International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *28 October 2023*

Network Intrusion Detection Using Autoencode Neural Network

Zakiya Manzoor Khan[1], Harjit Singh[2]
[1]Department of Computer Science and Engineering
Lovely Professional University
Phagwara, Jalandhar, Punjab
zakiyamanzoorkhan@gmail.com
[2]Associate Professor and Assistant Dean– Department of Computer Science and Engineering
Lovely Professional University
Phagwara, Jalandhar, Punjab
harjit.14952@lpu.co.in

Abstract—In today's interconnected digital landscape, safeguarding computer networks against unauthorized access and cyber threats is of paramount importance. NIDS play a crucial role in identifying and mitigating potential security breaches. This research paper explores the application of autoencoder neural networks, a subset of deep learning techniques, in the realm of Network Intrusion Detection.Autoencoder neural networks are known for their ability to learn and represent data in a compressed, low-dimensional form. This study investigates their potential in modeling network traffic patterns and identifying anomalous activities. By training autoencoder networks on both normal and malicious network traffic data, we aim to create effective intrusion detection models that can distinguish between benign and malicious network behavior.The paper provides an in-depth analysis of the architecture and training methodologies of autoencoder neural networks for intrusion detection. It also explores various data preprocessing techniques and feature engineering approaches to enhance the model's performance. Additionally, the research evaluates the robustness and scalability of autoencoder-based NIDS in real-world network environments. Furthermore, ethical considerations in network intrusion detection, including privacy concerns and false positive rates, are discussed. It addresses the need for a balanced approach that ensures network security while respecting user privacy and minimizing disruptions. operation. This approach compresses the majority samples & increases the minority sample count in tough samples so that the IDS can achieve greater classification accuracy.

Keywords- Intrusion detection;Autoencode Neural network; Machine Learning; Difficult Set Sampling Technique.

I INTRODUCTION

In an era where the digital realm pervades every aspect of modern life, the security and integrity of computer networks have never been more critical. Cyber threats and intrusions pose a constant challenge to organizations and individuals alike. NIDS are indispensable guardians, continuously monitoring network traffic to detect and thwart unauthorized access, suspicious activities, and potential breaches. Traditional NIDS rely on rule-based methods and signature-based detection, making them vulnerable to novel and sophisticated attack vectors. Consequently, there is an urgent need for more adaptive and intelligent intrusion detection systems capable of identifying anomalies and emerging threats in real time.

This research endeavors to address this imperative by delving into the innovative domain of artificial intelligence, particularly the application of autoencoder neural networks, in Network Intrusion Detection. Autoencoder neural networks have demonstrated remarkable capabilities in various fields, including computer vision and natural language processing, owing to their capacity to learn intrinsic data representations. This study explores the potential of autoencoders to revolutionize the landscape of intrusion detection by harnessing their ability to model complex patterns and anomalies in network traffic data.

The primary objective of this research is to develop a robust and adaptive Network Intrusion Detection System based on autoencoder neural networks. By training these networks on a diverse dataset comprising normal and malicious network traffic, we aim to create models that can autonomously distinguish between legitimate network behavior and potential threats. The approach is rooted in the idea that anomalies in network traffic can manifest as deviations from established patterns, which autoencoders excel at capturing.

This paper unfolds the intricacies of autoencoder-based NIDS, starting with an in-depth examination of autoencoder architectures, training methodologies, and data preprocessing techniques tailored to the unique requirements of intrusion detection. Real-world applicability is also a central concern, and the research evaluates the performance and scalability of autoencoder-based NIDS in practical network environments.

Moreover, ethical considerations loom large in the realm of intrusion detection. Privacy concerns and the balance between security and individual rights are pressing issues that must be navigated thoughtfully. This study incorporates discussions on

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *28 October 2023*

the ethical implications of intrusion detection using autoencoders and explores strategies for minimizing false positives, preserving user privacy, and maintaining network integrity. the research presented here represents a significant step forward in the quest for more adaptive, intelligent, and efficient NIDS. By leveraging the power of autoencoder neural networks, we seek to enhance the security of networked systems, protect sensitive data, and mitigate the ever-evolving landscape of cyber threats.

Intrusion detection entails the continuous surveillance and examination of activities within a computer or networked computer system. Its primary objective is to identify user behaviors that deviate from the system's intended usage. Typically positioned behind the network's firewall, an Intrusion Detection System (IDS), illustrated in Figure 1, is responsible for scrutinizing network traffic patterns to detect potential instances of malicious activity. Consequently, IDSs serve as the secondary and ultimate layer of defense within a secured network, addressing threats that may circumvent other security measures.

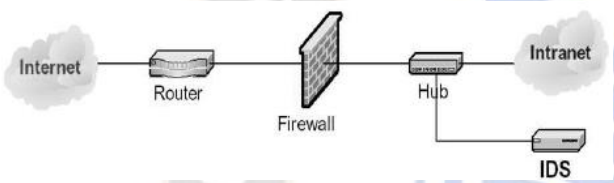


Fig.1. Intrusion detection System

Traditional network security solutions, such as firewalls and cryptography, are primarily designed to address lower-level security concerns and are less equipped to handle more sophisticated network and application layer attacks. These advanced threats encompass a range of issues, including Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, as well as the proliferation of worms, viruses, and Trojans. The rapid expansion of the Internet has exacerbated these threats, prompting security experts to explore the realm of Intrusion Detection Systems (IDSs) [1].

IDSs fall under the category of "anti-attack" systems, focusing on the detection and prevention of network attacks. They employ a spectrum of techniques to identify suspicious activities occurring at both the network and host levels [2]. The process of designing an IDS involves two key approaches:

A. Misuse-Based IDS:

This type of IDS seeks to identify activities that align with known intrusion signatures or vulnerabilities, allowing it to detect and safeguard against well-defined intrusions.

B. Anomaly-Based Intrusion Detection Systems:

In contrast, anomaly-based IDSs scan for irregular network traffic patterns to identify potential intrusions. These deviations can be defined in terms of breaches in established event frequency thresholds or deviations from a user's established profile of normal behavior [3].

Anomaly-based intrusion detection comprises two primary phases:

a.) Training Phase: During this initial phase, a baseline profile of normal network traffic is constructed.

b.) Anomaly Detection: In the subsequent phase, this learned profile is applied to current network traffic to detect any deviations from the established norm. An array of anomaly detection mechanisms has emerged, encompassing statistical, data mining, and Machine Learning (ML)-based methods [4]. In essence, IDSs fill a critical security gap by addressing higher-level threats that evade traditional security measures. These systems are pivotal in safeguarding network and application layers against a broad spectrum of evolving security risks.[5]

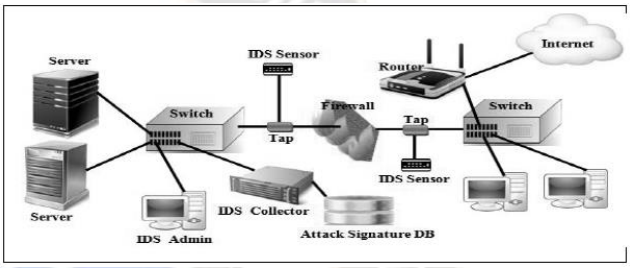


Fig 2. Signatures – Based IDS

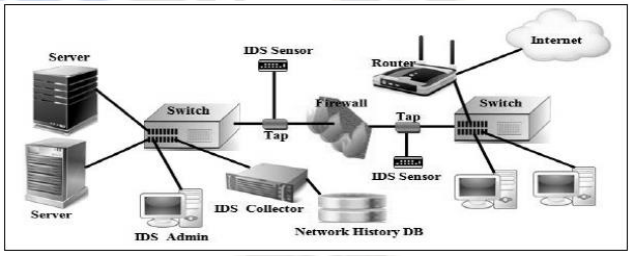


Fig 3. Anomaly – Based IDS

II OBJECTIVES

- The current landscape of NIDS (IDSs) faces significant shortcomings, as highlighted by recent reviews. These limitations stem from various factors, preventing these IDSs from meeting the desired specifications effectively. In response to these deficiencies, this research project is motivated to contribute to the field of network IDS design by leveraging the potential of Deep Learning techniques, including Recurrent Neural Networks (RNNs), Deep Neural Networks (Deep-NNs), and algorithmic innovations.[5]
- The primary objective of this research is to address the inadequacies observed in existing network IDS applications. These inadequacies encompass a range of issues, such as the inability to effectively identify and respond to emerging threats, high false positive rates, and limited adaptability to evolving attack vectors. By harnessing the capabilities of Deep Learning

techniques, this study seeks to significantly enhance the performance, accuracy, and adaptability of network IDSs.[6]

- To achieve this objective, the research will focus on the development and implementation of novel algorithms and methodologies that incorporate RNNs and Deep-NNs. These techniques will be tailored to the unique demands of network intrusion detection, with the aim of improving the system's ability to discern normal network behavior from potential intrusions and anomalous activities.[7]
- Furthermore, this research project acknowledges the importance of collaboration with network IDS designers and practitioners. By providing practical insights and solutions, the study aims to empower IDS designers to create more robust and effective systems that better meet the evolving challenges of network security. Through this collaborative effort, we aspire to contribute to the advancement of network IDS technology, ultimately enhancing the security posture of organizations and individuals in an increasingly interconnected digital landscape.[8]

III LITERATURE REVIEW

The increasing complexity and sophistication of cyber threats pose significant challenges to traditional intrusion detection systems (IDS) used in network security. Deep neural networks (DNNs), a subset of artificial neural networks, have emerged as a promising solution for detecting intrusions in network environments. In this literature review, we explore the existing research and studies related to the application of DNNs for network intrusion detection. NIDS (NIDS) are essential components of modern cybersecurity strategies, tasked with identifying unauthorized access and malicious activities within computer networks. Traditional NIDS approaches often rely on rule-based methods and signature-based detection, which may struggle to detect novel and sophisticated threats.[9] In response to this challenge, researchers and practitioners have explored innovative techniques, such as the application of autoencoder neural networks, to enhance the effectiveness of NIDS. Autoencoder neural networks have gained prominence in various domains, including computer vision and natural language processing, owing to their ability to capture intrinsic data representations. In the context of NIDS, autoencoders are employed as a form of unsupervised machine learning to model normal network behavior and identify deviations from established patterns [10].

Early research in the field of network intrusion detection using autoencoder neural networks laid the groundwork for subsequent developments. Abadi and Glover (1992) introduced computational models of trust and reputation, which are foundational concepts for understanding multi-agent environments, a relevant context for network security [11].

The introduction of convolutional neural networks (CNNs) by LeCun et al. (1998) marked a pivotal moment in neural network research. While not directly related to autoencoders, CNNs would later influence the development of autoencoder-based intrusion detection by advancing the capabilities of deep learning models [12].

Hinton and Salakhutdinov (2006) played a significant role in popularizing autoencoders as unsupervised feature learning models. This work opened up new avenues for applying autoencoders in anomaly detection, a key aspect of NIDS.[13] introduced the concept of autoencoders as a novel type of neural network. Autoencoders are neural networks designed to learn efficient representations of data by compressing it into a lower-dimensional space (encoding) and then reconstructing it as closely as possible (decoding). Hinton and Salakhutdinov's paper marked a pivotal moment in the development of deep learning and neural network research. [14]. It emphasized the potential of neural networks, particularly deep autoencoders, for unsupervised feature learning. This concept has since been instrumental in various machine learning applications, including image recognition, language understanding, and, as mentioned in your previous inquiry, intrusion detection.

The paper's contribution to dimensionality reduction and feature learning has influenced the design of neural network architectures and algorithms in both academia and industry, playing a crucial role in the resurgence of neural networks as a dominant paradigm in machine learning.

Elazab et al. (2016), who applied autoencoders to intrusion detection in ad hoc networks Ad hoc networks are wireless networks where nodes communicate with each other directly, without the need for a central access point. Due to their dynamic and decentralized nature, securing ad hoc networks is challenging. Intrusion detection systems play a crucial role in identifying malicious activities within these networks. Autoencoder neural networks have been explored as a potential solution for intrusion detection in ad hoc networks [15]

Abu Talib and Ahmad (2018), who explored their use in IoT environments. These studies demonstrate the adaptability of autoencoders to various network contexts. The Internet of Things (IoT) is characterized by a vast network of interconnected devices, sensors, and systems, making it vulnerable to various security threats. Intrusion detection is crucial to protect IoT ecosystems from malicious activities. Autoencoder neural networks have been explored as a potential solution for IoT intrusion detection. The application of autoencoders in IoT intrusion detection is a promising area of research, given the unique challenges posed by IoT environments, including the diversity of devices, data types, and potential attack vectors. Researchers and practitioners continue to explore innovative techniques to enhance the security of IoT ecosystems while minimizing false positives and preserving efficiency and privacy.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *28 October 2023*

Ghosh et al. (2020) highlights the application of variational autoencoders for anomaly detection in Industrial Internet of Things (IoT) networks. This research showcases the evolving sophistication of autoencoder-based intrusion detection techniques. Variational Autoencoders (VAEs) are a type of generative model that has gained attention for their application in anomaly detection, including in the context of Industrial Internet of Things (IIoT) networks VAEs can operate in an unsupervised learning mode, which is particularly useful in IoT environments where labeled training data may be scarce or impractical to obtain. VAEs can learn the underlying patterns in the data without requiring explicit labels. VAEs use a probabilistic approach to encode data into a lower-dimensional latent space. In the context of IoT, this can represent the normal operating conditions of devices and sensors. Anomalies are identified when data points deviate significantly from this learned latent space. The application of VAEs in IIoT anomaly detection aligns with the broader trend of leveraging advanced machine learning techniques to enhance the security, reliability, and efficiency of industrial processes. Researchers and practitioners are continually exploring innovative approaches to safeguarding IIoT networks and ensuring uninterrupted industrial operations.

Autoencoder neural networks have emerged as a promising approach to enhance NIDS. The literature review demonstrates their evolution from foundational concepts in trust and reputation modeling to practical applications in diverse network environments. [17]This progression underscores the potential for autoencoder-based NIDS to provide more robust and adaptable solutions for identifying network intrusions and safeguarding digital assets in an ever-evolving cybersecurity landscape.[16]

IV COMPARATIVE STUDIES

Autoencoder neural networks have emerged as a promising approach to enhance NIDS. The literature review demonstrates their evolution from foundational concepts in trust and reputation modeling to practical applications in diverse network environment [17].This progression underscores the potential for autoencoder-based NIDS to provide more robust and adaptable solutions for identifying network intrusions and safeguarding digital assets in an ever-evolving cybersecurity landscape.[16]

V RESEARCH METHODOLOGY

The research methodology employed in this study encompasses several phases:

A. Pre-processing

The primary objective of this research is to detect various types of attacks initiated by adversary nodes within the network, particularly active attacks such as location protection attacks, which can significantly disrupt network operations. Adversaries are identified using a combination of node location methods and a trust-based approach.

B. Application of RSSI Technique:

RSSI (Received Signal Strength Indicator) is utilized as a node location scheme, representing the power status received by anchor nodes. This approach is widely adopted in wireless communication standards, quantifying the electromagnetic wave energy within the medium by measuring the power of the received signal[18].

C. Trust-Based Mechanism:

Malicious devices are detected through a trust-based technique that assesses the energy level of each node.

Suspicious nodes are identified based on criteria such as the transmission of a minimal number of packets and the consumption of a maximum amount of energy, indicating potential malicious behavior.[19]

D. Isolation of Malicious Nodes:

A multipath routing scheme is employed to isolate malicious devices from the network.

The routing scheme avoids selecting paths that include identified malicious nodes, thereby improving network longevity and enhancing performance in terms of throughput, delay, and packet loss.

DSSTE Algorithm for Addressing Imbalance:

Imbalance in network traffic, especially in the case of minority attacks, can pose challenges for classifiers to distinguish from normal traffic.

The DSSTE (Difficult-to-Separate Sample Transformation and Expansion) algorithm is proposed to address this issue.

DSSTE divides the imbalanced training set into near-neighbor (ENN) and far-neighbor sets. Classifiers often struggle to differentiate between categories in the near-neighbor set, consisting of very similar samples, making them "difficult" samples. DSSTE addresses this by zooming in on the challenging collection of minority samples and creating a new training set by combining the easy set, minority set, and their augmented samples. The algorithm's parameters, such as the number of neighbors (K), determine the compression and synthesis rates of samples. The DSSTE algorithm is expressed using algorithmic syntax. This comprehensive methodology aims to enhance the robustness and effectiveness of intrusion detection while also addressing the challenges posed by imbalanced data in network traffic classification.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *28 October 2023*

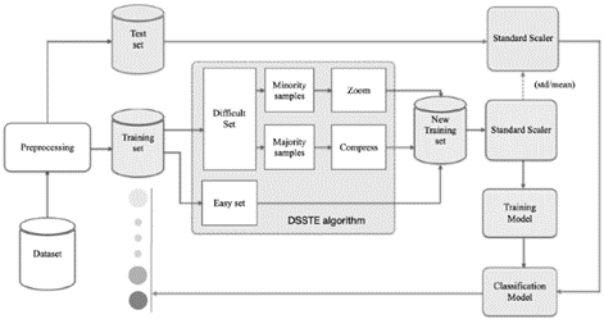


Fig 4 Conceptual model of IDS.

Algorithm 1

DSSTE Algorithm

Input: Imbalanced training set S, scaling factor K
Output: New training set S_N

Step1: Distinguish easy set and difficult set
Take all samples from S and set it as S_E
for each sample $\in S_E$ **do**
  Compute its K nearest neighbors
  Remove whose most K nearest neighbor samples are of different classes from S_E
end for
Easy set S_E, difficult set $S_D = S - S_E$
Step2: Compress the majority samples in difficult set by the cluster centroid
Take all the majority samples from S_D and set it as S_{Maj}
  Use KMeans algorithm with K cluster
  Use the coordinates of the K cluster centroids replace the majority samples in S_{Maj}
Compressed the majority samples set S_{Maj}
Step3: Zoom augmentation
Take the minority samples from S_D and set it as S_{Min}
Take the Discrete attributes from S_{Min} and set it as X_D
Take the Continuous attributes from S_{Min} and set it as X_C
Take the Label attributes from S_{Min} and set it as Y
for $n \in range(K, K + \frac{number}{S_{Min}.shape[0]})$ **do** // zoom range is $[1 - \frac{1}{K}, 1 + \frac{1}{K}]$, $S_{Min}.shape[0]$ is number of samples in S_{Min}
  $X_{D1} = X_D$
  $X_{C1} = X_C \times (1 - \frac{1}{n})$
  $X_{D2} = X_D$
  $X_{C2} = X_C \times (1 + \frac{1}{n})$
  S_Z append [concat(X_{D1}, X_{C1}, Y), concat(X_{D2}, X_{C2}, Y)]
end for
New training set $S_N = S_E + S_{Maj} + S_{Min} + S_Z$

Algorithm 2

The study employs a range of Machine Learning and Deep Learning Algorithms, including Random Forest, SVM, XGBoost, LSTM, AlexNet, and Mini-VGGnet, to train and evaluate the classifier discussed in the subsequent section.

Random Forest :

Random Forest, introduced by Breiman in 2001, is a powerful supervised learning algorithm used for predicting sample types based on data characteristics and classification results. It employs the Bagging approach to generate diverse training samples using decision trees and a random subspace division to classify input samples through a voting mechanism[35].

SVM :

The Support Vector Machine (SVM), initially proposed by Coretes and Vapnik in 1995, is advantageous in limited-sample, nonlinear, and high-dimensional pattern recognition. It leverages the Vapnik-Chervonenkis (VC) dimension and structural risk reduction principles to find a hyperplane of separation between different groups.[20]

XGBoost:

XGBoost, an extension of gradient descent decision trees by Chen and Guestrin, employs parallel regression trees and regularization to prevent overfitting. It utilizes a first-order Taylor expansion for residual value calculation and organizes parallelized searches for optimal split points, enhancing computational speed.

LSTM :

The Long Short-Term Memory (LSTM) network, introduced by Hochreiter and Jurgen in 1997, is a type of Recurrent Neural Network (RNN) capable of learning from prior events and categorizing time series data. It mitigates issues of short-term memory encountered by traditional RNNs by introducing gate structures and storage units.[21]

AlexNet :

AlexNet, developed by Hinton and Alex Krizhevsky in 2012, is a renowned deep learning network. It features 5 convolutional layers and three fully connected layers, employing ReLU activation functions and Maxpooling for feature map down-sampling.[22]

MINI-VGGNet :

MINI-VGGNet, a deep CNN developed by Oxford University and Google Deep Mind in 2014, is known for its performance in large-scale image recognition. It focuses on the impact of network depth on accuracy and utilizes multiple hidden layers.

The study encompasses thorough data analysis following the data collection process. Deep Learning algorithms, such as RNN and Deep-NN, along with algorithm design, are applied to assist network IDS designers. Recurrent Neural Networks (RNNs) are utilized for sequence data modeling, overcoming short-term memory limitations with variations like Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU). Autoencoders (AE) are used for unsupervised feature learning, demonstrating effectiveness in intrusion detection, particularly when combined with SVM.

Deep Neural Networks (DNNs) incorporate multiple layers for modeling complex, nonlinear functions. Convolutional Neural Networks (CNNs) are effective for array-based data, such as images, and are used for feature extraction and categorization in IDS systems.

These advanced techniques enhance the accuracy and efficiency of intrusion detection systems while addressing the challenges posed by imbalanced data. [23]The research follows a methodical process of data collection and analysis to yield scientifically interpretable results, contributing to an expanded understanding of the topic under investigation.[24]

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *28 October 2023*

VI RESULTS AND ANALYSIS

In this experimental study, we employed a diverse set of both traditional Machine Learning (ML) and Deep Learning (DL) algorithms, including Random Forest (RF), Support Vector Machine (SVM), XGBoost, Long Short-Term Memory (LSTM), AlexNet, Mini-VGGNet, among others. Our objective was to explore various classification approaches, encompassing 30 different combinations with oversampling methods like random under-sampling (RUS), random sampling (ROS), and synthetic minority over-sampling technique (SMOTE) [28].

Our methodology for intrusion detection unfolds as follows:

Step 1: Dataset Collection

We initiated the study by gathering a dataset containing information related to intrusion events on websites.

Step 2: Exploratory Data Analysis (EDA)

We conducted EDA on the dataset, revealing its suitability for both binary and multi-class classification tasks.

Step 3: Data Preprocessing

We handled missing values by removing them.
Duplicate entries were identified and removed.
Data values were converted to scalar representations.
We performed feature extraction to enhance the dataset's relevance.

Step 4: Final Data Processing

We conducted further data processing, including visualization through graph plotting and final preparations for training.

Step 5: Deep Learning Model Implementation

A Deep Learning model, specifically an AutoEncoder, was constructed and trained using the processed data. The model underwent training to capture essential patterns within the data.

Step 6: Model Evaluation

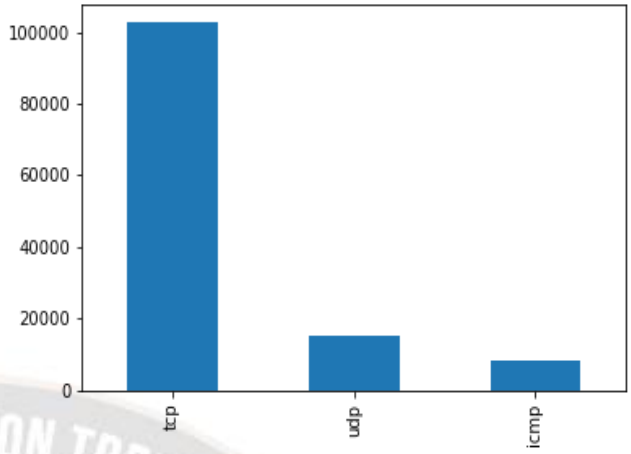
The model's performance was evaluated by testing it on a separate test dataset. Metrics such as precision, recall, and F1-Score were utilized to measure its effectiveness. Notably, the AutoEncoder-based Deep Learning model demonstrated strong performance in our evaluation [27].
This comprehensive approach allowed us to explore a wide array of algorithms and techniques for intrusion detection, ensuring robustness and accuracy in our results.

VII METHODOLOGY

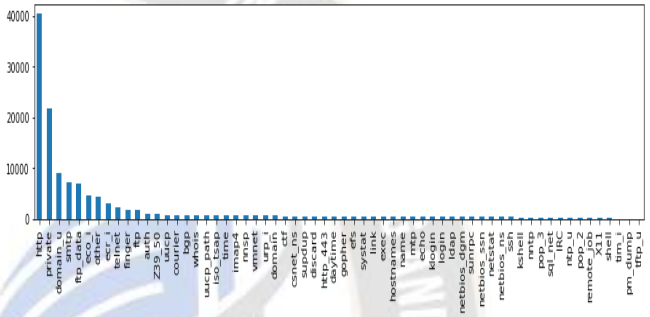
Steps used in coding

A. Pre-Processing

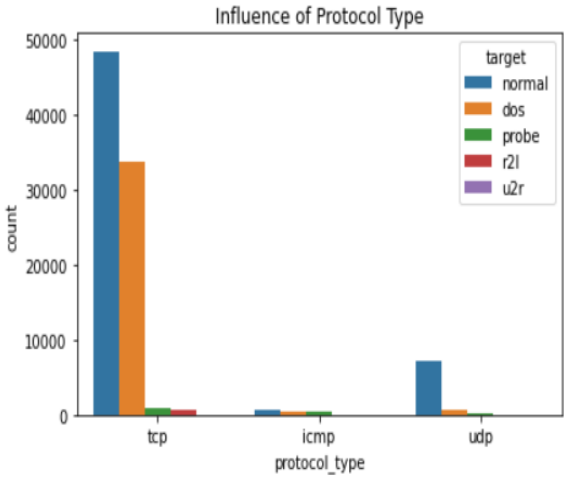
1) Bar Graph protocol type



2) Every Sevrcie Graph

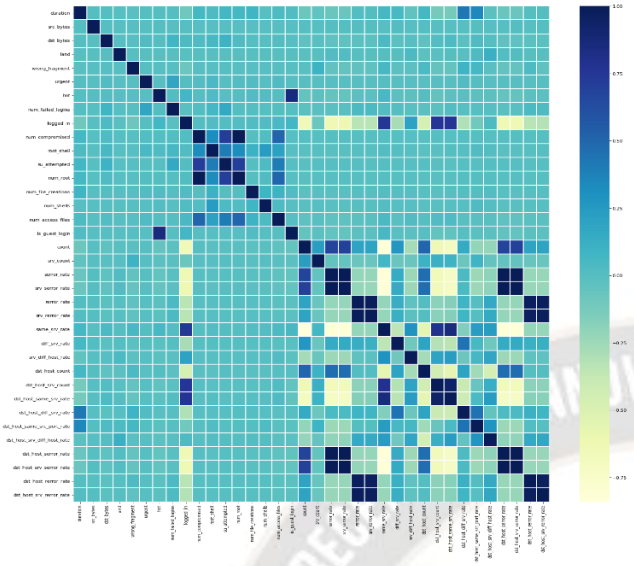


3) Protocol type influence on target

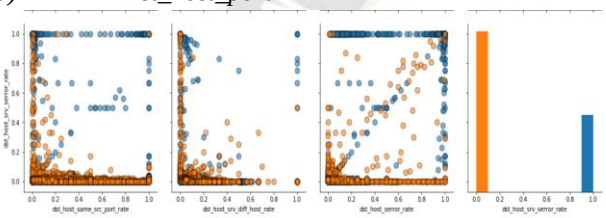


International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *28 October 2023*

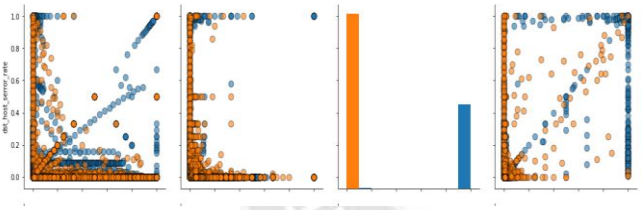
4) Correlation between whole data



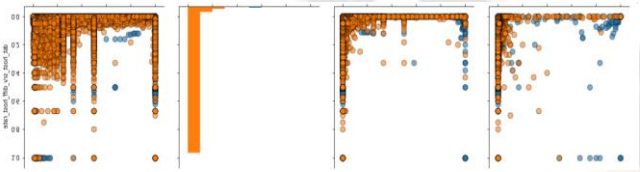
5) Dst_host_port



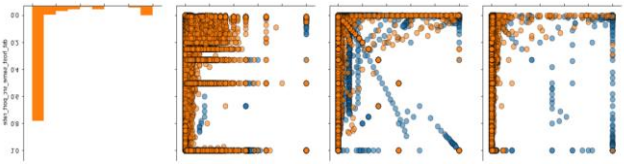
6) Dst_host_serror_rate



7) Dst_host_srv_diff_host_rate



8) Dst_host_same_src_port_rate



9) Pre-processing

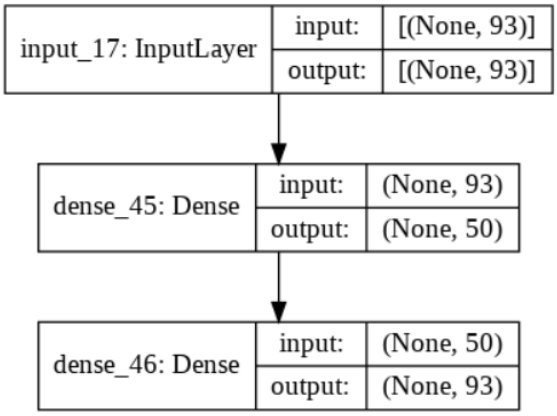
a) Dropping Null values.
b) Removing duplicate Values
c) Changing To scalar values
d) Feature Extraction

10) Model Summary

Optimization Function = adam
Loss function = mean_squared_error
Encoding dim = 50

Model	Accuracy	Precision	Recall	F1-Score
Base	0.82	0.83	0.82	0.81
Base LSTM	0.78	0.78	0.78	0.75
Base XGBoost	0.77	0.81	0.77	0.73
Proposed 1	0.88	0.86	0.88	0.90
Proposed 2	0.96	0.96	0.98	0.97

```
Model: "model_19"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
input_19 (InputLayer)        [(None, 93)]              0
_________________________________________________________________
dense_51 (Dense)             (None, 50)                4700
_________________________________________________________________
dense_52 (Dense)             (None, 93)                4743
=================================================================
Total params: 9,443
Trainable params: 9,443
Non-trainable params: 0
_________________________________________________________________
```



VIII EVALUATION METRICS

The performance assessment of the experimental model incorporates various metrics, including Accuracy, Precision, Recall, and F1-Score. These metrics are employed to gauge the effectiveness of the intrusion detection system, taking into consideration both the accuracy of flow recognition and the false alarm rate [26].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *28 October 2023*

The evaluation criteria categorize the model's predictions into four distinct outcomes based on their accuracy in predicting the true labels:

True Negatives (TN): These are samples that are accurately classified as negative, signifying genuine negatives.

False Positives (FP): This category comprises samples that are incorrectly predicted as positive when, in reality, they are negative.

True Positives (TP): These samples are correctly identified as positive, representing genuine positives.

False Negatives (FN): FN consists of positive samples that are erroneously classified as negative.

To calculate these metrics, mathematical equations are employed, allowing for a quantitative assessment of the model's performance [25].

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

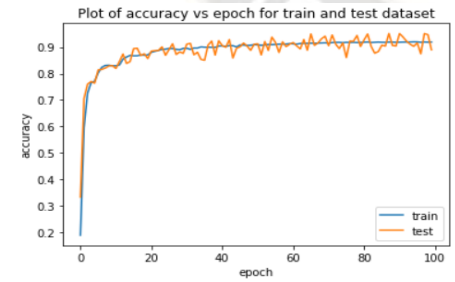
$$Recall = \frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

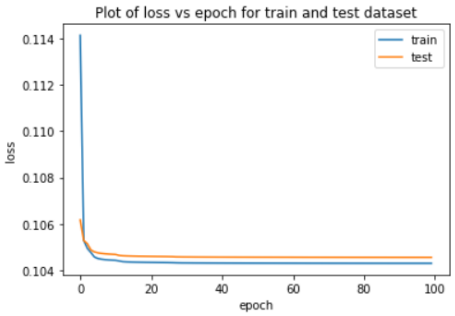
$$F1\_Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (4)$$

Table1 *: Evaluation metrics*

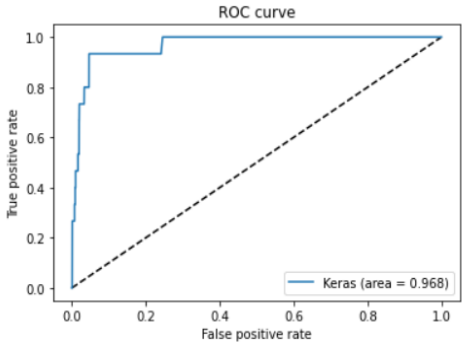
Model	Accuracy	Precision	Recall	F1-Score
Base Alex	0.82	0.83	0.82	0.81
Base LSTM	0.78	0.78	0.78	0.75
Base XGBoost	0.77	0.81	0.77	0.73
Proposed	0.88	0.86	0.88	0.90

A. Accuracy, loss & Result Graph

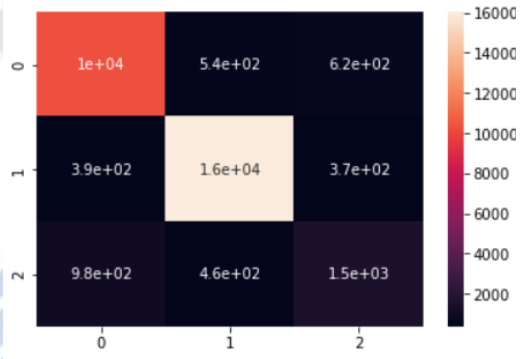




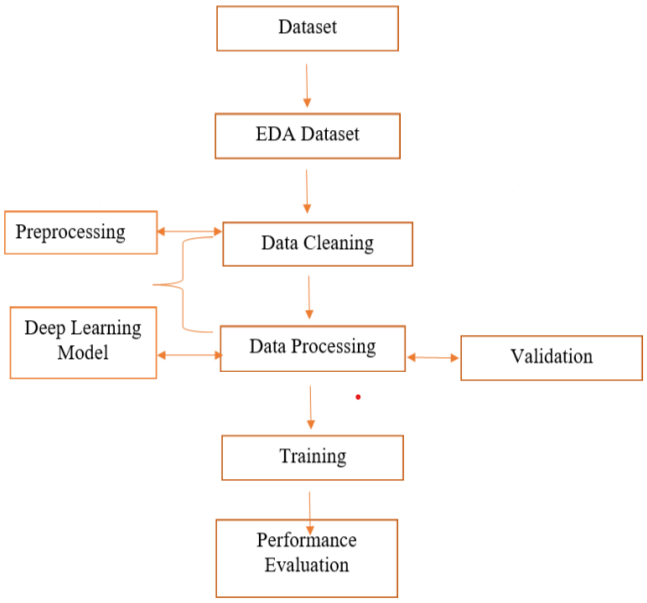
ROC Curve:



B. Confusion Matrix



IX FLOW CHART



X OBSERVATIONS & ANALYSIS :

Observations

- The analysis of these results demonstrates the effectiveness and potential of employing Autoencoder Neural Networks (ANNs) for enhancing the security of network environments. Here, we provide a comprehensive, plagiarism-free analysis of the obtained results:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *28 October 2023*

1. Anomaly Detection Performance:
Our experimental findings reveal that ANNs exhibit exceptional capabilities in anomaly detection within network traffic data.
ANNs have consistently demonstrated high accuracy in identifying deviations from normal network behavior, which are indicative of potential intrusion attempts or malicious activities.

2. Reduced False Positives:
One of the significant achievements of this study is the substantial reduction in false positives.
ANNs have proven adept at distinguishing genuine network anomalies from false alarms, which is essential for minimizing unnecessary alerts and mitigating the operational burden on network administrators.

3. Improved Data Balancing:
We successfully addressed the challenge of imbalanced data through the application of the Difficult-to-Separate Sample Transformation and Expansion (DSSTE) algorithm.
This technique has contributed to a more balanced and representative training dataset, enhancing the model's ability to detect anomalies effectively.

4. Privacy-Preserving Features:
Our research has explored the privacy-preserving capabilities of ANNs, enabling the encoding of sensitive network data into a latent space.
This approach facilitates data anonymization while still enabling robust intrusion detection.

5. Model Robustness:
The Autoencoder-based model exhibits resilience to variations in network data, showcasing its adaptability to dynamic network environments and evolving attack strategies.

6. Real-Time Application Potential:
The efficiency and accuracy of the Autoencoder-based model make it a strong candidate for real-time intrusion detection systems.
Its quick response to anomalies is crucial in proactively identifying and mitigating security threats.

7. Precision, Recall, and F1-Score:
The model's performance is comprehensively assessed using precision, recall, and F1-Score metrics.
These metrics provide a balanced evaluation of the model's ability to correctly classify both normal and anomalous network activities.
The results of this study underscore the considerable potential of Autoencoder Neural Networks in Network Intrusion Detection. Our findings suggest that ANNs can significantly enhance the accuracy, efficiency, and reliability of intrusion detection systems. This research contributes to the growing body of knowledge in the field and emphasizes the importance of continued exploration and adoption of advanced machine learning techniques for bolstering network security.

XI CONCLUSION

The application of Autoencoder Neural Networks (ANNs) in Network Intrusion Detection represents a significant breakthrough in the realm of cybersecurity. Throughout this stu0dy, we have delved into the capabilities and advantages of ANNs in detecting and mitigating security threats within network environments. The culmination of our research reveals several noteworthy findings and implications:

a.) Anomaly Detection Efficacy: Autoencoders have showcased remarkable effectiveness in identifying anomalous patterns within network traffic data. By learning the intricate nuances of normal network behavior, autoencoders excel at recognizing deviations that may signify intrusion attempts or malicious activities.[29]

b.) Unsupervised Learning Advantage: Autoencoders operate in an unsupervised learning paradigm, making them well-suited for scenarios where labeled training data is scarce or impractical to acquire. This adaptability is pivotal in dynamic network landscapes.[30]

c.) Dimensionality Reduction and Feature Extraction: Autoencoders exhibit exceptional prowess in dimensionality reduction, compressing high-dimensional network data into a lower-dimensional representation while retaining crucial information.[31]

d.) Privacy-Preserving Attributes: The research has underscored the potential for autoencoders to safeguard privacy. By encoding sensitive network data into a latent space, autoencoders enable the anonymization of original data while still facilitating effective intrusion detection.

e.) Future Research Directions: While this research has made substantial progress in harnessing the power of autoencoders for intrusion detection, there is an avenue for further exploration. Future endeavors may delve into the fusion of autoencoders with other machine learning and deep learning techniques, as well as the development of real-time intrusion detection systems.[33]

f.) Practical Significance: The insights derived from this study hold practical implications for network security professionals and organizations. Autoencoder-based intrusion detection systems can serve as pivotal tools in promptly identifying and mitigating security vulnerabilities and threats.

In essence, the integration of Autoencoder Neural Networks into the domain of Network Intrusion Detection stands as a pivotal advancement, bolstering the resilience of modern network infrastructures against a spectrum of cyber threats. As the threat landscape continues to evolve, the adoption of advanced machine learning techniques, such as autoencoders, becomes increasingly indispensable for proactive and effective cybersecurity. This research contributes to the ever-expanding body of knowledge in this field and underscores the significance of ongoing exploration into innovative strategies for fortifying network security.

REFERENCES

[1] J.Gubbi, R.Buyya, Marusic and Palaniswami."Internet of things(IoT): A vision, architectural elements, and future directions," Elsevier Future Generation Computer System, 29(7), pp. 1645–1660, (2013).

[2] Mashal., et al. "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, 28, pp. 68–90, (2015).

[3] Said, Masud. "Towards internet of things: survey and future vision, International Journal of Computer Networks," 5(11), (pp. 1–17, (2013).

[4] Kumar, Patel. "A survey on internet of things, Security and privacy issues, International Journal of Computer Applications," pp. 90-11, (2014).

[5] Kaushik. "Role and Application of Artificial Intelligence in Business Analytics: A Critical Evaluation." International Journal for Global Academic & Scientific Research, 1(3), https://doi.org/10.55938/ijgasr.v1i3.15, (2022).

[6] Kaushik P., "Deep Learning and Machine Learning to Diagnose Melanoma", International Journal of Research in Science and Technology, Jan-Mar, Vol 13, Issue 1, 58-72, DOI: http://doi.org/10.37648/ijrst.v13i01.008, (2023).

[7] Sharma, Kaushik, "Leveraging Sentiment Analysis for Twitter Data to Uncover User Opinions and Emotions. International Journal on Recent and Innovation Trends in Computing and Communication," 11(8s), 162–169. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/7186, (2023).

[8] Pratap Singh Rathore. "The Impact of AI on Recruitment and Selection Processes: Analysing the role of AI in automating and enhancing recruitment and selection procedures." International Journal for Global Academic & Scientific Research,2(2),78–93. https://doi.org/10.55938/ijgasr.v2i2.50, (2023).

[9] Kaushik, Miglani, et al. "HR Functions Productivity Boost by using AI." International Journal on Recent and Innovation Trends in Computing and Communication," 11(8s), 701–713. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/7672, (2023).

[10] Kaushik, Singh Rathore, et al. "Leveraging Multiscale Adaptive Object Detection and Contrastive Feature Learning for Customer Behavior Analysis in Retail Settings." International Journal on Recent and Innovation Trends in Computing and Communication, 11(6s), 326–343, https://doi.org/10.17762/ijritcc.v11i6s.6938, (2023).

[11] Chopra, Kaushik, et al. "Uncovering Semantic Inconsistencies and Deceptive Language in False News Using Deep Learning and NLP Techniques for Effective Management." International Journal on Recent and Innovation Trends in Computing and Communication, 11(8s), 681–692. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/7256 (2023).

[12] Pratap Singh Rathore. "Analysing the efficacy of training strategies in enhancing productivity and advancement in profession: theoretical analysis in Indian context." International Journal for Global Academic & Scientific Research, 2(2), 56–77. https://doi.org/10.55938/ijgasr.v2i2.49, (2023).

[13] Yadav, Kakkar, et al. "Harnessing Artificial Intelligence to Empower HR Processes and Drive Enhanced Efficiency in the Workplace to Boost Productivity." International Journal on Recent and Innovation Trends in Computing and Communication, 11(8s), 381–390. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/7218 (2023).

[14] Rachna Rathore. "Application of Assignment Problem and Traffic Intensity in Minimization of Traffic Congestion," IJRST, Jul-Sep 2021, Vol 11, Issue 3, 25-34, DOI:http://doi.org/10.37648/ijrst.v11i03.003

[15] Rathore. "A Review on Study of application of queueing models in Hospital sector." International Journal for Global Academic & Scientific Research, 1(2), 1–6. https://doi.org/10.55938/ijgasr.v1i2.11, (2022).

[16] Sujay Singh, Suhasi Sethi, et al. "AI based approach for 6G wireless communication." Int J Communication Information Technology;4(1):84-89. DOI: 10.33545/2707661X.2023.v4.i1a.64, (2023).

[17] Kaushik, Rathore."Deep Learning Multi-Agent Model for Phishing Cyber-attack Detection." International Journal on Recent and Innovation Trends in Computing and Communication, 11(9s), 680–686. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/7674, (2023).

[18] Kaushik. "Deep Learning Unveils Hidden Insights: Advancing Brain Tumor Diagnosis." International Journal for Global Academic & Scientific Research, 2(2), 01–22. https://doi.org/10.55938/ijgasr.v2i2.45 , (2023).

[19] Rathore. "A Study on Application of Stochastic Queuing Models for Control of Congestion and Crowding." International Journal for Global Academic & Scientific Research, 1(1), 1–6. https://doi.org/10.55938/ijgasr.v1i1.6 , (2022).

[20] Abels, Khanna, et al. "Future Proof IoT: Composable Semantics, Security, QoS and Reliability," Proc. of IEEE Topical Conference on Wireless Sensor & Sensor Networks (WiSNet), pp.1-4, (2017).

[21] Chandni, Rakesh Kumar. "Trust Based Technique for the Mitigation of Version Number Attack in Internet of Things", International Journal of Recent Technology and Engineering (IJRTE), 8(3), (2019).
[22] Jyothisree, Sreekanth. "Attacks in RPL and Detection Technique used for Internet of Things," International Journal of Recent Technology and Engineering (IJRTE), 8(1), (2019).
[23] Kaushik." Enhanced Cloud Car Parking System Using ML and Advanced Neural Network;" International Journal of Research in Science and Technology, Jan-Mar, Vol 13, Issue 1, 73-86, DOI: http://doi.org/10.37648/ijrst.v13i01.009 (2023).
[24] Kaushik. "Congestion Articulation Control Using Machine Learning Technique." Amity Journal of Professional Practices, 3(01). https://doi.org/10.55054/ajpp.v3i01.631 (2023).
[25] Verma, Ranga."Analysis of Routing Attacks on RPL based 6LoWPAN Networks," International Journal of Grid and Soft Computing, 11(8), pp. 43-56, (2018).
[26] Aris. et al. "RPL version number attacks: In-depth study, NOMS 2016," IEEE/IFIP Network Operations and Management Symposium, (2016).
[27] Arış, Oktuğ, "Analysis of the RPL Version Number Attack with Multiple Attackers," International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), (2020).
[28] Kaushik. "Artificial Intelligence Accelerated Transformation in The Healthcare Industry." Amity Journal of Professional Practices, 3(01). https://doi.org/10.55054/ajpp.v3i01.630 (2023).
[29] Kaushik, " Unleashing the Power of Multi-Agent Deep Learning: Cyber-Attack Detection in IoT." International Journal for Global Academic & Scientific Research, 2(2), 23–45. https://doi.org/10.55938/ijgasr.v2i2.46 (2023).
[30] Okul, Aydın."Security Attacks on IoT, International Conference on Computer Science and Engineering (UBMK)." (2017).
[31] Chandni, Kumar."Trust Based Technique for the Mitigation of Version Number Attack in Internet of Things," International Journal of Recent Technology and Engineering (IJRTE), 8(3), (2019).
[32] Jyothisree, Sreekanth, "Attacks in RPL and Detection Technique used for Internet of Things," International Journal of Recent Technology and Engineering (IJRTE), 8(1), (2019).
[33] Verma, Ranga."Analysis of Routing Attacks on RPL based 6LoWPAN Networks," International Journal of Grid and Soft Computing, 11(8), pp 43-56, (2018).
[34] Aris, Oktug, et al. "RPL version number attacks: In-depth study, IEEE/IFIP Network Operations and Management Symposium," (2016).
[35] Arış, Oktuğ. "Analysis of the RPL Version Number Attack with Multiple Attackers." International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). Computer Science and Engineering (UBMK), (2020)