Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 01, January- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

ACCURACY AND PERFORMANCE ENHANCEMENT OF IDS SYSTEM USING MACHINE LEARNING MECHANISM IN IOT

Tina Yadav
Research Scholar
Baba Mastnath University,Asthal Bohar, Rohtak
Email- tinayadav772@gmail.com

Dr. Devender Kumar
Assistant Professor
Baba Mastnath University,Asthal Bohar, Rohtak
Email- devenderkumar@bmu.ac.in

Abstract: This research explores the imperative need for heightened security measures in the IoT landscape and delves into the enhancement of accuracy and performance within (IDS) through the integration of ML mechanisms. With the increasing ubiquity of interconnected devices, safeguardingIoT ecosystems from cyber threats has become paramount. Leveraging machine learning algorithms, our study focuses on the dynamic analysis of network traffic patterns, discerning between normal and malicious activities in real-time. The methodology encompasses feature engineering to extract pertinent information from diverse IoT data sources and the strategic selection of machine learning models for adaptive learning. Addressing challenges such as data imbalance and resource constraints, the research also assesses the impact of the enhanced IDS system on network performance. By optimizing computational efficiency and exploring parallel processing, the aim is to minimize latency and resource utilization while maintaining a high level of accuracy. The findings this study hold important implications for bolstering the security posture of IoT environments, providing a scalable and adaptive solution to counter emerging cyber threats.

Keywords:IDS, Machine Learning, Accuracy, Performance, IoT

1. INTRODUCTION

Machine learning plays a pivotal role in IDS within IoT environments, significantly enhancing the system's efficacy in safeguarding interconnected devices. The dynamic and diverse nature of IoT ecosystems poses unique challenges for traditional rule-based approaches to intrusion detection. MLA, however, excel in adapting to this complexity. By leveraging techniques such as anomaly detection and behavioral analysis, ML models can learn the normal patterns of communication and behavior for various IoT devices. This adaptability allows the IDS to evolve over time, staying resilient against emerging cyber threats. Additionally, ML aids in pattern recognition, identifying subtle and complex attack patterns that might go unnoticed by rule-based systems. Moreover, machine learning helps mitigate false positives, refining the decision-making process and reducing unnecessary alarms. The scalability of ML models is particularly advantageous in large-scale IoT environments, enabling the analysis of vast datasets generated by numerous interconnected devices. Integrating threat intelligence feeds further fortifies the IDS against known threats, while resource optimization ensures that the system operates efficiently, even in resource-constrained IoT devices. In essence, ML empowers IDS in IoT systems to provide adaptive, accurate, and proactive security measures essential for the evolving landscape of interconnected devices.

Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 01, January- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

1.1 Background

In the course of this research, the subject of intrusion detection will be investigated in great detail. Despite the fact that IDS investigations have been carried out over the course of many decades, researchers continue to remain concerned about the reliability of their results. To enhance the detection capabilities of IDS-based IoT applications, several machine learning methods will be used. In order to set the stage for future developments in the field, this research would look at the present level of intrusion detection systems. LSTM models that are built on RNNs are something that researchers can consider employing for the purpose of doing security assessments. For the purpose of improving both accuracy and efficiency, a filtering system would be used. In addition, the performance of the recommended IDS model will be evaluated in comparison to that of the conventional model for IoT applications. There may be a clear connection between the growing popularity of accessing internet resources and the increases in the number of cyber attacks that have occurred. Any sensitive information that is sent across a network is vulnerable to attack from both within and outside the system. The aggressor may carry out this assault either manually or automatically, depending on their preference. Both the efficiency and the severity of these attacks are only going to increase in the future. Attempts to put a halt to this specific group of hackers are getting more difficult. Criminals operating online, often known as cybercriminals or cyber attackers, are the persons who are responsible for these kinds of data breaches. There are instances when individuals or organizations who have extensive domain knowledge in the subject may sometimes recommend intrusion detection systems (IDS) that are innovative, adaptable, and dependable in IoT.

1.2Intrusion Detection System

The term "intrusion detection system" (IDS) may refer to either a physical device or a piece of software that scans a network for signs of intrusion or policy violations. Security information and event management (SIEM) systems normally either notify administrators of any intrusion activity or violations or collect them centrally. In order to differentiate between legitimate and harmful activities, a SIEM system integrates data from many sources and use alert filtering mechanisms.Firewalls may be configured to protect anything from a single machine to an entire network. These days, NIDSs and HIDSs are the two main categories used to describe these kinds of systems. An HIDS would be a system that keeps tabs on critical OS files, whereas an NIDS would be one that examines all incoming network traffic. It is also feasible to categorize IDS based on detecting method. Two of the most popular variations are signature-based detection (which uses machine learning to identify malicious patterns) and anomaly-based detection (which uses historical data to identify traffic that deviates from a predetermined model of "good" traffic). Recognizing the possible danger based on the reputation ratings is another typical variation. Intruder detection systems (IDS) may react to certain types of incursions. Intrusion prevention systems are often known as systems with reaction capabilities. As an example, a honeypot may be used to attract and profile malicious traffic, and intrusion detection systems can be enhanced with specialized tools to fulfill particular needs.

Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 01, January- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

1.3 Taxonomy of IDS

Depending on your preferences, it might be a piece of hardware or an application that runs on a computer. The monitoring of any potentially malicious conduct that may have taken place on a system or network is carried out by it. There is a significant contribution that it contributes to the assurance of the security of the data. When it comes to identifying all types of network threats with pinpoint precision, it is one of the most cutting-edge solutions available. Inorder to ascertain the state of the network, a system that is based on the network examines many activities, including the quantity of traffic, the IP address, the service ports, and the protocol. IDS are responsible for monitoring network traffic in order to identify any unexpected activity. In addition, it notifies users of any behavior that has been detected as soon as it is discovered. A software application that is capable of running on a network is what this is called. A comprehensive scan of the system is carried out in order to keep an eye out for any potentially harmful behavior or breaches of the protocol. The term "intrusion detection system" refers to a collection of several components. One of the components is the array of sensors that produce security events. Consequently, the intrusion detection system is going into overdrive as a result of this. Additionally, there is a console. Intrusion detection systems are designed to check for indications of known attacks or deviations while they are performing ordinary activities. The protocol and application layers are the ones that investigate deviations and abnormalities once they have been sent up the stack.

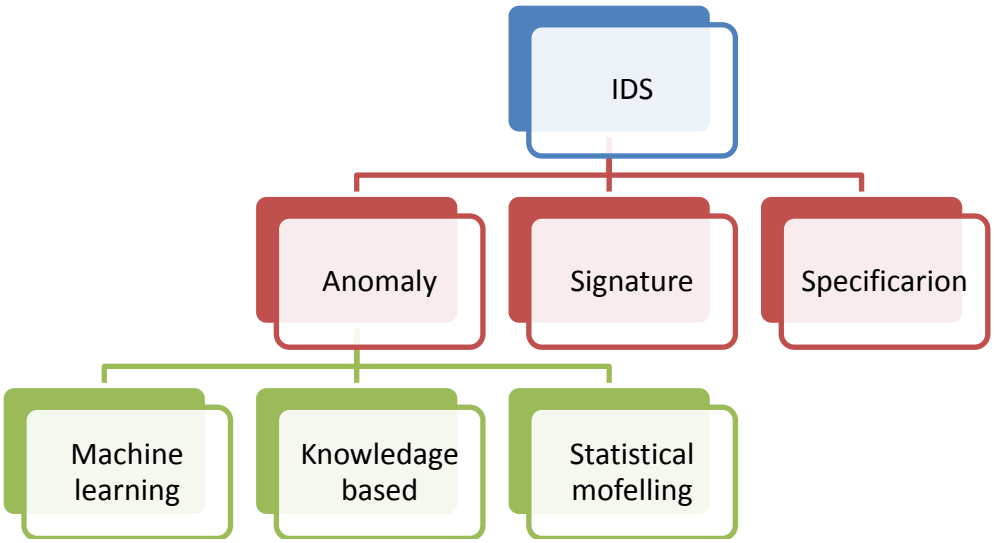

Fig 1 IDS Classification

System for the Prevention of Intrusion: For a very long time, intrusion detection systems have been investigated as a potential safety precaution. It mostly operates at the network layer inside the Internet of Things system. IDS must be able to work with a very low processing capacity in order to be designed for intelligent systems that are reliant on the Internet of Things. It is necessary to have a quick response time for this. This is intended to handle a significant volume of data in a short period of time.

Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 01, January- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

1.4 MACHINE LEARNING

ML may be referred to as algorithms, and it is because of these algorithms that software programs are able to forecast output in a highly precise manner. Furthermore, for this goal, there is no need for programming. When it comes to the algorithms that are employed in machine learning, historical records are used as input in order to make predictions about contemporary output values. It is possible to apply machine learning for a variety of purposes, including the identification of fraud, the filtering of trash, the detection of cyber threats, BPA, and predictive maintenance.When it comes to the classification of classical machine learning, the method by which an algorithm increases its accuracy in producing predictions is described. There are two strategies that are used the most frequently: unsupervised learning and supervised learning. The goal of the scientific community is to make predictions regarding the selection of algorithms based on evidence.When supervised machine learning is used, the only way for an algorithm to be taught is by using labeled inputs and the results that are expected.When employing unsupervised machine learning (ML) approaches, it is not necessary to classify the data in any way. It is their responsibility to search for patterns in the data that has not been labeled in order to break it down into more digestible pieces for future analysis. Currently, it is being used in a broad variety of different industries. One of its many applications is in the recommendation engine that Facebook utilizes for its News Feed. If a member of a certain group often takes the time to read the posts that are associated with that group, the recommendation engine could start giving those posts more priority. The engine is now working behind the scenes to improve the members' behaviors about their use of the internet. A modification will be made to the News Feed in the event that member's reading habits change and he or she is unable to keep up with the posts from that specific group throughout the course of the subsequent weeks.

1.5 DEEP LEARNING

What is referred to as "deep learning" in field of ML is the process of teaching computers to learn via repeated practice. Deep learning is used by autonomous cars to differentiate between a variety of objects, including people and stop signs, among other things. Deep neural networks, also known as DNN, are used for analysis and classification, while convolution neural networks (CNN) are utilized for analysis, recognition, and vision. RNN and LSTM are used for the purposes of classification and prediction. For the purpose of IDS detection and classification, an RNN and an LSTM would be used in the current study.

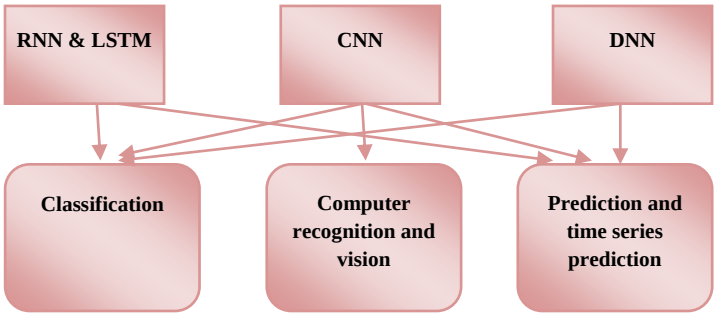

Fig 2different deep learning models

1.6Long Short-Term Memory (LSTM) Model

Use of "LSTMs," a specific kind of RNN, has the potential to be of great assistance in a variety of other activities. Recurrent neural networks are nearly entirely responsible for these findings making their way into the world. LSTMs steer clear of the problem of long-term reliance in a direct manner. The fact that they are able to recall information for extended periods of time without exerting any effort is something that they consider to be absolutely natural. A fundamental structure, which may be thought of as a repeating sequence of neural network modules, is present in every recurrent neural network. There is a difference between the repeating module structure of an LSTM chain and that of an LSTM. There are four levels in neural networks, each of which interacts in a distinct way. Neural networks are not just one level.

2. LITERATURE REVIEW

A rigorous, comprehensive, and in-depth study on IDS, ML, and LSTM was carried out in order to carry out the research project with the title "Role of Machine Learning in Building Intrusion Detection System." For your convenience, a concise summary of those earlier research publications is presented here:

2009 was the year when M. Tavallaei and its colleagues [1] finished their analysis of the KDD CUP 99 data set.

In 2011, J. Martens and I. Sutskever [2] focused their attention on the process of learning recurrent neural networks. A novel approach to the detection of intrusions was presented by M. Sheikhan and colleagues [3] in the year 2012. For this particular purpose, they used a more compact RNN. It used an approach that was based on feature grouping. A comprehensive analysis of the NSL-KDD dataset was suggested by S. Revathiet et al. [4] over the year 2013.

We made use of a number of different machine learning algorithms. This action was taken in order to detect any attempted intrusions. The most current intrusion detection systems that were still in the process of being developed in 2014 were investigated by researchers W. Li et al. [5]. KNN algorithmic routines served as the foundation for the development of their system. One of the mechanisms for a wireless sensor network was developed.

In the year 2016, A. L. Buczak and colleagues [6] conducted a survey on the subject of information extraction and automated learning algorithms. Their primary focus was on finding techniques to circumvent the detection of intrusions in the first place. The detection of an intrusion was achieved by the use of methods that coupled the extraction of information with machine learning.

In the year 2016, A. Javaid and colleagues [7] made reference to deep learning. In addition to this, they directed their efforts on the creation of an intrusion detection system that was very efficient.

A study that was conducted in 2016 by Bo Dong and colleagues [8] looked on classification algorithms for network traffic. After arriving at the conclusion that a number of different techniques would be adopted as a component of a free information package, they proceeded to put those strategies into action. They used this collection of genuine instances to devise the most effective strategy for detecting intrusions, which they presented to the audience. Deep learning was the best choice for the time being because of its capacity to make predictions when it came to the situation. As a result of this, deep learning strategies were already being used in several sectors, such as organizational structure and structural identification. When security events were monitored, data was collected for the purpose of intrusion detection analysis. This analysis was then used to ascertain the present condition of the network. Existing methods of intrusion detection that made advantage of automatic learning shown improved accuracy and efficiency.

Additionally, in 2016, T.A. Tang [9] and colleagues proposed the concept of deep learning. The identification of network intrusions was the purpose of each respective approach. The research was centered on software-defined networking as its primary emphasis.

During the year 2017, Chuanlong Yin and colleagues [10] provided a model and method for the use of an identification system that is based on neural networks. In addition to this, they evaluated the effectiveness of the design in relation to dual and multiple class structures. There are other elements that influence accuracy, such as the density of neurons and the influence that varying learning rates have on the number of neurons. One of the datasets that was employed was NSL-KDD. With the help of the RNN-IDS classification model, it was found out that it is feasible to appropriately describe the data. The classification model was substantially more effective and accurate than other automated learning techniques. This was the case when compared to other approaches. The accuracy of the intrusion detection system was improved by using their design. Detecting intrusions was made possible by the use of the most cutting-edge research tool.

The analysis of the pre-processing of the data was conducted out by N. Paulauskas and colleagues in the year 2017 [11]. The influence of pre-processing data on IDS approaches was taken into consideration by them.

Within the scope of their research, the NSL-KDD dataset was employed. IDS was suggested by P. S. Bhattacharjee and colleagues [12] in the year 2017. For the objective of doing this in 2017, they made use of the NSL-KDD data collection.

During the year 2017, R. A. R. Ashfaq [13] conducted research on a semi-supervised learning strategy that was based on fuzziness. They conducted research into a system that protects against intrusions.

In 2018, the detecting system was put into place by Sara A. Althubiti and her colleagues [14]. They were the ones responsible for its implementation. Their group made use of the Coburg IDS data package in order to accomplish this task. Moreover, this researcher used the LSTM and DSL techniques. Approximately 85 microns of precision was achieved as a result of their study.

It was determined that this degree of accuracy was satisfactory. Their LSTM outputs were evaluated in comparison to the most sophisticated methods in order to fulfill the requirements of our evaluation criteria. This was accomplished via the use of a number of different strategies, including authenticity and adaptability. In 2018, Meira, Jorge [15] conducted a comparative study of the results obtained using unsupervised techniques. Their study was essential in identifying new cyber attacks, which was a big contribution. In 2018, Kolli [16] concentrated on Cyber Situational Awareness (CSA) for Persistent Threat Control. They contemplated using a Distributed Intrusion Detection System. In 2018, Clotet [17] examined real-time anomaly-based intrusion detection systems. This method was taken into consideration for the detection of cyberattacks. At the level of critical infrastructures, their system was able to function at the industrial process level. According to Peisong Li et al. [18], an upgraded DBN and GA were used in the development of an IDS in 2019. The development of DBN network topologies via iterative processes resulted in the creation of various network architectures that could accommodate a variety of attacks, including low-frequency attacks and other types of attacks. A distributed backbone network (DBN) that optimizes network structure should be developed in order to guarantee intrusion detection. It is possible to construct an infinite number of hidden layers by using a genetic algorithm. There is no limit to this number. The development of neurons in the "hidden layer" occurs in a way that is analogous to this. The speed of detection was achieved by reducing the complexity of the system to the greatest extent that was practically possible. Improving the performance of an IDS might be accomplished via the use of this method. In the year 2019, Arul [19] will be using ANN in their study that is based on IDS. An investigation of intrusion detection systems was carried out by Khraisat [20] in 2019. An examination of IDS-related approaches, datasets, and difficulties was carried out by the author. Regarding the implementation of Intelligent Intrusion Detection Systems in 2019, R. Vinayakumar [21] presented the Deep Learning Approach. Some of the alternate methods of automated learning that were used by Qusay H. Mahmoud et al. [22] in the year 2020 include SVM, DT, and RF. Most current information package, IoTID20, may be used to enable new IDS in IoT networks. During their investigation, they took into consideration hessian-free optimization. An effective intrusion detection system was suggested by Y. Zhou [23] in the year 2020 at the time. Feature selection and ensemble classifier worked together to form the foundation of this system. It was in the year 2020 when Y. J. Chew [24] pondered decision Tree. They took into consideration the vulnerable Pruning in the Network-dependent IDS. The Novel Intrusion Detection Model was suggested by Song, Yajie, and Bu [25] in the year 2020.

3.PROBLEM STATEMENT

Taking into consideration the results of earlier research in IDS, it has become abundantly evident that more efforts for the purpose of improving accuracy are required. Additionally, it has been shown that the amount of time required for each stage of the training process is also influenced by a variety of other factors. The answers that are delivered by conventional research are insufficient when it comes to the identification of intrusions that are successful. On the subject of IDS, a variety of studies have been conducted, and a handful of those studies have made significant contributions to the field. Over the course of its development, the machine learning model has already made use of soft computing methods. Throughout the course of prior research,

a variety of methods have been used for the intended objective of teaching. One of the most major shortcomings of the research is its lack of accuracy. The training of a network model also takes a much longer amount of time than it did in the prior era. As a result of these findings, a new model was built that can be taught in a much shorter length of time compared to the models that came before it. The most recent study led to the construction of a machine learning model that featured a hidden layer, which eventually resulted in enhanced accuracy. This was accomplished via development of the model. It is predicted that the proposed study would result in more quick data training and more accurate prediction when compared to the research that has been done in the past. Although a great number of research have been carried out on intrusion detection systems (IDS), it has been observed that there is still a substantial challenge to overcome in terms of enhancing the reliability of IDS detection. Deep learning is a method that may produce the same or better results in less time than the present state of the art in intrusion detection system (IDS) detection and classification, which is inefficient and might potentially profit from the adoption of such a technology.

4. Proposed work

In this part, the problems that have been found in previous study have been compared to our suggested work. This is followed by the presentation of the research goals. There has been an explanation of the LSTM mechanism that was utilized in the study, and the two models that were generated for the suggested implementation have also been described. Here is an explanation of the data set that was used for training the categories and the subcategories that were utilized in the study.The work that has been proposed has used the LSTM mechanism. The concept of artificial RNN design has been addressed in relation to long-term and short-term memory. This technique is used rather often in the area of deep learning. It is generally agreed that LSTM networks are well suited to carry out classification and processing tasks. In addition to this, it is making predictions based on the various time series data. In a time series, there is a possibility that there may be delays of unknown time intervals between major occurrences.

A recurrent neural network and an LSTM are both examples of control flows that are comparable. The processing of information and the transmission of that information for further dissemination is shown below. The operations that take place inside the cells of the LSTM are what enable it to remember or forget data. When switching from RNN to LSTM, there will be an increase in the number of controlling knobs installed. By doing so, flow and mixing of inputs are controlled according to the weights that have been taught. Thus, LSTM is providing the highest level of control-ability in addition to superior outcomes. Nevertheless, it is more difficult and expensive. Time series forecasting is one of the applications of LSTM, which is also useful for time series. A model of this kind is designed for the purpose of solving Sequence Prediction issues and predicting time series. There are around 80 network characteristics and three label features included in the IoTID20 dataset. Binary, category, and sub-category are the characteristics that are included in the label.

The research project titled "A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks" is the source of the data set. : the dataset is supplied to the Matlab

script for training purposes so that the network may be trained effectively. A training session was conducted on 70% of the data set, while testing was carried out on 30% of the data set. In order to facilitate further testing, the trained network "net" is saved in the system. Two distinct models have been used in the implementation of the LSTM, resulting in the creation of two distinct trained networks. The first model just makes use of a single LSTM layer, but the second model makes use of two LSTM layers in addition to a drop out layer.

4.1 PROCESS FLOW

Algorithm for model 1

1. Acquire dataset of the IDS.
2. To train dataset, choose characteristics that you must use.
3. Determine the proportion of training to testing, and set it at 70% to 30%.
4. Implement the LSTM layer
5. Apply the layer that is totally linked
6. Sixth, apply the soft max layer.
7. Carry out the categorization work
8. Carry out decision-making in order to determine if the label is the typical attack or a specific sort of assault.

4.2 WORKING OF PROPOSED MODEL

IDS Dataset has been taken into consideration for training purposes in the proposed model, and attributes have been removed from consideration for the ship method. Certain qualities that have a single value in every circumstance are removed from consideration. Subsequent to the filtering of the data set, the feature selection procedure is implemented. Next, the data is divided into two categories: 70% for training and 30% for testing. First, the LSTM layer, followed by the fully connected layer, and finally the softmax layer are applied in that order. The determination of the IDs is accomplished by classification. True positive, false positive, true negative, and false negative are the results that are obtained after the predicted value has been obtained. The confusion matrix is then constructed by taking into consideration both the predicted value and the actual value. When attempting to determine overall accuracy, it is necessary to gather the accuracy, precision, recall, and f1-score.

Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 01, January- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

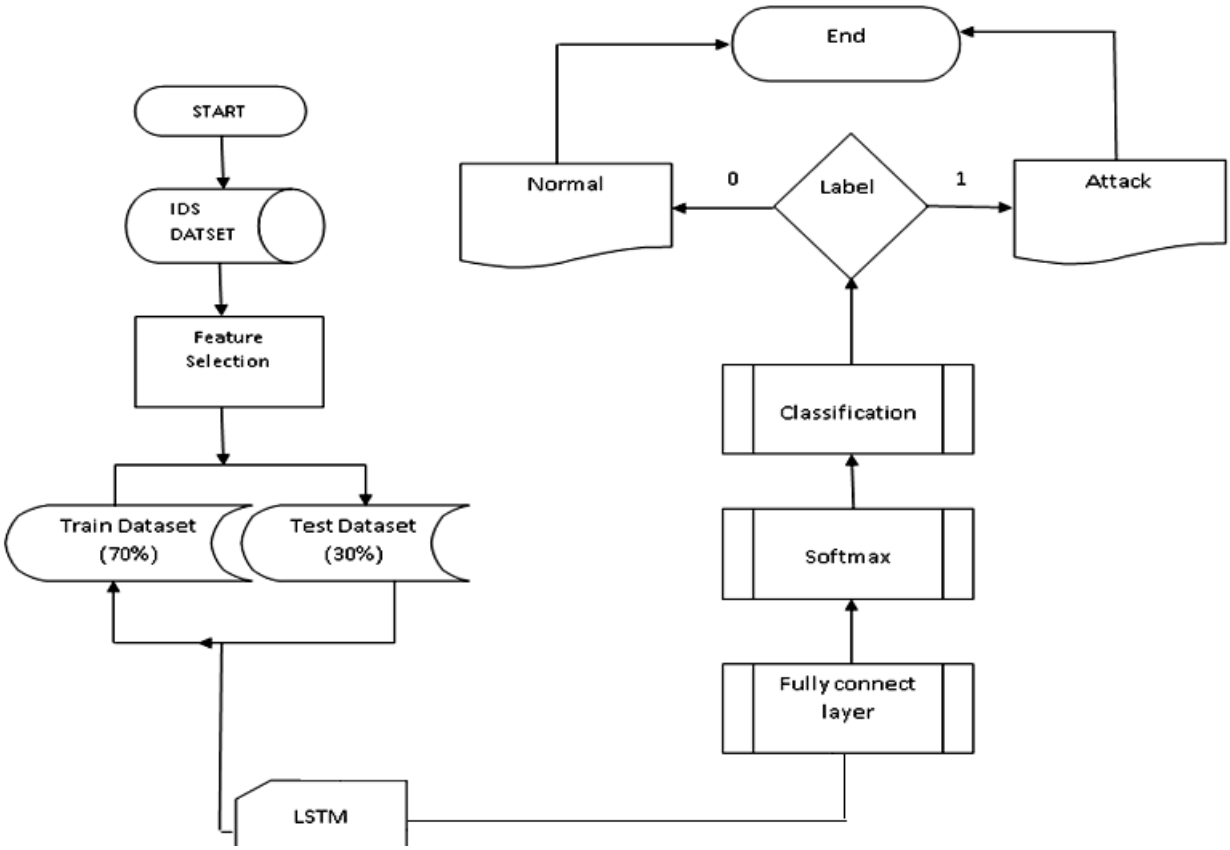

Fig 4 Flow chart of proposed Model

[5] RESULT AND DISCUSSION

The present research is considering 4 categories while taking the IDS dataset. Table 2 is presenting 4 categories of attack. Table 2 is presenting confusion matrix in case of traditional work.

Table 2. Confusion matrix for traditional work

	1	**2**	**3**	**4**
1	908	29	21	42
2	27	884	39	50
3	49	25	857	69
4	19	67	57	857

Results

TP: 3506 and Overall Accuracy: 87.65%

Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 01, January- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Table 3. Accuracy chart for traditionalwork for IDS

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	1003	1000	95.33%	0.91	0.91	0.91
2	1005	1000	94.08%	0.88	0.88	0.88
3	974	1000	93.5%	0.86	0.88	0.87
4	1018	1000	92.4%	0.86	0.84	0.85

Confusion matrix for proposed approachpresents in Table 3.

Table 4. Confusion matrix for proposed work

	1	2	3	4
1	952	16	11	21
2	16	928	21	35
3	26	19	920	35
4	11	36	30	923

Results

TP: 3723 and Overall Accuracy: 93.08%

Table 5. Accuracy parameters of Proposed work

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	1005	1000	97.48%	0.95	0.95	0.95
2	999	1000	96.43%	0.93	0.93	0.93
3	982	1000	96.45%	0.92	0.94	0.93
4	1014	1000	95.8%	0.92	0.91	0.92

Comparison of Accuracy parameters

Table 6presents comparison of accuracy in case of conventional and proposed approach.

Table 6. Comparison of accuracy

Conventional	Proposed
95.33%	97.48%
94.08%	96.43%
93.5%	96.45%
92.4%	95.8%

By considering table 6, figure compares traditional and proposed work.

Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 01, January- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

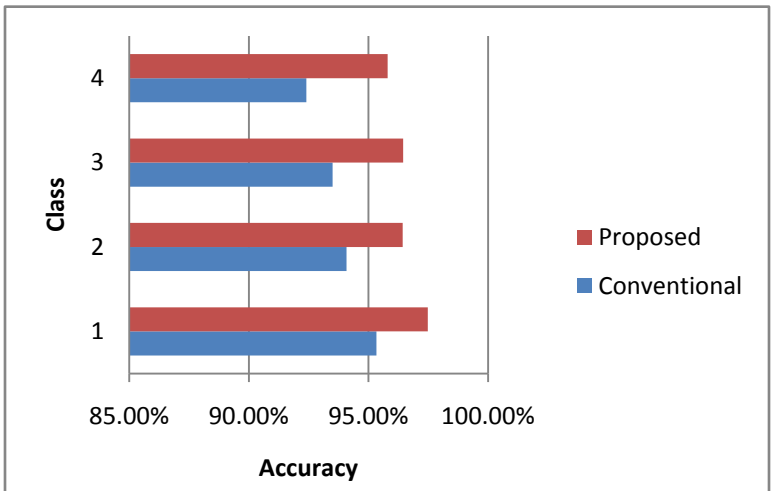

Fig 5. Comparison of accuracy

Table 7presents the comparison of precision.

Table 7. Comparison of Precision

Conventional	Proposed
0.91	0.95
0.88	0.93
0.86	0.92
0.86	0.92

By considering table 7 following figure has been graphed

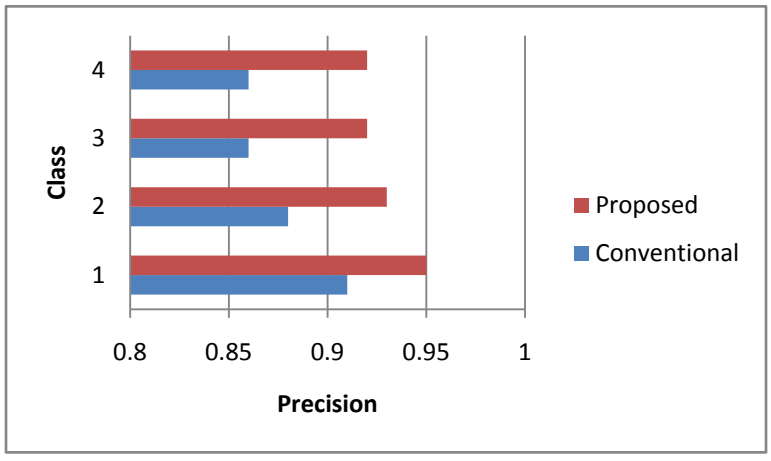

Fig 6. Comparison of Precision

Table 8 presents the comparison of Recall values.

Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 01, January- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Table 8. Comparison of recall

Conventional	Proposed
0.91	0.95
0.88	0.93
0.88	0.94
0.84	0.91

Considering the above table following chart has been plotted

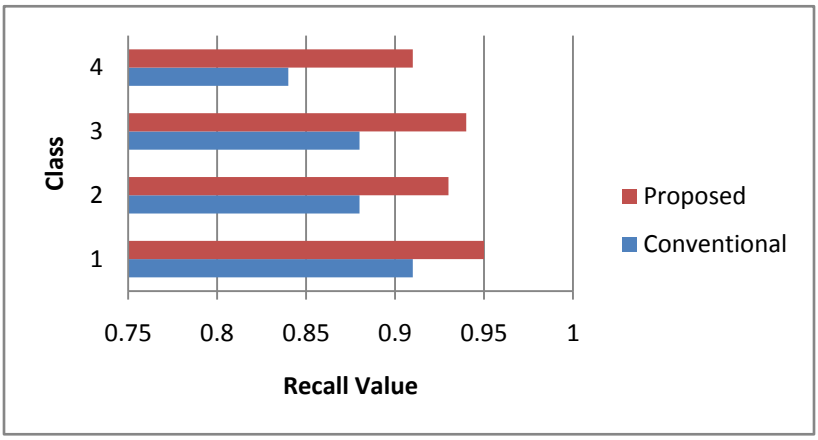

Fig 7. Comparison of Recall

Table 9 presents comparison of the F-score.

Table 9. Comparison of F1 score

Conventional	Proposed
0.91	0.95
0.88	0.93
0.87	0.93
0.85	0.92

Considering table 9 following figure has been shownx

Journal of Interdisciplinary and Multidisciplinary Research (JIMR)
E-ISSN:1936-6264| Impact Factor: 8.886|
Vol. 18 Issue 01, January- 2023
Available online at: https://www.jimrjournal.com/
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

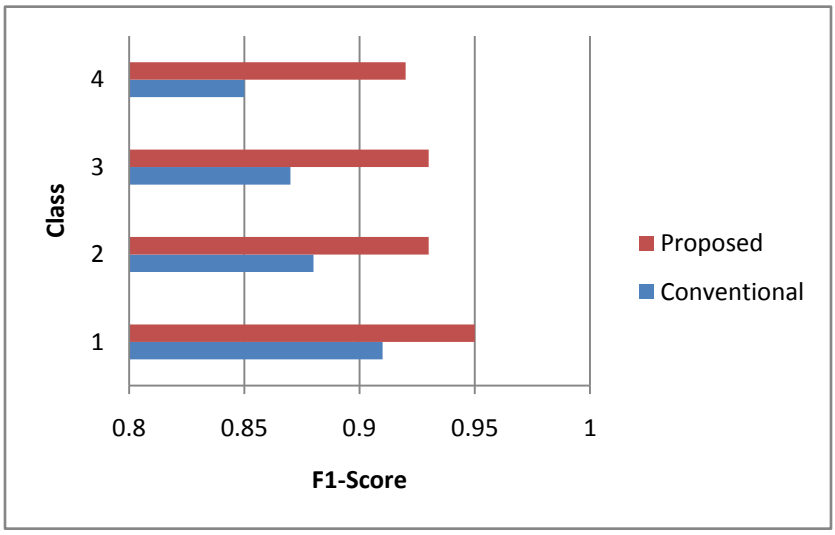

Fig 8. Comparison of f1-score

6. CONCLUSION

In conclusion, the endeavor to enhance the accuracy and performance of IDS in the context of IoT through the integration of machine learning mechanisms represents a pivotal advancement in cybersecurity. As the IoT ecosystem burgeons, traditional rule-based approaches struggle to keep pace with the dynamic and diverse nature of connected devices. The application of machine learning offers a transformative solution, enabling adaptive learning, anomaly detection, and behavioral analysis that surpasses the limitations of conventional systems. The findings of this research underscore the potential for continuous evolution in threat detection capabilities, addressing the intricate challenges posed by emerging cyber threats. The promising results in reducing false positives, optimizing resource utilization, and improving overall system scalability contribute significantly to the robustness of IoT security. Looking ahead, the fusion of machine learning with IDS not only fortifies the defense against known threats but also positions the system to proactively identify and mitigate novel attack vectors. This research lays the groundwork for a more resilient and responsive security paradigm in the ever-expanding landscape of interconnected devices, underscoring the importance of leveraging machine learning for the continued advancement of IoT security.

7. Scope of research

The future scope of enhancing the accuracy and performance of Intrusion Detection Systems (IDS) using machine learning mechanisms in IoT is promising and multifaceted. As the Internet of Things (IoT) continues to expand, the security challenges associated with interconnected devices are expected to grow in complexity. Therefore, the research and development in the realm of IDS with machine learning applications are likely to play a critical role in shaping the future of IoT security. The ideas and suggestions that are associated with this research will have

a big impact on the methodology that is employed to accurately anticipate IDS. The most recent study needs to give a strategy that is both adaptable and scalable for identifying intrusions into intrusion detection systems (IDS), taking into mind the training model. It is anticipated that the suggested model's overall accuracy would increase by virtue of the fact that it will be trained using a big dataset. It is imperative that more research remain based on the same paradigm if we want to achieve advancements in IDS detection. It is anticipated that the study will have important ramifications for the enhancement of the capability to anticipate IDS.

REFERENCES

1. M. Tavallaee, E. Bagheri, W. Lu, and A. A. A. Ghorbani, ‘‘A detailed analysis of the KDD CUP 99 data set,’’ inProc. IEEE Symp. Comput. Intell.Secur. Defense Appl., Jul. 2009, pp. 1–6.
2. J. Martens and I. Sutskever, ‘‘Learning recurrent neural networks with hessian-free optimization,’’ presented at the 28th Int. Conf. Int. Conf.Mach. Learn., Bellevue, WA, USA, Jul. 2011, pp. 1033–1040.
3. M. Sheikhan, Z. Jadidi, and A. Farrokhi, ‘‘Intrusion detection using reduced-size RNN based on feature grouping,’’Neural Comput. Appl.,vol. 21, no. 6, pp. 1185–1190, Sep. 2012.
4. S. Revathi and A. Malathi, ‘‘A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection, ’’Int. J. Eng.Res. Technol., vol. 2, pp. 1848–1853, Dec. 2013.
5. W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, ``A new intrusion detection system based on KNN classi_cation algorithm in wireless sensor network,"J. Elect. Computer. Eng., vol. 2014, Jun. 2014, Art. no. 240217.
6. L. Buczak and E. Guven, ‘‘A survey of data mining and machine learning methods for cyber security intrusion detection,’’IEEE Commun.Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.
7. Javaid, Q. Niyaz, W. Sun, and M. Alam, ‘‘A deep learning approach fornetwork intrusion detection system,’’ presented at the 9th EAI Int. Conf.Bio-inspired Inf. Commun. Technol. (BIONETICS), New York, NY, USA,May 2016, pp. 21–26.
8. B. Dong and X. Wang, “Comparison deep learning method to traditional methods using for network intrusion detection,” in Proc. IEEE ICCSN,2016, pp. 581–585
9. T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho,‘‘Deep learning approach for network intrusion detection in soft-ware defined networking,’’ inProc. Int. Conf. Wireless Netw. MobileCommun. (WINCOM), Oct. 2016, pp. 258–263.
10. Chuanlong Yin, Yuefei Zhu, A Deep Learning Approach for IntrusionDetection Using Recurrent Neural Networks, IEEE Access, Received September 5, 2017, accepted October 5, 2017, date of publication October 12, 2017, date of current version November 7, 2017.
11. N. Paulauskas and J. Auskalnis, ‘‘Analysis of data pre-processing influence on intrusion detection using NSL-KDD dataset,’’ inProc. Open Conf.Elect., Electron. Inf. Sci. (eStream), Apr. 2017, pp. 1–5.

12. P. S. Bhattacharjee, A. K. M. Fujail, and S. A. Begum, ‘‘Intrusion detection system for NSL-KDD data set using vectorised fitness function in genetic algorithm,’’Adv. Comput. Sci. Technol., vol. 10, no. 2, pp. 235–246, 2017.
13. R. A. R. Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He,‘‘Fuzziness based semi-supervised learning approach for intrusion detec-tion system,’’Inf. Sci., vol. 378, pp. 484–497, Feb. 2017.
14. Althubiti, Sara & Jones, Eric & Roy, Kaushik. (2018). LSTM for Anomaly-Based Network Intrusion Detection. 1-3. 10.1109/ATNAC.2018.8615300.
15. Meira, Jorge. (2018). Comparative Results with Unsupervised Techniques in Cyber Attack Novelty Detection. Proceedings. 2. 1191. 10.3390/proceedings2181191.
16. Kolli, Satish& Lilly, Joshua &Wijesekera, Dusminda. (2018). Providing Cyber Situational Awareness (CSA) for PTC Using a Distributed IDS System (DIDS). V001T03A004. 10.1115/JRC2018-6142.
17. Clotet, Xavier &Moyano, José & León, Gladys.(2018). A real-time anomaly-based IDS for cyber-attack detection at the industrial process level of Critical Infrastructures.International Journal of Critical Infrastructure Protection.23. 10.1016/j.ijcip.2018.08.002.
18. P. Li and Y. Zhang, "A Novel Intrusion Detection Method for Internet of Things," 2019 Chinese Control And Decision Conference (CCDC), Nanchang, China, 2019, pp. 4761-4765, doi: 10.1109/CCDC.2019.8832753.
19. A. Arul Anitha and L. Arockiam, “ANNIDS: Artificial neural network based intrusion detection system for internet of things,” Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 11, pp. 2583–2588, 2019, doi: 10.35940/ijitee.K1875.0981119.
20. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” Cybersecurity, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.
21. 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, no. c, pp. 41525–41550, 2019, doi: 10.1109/Access.2019.2895334.
22. Ullah, Imtiaz, and Qusay H. Mahmoud. "A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks." Canadian Conference on Artificial Intelligence. Springer, Cham, 2020.
23. Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an Efficient Intrusion Detection System Based on Feature Selection and Ensemble Classifier,” Comput. Networks, p. 107247, 2020, doi: 10.1016/j.comnet.2020.107247.
24. Y. J. Chew, S. Y. Ooi, K. S. Wong, and Y. H. Pang, “Decision Tree with Sensitive Pruning in Network-based Intrusion Detection System,” Lect. Notes Electr. Eng., vol. 603, pp. 1–10, 2020, doi: 10.1007/978-981-15-0058-9_1.
25. Song, Yajie& Bu, Bing & Zhu, Li. (2020).A Novel Intrusion Detection Model Using a Fusion of Network and Device States for Communication-Based Train Control Systems.Electronics. 9. 181. 10.3390/electronics9010181.