ISSN 2277-2685
IJESR/April-June. 2025/ Vol-15/Issue-2s/65-77
Korra Pravalika *et. al.*, / International Journal of Engineering & Science Research

Abnormal Traffic Detection Based On Attention And Big Step Convolution

K Shireesha, Korra Pravalika, J Jahnavi
Assistant Professor, Department Of CSE, Sri Indu College Of Engineering And Technology, India
[2,3]B. Tech Students, Department Of CSE, Sri Indu College Of Engineering And Technology, India

ABSTRACT

Abnormal traffic detection is critical to network security and quality of service. However, the similarity of features and the single dimension of the detection model cause great difficulties for abnormal traffic detection, and thus a big-step convolutional neural network traffic detection model based on the attention mechanism is proposed. Firstly, the network traffic characteristics are analyzed and the raw traffic is preprocessed and mapped into a two-dimensional grayscale image. Then, multi-channel grayscale images are generated by histogram equalization, and an attention mechanism is introduced to assign different weights to traffic features to enhance local features. Finally, pooling-free convolutional neural networks are combined to extract traffic features of different depths, thus improving the defects such as local feature omission and overfitting in convolutional neural networks. The simulation experiment was carried out in a balanced public data set and an actual data set. Using the commonly used algorithm SVM as a baseline, the proposed model is compared with ANN, CNN, RF, Bayes and two latest models. Experimentally, the accuracy rate with multiple classifications is 99.5%. The proposed model hasthe best anomaly detection. And the proposed method outperforms other models in precision, recall, and F1. It is demonstrated that the model is not only efficient in detection, but also robust and robust to different complex environments.

1.INTRODUCTION

Internet technology is widely used in all walks of life, and has strongly contributed to the development of economy and society. However, as the current mainstream network security and defense technologies still have many shortcomings, the huge application requirements also make the security configuration of the entire network becomes particularly complex, resulting in the entire network facing the threat of extremely vulnerable to attacks. At the same time, due to the openness of the TCP/IP network architecture, computer viruses spread more widely through disguise, which affects the normal operation of the network and causes social and economic downturn. How to take effective methods to analyze data information to predict the current network development, find abnormalities and take appropriate handling measures is of great significance to maintain network security.

Anomalous traffic detection can be achieved with the help of network trafficclassification. According to its core idea there are mainly the following approaches: port-based,deep packet detection based , and machine learning based . Machine learning consists of traditional machine learning and deep learning. In the early days, when the Internet was small and the traffic types were simple, the first two methods had stable performance and achieved good classification results However, with the continuous emergence of new Internet applications, traffic types are increasing and traffic components are becoming more complex, which reduces the

classification effect. Machine learning improvement methods are proposed to address the limitations of the above methods. Machine learning is to extract statistical features of network traffic and classify them with reliable efficiency and high accuracy. It also has a wide range of application prospects.

2.LITERATURE SURVEY

1) Abnormal Traffic Detection Based on Attention and Big Step Convolutional Neural Networks

Omar Azib Alkhudaydi ,Moez Krichen , D. Alghamdi 1ORCID, This study introduces a novel approach to abnormal traffic detection that leverages big-step convolutional neural networks (CNN) enhanced with an attention mechanism. The process begins with the analysis of network traffic characteristics, followed by the preprocessing of raw traffic data, which is transformed into two-dimensional grayscaleimages. Through histogram equalization, multi-channel grayscale images are generated to enrich the feature space. The attention mechanism plays a crucial role by assigning varying weights to different traffic features, thereby emphasizing local features that are critical for accurate detection. Unlike traditional CNNs that rely on pooling operations, the proposed model employs pooling-free convolutional networks to extract features at different depths. This approach mitigates common CNN issues such as local feature omission and overfitting. The model's performance was validated through simulations on both a balanced public dataset andan actual dataset. When compared with a baseline Support Vector Machine (SVM) and other models like ANN, CNN, RF, Bayes, and recent advancements, the proposed model achieved asuperior multi-class classification accuracy rate of 99.5%. It consistently outperformed other models in terms of precision, recall, and F1-score, demonstrating both high detection efficiency and robustness in complex network environments.

2) An Abnormal Traffic Detection Method Using GCN-BiLSTM-Attention in the Internetof Vehicles Environment

Ana-Belén Gil-González, Ana Luis-Reboredo, Belén Pérez-Lancho,This paper presents an innovative method for detecting abnormal traffic in the Internet of Vehicles (IoV) environment, utilizing a combination of Graph Convolutional Networks (GCN), Bidirectional Long Short-Term Memory (BiLSTM) networks, and an attention mechanism. The method begins by embedding nodes into a graph structure for each time slot, generating enhanced traffic features by leveraging the source and destination IP address representation vectors. GCNs are employed to capture spatial correlations between data streams, while BiLSTM networks extract temporal features, enhancing the model's ability to predict and classify traffic anomalies accurately. The introduction of an attention mechanismfurther refines this process by highlighting key information within the data stream. This comprehensive approach addresses the limitations of existing methods, such as high computational costs and inefficiencies in handling non-Euclidean data structures. Experimental results demonstrate that the proposed model effectively improves the accuracy and robustness of anomaly detection, outperforming traditional methods and ensuring reliableperformance in the dynamic and complex IoV environment.

3)Multi-Scale Convolutional Feature Fusion Network Based on Attention Mechanism for IoT Traffic

Jalilisadrabad S, Behzadfar M, Moghani Rahimi K, This research introduces a multi-scale convolutional feature fusion network designed to enhance the detection of Internet of Things (IoT)

traffic anomalies. The model integrates multi-scale convolutional features with an attention mechanism to improve the extraction and importance recalibration of deep features across various scales. This method starts with the preprocessing of raw traffic data into two-dimensional images. These images undergo histogram equalization to generate multi-channel representations. The attention mechanism assigns weights to different features, enhancing critical local features and improving detection accuracy. The multi-scale convolutional network ensures that features from different scales are fused effectively, capturing both global and local patterns in the data. Extensive experiments demonstrate that this approach significantly outperforms traditional methods in detecting malicious IoT traffic, showcasing superior precision, recall, and F1- scores. The proposed model's robustness and efficiency make it highly suitable for deploymentin diverse and complex IoT environments, where timely and accurate anomaly detection is crucial.

4) A Malicious Traffic Detection Method Based on Attention Mechanism

Martínez-Mozos OM, Sandulescu V, Andrews S, The study proposes a novel method for detecting malicious network traffic using a convolutional neural network (CNN) enhanced with an attention mechanism. The model preprocesses raw network traffic data into two-dimensional grayscale images, which are then subjected to histogram equalization to create multi-channel representations. The attention mechanism is employed to dynamically adjust the importance of features across both channel and spatial dimensions. This approach ensures that the model focuses on the most relevant features, thereby enhancing detection accuracy and reducing false positives. The CNN architecture used in this study is designed to extract deep features without relying on pooling operations, which helps to mitigate issues such as overfitting and local feature omission. The model's effectiveness was validated through extensive experiments, showing that it significantly outperforms traditional methods and recent advancements in terms of precision, recall, and F1-score. The proposed method demonstrates high efficiency and robustness, making it well-suited for real-time deployment in complex network environments where accurate detection of malicious activities is critical

5) Research on Anomaly Network Detection Based on Self-Attention Mechanism

Zangróniz R, Martínez-Rodrigo A, Pastor JM, This paper explores a deep neural network model for anomaly detection in network traffic, integrating self-attention mechanisms with cyclic neural networks and convolutional neural networks (CNN). The approach begins with the transformation of raw network traffic data into two-dimensional grayscale images. These images undergo preprocessing steps such as histogram equalization to enhance feature representation. The self-attention mechanism is incorporated to focus on the most relevant features in the data, improving the model's ability to detect anomalies accurately. By combining cyclic neural networks for capturing temporal dependencies and CNNs for extracting spatial features, the model achieves a comprehensive analysis of network traffic patterns. Extensive experiments on various datasets demonstrate that the proposed method outperforms traditional models andrecent advancements in terms of precision, recall, and F1-score. The model's robustness and adaptability to different network environments highlight its potential for effective deploymentin real-time anomaly detection systems, ensuring high accuracy and reliability in identifying network anomalies.

3.SYSTEM ANALYSIS

EXISTING SYSTEM

Shi et al. proposed a cost-sensitive SVM (CMSVM) for the network traffic imbalance problem. The model uses a multi-class SVM with an active learning algorithm to solve the imbalance problem for different applications by adaptive weights. Cao et al. proposed a real-time network classification model with SPPSVM. The model uses the feature selection method ofprincipal component analysis (PCA) to reduce the dimensionality of the original data and uses animproved particle swarm optimization algorithm to obtain the optimal parameters. The classification accuracy is higher compared to the traditional SVM model. Farid et al. combined naive bayes and decision trees for anomalous traffic detection while eliminating redundant attributes of the traffic data. The proposed algorithm improves the detection rate. Machine learning based classification methods usually require manual feature design and selection, which cannot cope with the evolution of networks nowadays.

PROPOSED SYSTEM

System analysis Attention and Big Step Convolutional Neural Network (ABS-CNN) model based on the attention mechanism . To solve the problems such as similar features leading to worse classification results, the attention mechanism is invited to assign attention weights to data sequences to distinguish subtle features. To solve the problems such as similar features leading to worse classification results, the attention mechanism is invited to assignattention weights to data sequences to distinguish subtle features. Experiments show that the model with enhanced features has higher classification accuracy and better robustness.

histogram equalization to solve the problem of single modeldimensionality. The traffic data is first processed into grayscale images .

then the images are histogram equalized. Combined with improved multi-channel convolution to automatically extract and fuse multi-field fine-grained features. The experiments show that the traffic with histogram equalization performed is relatively well-defined, which results in better model detection performance and better robustness. To address the reduced correlation of traffic sequences due to pooling, the traffic features are extracted by combining big-step convolution. And big-step convolution is also called stepwise convolution. Stepwise convolution preserves the sequence-related features extracted by the convolution layer and reduces the harm of accuracy loss due to information loss.

4.SYSTEM REQUIREMENTS

Functional Requirements

Functional requirements will vary for different types of software. For example, functional requirements for a website or mobile application should define user flows and various interaction scenarios.

The major modules of the project are

1. Service Controller
2. Client Service

Non-Functional Requirements

Nonfunctional requirements are not related to the system's functionality but rather define how the system should perform. They are crucial for ensuring the system's usability, reliability, and efficiency, often influencing the overall user experience. We'll describe the main categories of nonfunctional requirements in detail further on

Hardware Requirements

- System : i5
- Hard Disk : 40 GB.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- RAM : 512 Mb.

Software Requirements

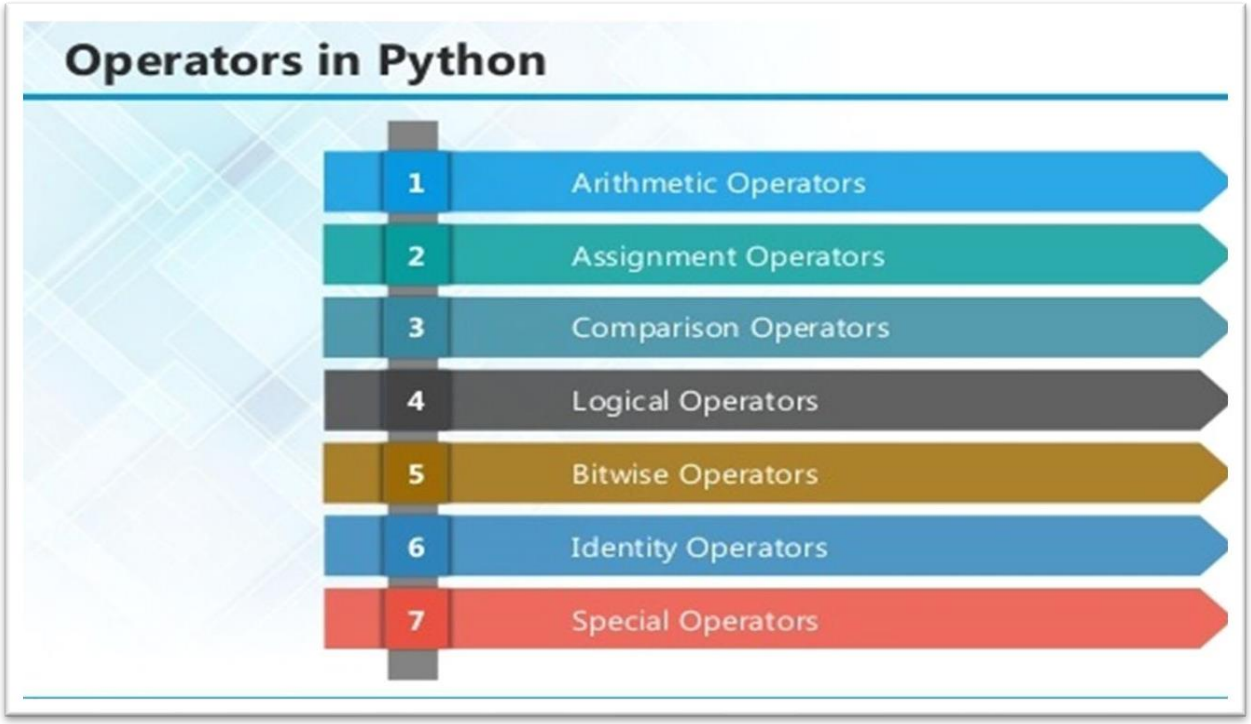
- Operatingsystem: Windows 11 Ultimate.
- CodingLanguage: Python.
- Front-End : html.
- Back-End : Django-ORM.
- Designing : Html, css, javascript.
- Data Base : MySQL (WAMP Server).

Software Environment

PYTHON

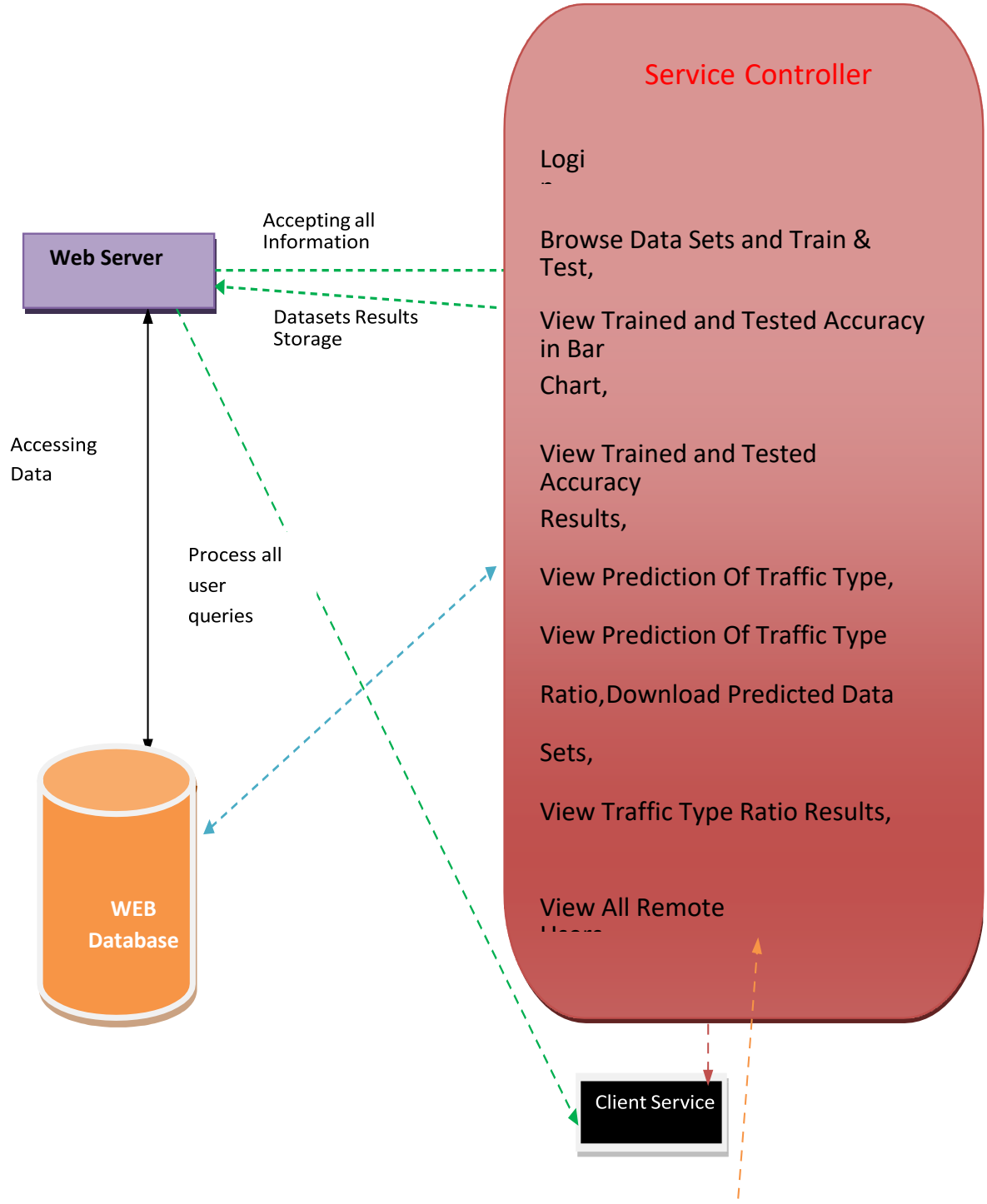
Python is a **high-level, interpreted**, **interactive** and **object-oriented scripting language**. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages.

- **Python is Interpreted:** Python is processed at runtime by the interpreter. You do not need to compile your program before executing it. This is similar to PERL and PHP.
- **Python is Interactive:** You can actually sit at a Python prompt and interact with the interpreter directly to write your programs.
- **Python is Object-Oriented:** Python supports Object-Oriented style or technique of programming that encapsulates code within objects.
- **Python is a Beginner's Language:** Python is a great language for the beginner-level programmers and supports the development of a wide range of applications from simple text processing to WWW browsers to games.



5-SYSTEM DESIGN

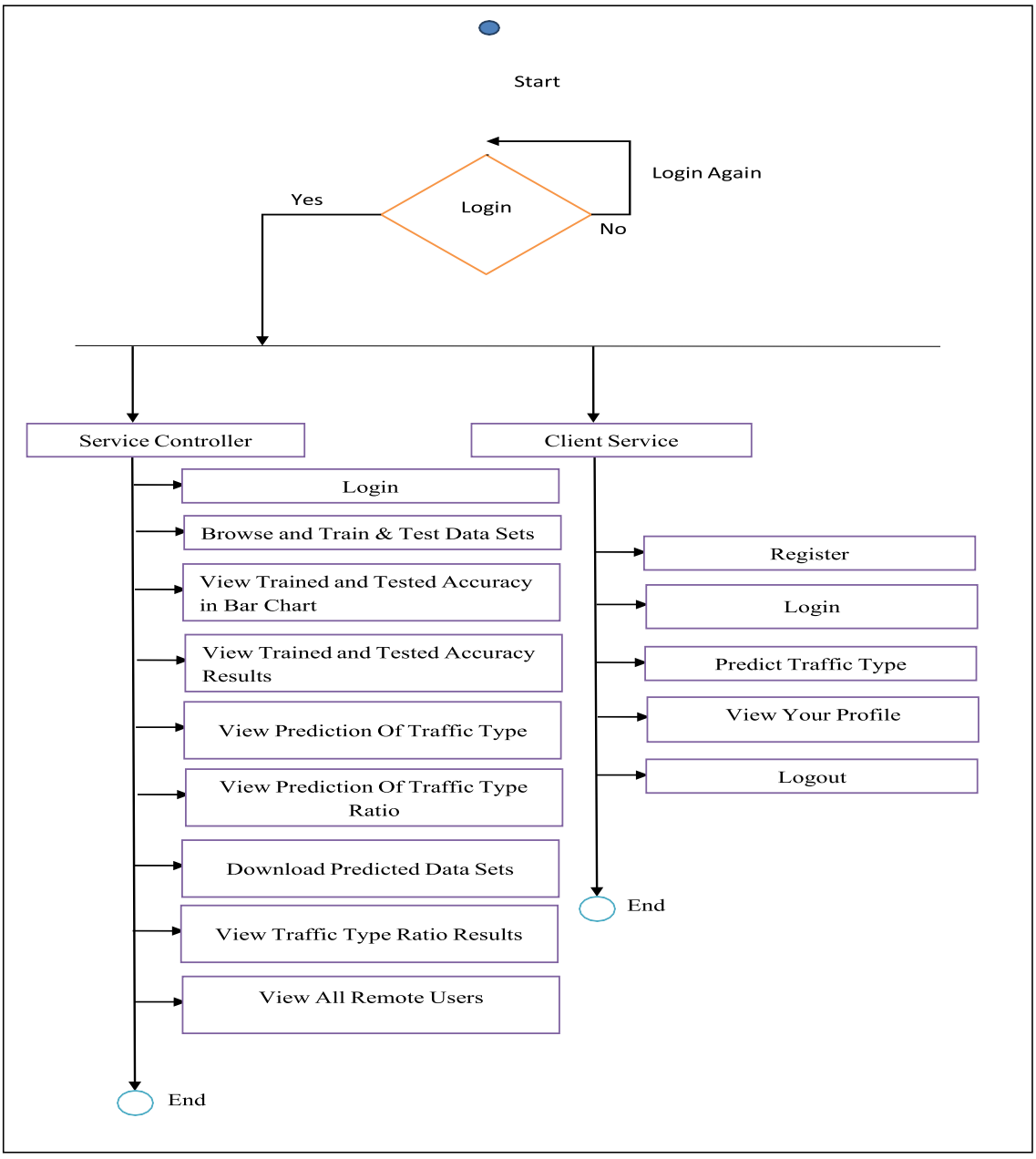
System Architecture



Register and login,Predict traffic type,View your profile.

Activity Diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.



6INPUT/OUTPUT DESIGN

Input design

considering the requirements, procedures to collect the necessary input data in most efficiently designed. The input design has been done keeping in view that, the interaction of the user with the system being the most effective and simplified way. Also the measures are taken for the following

- Controlling the amount of input
- Avoid unauthorized access to the classroom.
- Eliminating extra steps
- Keeping the process simple
- At this stage the input forms and screens are designed.

Output design

All the screens of the system are designed with a view to provide the user with easy operations in simpler and efficient way, minimum key strokes possible. Instructions and important information is emphasized on the screen. Almost every screen is provided with no errorand important messages and option selection facilitates. Emphasis is given for

speedy processingand speedy transaction between the screens. Each screen assigned to make it as muchuser friendlyas possible by using interactive procedures. So to say user can operate the system without much help from the operating manual.

7. IMPLEMENTATION

Service Controller

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Browse Data Sets and Train& Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Traffic Type, View Prediction Of Traffic Type Ratio, Download Predicted Data Sets, View Traffic Type Ratio Results, View All RemoteUsers**.**

Remote Access User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Register And Login, Predict Traffic Type, View Your Profile.

8-SCREENSHOTS

Fig 1: Client Server Login

Fig 2: Service Controller Login

Fig 3: Service Controller Home

Fig 4: Service Controller View Healthcare Datasets Trained & Testedresults

Fig 5: Service Controller View Trained & Tested Accuracy And barChart

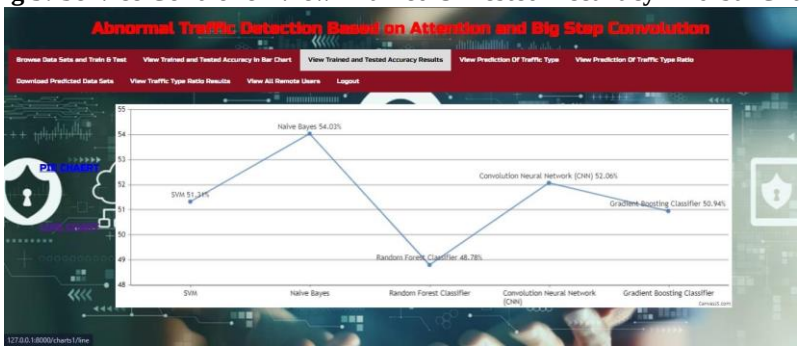


Fig 6: Service Controller Operation View Trained and Tested AccuracyResults

Fig 7: Service Controller View prediction of Traffic Type

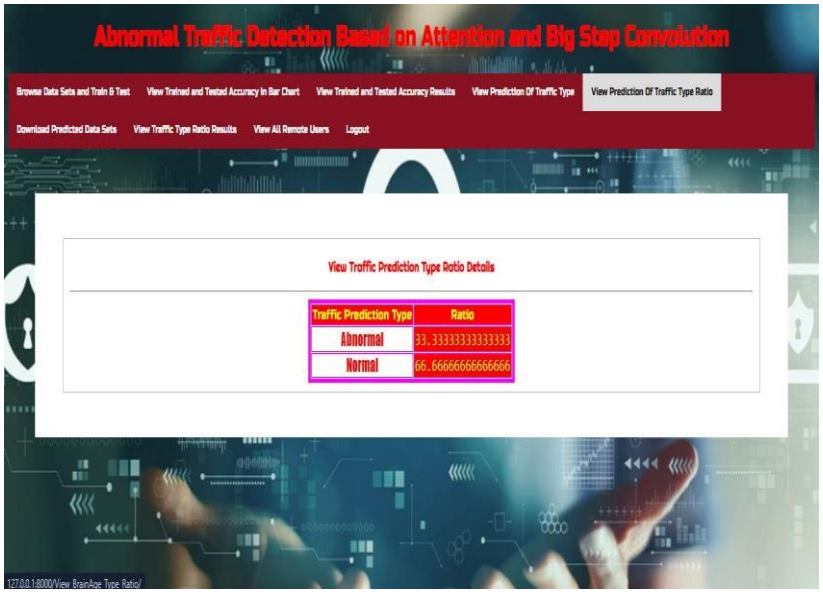


Fig 8: Service Controller Operation View Traffic Prediction Type Ratio

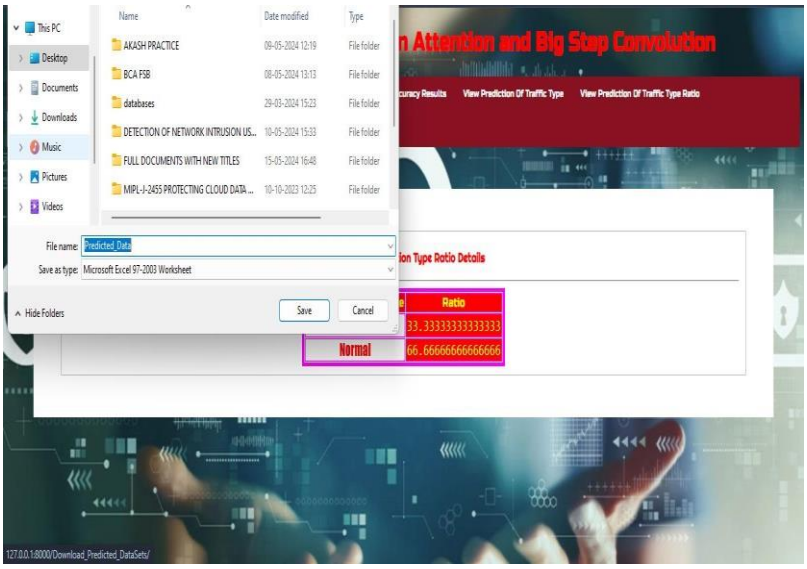


Fig 9: Service Controller Download predicted dataset

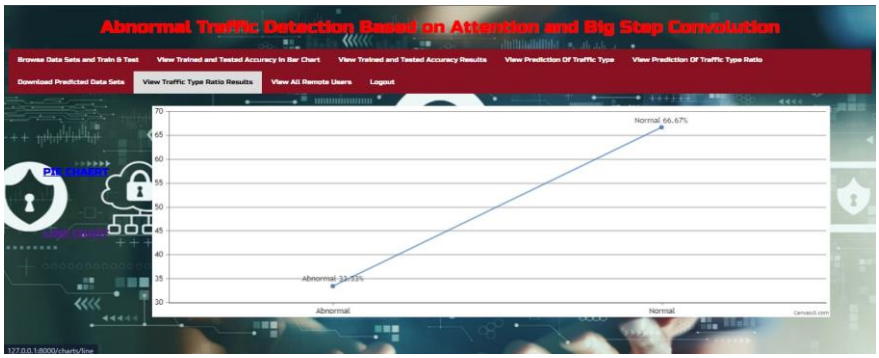


Fig 10: Service Controller Operation View Traffic type ratio results

Fig 11: Service Controller Operation View All the Client Service

9-CONCLUSION

To address the difficulties caused by similar features and single model structure on

abnormal traffic detection, this paper proposes a detection model based on attention and big-step convolution. Experiments were conducted on both publicly available dataset and real environment crawls dataset. The efficiency of the model is seen through performance analysis.The results of the ablation analysis show that ABS-CNN introduces anattention mechanism to assign attention weights for different features, which enhances the differentiation of features and relieves the difficulties caused by feature similarity. ABSCNN introduces histogram equalization in data preprocessing, which improves the structure of single channel in the model and enhances the detection performance of the model. At the same time, removing the pooling layer retains the sequence-related features, which reduces the training parameters, improves the operation efficiency and achieves efficient abnormal traffic detection ABS-CNN experiments on traffic crawled by real environment and has excellent detection results. The traffic captured by the real environment is encrypted traffic. ABS-CNN not only achieves efficient classification of encrypted traffic.

REFERENCES

[1] O. Salman, I. H. Elhajj, A. Kayssi, and A. Chehab, ‘‘A review on machine learning–based approachesfor internet traffic classification,’’ Ann. Telecommun., vol. 75, nos. 11–12, pp. 673–710, Dec. 2020.

[2] A. Madhukar and C. Williamson, ‘‘A longitudinal study of P2P traffic classification,’’ in Proc. 14th IEEE Int. Symp. Modeling, Anal., Simulation, Monterey, CA, USA, Sep. 2006, pp. 179–188, doi: 10.1109/MASCOTS. 2006.6.

[3] S. Sen, O. Spatscheck, and D.Wang,

''Accurate, scalable in-network identification of P2P P2P traffic using application signatures,'' in Proc. 13th Int. Conf. World Wide Web, New York, MY, USA, May 2004, pp. 512–521.

[4] L. Ding, J. Liu, T. Qin, and H. Li, ''Internet traffic classification based on expanding vector of flow,''Comput. Netw., vol. 129, pp. 178–192, Dec. 2017.

[5] T. Liu, Y. Sun, and L. Guo, ''Fast and memory-efficient traffic classification with deep packet inspection in CMP architecture,'' in Proc. IEEE 5th Int. Conf. Netw., Archit., Storage, Macau, China, Jul. 2010, pp. 208–217, doi: 10.1109/NAS.2010.43.

[6] N. Cascarano, L. Ciminiera, and F. Risso, ''Optimizing deep packet inspection for high-speed trafficanalysis,'' J. Netw. Syst. Manage., vol. 19, no. 1, pp. 7–31, Mar. 2011.

[7] G. Aceto, A. Dainotti, W. de Donato, and A. Pescape, ''PortLoad: Taking the best of two worlds in traffic classification,'' in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM), San Diego, CA, USA, Mar. 2010, pp. 1–5, doi: 10.1109/INFCOMW.2010.5466645.

[8] L. Vu, C. T. Bui, and Q. U. Nguyen, ''A deep learning based method for handling imbalanced problemin network traffic classification,'' in Proc. 8th Int. Symp. Inf. Commun. Technol., Dec. 2017, pp. 333– 339.

[9] P. Wang, F. Ye, X. Chen, and Y. Qian, ''Datanet: Deep learning based encrypted network traffic classification in SDN home gateway,'' IEEE Access, vol. 6, pp. 55380–55391, 2018.

[10] J. H. Shu, J. Jiang, and J. X. Sun, ''Network traffic classification based on deep learning,'' J. Phys., Conf. Ser., vol. 1087, Sep. 2018, Art. no. 062021.

[11] D. Bahdanau, K. H. Cho, and Y. Bengio, ''Neural machine translation by jointly learning to align and translate,'' 2014, arXiv:1409.0473.

[12] C.Wang, T. Xu, and X. Qin, ''Network traffic classification with improved random forest,'' in Proc.11th Int. Conf. Comput. Intell. Secur. (CIS), Shenzhen, China, Dec. 2015, pp. 78–81, doi: 10.1109/CIS.2015.27.

[13] Z. Yuan and C. Wang, ''An improved network traffic classification algorithm based on Hadoop decision tree,'' in Proc. IEEE Int. Conf. Online Anal. Comput. Sci. (ICOACS), Chongqing, China, May 2016, pp. 53–56, doi: 10.1109/ICOACS.2016.7563047.

[14] A. V. Phan, M. L. Nguyen, and L. T. Bui, ''Feature weighting and SVM parameters optimization based on genetic algorithms for classification problems,'' Appl. Intell., vol. 46, no. 2, pp. 455–469, Mar.2017.

[15] B. Schmidt, A. Al-Fuqaha, A. Gupta, and D. Kountanis, ''Optimizing an artificial immune system algorithm in support of flow-based internet traffic classification,'' Appl. Soft Comput., vol. 54, pp. 1–22,May 2017.

[16] S. Dong, ''Multi class SVM algorithm with active learning for network traffic classification,'' ExpertSyst. Appl., vol. 176, Aug. 2021, Art. no. 114885.

[17] J. Cao, Z. Fang, G. Qu, H. Sun, and D. Zhang, ''An accurate traffic classification model based on support vector machines,'' Int. J. Netw. Manage., vol. 27, no. 1, Jan. 2017, Art. no. e1962.

[18] D. Md. Farid, N. Harbi, and M. Zahidur Rahman, ''Combining Naive Bayes and decision tree for adaptive intrusion detection,'' 2010, arXiv:1005.4496.

[19] G. D'Angelo and F. Palmieri, ''Network traffic classification using deep convolutional recurrent autoencoder neural networks for spatial–temporal features extraction,'' J. Netw. Comput. Appl., vol. 173, Jan. 2021, Art. no. 102890.

[20] X. Ren, H. Gu, and W. Wei, ‘‘Tree-RNN: Tree structural recurrent neural network for network trafficclassification,’’ Expert Syst. Appl., vol. 167, Apr. 2021, Art. no. 114363.

[21] T. Shapira and Y. Shavitt, ‘‘FlowPic: A generic representation for encrypted traffic classification and applications identification,’’ IEEE Trans. Netw. Service Manage., vol. 18, no. 2, pp. 1218–1232, Jun.2021.

[22] H. Li, H. Ge, H. Yang, J. Yan, and Y. Sang, ‘‘An abnormal traffic detection model combined BiIndRNN with global attention,’’ IEEE Access, vol. 10, pp. 30899–30912, 2022.

[23] K. Lin, X. Xu, and F. Xiao, ‘‘MFFusion: A multi-level features fusion model for malicious traffic detection based on deep learning,’’ Comput. Netw., vol. 202, Jan. 2022, Art. no. 108658.

[24] K. Lin, X. Xu, and H. Gao, ‘‘TSCRNN: A novel classification scheme of encrypted traffic based onflow spatiotemporal features for efficient management of IIoT,’’ Comput. Netw., vol. 190, May 2021, Art. no. 107974.

S. Izadi, M. Ahmadi, and R. Nikbazm, ‘‘Network traffic classification using convolutional neural network and ant-lion optimization,’’ Comput. Electr. Eng., vol. 101, Jul. 2022, Art.