International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Neural Network Based Attack Path Prediction Using Machine Learning in Cyber Security System

Aksaya Dharani[1], Dr. M. Usha[2], Jenifer Shylaja[3], Mahalakshmi[4], Mary Hanna Priyadharshini[5]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: People are more susceptible to cyber dangers since our culture is becoming more and more dependent on internet access for everyday chores. The demand for strong security measures is growing as technology progresses. More and more people are looking for antivirus software or other systems that can identify new threats. An intrusion detection system is one popular option; it makes use of cutting-edge technology like ICF-GAN and Artificial Neural Network (ANN). Various types of network intrusions may be detected and prevented by this technology because it allows the monitoring of patterns of traffic and the identification of abnormalities, an Intrusion Detection System (IDS) is beneficial for any network. Increasing the precision of identifying breaches and facilitating preventative actions against possible dangers are the primary goals of the current body of research in this area. Datasets such as the UNSW-NB15 are often used for preliminary data analysis to help with this kind of study. For researchers interested in monitoring network traffic and finding patterns that might indicate security issues, this dataset is a great resource. The goal is to build a system that reliably detects problems, protects against attackers and immediately takes measures to solve information security problems.

Keywords: *IDS, UNSW-NBIS, ANN, Cyber Security, ICF-GAN.*

1. Introduction

Digital technology has become widespread in today's networked society, impacting our everyday duties and interactions. The internet has completely transformed our lives and careers, from banking networking. The danger of online dangers and assaults, however, is rising in tandem with our reliance on digital media. Gaining unauthorized access, stealing sensitive information, or disrupting important services may be achieved by malicious actors via exploiting vulnerabilities in networks, apps, and devices. Safeguarding our digital infrastructure is becoming increasingly difficult since both technology and fraudsters' strategies are evolving at a fast pace. Building strong systems for intrusion detection that can identify and react to malicious network activity is one possible option. An infrastructure-free wireless network called a Wireless Sensor Network (WSN) is set up ad hoc using a large number of wireless sensors to monitor environmental, physical, and system condition.

The wireless sensor network overview is shown in Fig.1.As the first line of defence against any security breaches, intrusion detection system keeps an eye on network traffic, looks for trends, and flags any unusual activity. Ransomware transmission, illegal entry attempts, and denial-of-service assaults are just a few of the many intrusions that IDS is able to detect by using sophisticated algorithms like ANN and ICF-GAN. One of the most popular the internet to social benchmark datasets for intrusion detection, the UNSW-NBIS gives re information on network traffic, which is useful for studying new threats and creating detection algorithms. Long-short-term memory (LSTM) is a type of recurrent neural network that can store long-time dependencies of sequential data. The main motivate is to retrieve the optimal features for classification by using different techniques, to build a model for attack detection and analyse it and to compare the performance and result of model in terms of popular metrics.

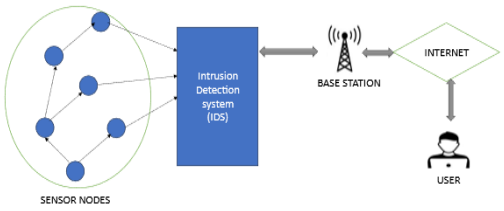

Fig. 1. Overview of Wireless sensor network

Fig.2 below shows the intrusion detection system. They solve the vanishing gradient problem that plagues

[1] *PG Scholar, Velammal Engineering College, Chennai-600066 aksayaitvec@gmail.com*
Associate Professor, Velammal Engineering College, Chennai,600066, India
Usha.m@velammal.edu.in[1]
[3] *Assistant Professor,Vel Tech High Tech Dr.Rangarajan Dr.Sakuntala Engineering College,Chennai-600062 jenifershylaja@velhightech.com*
[4] *Assitant Professor, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College,Chennai-600062*
[5] *Assitant Professor, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai-600062*

conventional neural network by controlling the flow of data using gates and a memory element, allowing data to be retained or discarded as needed.

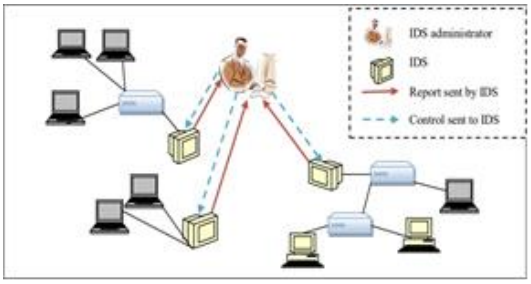

Fig.2.Intrusion Detection System [13]

LSTMs are widely used in many different applications, including time series forecasting, speech recognition, and natural language processing. Convolutions can be used while making advantage of the traceback feature of long short-term memory in LCRN (Long Term Recurrent Convolutional Network) type architectures, which are created by combining recurrent and convolutional neural networks. The field of machine learning has benefited greatly from this application. The purpose of this research is to identify intrusion detection systems (IDS) and their strengths and weaknesses in identifying and mitigating network security risks. We want to learn how different identification methods work and where they fail through an in-depth analysis of the UNSW-NBIS data. Our ultimate goal is to make a positive contribution to ongoing efforts to strengthen cybersecurity and improve the effectiveness of intrusion detection devices in this globally connected environment.

2. Literature Survey

A suggested semantic improved intrusion detection (I-D) technique is aimed at improving the detection accuracy, false detection rate, and missed detection rate of previous methods for Smart Substations are (I-S) secondary system networks. A foundational architecture for network information security protection is established on network I-D after an examination of the supplementary network of IS as well as current security issues. After that [6], CNN and BiLSTM are integrated to build the general framework of the I-S secondary network I-D. Lastly, the detection accuracy is significantly improved by including the semantic examination of LDA (Latent Dirichlet Allocation) to the network ID model. Using the same set of parameters, the simulation tests compare the suggested strategy to the other two. An Intrusion [7] identification framework for complicated networks called CNN-BiLSTM is proposed in this study. In order to close the data gap, the model applies data over-sampling to the imbalanced dataset. To optimize the breach detection system, it on techniques and processes that integrate, cooperate, and are selective. The optimized [8] classifier enhances the precision of intrusion detection. The model is evaluated alongside two-dimensional convolutional neural networks and particle swarm optimization algorithms for support vector machines to confirm the method's detection performance. The model improves intrusion detection accuracy and does adequately for small sample detection, according to the experimental data. An overview [9] of machine learning methods for intrusion detection is the focus of this work. Logistic regression, decision trees, random forests, SVMs, KNNs, naive Bayes, and other machine learning classify methods work well for intrusion detection. This study examines the character behaviours of intrusion detection applications that utilize classification algorithms based on machine learning. This technique [10] raises concerns about the possible vulnerability of personal information in the raw data, which might lead to legal consequences for providers. Consequently, this study suggests an Improved FedAvg, which is an upgrade to the current FedAvg method for detecting intrusions in networks. This approach improves the model's performance while using the full potential of federated learning to preserve data privacy and drastically decrease the transfer of model weights.

3. Strategies of Implementation

The proposed methodology for developing an effective Intrusion Detection System (IDS) using machine learning techniques encompasses several key stages: data collection, preprocessing, feature extraction, and classification,

3.1. Data Collection

This study was conducted using the UNSW-NB15 dataset. This current dataset is a much better replacement for the old KDD cup dataset, which is now somewhat outdated and full of anomalies. This dataset has better class balance than previous intrusion detection datasets. The UNSW-NB15 dataset is large enough to train an accurate model even with low redundancy.

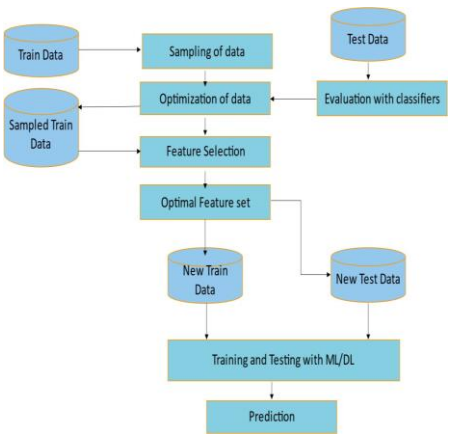

Fig. 3. Process Flow for UNSW NB15 dataset

Prior to the release of UNSW NB15, the dataset KDD CUP'99 was commonly used for intrusion detection systems (IDS). However, when practicing classification, the extreme imbalance of the KDD CUP'99 dataset causes dimensionality problems. It also has inconsistent test and training data in terms of attack records. It has a large number of DOS and normal entries, with the rest missing, resulting in an imbalance between attack types and between normal and attack. Conversely, the UNSW NB15 dataset exhibits greater balance as the process are detailed as shown in the Fig.3. Although pre-built training and testing sets are available in the UNSW NB15, their imbalance and the possibility of duplicate records leading to dimensionality issues are still issues. This work created new training and testing datasets from the raw records in the entire dataset in order to address the imbalance and duplication.

3.2 Preprocessing

The data is pre-processed after collection to make sure it is fit for analysis and of high quality. Some examples of preprocessing jobs include filling in missing data, eliminating outliers, and bringing features into a consistent range by normalization or scaling. It is also possible to encode categorical variables such that they may be more easily used in machine learning models.

Data Cleaning: Clearing out the dataset by removing any missing values. We found that the features are continuous and can be useful for classification.

Data transformation: After describing each feature, we found that the data is highly distorted and needs to be normalized before viewing. Some features were categorical, we coded these features to include in training. Although coded variables do not allow

Data reduction: to better understand the distribution of features, we removed outliers from the dataset before the data visualization step. However, we included all 175,341 samples from the selected features in the final training.

3.2. Feature Extraction

Feature extraction is an essential process for extracting useful information from unstructured data. The use of statistics, Knowledge gain, and reduction in dimensionality methods including Principal Component Analysis (PCA) are just a few of the tools at your disposal for extracting useful characteristics that aid in the identification of network intrusions. The objective is to minimize noise and redundancy while preserving the most discriminative characteristics.

3.3.1. Data Visualization

We plotted count plots to visualize the number of normal and attack samples in the dataset. We used python ‘s seaborn library for all the graphical representations. The fig.1 represents the count plot which helps us visualize the number of normal and attack samples in the dataset (0 is for normal class and 1 is for attack class).

Number of attack sample = 119341

Number of normal samples=56000

This attack sample and normal samples are visualized and analysed using univariate analysis and Bivariate analysis. Univariate analysis is when we analyse each feature of a dataset to detect anomalies, and observe skewness and other relevant information from data, which will ultimately assist us to choose the optimal features for training[8].Bivariate analysis is when one feature is analysed with respect to other. This type of analysis helps us to find correlated features, and also lets us observe how the data for one feature is distributed with respect to another feature [9].

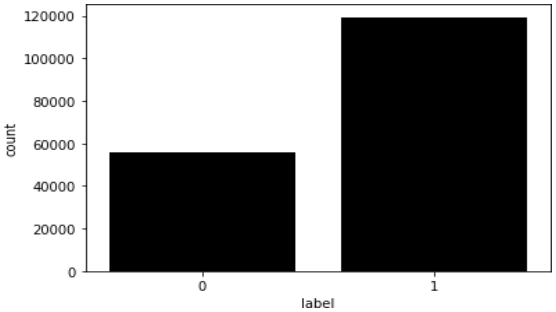

Fig. 4. Attack sampling

3.3.2. Neural Network implementation for UNSW NB15

A computational technique called Neural Network or Artificial Neural Network mimics the neurons in the human brain. Different methods are used to assemble these neurons into networks. Layers such as input, output, and hidden layers are used to group them. For large datasets, stochastic gradient descent (SGD) is the most used ANN [12]. The SGD is an optimization method created for online education. It is a straightforward, effective method that is quickly gaining popularity for training NNs for extensive learning. SGD is an online iterative adaptation of the gradient descent approach. Instead of calculating the gradient of the entire training set, it computes the gradient of one randomly selected example (xt, yt) at each iteration t (1). Let the NN parameter, loss function, and gradient of loss with respect to the w parameter be represented, respectively, by the variables w, l(wt), and l(wt). SGD starts with initial parameter w0 and updates it as follows at step t:

$$wt+1 = wt - \eta t\ (\lambda wt + \nabla l(w, x, yt))$$
(1)

Where t is the learning rate and l (wt, xt, yt) is the gradient computed using just the single example (xt, yt). Using a gradient of a small subset St of size n randomly picked from the training set at each step t, mini-batch SGD update parameter.

$$wt + 1 = wt - \eta t(\lambda wt + \frac{1}{n} \sum \nabla l(w_t, x_i, y_i)) \quad (2)$$

$$(xi\, yi) \epsilon St$$

3.3.3. Convolutional Neural Networks and LRCN the implementations

The foundation of convolutional neural networks is a mathematical process called a convolution, which improves performance with larger datasets and aids in the identification of significant features. As demonstrated by earlier CNN design implementations, this neural network performs better with larger datasets. CNN is one of the suggested solutions here because of the size of the UNSW NB15 dataset (with the use of all 4 CSV files). Convolutions can be used while making advantage of the traceback feature of long short-term memory in LCRN (Long Term Recurrent Convolutional Network) type architectures, which are created by combining recurrent and convolutional neural networks. The field of machine learning has benefited greatly from this application.

Our proposed system is a developing system of the following two models. The first model depended on the direct applying of machine learning classification algorithms after pre-processing the dataset. The accuracy of this model is perfect, but it takes long prediction time to predict the whole dataset as normal or attack. Moreover, the dataset we worked on is KDD CUP99 which is a standard network attack dataset but an older one. For this reason, we have applied some more machine learning classification algorithms along with the existing ones on another advanced dataset UNSW NB15. This second model trains the dataset and tests it‘s working for three sets of data. First for binary classification, second for Multiclass and the third for a concatenated group of attacks which are clubbed together because of overfitting or underfitting issue. To evaluate the accuracy, F1 score, precision, and recall of both datasets in terms of system efficiency and robustness.

The combination of Convolutional Neural Networks and Recurrent Neural Networks result in LCRN (Long Term Recurrent Convolutional Network) type architectures which allow the use of convolutions while utilizing the traceback property of Long Short-Term Memory. This implementation has yielded many positive results in the field of machine learning. Hence, this is the final proposed model as it will provide an insight on how well these two architectures (RNN and CNN) can work together on this dataset as well as in comparison to their individual models.

Based on the below table.1, we can clearly see that many implementations of ML/DL techniques have been done where DO_IDS [83] results in 92.8%, a simple implementation of Artificial Neural Network (ANN) with XG Boost for feature extraction results in a minimum of 77.51%. It is deduced that by trying the feature extraction with hybrid classification methods, the accuracy can be increased because of which the system can be made more secure. Our model O_LRCN with a combination of Correlation matrix and Xtra Trees as feature reduction techniques gives an overall accuracy of 94.55.

Methods	**Techniques**	**Accuracy**
DO_IDS [14]	GA	92.8
RUS Boost [15]	Correlation matrix	92
MDPCA-DBN [16]	Fuzzy aggregation	82.08
CNN-BiLSTM[11]	O-SS-SMOS	77.71
ANN [12]	XG Boost	77.51
DBN [14]	Correlation matrix	85.73
LRCN	**Correlation matrix, Xtra Trees**	**94.55**

Table.1. Result comparison of different model vs LRCN

4.Result and analysis

In the current model, computational models have been developed to identify and classify the activities with the network based on the best and relevant parameters. Literature study reveals that there is a lot of scope for improvising the techniques implemented to enhance the intrusion detection process. So, implementing hybrid techniques instead of one can have a good impact on overall evaluation. In the initial stage the features of the most widely used network attack dataset KDD CUP99 were reduced and optimized, and a cross validation is done using machine learning for all the attack classes. Secondly, the implemented techniques are validated by applying to another dataset UNSW NB15 and the results are compared with earlier implementations. Further on to the optimized features CNN, RNN and LRCN are implemented to compare the results against machine learning techniques. Using hybrid techniques, the accuracy increased in comparison to single techniques and a model has been constructed that compares

accuracy results using Machine learning and Deep learning techniques. The current study has developed a hybrid model that could possibly be utilized for network attack detection and classification. Previously, the models were more focussed in increasing the accuracy than reducing the False positive rates and classifying the attacks. Moreover, our model considers both overfitting and underfitting issues in the dataset by creating a concatenated class of attacks and applying CNN, RNN and LRCN models. None of the previously done works showcases this to the best of our knowledge.

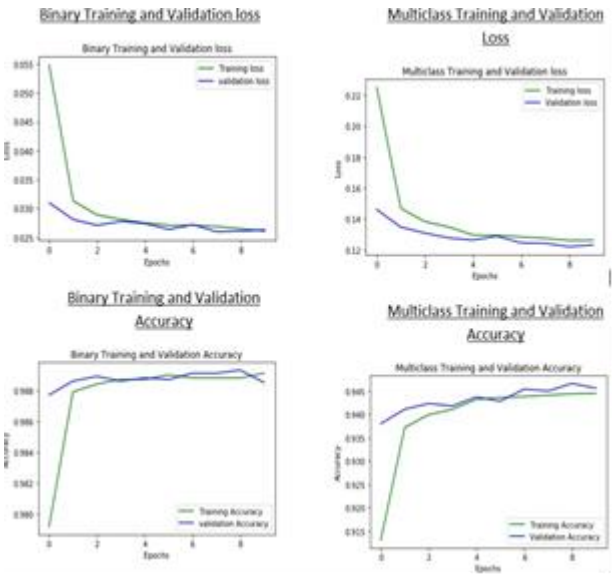

Fig.5. Training and Validation loss and accuracy

Looking at our implementation and other related works on the UNSW NB15 Dataset, we can see how well binary classification has been implemented on the dataset and thus allows for accurate classification between attack and normal. However, our implementation of LRCN with minimal parameters also helps illustrate how less complexity of the model and fewer training instances are sufficient for accurate binary classification on the dataset.

From above Fig.5, It is quite evident looking at multiclass implementations in related papers that macro results have not reached accurate implementation yet. This misclassification is due to the unbalanced nature of the dataset that results in overfitting on particular groups and underfitting on others, a dimensionality issue which can be best solved by removing the unbalanced problem in the dataset. In our implementation, it is clearly seen that the first multiclass model performed poorly, as expected. This resulted in the initial grouping of the classes, i.e., taking the classes with the least number of records as a factor and the observational results of classes that exhibited underfitting when reviewing real time data as another, when selecting which groups to concatenate. As this resulted in better macro metrics, we implemented the same process of selecting classes to concatenate to remove dimensionality issues furthermore. Implementing this two times more helped us reach our optimal result.

4. Conclusion

This paper gives an understanding to how the three widely used architectures CNN, RNN and LRCN work on the UNSW NB15 dataset. It also represents the concatenation of attacks categories for better results as well as the proposed implementation of the same dataset. Looking at our implementation and other related works on the UNSW NB15 Dataset, we can see how well binary classification has been implemented on the dataset and thus allows for accurate classification between attack and normal. However, our implementation of LRCN with minimal parameters also helps illustrate how less complexity of the model and fewer training instances are sufficient for accurate binary classification on the dataset. In multiclass implementations in related papers that macro results have not reached accurate implementation yet. This misclassification is due to the unbalanced nature of the dataset that results in overfitting on particular groups and underfitting on others, a dimensionality issue which can be best solved by removing the unbalanced problem in the dataset. It is clearly seen that the first multiclass model performed poorly, as expected. This resulted in the initial grouping of the classes, i.e., taking the classes with the least number of records as a factor and the observational results of classes that exhibited underfitting when reviewing real time data as another, when selecting which groups to concatenate. As this resulted in better macro metrics, we implemented the same process of selecting classes to concatenate to remove dimensionality issues furthermore. Implementing this two times more helped us reach our optimal result. This can be seen in the proposed model section of the paper and is our approach to solve the macro result misclassification issue present in previous implementations seen done on the UNSW NB15 Dataset and its predecessors. The implementation in this paper can be taken forward by attempting to reach accurate results in the approach of concatenation of groups into the multiclass classification approach and by further developing individual models to classify the concatenated group into its different attacks for further classification.

References

[1] Kiran, S. W. Prakash, B. A. Kumar, Likhitha, T. Sameeratmaja and U. S. S. R. Charan, "Intrusion Detection System Using Machine Learning," 2023 International Conference on Computer Communication and Informatics (ICCCI),

Coimbatore, India, 2023, pp. 1-4, doi: 10.1109/ICCCI56745.2023.10128363.

[2] M. Kohler and B. Kohler, "Analysis of Convolutional Neural Network Image Classifiers in a Rotationally Symmetric Model," in IEEE Transactions on Information Theory, vol. 69, no. 8, pp. 5203-5218, Aug. 2023, doi: 10.1109/TIT.2023.3262745.

[3] P.Zhang, G. Tian and H. Dong,"Research on network intrusion detection based on Whitening PCA and CNN," 2023 7th International Conference on Smart Grid and Smart Cities (ICSGSC), Lanzhou, China, 2023, pp. 232-237, doi:10.1109/ICSGSC59580.2023.10319169.

[4] G. de la Cruz, M. Lira, O. Luaces and B. Remeseiro, "Eye-LRCN: A Long-Term Recurrent Convolutional Network for Eye Blink Completeness Detection," in IEEE Transactions on Neural Networks and Learning Systems, vol. 35, no. 4, pp. 5130-5140, April 2024, doi: 10.1109/TNNLS.2022.3202643.

[5] Xiang, C. Zhang, J. Wang and B. Wang, "Network Intrusion Detection Method for Secondary System of Intelligent Substation based on Semantic Enhancement," 2022 4th International Conference on Electrical Engineering and Control Technologies (CEECT), Shanghai, China, 2022, pp. 796-800,doi:10.1109/CEECT55960.2022.10030264

[6] J. Li, "Network Intrusion Detection Algorithm and Simulation of Complex System in Internet Environment," 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2022, pp. 520-523, doi: 10.1109/ICIRCA54612.2022.9985720.

[7] Chen, X. Xu, G. Wang and L. Yang,"Network intrusion detection model based on neural network feature extraction and PSO-SVM," 2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 2022, pp. 1462- 1465, doi:10.1109/ICSP54964.2022.9778404.

[8] P. Vincent, H. Larochelle, I. Lajoie, Y. Bengio, and P.-A. Manzagol,Stacked Denoising Autoencoders: Learning Useful Representations in a Deep Network with a Local Denoising Criterion,‖ p. 38.

[9] N. Moustafa and J. Slay, ―The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,‖ *Inf. Secur. J. Glob. Perspect.*, vol. 25, no. 1–3, pp. 18–31, Apr. 2016, doi: 10.1080/19393555.2015.1125974.

[10] J. Ren, J. Guo, W. Qian, H. Yuan, X. Hao, and H. Jingjing, ―Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms,‖ *Secur. Commun. Netw.*, vol. 2019, p. e7130868, Jun. 2019, doi: 10.1155/2019/7130868.

[11] C. Seiffert, T. M. Khoshgoftaar, J. Van Hulse, and A. Napolitano,―RUSBoost: A Hybrid Approach to Alleviating Class Imbalance,‖ *IEEE Trans. Syst. Man Cybern. - Part Syst. Hum.*, vol. 40, no. 1, pp. 185–197, Jan. 2010, doi: 10.1109/TSMCA.2009.2029559.

[12] Y. Yang, K. Zheng, C. Wu, X. Niu, and Y. Yang, ―Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks,‖ *Appl. Sci.*, vol. 9, no. 2, Art. no. 2, Jan. 2019, doi: 10.3390/app9020238.

[13] K. Jiang, W. Wang, A. Wang, and H. Wu, ―Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network,‖ *IEEE Access*, vol. 8, pp. 32464–32476, 2020, doi: 10.1109/ ACCESS.2020.2973730.

[14] S. M. Kasongo and Y. Sun, ―Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset,‖ *J. Big Data*, vol. 7, no. 1, p. 105, Dec. 2020, doi: 10.1186/s40537-020-00379-6.

[15] S. Almogren, ―Intrusion detection in Edge-of-Things computing,‖ J. Parallel Distrib. Comput., vol. 137, pp. 259–265, Mar. 2020, doi: 10.1016/j.jpdc.2019.12.008.

[16] S. Doshi, ―Analyze the data through data visualization using Seaborn,‖ *Medium*, Feb. 09, 2019. https://towardsdatascience.com/analyze-the-data- through-data-visualization-using-seaborn-255e1cd3948e (accessed Oct. 21,2022).

[17] Mohan, A., Dinesh Kumar, R. and J., S. 2023. Simulation for Modified Bitumen Incorporated with Crumb Rubber Waste for Flexible Pavement. International Journal of Intelligent Systems and Applications in Engineering. 11, 4s (Feb. 2023), 56–60.

[18] R.Gopalakrishnan, Mohan, "Characterization on Toughness Property of Self-Compacting Fibre Reinforced Concrete", Journal of Environmental Protection and Ecology 21, No 6, 2153–2163 (2020).

[19] Vidhya Lakshmi Sivakumar, A.S. Vickram, Ragi Krishnan, Titus Richard, "AI-Enhanced Decision Support Systems for Optimizing Hazardous Waste Handling in Civil Engineering," SSRG International

Journal of Civil Engineering, vol. 10, no. 11, pp. 1-8, 2023. Crossref, https://doi.org/10.14445/23488352/IJCE-V10I11P101

[20] V. Sundaram, Vidhya Lakshmi Sivakumar, Anand Raju, A. Saravanan, Titus Richard, "The Role of 3D Printing in Engineering and its Historical Perspective in Civil Engineering - A Review," SSRG International Journal of Civil Engineering, vol. 10, Vidhya Lakshmi Sivakumar, A.S. Vickram, Ragi Krishnan, Titus Richard, "AI-Enhanced Decision Support Systems for Optimizing Hazardous Waste Handling in Civil Engineering," SSRG International Journal of Civil Engineering, vol. 10, no. 11, pp. 1-8, 2023. Crossref, https://doi.org/10.14445/23488352/IJCE-V10I11P101

[21] V. Sundaram, Vidhya Lakshmi Sivakumar, Anand Raju, A. Saravanan, Titus Richard, "The Role of 3D Printing in Engineering and its Historical Perspective in Civil Engineering - A Review," SSRG International Journal of Civil Engineering, vol. 10, no. 12, pp. 58-68, 2023. Crossref, https://doi.org/10.14445/23488352/IJCE-V10I12P107 no. 12, pp. 58-68, 2023. Crossref, https://doi.org/10.14445/23488352/IJCE-V10I12P107