	0.74	1.50	-0.64	93.74
3	6.60	4.51	6.61	-4.13	0.21	-3.65	-1.88	-1.62	11.72	8.02	70.07
4	4.13	1.00	2.97	-10.0	6.55	13.46	-6.40	-0.80	4.51	-3.19	75.38
5	-13.1	-2.97	-3.66	4.85	-5.64	3.54	-1.65	0.67	1.34	-0.43	93.87
6	-7.77	-4.71	-6.36	-7.57	6.35	3.390	11.18	-0.54	-2.46	2.10	88.33
7	15.94	-8.81	-11.8	1.17	-3.08	-0.23	-1.15	0.94	-1.63	-0.08	81.87
8	2.06	-1.92	-4.13	-3.69	-6.63	-10.9	7.05	-7.28	3.21	-3.69	80.89
9	-5.93	-8.30	5.09	-2.03	8.35	-6.38	-6.97	-3.46	-7.04	-2.37	81.45
10	2.02	-3.04	10.04	8.28	-4.04	2.12	4.02	7.19	-4.26	7.20	87.74
11	5.79	-10.9	12.54	3.22	1.32	0.09	1.79	-0.66	-0.32	-2.41	80.97
12	16.84	-8.33	-12.4	2.11	-1.23	0.00	-1.88	1.13	0.03	-0.49	81.26
13	1.54	17.16	-1.31	11.33	8.78	0.23	2.23	1.91	1.93	-2.62	76.37
14	-12.7	-4.30	-1.63	-2.63	1.86	-4.47	-3.57	1.94	3.93	0.54	81.89

TABLE-3 :Sample Evaluation Results

Using the above samples as input, we construct a deep learning model based on the security control points of business systems, with a threshold of 0.5as the mean square error reduction. Another 5 business systems are deployed in the same network domain, and the corresponding security control point scores are obtained through vulnerability analysis and penetration testing .Based on the scores, a test set is constructed to evaluate the trained decision-tree model. We use three indicators ,namely mean absolute percentage error (MAPE),mean square error (MSE), and coefficient of determination(R2), to evaluate the fitting degree of the constructed model, which is calculated as follows:

Where n is the number of samples, yi is the true value of the comprehensive score for the i-th sample, ˆ yi is the predicted value of the comprehensive score for the i-th sample, and ¯ y is the mean value of the true comprehensive score for the n samples. According to Table5, the mean absolute percentage e error (MAPE)of the test result MAPE is0.029,which is close to 0, indicating that the predicted values of the comprehensive score obtained through the model have a small error. The MAPE represents the accuracy of the model's pre dictions. In this case, a MAPE of 0.029or 2.9%means that on average, the model's predictions of comprehensive scores for the business systems are very close to the actual scores. It indicates that the model can reliably estimate the security status of these systems, which is crucial in security assessment. A low MAPE suggests that the model's predictions are highly trustworthy and can be used safely

System Number	y_i	$\hat{y}_i$	$(\hat{y}_i - y_i)^2$	$(y_i - \bar{y})^2$	$\frac{\hat{y}_i - y_i}{y_i}$	MAPE	MSE	R^2
1	88.5	88.035	0.216225	81	0.0052542			
2	71.13	75.12	15.9201	70.0569	0.0560945			
3	72.02	70.15	3.4969	55.9504	0.0259650	0.0293609	7.44151	0.9197
4	72.18	76.37	17.5561	55.5824	0.0580493			
5	93.67	93.805	0.018225	200.7889	0.0014412			

TABLE-4:Evaluation results of test set

The Coefficient of Determination, commonly referred to as R-squared (R^2), is a key metric that measures how effectively a model's predictions explain the variance in the actual outcomes. In this context, an R^2 value of 0.9 signifies that approximately 90% of the variance in actual comprehensive security scores can be explained by the model's predictions. This high value indicates that the model is highly effective in capturing the underlying patterns and trends related to security control point scores. As a result, the model proves to be a valuable tool for evaluating the security posture of business systems. The combination of a high R^2 and a low Mean

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Absolute Percentage Error (MAPE) further confirms the model's accuracy and reliability in predicting security grades. This level of precision is crucial for organizations as it supports informed decision-making in their security strategies and resource planning. Overall, the model's strong performance underscores its practical utility in real-world security assessment and threat identification.

Screen Shots:

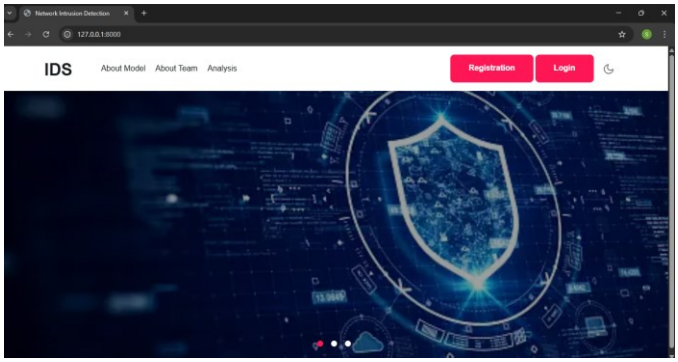

FIGURE-5:Home page of Intrusion detection website

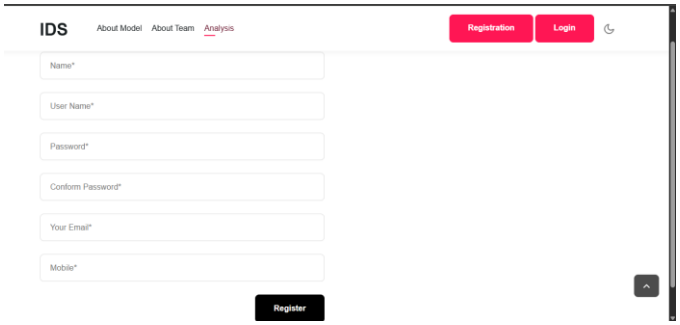

FIGURE-6:Registration page for intrusion detection system

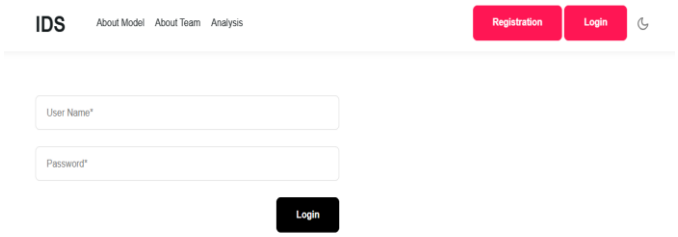

FIGURE-7:Login page for intrusion detection system

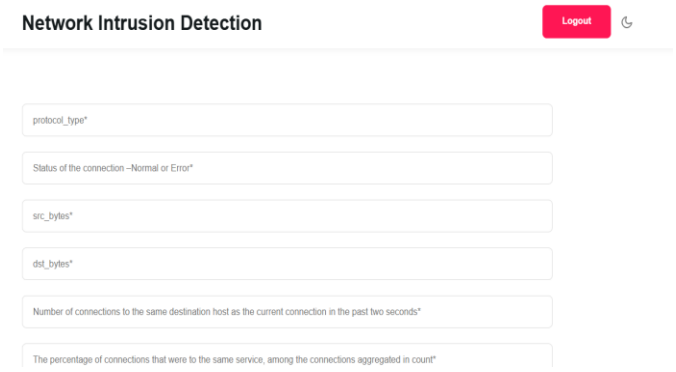

FIGURE-8:Test set characteristics to be entered for prediction

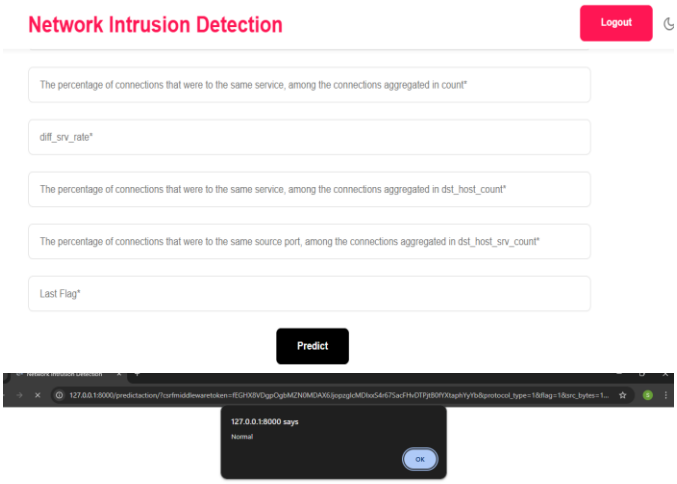

FIGURE-9:Prediction of intrusion detection as normal

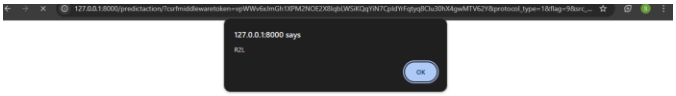

FIGURE-10:Prediction of intrusion detection

V. CONCLUSION

We have set out to improve the evaluation of network security grades in this study by leveraging the potential of deep

learning models and data analysis methods. We developed a unified data analysis system that incorporates cutting-edge models such as the incredibly effective EfficientNet, ResNet-50, XceptionNet, and VGG19. Our results have shown that the EfficientNet model is a good option for single detection jobs because of its impressive 99.93% detection accuracy and minimal computing resource consumption. We then conducted situational assessments of network security on 14 commercial systems using the CART regression tree model. Our model's test results indicate that the correlation coefficient (R2) is 0.9 and the Mean Absolute Percentage Error (MAPE) is 0.029 and R2 is 0.9 for the correlation coefficient. These metrics highlight the potential of our suggested methodology to transform security assessments and show that it has a high predictive power. This study is important for reasons other than model performance. Additionally, we have investigated the use of deep learning models, specifically EfficientNet. High accuracy can be achieved with these models, but their tiny training gradients open the door to more effective training and deployment in real-world situations. We propose a new method that incorporates these deep learning-based prediction security scores into a regression tree model. A complete answer is offered by this holistic security grade protection assessment system. It promises a multifaceted approach to security with its proactive defence mechanisms, quick event responses, and post-event checks. Develop a security strategy with multiple facets. Additionally, a number of issues with conventional security assessments, including subjectivity, fuzziness, inconsistency, and poor flexibility, may be resolved by our research. We may dynamically connect network security with disciplines like automated production lines, machinery manufacture, electrical and electronic engineering, and control science by introducing deep learning techniques and analysing sophisticated data. In the future, our work will set the stage for more developments. In order to cover a wider range of network security scenarios, future research should concentrate on improving deep learning models, investigating novel data analysis approaches, and broadening the scope of this assessment system. In an era of continuously changing complexity, our work provides a promising path towards smarter, more accurate, and more flexible security evaluations. In conclusion, this research plays an important role in modernizing and improving network security assessments. Through deep learning, data analysis, and artificial intelligence , we have created a robust and efficient security grade protection assessment system that can cater to the diverse security assessment needs of various industries. The insights gained from this study have the potential to reshape the landscape of security assessments and empower the organizations to stay ahead in an ever-changing digital environment.

VI. FUTURE SCOPE:

The combination of network security grade protection with deep literacy(DL) for intrusion discovery systems(IDS) represents a promising advancement in cybersecurity. As cyber pitfalls continue to evolve, deep literacy ways offer important capabilities for enhancing real- time trouble discovery. These models can dissect vast volumes of network business and identify both known and preliminarily unseen pitfalls, including zero- day attacks, by feting subtle anomalies in geste likewise, DL- grounded IDS can significantly reduce false positive and false negative rates, leading to more accurate and dependable trouble discovery. A crucial aspect of this advancement is the development of dynamic evaluation fabrics for security. Traditional static grading systems are being reimagined into adaptive models that respond to real- time data and pitfalls. These systems incorporate colorful criteria similar as IDS performance, network business patterns, and vulnerability assessments to give a further comprehensive and continuously streamlined view of the network's security grade. Another area of unborn growth lies in the integration of DL- grounded IDS with arising technologies like the Internet of effects(IoT), edge computing, and 5G networks. In similar surroundings, DL models can be stationed at the network edge to give localized and real- time intrusion discovery. These systems can acclimatize to the specific conditions of distributed and high- speed networks, helping to cover massive volumes of data generated by smart bias and coming- generation communication systems. Scalability and robotization are also pivotal factors of the unborn compass. Deep literacy enables the creation of security systems that can gauge with the network and automatically acclimate their discovery strategies grounded on evolving pitfalls. Evaluation fabrics, too, can be automated, allowing nonstop monitoring and reporting of network health and the effectiveness of defense mechanisms. As deep literacy becomes more deeply bedded in security architectures, there will be a growing emphasis on resolvable AI(XAI). This will help cybersecurity professionals understand and interpret the opinions made by IDS models, fostering trust and responsibility. resolvable models will play a vital part in integrating security grading with stoner-friendly perceptivity that network directors can act upon. Another significant development will be in nonstop literacy and model streamlining. Deep literacy models used in intrusion discovery need to acclimatize constantly as bushwhackers develop new strategies. Online literacy ways and allied literacy where multiple decentralized systems collaboratively learn without participating raw data — will insure that models remain up- to- date and flexible. In the environment of assessing and perfecting these systems, unborn exploration will concentrate on benchmarking and developing evaluation methodologies that can reliably assess DL- grounded IDS performance and their impact on network security grades. Formalized datasets and criteria will support relative analysis and drive advancements in both model delicacy and security evaluation strategies. likewise, integrating trouble intelligence with deep literacy models will give fortified environment and bettered trouble

discovery. Graph neural networks(GNNs), for case, can be used to model connections among network realities and identify complex patterns in trouble geste , thereby enhancing situational mindfulness and visionary defense mechanisms. Looking ahead, implicit exploration directions include the development of mongrel DL models that combine the strengths of convolutional neural networks(CNNs), intermittent neural networks(RNNs), and mills for further robust and flexible intrusion discovery. also, inimical training ways will be critical for making DL models more flexible against attempts to deceive them. Assiduity-specific evaluation fabrics will also crop , acclimatized to the unique security requirements of sectors like healthcare, finance, and critical structure. In summary, the integration of network security grade protection with deep literacy- grounded intrusion discovery systems has immense eventuality. It offers a path toward intelligent, adaptive, and independent security results that not only descry pitfalls more effectively but also stoutly assess and strengthen the security posture of networks over time.

VII. REFERENCES:

[1] C. Hu and C. Lv, ‘‘Method of risk assessment based on classi f ied security protection and fuzzy neural network,’’ in Proc. Asia Pacific Conf. Wearable Comput. Syst., Shenzhen, China, Apr. 2010, pp. 379–382.

[2] C. Cai, ‘‘Study on the protection of e-government external network level protection,’’ in Proc. 7th Int. Conf. Mechatronics, Comput. Educ. Informa tionization (MCEI). Amsterdam, The Netherlands: Atlantis Press, 2017, pp. 415–417.

[3] D. Sun and B. Wang, ‘‘Research on the design of the implementation plan of network security level protection of information security,’’ in Proc. 7th Int. Symp. Mechatronics Ind. Informat. (ISMII), Zhuhai, China, Jan. 2021, pp. 227–231.

[4] W. W. Zhi, X. X. Zhou, and L. Yang, ‘‘Application of fuzzy com prehensive method and analytic hierarchy process in the evaluation of network security level protection research,’’ in Proc. Int. Conf. Mech. Eng., Intell. Manuf. Automat. Technol. (MEMAT), Guilin, China, 2021, Art. no. 012187.

[5] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, ‘‘Long short term memory recurrent neural network classifier for intrusion detection,’’ in Proc. Int. Conf. Platform Technol. Service (PlatCon), Jeju, South Korea, Feb. 2016, pp. 1–5.

[6] M.-J. KangandJ.-W. Kang, ‘‘Intrusion detection system using deep neural network for in-vehicle network security,’’ PLoS ONE, vol. 11, no. 6, Jun. 2016, Art. no. e0155781.

[7] C. Yin, Y. Zhu, J. Fei, and X. He, ‘‘A deep learning approach for intru sion detection using recurrent neural networks,’’ IEEE Access, vol. 5, pp. 21954–21961, 2017.

[8] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, ‘‘Deep learning approach combining sparse autoencoder with SVM for network intrusion detection,’’ IEEE Access, vol. 6, pp. 52843–52856, 2018.

[9] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, ‘‘Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,’’ J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102419.

[10] H. Bao, H. He, Z. Liu, and Z. Liu, ‘‘Research on information security situation awareness system based on big data and artificial intelligence technology,’’ in Proc. Int. Conf. Robots Intell. Syst. (ICRIS), Jun. 2019, pp. 318–322.

[11] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, ‘‘Deep learning approach for intelligent intrusion detection system,’’ IEEE Access, vol. 7, pp. 41525–41550, 2019.

[12] R. Vinayakumar, K. P. Soman, and P. Poornachandran, ‘‘Applying con volutional neural network for network intrusion detection,’’ in Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI), Sep. 2017, pp. 1222–1228.

[13] S. H. D. Lin, C. Feng, Z. H. D. Chen, and K. X. Zhu, ‘‘An efficient segmentation algorithm for vehicle body surface damage detection,’’ Data Acquisition Process., vol. 36, no. 2, pp. 260–269, 2021

[14] S. Sathyadevan and R. R. Nair, ‘‘Comparative analysis of decision tree algorithms: ID3, C4.5 and random forest,’’ in Computational Intelligence in Data Mining, vol. 1. India: Springer, 2015, doi: 10.1007/978-81-322 2205-7_51.

[15] F.Esposito, D. Malerba, G. Semeraro, and J. Kay, ‘‘A comparative analysis of methods for pruning decision trees,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 5, pp. 476–493, May 1997.