Vol. 05, No. S1 (2023) 103-110, doi: 10.24874/PES.SI.01.013

Proceedings on Engineering Sciences

www.pesjournal.net

DEEP LEARNING-BASED INTRUSION DETECTION AND PREVENTION IN WIRELESS COMMUNICATION

Akash Kumar Bhagat[1]
Prashant Kumar
Pawan Bhambu
Pandey V. K.
Om Prakash
Raghu N.

Received 17.05.2023.
Accepted 10.07.2023.

Keywords:

Intrusion detection system (IDS), wireless sensor network (WSN), deep learning (DL), transfer deep multicolumn convolution neural network (TDMCNN).

ABSTRACT

Wireless sensor networks (WSNs) are made up of a large number of sensor nodes which collect data and send it to a centralized location. Nevertheless, the WSN has several security difficulties because of resource-constrained nodes, deployment methodologies, and communication channels. So, it is very necessary to identify illegal access in order to strengthen the safety measures of WSN. The use of network intrusion detection systems (IDS) to safeguard the network is now standard procedure for any communication system. While deep learning (DL) methods are often utilized in IDS, their efficacy falls short when faced with imbalanced attacks. An IDS based on a novel transfer deep multicolumn convolution neural network (TDMCNN) technique was presented in this study to address this problem and boost performance. The most significant features of the dataset are chosen using a cross-correlation procedure and then included into the suggested methods for detecting intrusions. The accuracy, precision, sensitivity, and specificity are used to conduct the analysis and comparison. The experimental findings verified the effectiveness of the suggested method over the status quo of deep learning models for attack detection.

1. INTRODUCTION

The standard of living from mobiles to wireless communications (WC) access has been significantly impacted by the exponential rise of WC over the last decade. These networks are also very susceptible to hacking assaults that might range between simply listening to active interference, due to the utilization of WC connectivity. One of the attacks that have the most impact on these networks is the black hole attack. Using an Intrusion Detection System (IDS) will shield the network from this assault. IDS are used to describe the practice of checking over communications systems, processes, and applications to find any instances of malicious activity, illegal access, or abuse. Intrusion detection's main objective is to identify any unusual activity that might undermine the confidence, security, or accessibility of computer networks, data, or network

[1] Corresponding author: Akash Kumar Bhagat
Email: akash.b@arkajainuniversity.ac.in

resources (Moudni et al., 2019).The networks are seen as being among the most exposed points for various threats and security attacks. Several research projects have concentrated on the initial security layer, the preventive layer, in an effort to address this problem. Hence, more secure methods of authentication, permission, and cryptography have been suggested by research. Even with the implementation of such robust protective measures, a system could still be penetrated by a persistent adversary utilizing cutting-edge methods or powerful processing power. Hence, an intrusion detection layer must come before any prevention layer. This served as the impetus for the creation of IDS. The majority of commercially available IDS use signature based techniques. The networks, systems, and programs getting examined, as well as the kinds of threats and attack routes that may attempt to compromise them, must all be well understood in order for IDS to be effective. It also requires for ongoing security event monitoring and analysis, as well as the capacity to react quickly and efficiently to any detected problems (Illy et al., 2019) .IDS may be carried out using a variety of methods, including that of behavioral, anomalous, and signature-based detection. Using a collection of recognized attack signatures, signature-based detection looks for any matches by analyzing the data being transmitted to the database. Detecting anomalies requires locating any traffic patterns or anomalous activity that differs from typical network behavior. Analyzing user activity is part of behavior modification detection that examines for any unusual activity or departure from typical user behavior. Attacks may be prevented with intrusion prevention systems (IPS). These systems use methods including network filtering, encryption, and access control to prevent illegal access and stop data breaches. Although encryption protects information by encrypting it so that it's able to only be viewed by authorized parties, access control entails restricting network access based on user identities. Analytic techniques include examining network activity and preventing any that is considered dangerous or suspicious (Parsamehr et al., 2019; Fu, et al., 2023).The value of WC for interaction across borders cannot be overstated. Throughout this age of communication, the rapid technological advancement over the last decades has enhanced the standard of living on Earth. WC allows organizations to communicate with one another through transmission networks. The infrastructure-based WC depicted in dependent on an infrastructure, with nodes routing data to a base station over pre-established paths. IDS are used to detect suspicious activity and unwanted access in WC. To find possible threats, these systems use a number of methodologies, including behavior-based detection, exceptional situation detection, and signature-based detection. Although anomaly-based detection examines for differences from expected network activity, signature-based detection compares the network traffic to known attack patterns. Behavior-based detection includes examining network users' and devices' actions to spot unusual activity (Khan et al., 2020).The existence now includes a significant amount of internet use. For everyone, using the internet has become essential. Hence, it is important to maintain security as the usage of the internet for personal purposes increases. Many attacks are seen against the network or system. Preventing harmful activity on the system IDSs provide certain information to other assisting systems, including: Identification of the invader and their location, kind of intrusion, and place of intrusion. Given that it provides additional details about an incursion, such information may be helpful in reducing and resolving the causes of assaults. Thus, intrusion system detection is helpful for network security. IDS are a means of identifying and differentiating. Wide-ranging security measures are not a stand-alone safety precaution in a network area or unit (Waskl et al., 2020; Santhosh Kumar et al., 2023). WSNs are useful in a lot of industries because of its straightforward and simple usage characteristics. A valid network activity that can additionally be done quietly or actively is intrusion. If the first line of defense in a security system, intrusion prevention, is unable to prevent invasions, intrusion detection will next take action. IDSs provide one or more of the appropriate details to the other supporting systems in any security concern as a result of network users discovering some problematic behavior in a system: Identification of the intrusion, its position, the intrusion instance, the behavior, and the intrusion model layer that the intrusion takes place. WSNs are unique in having limited power supplies, slow transmission speeds, tiny memory sizes, and limited data storage (Sharma and Athavale 2020; Si-Ahmed et al., 2023)The IDS concept seeks to spot a threat or intrusion into the system, and it constantly analyzes the network by seeing potential occurrences and documenting them by stopping them. Intrusion detection and prevention system (IDPS), that combine different systems, is used to monitor and capitalize on network activity, assess it for potential security policy breaches, and execute intrusion detection and stop to identify occurrences. IDS are security technologies that watch network traffic and look for signs of unusual behavior. In alert administrators of possible risks and enabling them to take action even before harm is done, IDS may be used to stop intrusions in wireless communications (Sicato et al., 2020). In this research, we offer a transfer deep multicolumn convolution neural network (TDMCNN) approach for intrusion detection and prevention in wireless communications.

The remaining segments of the paper are set up as follows: Segment II provides a related works, Segment III describes the proposed method, and Segment IV presents and discusses experimental findings sets and simulation outcomes. The analysis is concluded in Segment V, which also recommends additional studies.

2. RELATED WORKS

(Tabassum et al., 2019) analyzed the most current Intrusion Detection methods for IoT networks, with a stronger emphasis on hybrid and intelligent methods. Furthermore, it provides an extensive analysis of the IoT layers, communication protocols, and security concerns, confirming the need of IDS in both layered and protocol methods. In order to determine possible future possibilities for IDS deployment, this poll evaluates the disadvantages and benefits of each strategy.

(Kumar et al., 2021) protected against four kinds of attacks in this article, including exploit DoS, probe, and generic, via a revolutionary unified intrusion detection system (UIDS) for the IoT. Furthermore, the system can identify common types of network traffic. The internet-based wireless connectivity between several devices in IoT-based systems exposes them to various security risks. The majority of IDS-related research relies on the KDD99 or NSL-KDD 99 data sets, that aren't capable of detecting modern attacks.

(Lokman et a., 2019)presented an all-encompassing strategy called IDS that has proven to be a useful tool for protecting networks and information systems throughout the decades. The following components detection techniques, deployment strategies, assault tactics, and finally technical challenges thus advised a thorough analysis of IDS as identified in the literature. Also included in our contributions were categories for the anomaly based IDS, such as frequency based regression, statistical based, and hybrid based.

(Alladi et al., 2021) presented a Deep Learning Engines (DLE) based intrusion detection architecture that uses artificial intelligence (AI) to recognize and categorize automobile movement in Internet of Vehicles (IoV) connections into groups for potential cyber attacks. In addition, rather of running on remote clouds, these DLEs will be deployed on Multi access Edge Computing (MEC) servers. These servers will take into consideration the mobility of the cars as well as the real-time needs placed on the network for the Internet of Vehicles. The efficacy of the suggested method is demonstrated through extensive experimental results utilizing common assessment metrics and average recognition time on a MEC test bed.

(Umba et al., 2019) presented the Artificial Intelligence (AI) methodologies that are used to discover intrusions in Software-Defined Wireless Sensor Networks (SDWSNs). Also, the authors identified the cryptographic schemes as well as the security risks that are related with SDWSNs. It is demonstrated that hostile attacks on SDWSNs may be thwarted using a two-level security model that combines AI approaches with cryptographic protocols.

(Deng et al., 2019) addressed the current concerns with IoT network security and emphasizes the need for intrusion detection. The discussion and analysis of the use of various intrusion detection methods on IoT architecture. In order to plan for the next stage of study, compare way various intrusion detection methods are used. Exploring network infiltration technologies via the use of data mining, machine learning and other approaches is becoming more popular. It is very difficult to raise the detection performance of the detection of network intrusions using only one class characteristic or detection model at a time.

(Satam and Hariri 2020) introduces the Wireless Intrusion Detection System (WIDS), a technique to anomalous behavior analysis that can accurately and efficiently identify assaults on Wi-Fi networks. In order to determine if a flow of data sent over Wi-Fi is legitimate or fraudulent, models built using machine learning are employed to simulate the typical actions taken by the Wi-Fi protocol. The method was examined in great detail by making use of a wide variety of datasets that were gathered locally at the University of Arizona in addition to the AWID family of datasets. Method can correctly identify any attack on Wi-Fi standards with a negligibly low rate of false positives and false negatives.

(Radoglou-Grammatikis and Sarigiannidis 2019) analyzes 37 examples to look at the role that IDPSs play in the SG paradigm. More specifically, these systems may be thought of as a secondary defensive system that strengthens cryptographic operations by quickly identifying and averting possible security breaches. For instance, unless a cyber attack is successful in circumventing the essential encrypted communications and permission processes, the IDPS processes may act as another layer of defense, able to alert the system administrator to the existence of the particular attack or facilitating the acceptable preventive actions. This helps ensure that the system remains secure.

3. PROPOSED METHODOLOGY

3.1. Dataset

The NSL-KDD dataset, created by MahbodTavallaee et al., was utilized in this study. This is the updated and modified KDD dataset (Abhale, 2023).

3.2. Feature extraction using Cross Correlation

The feature extraction of cross-correlation is applied because both sets of data are associated and because these correlations may be exploited. Hence, a smaller amount of data and fewer computations will be required since certain data won't be utilized. The following equation may be used to determine the cross-correlation between two sequences, w (m) andz (m):

$$D\big(w(m); z(m)\big) = \sum_{n=-\infty}^{\infty} w(n) z\,(n+m) \qquad (1)$$

The cross-correlation between two sequences, w (m) and z (m), will reach its highest possible value if the two sequences are identical.

The cross-correlation is utilized in a variety of domains, including the detection of network IDS. The next section provides a review of a number of techniques for detecting network IDS that make use of cross-correlation. The identification of variables on the basis of common data, that ultimately results in a method that is straightforward and efficient. A method for the identification of IDS that makes use of the information gain feature selection criteria. In addition to this, the worth of the features is determined by utilizing the mutual information, and any characteristics that are deemed improper are removed. In order to identify any irregularities in the flow of cyberspace traffic, the control and data plane traffic carried out a calculation known as cross-correlation. Demonstrated that the use of cross-correlation may improve the detection performance and identify IDS and assaults that last for just a brief period of time in the network data. An example of a meta-heuristic evaluation paradigm is the features correlation analysis and associate impact scale. Determined the level of IDS range threshold based on the most important characteristics of networks transaction data that was available for training. In their plan, the linear canonical correlation technique was used for the purpose of feature optimization, and the feature association effect scale was investigated using the optimum features that were chosen. According to the findings, the characteristic correlation has a substantial influence on minimizing the computational and temporal complexity of evaluating the features association impact scale.

3.3. Transfer Deep Multicolumn Convolution Neural Network

In the area of network security, TCNN may also be used in the role of IDS detection. In this scenario, the TCNN is trained on data pertaining to network traffic in order to identify abnormalities and IDS. Deep learning (DL) is used most often in situations that the new dataset is much shorter than the initial dataset that was utilized in the training of the pre-trained model. In terms of the preliminary training, DL gives us the ability to begin with the learned features on the dataset and then modify these features and possibly the structure of the model to fit the new task. DL of the TCNN pre-trained model, while simultaneously testing and modifying the network security as well as the dataset characteristic to assist in determined variables affects classification accuracy, despite having limited computational capabilities for intrusion detection and prevention in wireless communications.

These techniques are useful for enhancing trainable parameters in error back propagation to avoid the network security problem. This may contribute to the construction of deeper TCNN structures, that can assist enhance final performance for IDS. $E$is the nonlinear function that will be used for the convolutional route, and G represents the shortcut path for network.

$$z = E(w) + w \qquad (2)$$

$$z = E(w) + G(w) \qquad (3)$$

Construct a multi-column structured model for network security based on the detection of IDS. The approach is made up of a number of different recognizing modules, and every one processes recognition data on its own. Each recognition module is developed using a multi column convolutional neural network (MCNN) structure as the basis for its architecture. Its structure is made up of convolution layers and pooling layers.

A convolutional layer is the fundamental component that makes together the module. This layer comprises a base layer that is subsequently followed by a bias-add layer. Each module makes use of data from the temporal data, and the cost function is built to represent both the category of the emotion as well as the intensity that it is perceived. The following are specifics about the cost function:

$$cost(arousal, valence) = (1 - sim_{cos})\{(b_j^2 - b^2) + (u_j^2 - u^2)\} \qquad (4)$$

Where $sim_{cos}$is the degree of cosine similarity between the projected and real arousal-valences, and both are vectorized. The activation function is referred to as leackyReLU. After being reformatted into a rectangular shape, the input is then subjected to two conv3-16 layers processing, and that is accompanied by a maxpooling layer. After the maxpooling layers have been implemented and following these two conv3-32 layers. Layers that are completely related to one another are installed.

The culmination of these layers is the formation of folds, and each one correlates to a different valence and arousal. A MCNN for IDS may include various sorts of characteristics from the network traffic data in each of its columns. For instance, one column can concentrate on collecting statistical characteristics from network traffic, and an another column would focus on extracting information from payloads. A fusion layer, such as a weighted sum or concatenation, may then be used to merge the outputs from each column. The structure of our MCNN model is illustrated in Fig.1.

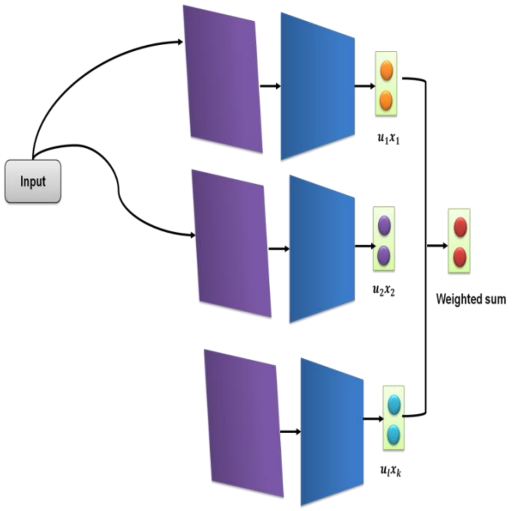

Figure 1. The multi column convolutional neural network structure of our model

The following formula is used to combine each module's individual choices (u_j) into a final decision (u_{final}), either via attack prevention or a prevention method:

$$u_{final} = \frac{\sum_{j=1}^{l} x_j u_j}{\sum_{j=1}^{l} x_j} \quad (5)$$

Where u_j is the choice from the j^{th}module is $u_{final}$the model's final decision, and $x_j$is the projected probability foru_j. The anticipated probability of the module serves as the source ofx_j, the weight term for the j^{th}choice. u_jHas a binary value of +1 or -1, with +1 denoting a high emotion state and -1 denoting a low emotion state. Quantize $u_j$in (0.0 ~ 1.0) into a nine-point measure in order to obtain u_j(1 ~ 9). Then, if the value after the metric is equal to or more than 5, it is converted to +1, and if it is less than 5, it is turned to -1.

The attack prevention uses the majority win principle that determines the outcome based on theu_j. value of the majority. As a result, the following formula is used to determine the attack prevention method outcome:

$$u_{final} = \left(\sum_{j=1}^{l} u_j > 0\right) \ ?+1\!:-1 \quad (6)$$

Table 1. The accuracies for valence and arousal with time complexity.

Type of Layer		Width	Filter Height	In-Layer	Out-Layer	No. of Parameters
	conv 3-16	3	3	1	16	144
conv	conv 3-16	3	3	16	16	2304
	conv 3-32	3	3	16	32	4608
	conv 3-32	3	3	32	32	9216
	fc-64	12	12	32	64	294,912
fc	fc-32			64	32	2048
	fc-16		-	32	16	512
	fc-2			16	2	32
			Total			313,776

The number of parameters in our model is estimated in Table 1. The TDMCNN architecture can be modified to include many columns of CNN layers, with each column concentrating on a particular component of the network traffic data, such as flow statistics, packet payload information, or header information. The TDMCNN can increase the IDS accuracy by learning different data representations.

4. RESULT AND DISCUSSION

Clearly Techniques are often applied in IDS nevertheless; the effectiveness is compromised while confronted with intrusions that are unbalanced. In this paper, an intrusion detection system (IDS) based on a TDMCNN approach was provided as a potential solution to this issue, as well as a means to improve performance. The efficiency of a proposed method is evaluated in comparison to that of existing approaches such as K-nearest neighbor (KNN) (Abdan, M. and Seno, 2022) and support vector machine (SVM) (Abdan, M. and Seno, 2022), Convolutional neural network (CNN) (Abdan, M. and Seno, 2022). These techniques are compared with previous techniques using several parameters including, accuracy, specificity, sensitivity, and precision.

4.1. Accuracy

The accuracy of the approaches used, the caliber of the data used for training and testing, and the capacity to react to changing attack patterns all play a role in the accuracy of IDS in wireless communications.

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (7)$$

where True Positives (TP) refer to the percentage of actual attacks that the system successfully detects, True Negatives (TN) to the percentage of regular network traffic that the system correctly identifies as such, False Positives (FP) to the percentage of regular network traffic that the system incorrectly identifies as an attack, and False Negatives (FN) to the percentage of actual attacks that the system fails to detect.

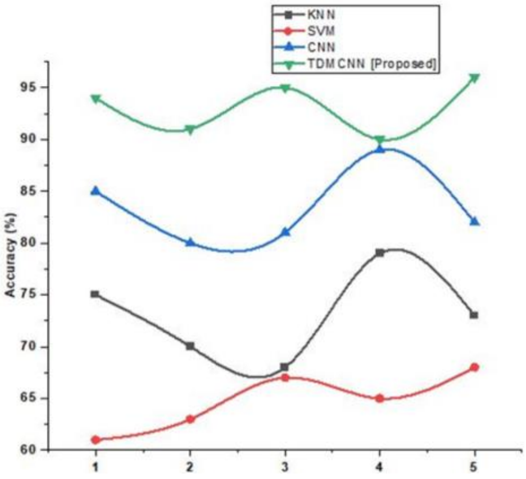

Figure 2. Accuracy

Table 2. Accuracy.

	Accuracy (%)			
	KNN	**SVM**	**CNN**	**TDMCNN [Proposed]**
1	75	61	85	94
2	70	63	80	91
3	68	67	81	95
4	79	65	89	90
5	73	68	82	96

Figure 2 shows the accuracy of the proposed and existing system. Accuracy in the recommended TDMCNN has been obtained by the identification and prevention of intrusions in wireless communications. CNN attained 89%, KNN attained 79%, and SVM attained 68%, whereas the proposed system reached 96% accuracy. It demonstrates that the suggested method is more accurate than the existing one. Table 2 depicts the values of accuracy.

4.1. Sensitivity

Sensitivity is a metric for intrusion detection and prevention system's capacity to recognize real assaults or intrusions in a wireless communication network, also known as true positives. Sensitivity is a crucial parameter to take into account when assessing the efficacy of IDS in wireless communications since it quantifies the system's capacity to identify real assaults and stop incursions.

$$\text{Sensitivity} = \frac{TP}{TP+FN} \tag{8}$$

False Negatives (FN) are the number of real attacks that the system incorrectly failed to identify, while True Positives (TP) is the number of actual assaults that the system successfully identified.

Table 3. Sensitivity.

METHOD	Sensitivity (%)
KNN	53
SVM	75
CNN	85
TDMCNN [Proposed]	92

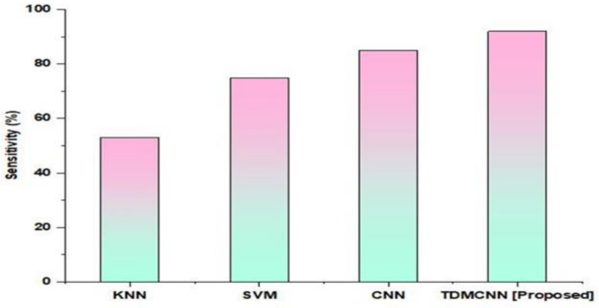

Figure 3. Sensitivity

Figure 3 shows the sensitivity of the proposed and existing system. The proposed TDMCNN has successfully attained sensitivity through the detection and prevention of intrusions in wireless communications. CNN attained 85%, KNN attained 53%, and SVM attained 75%, whereas the proposed system reached 92% accuracy. It demonstrates that the suggested method is more sensitivity than the existing one. Table 3 depicts the values of sensitivity.

4.2. Specificity

The specificity of an intrusion detection and prevention system refers to its capacity to recognize legitimate network traffic as benign in a wireless communication network and to accurately identify true negatives.

$$\text{Specificity} = \frac{TN}{TN+FP} \tag{9}$$

False Positives (FP) are the number of innocuous network traffic that the system wrongly identifies as an attack whereas True Negatives (TN) are the number of benign network traffic that the system properly identifies as such.

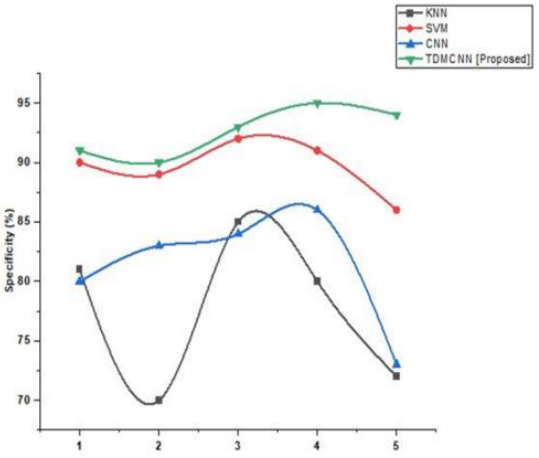

Figure 4. Specificity

Table 4. Specificity.

	Specificity (%)			
	KNN	SVM	CNN	TDMCNN [Proposed]
1	81	90	80	91
2	70	89	83	90
3	85	92	84	93
4	80	91	86	95
5	72	86	73	94

Figure 4 shows the specificity of the proposed and existing system. Specificity has been reached with the proposed TDMCNN through the process of intrusion detection and prevention in wireless communications. CNN attained 86%, KNN attained 85%, and SVM attained 91%, whereas the proposed system reached 95% specificity. It demonstrates that the suggested method is more specificity than the existing one. Table 4 depicts the values of specificity.

4.3. Precision

The ability of an intrusion detection and prevention system to accurately identify true positives real attacks in a wireless communication network is measured by its precision. Precision, an important criterion in analyzing the performance of a wireless intrusion detection and prevention system, measures its ability to accurately identify true attacks and reduce false positives.

$$Precision = \frac{TP}{TP+FP} \tag{10}$$

False Positives (FP) are the number of instances of regular network traffic that the system wrongly identifies as an attack, whereas True Positives (TP) are the number of genuine assaults that the system properly detects.

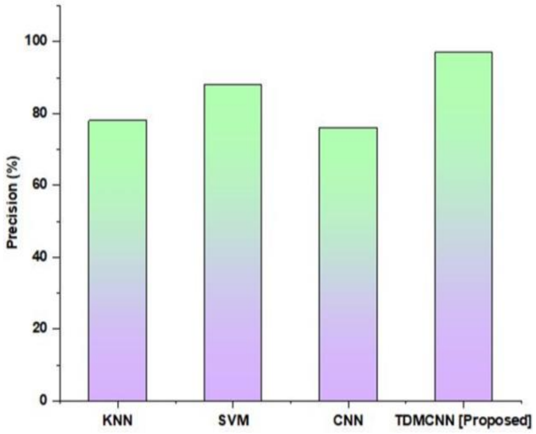

Figure 5. Precision

Figure 5 shows the precision of the proposed and existing system. The proposed TDMCNN has been successful in achieving precision through the detection and prevention of intrusions in wireless communications. CNN attained 86%, KNN attained 85%, and SVM attained 91%, whereas the proposed system reached 95% precision. It demonstrates that the suggested method is high precision than the existing one.

5. CONCLUSION

WSNs are made up of a large number of sensor nodes, each of which gather data and then transmit it to a single site for processing. Despite this, the WSN suffers from a number of security flaws due to the fact that its nodes have limited resources, their deployment methods, and their communication routes. So, it is of the utmost importance to locate instances of unlawful access in order to improve the security measures of WSN. IDS are the initials that are used to characterize the technique of checking over communications systems, processes, and applications in order to look for any instances of abusive behavior, unauthorized access, or malicious activities. The use of network intrusion detection systems (IDS) to safeguard the network is now standard procedure for any communication system. In conclusion, the TDMCNN model is a promising approach for intrusion detection in computer networks. The use of deep learning and pre-trained multicolumn convolutional neural networks improves the detection accuracy and reduces the training time. The model can be used for real-time intrusion detection in computer networks, which is crucial for ensuring the security of the network

Acknowledgement: Acknowledgments of people, grants, funds, etc. should be placed in a separate section before the reference list. The names of funding organizations should be written in full (optional). Do not include author biographies.

References:

Abdan, M., & Seno, S. A. H. (2022). Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET). Wireless Communications and Mobile Computing, 2022, 1-12. https://www.hindawi.com/journals/wcmc/2022/2375702/

Abhale, A. B. (2023). Deep Learning Perspectives to Detecting Intrusions in Wireless Sensor Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 18-26. https://ijisae.org/index.php/IJISAE/article/view/2504/1085

Alladi, T., Kohli, V., Chamola, V., Yu, F. R., & Guizani, M. (2021). Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles. *IEEE Wireless Communications*, *28*(3), 144-149. https://doi.org/10.1109/MWC.001.2000428

Deng, L., Li, D., Yao, X., & Wang, H. (2019). Retracted article: mobile network intrusion detection for IoT system based on transfer learning algorithm. Cluster Computing, 22, 9889-9904. https://10.1007/s10586-018-1847-2

Fu, R., Ren, X., Li, Y., Wu, Y., Sun, H., & Al-Absi, M. A. (2023). Machine Learning-Based UAV Assisted Agricultural Information Security Architecture and Intrusion Detection. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2023.3236322

Illy, P., Kaddoum, G., Moreira, C. M., Kaur, K., & Garg, S. (2019, April). Securing fog-to-things environment using intrusion detection system based on ensemble learning. In *2019 IEEE wireless communications and networking conference (WCNC)* (pp. 1-7). IEEE. https://doi.org/10.1109/WCNC.2019.8885534

Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. *Journal of Systems Architecture*, *105*, 101701. https://www.sciencedirect.com/science/article/pii/S1383762119305089

Kumar, V., Das, A. K., & Sinha, D. (2021). UIDS: a unified intrusion detection system for IoT environment. Evolutionary intelligence, 14, 47-59. https://10.1007/s12065-019-00291-w

Lokman, S. F., Othman, A. T., & Abu-Bakar, M. H. (2019). Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. *EURASIP Journal on Wireless Communications and Networking*, *2019*, 1-17. https://10.1186/s13638-019-1484-3

Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2019). Black hole attack detection using fuzzy based intrusion detection systems in MANET. *Procedia Computer Science*, *151*, 1176-1181. https://doi.org/10.1016/j.procs.2019.04.168

Parsamehr, R., Esfahani, A., Mantas, G., Radwan, A., Mumtaz, S., Rodriguez, J., & Martínez-Ortega, J. F. (2019). A novel intrusion detection and prevention scheme for network coding-enabled mobile small cells. *IEEE Transactions on Computational Social Systems*, *6*(6), 1467-1477. https://ieeexplore.ieee.org/abstract/document/8915743/

Radoglou-Grammatikis, P. I., & Sarigiannidis, P. G. (2019). Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access*, *7*, 46595-46620. https://doi.org/10.1109/ACCESS.2019.2909807

Santhosh Kumar, S. V. N., Selvi, M., & Kannan, A. (2023). A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things. *Computational Intelligence and Neuroscience*, *2023*. https://www.hindawi.com/journals/cin/2023/8981988/

Satam, P., & Hariri, S. (2020). WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol. IEEE Transactions on Network and Service Management, 18(1), 1077-1091. https://doi.org/10.1109/TNSM.2020.3036138

Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. (2023). Survey of Machine Learning based intrusion detection methods for Internet of Medical Things. *Applied Soft Computing*, 110227. https://arxiv.org/pdf/2202.09657.pdf

Sicato, J. C. S., Singh, S. K., Rathore, S., & Park, J. H. (2020). A comprehensive analyses of intrusion detection system for IoT environment. *Journal of Information Processing Systems*, *16*(4), 975-990. http://doi=10.3745/JIPS.03.0144

Sharma, R., & Athavale, V. A. (2019). Survey of intrusion detection techniques and architectures in wireless sensor networks. International Journal of Advanced Networking and Applications, 10(4), 3925-3937. http://dx.doi.org/10.35444/IJANA.2019.10044

Tabassum, A., Erbad, A., & Guizani, M. (2019, June). A survey on recent approaches in intrusion detection system in IoTs. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 1190-1197). IEEE. https://doi.org/10.1109/IWCMC.2019.8766455

Umba, S. M. W., Abu-Mahfouz, A. M., Ramotsoela, T. D., & Hancke, G. P. (2019, June). A review of artificial intelligence based intrusion detection for software-defined wireless sensor networks. In 2019 IEEE 28th International symposium on industrial electronics (ISIE) (pp. 1277-1282). IEEE. https://doi.org/10.1109/ISIE.2019.8781458

Waskle, S., Parashar, L., & Singh, U. (2020, July). Intrusion detection system using PCA with random forest approach. In *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 803-808). IEEE. https://ieeexplore.ieee.org/abstract/document/9155656/

Akash Kumar Bhagat
Arka Jain University, Jamshedpur,
Jharkhand, India
akash.b@arkajainuniversity.ac.in
ORCID 0000-0001-8717-764X

Prashant Kumar
Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
tmu.iqac@gmail.com
ORCID 0000-0002-5831-776X

Pawan Bhambu
Vivekananda Global University,
Jaipur, India
pawan.bhambu@vgu.ac.in
ORCID 0000-0001-7163-0163

Pandey V. K.
Noida Institute Of Engineering and
Technology, Greater Noida, Uttar
Pradesh, India
drvkpandey@niet.co.in
ORCID 0000-0003-3475-8672

Om Prakash
Galgotias University, Greater Noida,
Uttar Pradesh, India
Om.Prakash@galgotiasuniversity.edu.in
ORCID 0000-0001-7599-9873

Raghu N.
Jain Deemed to be University,
Bangalore, India
n.raghu@jainuniversity.ac.in
ORCID0000-0002-2091-8922