Detection Mechanism in IoT framework using Artificial Neural Networks

Rachna Jain (rachna_19802000@yahoo.com)  
JSS Academy of Technical Education Noida  https://orcid.org/0000-0001-9794-614X

Geetika Dhand  
Maharaja Surajmal Institute of Technology

Kavita Sheoran  
Maharaja Surajmal Institute of Technology

Amandeep Kaur  
Guru Tegh Bahadur Institute of Technology

Navyah Puri  
Guru Tegh Bahadur Institute of Technology

Nishtha Jatana  
Maharaja Surajmal Institute of Technology

Kashika Jain  
Amity University

Hiti Bansal  
Shiva Shiksha Sadan Sonepat

Panav Jain  
delhi public school Noida

Research Article

Keywords: Intrusion Detection, Machine Learning, Anomaly-based, Internet of Things(IoT), Deep Learning

Posted Date: March 22nd, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2610436/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.  
Read Full License
Abstract

Internet of Things (IoT) applications are now used more frequently due to the rapid expansion of wireless networking and the digital revolution. IoT helps in user-to-machine and machine-to-machine interaction. IoT objects have gained popularity because they can be accessed from anywhere. Healthcare, agriculture, smart cities, and the military are different domains where IoT objects are communicating with each other. The goal of anomaly-based techniques is to figure out which patterns are normal and which are aberrant. This approach of intrusion detection has the benefit of detecting original works of authorship intrusions. However, this technique has the drawback of frequently producing false positive results. To increase the effectiveness of anomaly-based intrusion detection methods, machine learning techniques are being evaluated. Anomaly-based intrusion detection techniques can be used by machine learning algorithms to watch active behavior and compare it to known intrusion footprints in order to stay aware of potential future attacks. In a hybrid approach, different identifying methods are combined in the same scheme. This technique will eliminate the weaknesses of a particular operation while improving the overall IoT system's reliability. In this research, we study intrusion-based systems using comparative analysis of several machine learning and deep learning algorithms. In the proposed work one hot encoding technique is used to deal with the categorical data. Different parameters like accuracy, F-1 score, precision, and recall value have been calculated. Experimental results prove that ANN yields 99.61% accuracy over other hybrid models. However, in Machine Learning, RandomForestClassifier yields the best results.

1. Introduction

IoT has enabled the collecting, processing, and communication of data in smart applications as an emergent technology breakthrough [7]. These innovative qualities have piqued the interest of city planners and health professionals, as IoT gains widespread adoption at the network's edge for real-time applications like eHealth and smart cities [1]. The rise in the number and sophistication of unknown cyber-attacks, on the other hand, has cast a pall over the adoption of these smart services. This is due to the fact that the diversity and distribution of IoT applications/services make IoT security hard and difficult [7], [3]. Furthermore, because of the unique service requirements of IoT, which cannot be met by centralized methods, attack detection in IoT is drastically different from previous techniques.

The fusion of the virtual and physical world leads to advancement in the computing paradigm involving artificial intelligence and other technologies [7]. There is a surge in connected networks because of society 5.0. The initiative of the Govt. of India is to develop 100 smart cities in the country. IoT technology helps to communicate among smart objects. IoT objects deployed with dynamic topology results in network vulnerabilities. Battery life of devices is an important criterion to prolong the life of sensor networks [22–25]. Critical factors determining the life of the battery are the transmission range of the sensor nodes and sensor reading frequency [1]. Security of the network is also a major concern in these wireless networks. Firewalls alone are insufficient to secure the network due to dynamic topology and difficulty in having physical access. [3] authors have analyzed routing security in RPL routing protocol for lossy networks especially those having low power as in the case of IoT. The authors have given a
complete statistical analysis involving various mitigation techniques used in RPL-based networks. [11] have enlisted attacks and countermeasures for proposing secure routing in Wireless Sensor Networks. The authors have emphasized the fact that end-to-end security is difficult to achieve in sensor networks as compared to conventional networks. The authors have suggested that cryptography alone is not sufficient to suggest secure routing in sensor networks. [14] have proposed a reputation-based RPL protocol that helps in the elimination of selective forwarding in IoT networks. Figure 1 displays the selective forwarding problem. The proposed protocol will consider the node’s reputation while making a routing decision. In this model, every node calculates firsthand reputation and secondhand reputation. Firsthand reputation is computed by direct node monitoring whereas secondhand reputation is computed by neighboring nodes. Security of the network is increased by limiting false alarms. Reputation-based RPL routing protocol has self-healing capabilities. Due to its healing nature, it is prone to attack by malicious nodes. Figure 1 shows the selective forwarding attack.

2. Literature Survey

[4] has developed a routing mechanism to strengthen the security of MANETS (Mobile Adhoc Networks) which form the backbone of IoT-based smart systems. The authors have implemented Calculator Key (CK) as well as Distribution Key (DK) to enhance the security of the network. Public and Private keys are generated using the CK node which is further passed to the DK node resulting in the secure transmission of data. The proposed technique results in energy saving of the network because only two nodes are involved in the generation of CK and DK. The advantage of the scheme is that all the nodes are not involved in the generation of keys resulting in energy savings for the network. The nodes chosen as CK and DK are selected based on the energy and trust value of the node.

Quality of Service (QoS) requirements in low latency networks such as IoT makes fog computing an attractive choice for meeting the requirements [8]. The flexibility and scalability of the network can be enhanced using Software Defined Networking (SDN). Fog nodes are having both computing and SDN capabilities but the deployment of these nodes is a crucial task. The proposed approach works well for both Industrial IoT (IIoT) and SDN topologies.

[18] proposed MFO-RPL (Moth Flame Optimization-RPL) routing protocol for applications in IoT. The authors have claimed that MFO is the most suitable algorithm for solving optimization problems. In the proposed algorithm fitness value of moths has been calculated. There is a petal formation between a source node and a destination node. In absence of petal formation packets are not blindly forwarded to the destination node. A community-inspired algorithm like MFO uses a Moth matrix (MO) and flame matrix. The moth position is updated using the logarithmic spiral mechanism. The results show that in the IoT ecosystem packet loss ratio has decreased and lesser frequency of rank changes.

[12] have suggested load-balancing techniques using the Firefly algorithm in Flying Ad Hoc Networks (FANETS). The simulation results suggest that the computational load equally divided among nodes helps in prolonging the network lifetime.
[19] has proposed trust-based route selection in MANETS. In the proposed routing protocol Efficient Trust Establishment Routing Evidence (ETERE), the I Trust value of nodes provides trusted routing evidence for securing paths in MANETS. Simulations performed on the NS-2 simulator have shown PDR and throughput of the network have been improved by 28% and 34% respectively. The authors have simulated a small area of 1000*1000 sq. m. and further want to expand to a large wide area helping the military and government.

The authors [9] have emphasized the importance of MQTT (Message Queue Telemetry Transportation) in the advancement of IoT technologies. The openness of the protocol makes it prone to different attacks such as DDoS, buffer overflow, etc. Intrusion detection for such applications is still an area of concern. The authors have suggested MQTT parsing engine embedded with IDS. The proposed model proves its efficacy by blocking a malformed packet. The author proposes a generic parsing engine applicable to IoT applications in the future.

[13] have exploited the communication protocol of a smart plug system for device scanning, brute force, spoofing, and firmware attacks. Security vulnerabilities of smart plugs have been thoroughly discussed. The authors have devised the guidelines for the smart plug.

[16] have suggested that being a lightweight rank-based protocol RPL is under security threats. Challenges faced are unsecured links and limited resources. Different methods are compared to mitigate these attacks.

[20] have proposed a technique (DSH-RPL) for detecting sinkhole attacks in RPL. The proposed protocol is divided into four phases. In the first phase, reliable RPL is created, and afterward sinkhole attack is detected. In the third phase, the malicious node is quarantined and in the last phase, encrypted data is transmitted. The proposed protocol has reduced the false negative rate.

[5] have emphasized the fact that IoT devices are the major building blocks of a cyber-physical system. Security and privacy of sensitive information are a must for the successful application of IoT devices. If there is an attack on any single device then there are consequences that affect major application areas like the industrial, environmental, and health sectors. The authors have suggested that sensitive information can be compromised using side-channel attacks. The authors have used Estimation Distribution Algorithm (EDA) to compute the Point of Interest (POI). Side Channel Attacks obtain secret keys using cryptographic devices. These attacks are only effective for small-size keys whereas long keys are extracted using the divide-and-conquer technique.

[21] have emphasized the role of machine learning techniques in the wireless domain. The authors have advocated the Long Short Term Memory (LSTM) model to predict the arrival of the packets for high traffic Unmanned Aerial Vehicles. It has been suggested that the Packet Arrival Prediction (PAP) model performs better with respect to different network parameters like delay and PDR etc.
have proposed self-adaptive cyber-physical systems. In the proposed model there are four different stages: monitor, plan, execute, and knowledge to complete the closed feedback loop. The authors have emphasized the fact that ordinary systems can be differentiated from self-adaptive systems. The architecture proposed in the paper discusses quality function. Business and adaptation goals are thoroughly analyzed. Threats to the validity of quality function have been elaborated.

have emphasized the fact that security threats are critical challenges to an IoT scenario. The authors have advocated the use of deep learning methods for detecting anomalies. The research paper has highlighted that signature-based methods, specification-based methods, anomaly-based approaches, and hybrid strategies are the four basic types of ID assaults. If the threshold is exceeded or the rules are broken, the IDS will detect a rare condition and respond appropriately. The proposed model offers an accuracy of 99.51%.

have suggested a peer-to-peer communication protocol for connected networks based on blockchain technology. The protocol aids in ensuring the contact mechanism's security and accommodates heterogeneity in functioning states. Currently, researchers are looking at adding blockchain into a multi-agent system.

3. Vulnerabilities Of IoT Ecosystem

The Internet of Things (IoT) is a vast network of smart gadgets that communicate constantly over the Internet. Given the tremendous rise of the Internet of Things as a new technology paradigm, which may involve safety-critical processes and sensitive data being uploaded to the internet, its security element is crucial. The smart home, health care, and transportation domains are all investigated in this article. It's possible that an interruption will occur during the operation of IoT devices, causing them to shut down. The taxonomy of security threats in IoT networks was created to aid IoT developers in better understanding the danger of security issues and incorporating better defenses. Different attacks in an IoT system are classified on the basis of authentication and availability of the devices.

Attacks based on availability are demonstrated as follows:

1. Sinkhole attack is the most prominent attack at the network layer. In this attack, the intruder aims to absorb the complete traffic originating from any region. A sinkhole attack can further lead to a selective forwarding attack. In this type of attack denial of service can also be clubbed.
2. Blackhole happens when a malicious node does not participate in packet forwarding which results in packet rejection and delay in transmission.
3. Greedy behavior happens due to the illusion of congestion in the neighborhood. In this attack, a greedy driver declares false congestion so that it can reach the destination quickly.
4. Broadcast tampering results in heavy attacks as it is related to the safety of the driver.
5. Denial of Service results in interruption of services. In this type of attack, unwanted data is injected into the network. Network services are degraded in it which is proportional to the time taken to recover the network.
Attacks on authentication are classified as follows:

1. Message Replay: In it, the attacker pushes forged messages to suppress the transmitted message.
2. Sybil: This attack is primarily aimed at peer-to-peer systems. It is aimed at distributed system environments. In it, the attacker behaves as different identities rather than a single identity.
4. Location Service spoofing: In the case of vehicular networks correct location information has to be sent. Wrong position information leads to malfunctioning and rerouting of data.

4. Proposed Methodology

In a data-gathering and processing module of attack detection, IDSs primarily include evidence of an attack. In the data gathering module, the input data from IoT systems were examined to determine interaction behavior using various machine learning approaches in the analysis module. Deep learning has made significant progress in a variety of fields and has proven to be a superior option to traditional machine learning. In addition, IDS with deep learning has shown promising outcomes. Deep learning-based approaches are more influential and suitable for traffic analysis to determine the normal and abnormal traffic in an IoT environment. Moreover, deep learning techniques can intelligently predict new attacks, unlike previous threats. Figure 2 gives a summary of the suggested intrusion detection model.

The first step in the process is data preprocessing, during which normalization is carried out to minimize variations in the feature values across dimensions. Since the data features are not uniform, normalization by lowering the computational complexity is crucial. The preprocessing phase maps the input data without changing the linear relationships by using the conventional min-max normalization. The normalization process is expressed as -

\[
y = \frac{y - \text{min}}{\text{max} - \text{min}}
\]

where y is the attribute value and min and max are the minimum and maximum values of the attribute.

Moreover, Fig. 3 presents IDS using deep learning models in the IoT environment.

1. Dataset Description

For intrusion detection, we used a publicly available NSL-KDD dataset from Kaggle. There are 43 columns and 125972 rows in the dataset. The dataset contains three different types of protocols: UDP, TCP, and ICMP. The final column labeled "attack," details the nature of attacks on networks.

2. Algorithms Used

1. Artificial Neural Network- A group of simulated neurons help compensate for an artificial neural network. Every neuron functions as a node that is linked to other nodes by connections that mimic biological axon-synapse-dendrite connections. The weight of each link controls how strongly one node
influences another. The ANN model yields the highest accurate results i.e. 99.61% accuracy for the network dataset.

2. **Random Forest Classifier**- It is a method of ensemble tree-based learning that consists of several decision trees extracted from a section at random among the practice examples. The products are ultimately classified based on the scores from different decision trees gathered by classifiers using a random forest. The RFC produced an accuracy of 99.62%, which is the second-highest among other ML models (after ANN).

3. **Decision Tree**- It belongs to the category of supervised learning algorithms. Decision tree algorithms can be used to address both regression and classification challenges. In order to solve problems, it uses a tree representation, in which each leaf node specifies a class tag, and the inside node of the tree contains the characteristics. The advantage of this method is that it is easy to use, explain, and demonstrate, but the drawback is that it necessitates a detailed examination of the transactions.

4. **K-Nearest Neighbors**- One of the simplest machine learning methods is KNN, which groups a set of attributes into the category that represents the dataset's k-nearest neighbors most frequently.

5. **Gradient Boosting**- Similar to other boosting techniques, it constructs the model in stages, but it generalizes them by enabling the optimization of any differentiable loss function. We performed gradient boosting over SVM(Kernel-RBF).

3. Model Interpretation and Discussion

Our research deals with intrusion detection over various networks using different Deep Learning and Machine Learning methodologies. We ran one hot encoding to deal with categorical data after preprocessing the data from our NSL-KDD dataset. Since we used deep learning models, our model evaluation has produced the best results so far, yielding 99.71% accuracy. Count Plots, Heat maps, confusion matrices, and other visual representations were plotted to graphically portray the results.

5. Results And Discussions

This section discusses the implementation outcomes of our model for intrusion detection using machine learning and deep learning algorithms. Utilizing the benchmark NSL-KDD dataset, the performance of the proposed intrusion detection model is verified. The dataset is split between training and testing the model in an 80:20 ratio. We used various Machine Learning techniques to develop our intrusion detection model, including Support Vector Machine, where we used the RBF kernel. We implemented K-Nearest Neighbors and Decision Tree, and in the ensemble model, we employed Random Forest Classifier, which has so far shown the highest performance. We deployed Artificial Neural Networks in addition to these algorithms for Deep Learning.

**Performance Evaluation**- An evaluation of our models' performance is known as performance evaluation. To assess how well a model operates, the performance evaluation methodologies listed below are used:

1. **TP (True Positive)**: This refers to the proportion of intrusion detection cases that are both considered and confirmed to be true.
2. **TN (True Negative):** This refers to the percentage of intrusion detection cases that are misclassified but are in fact untrue.

3. **FN (False Negative):** This refers to the percentage of intrusion detection cases that are falsely labeled as negative but are actually positive.

4. **FP (False Positive):** This refers to the proportion of intrusion detection cases that are misclassified as true but are in fact false.

The performance of the model can be further assessed using a few metrics that can be calculated. Here are a few examples of the measures this study used:

i. **Recall Value:** It indicates the actual positives that were accurately identified as having been positives and is given as follows:

   \[
   \text{Recall} = \frac{TP}{TP + FN}
   \]

ii. **Precision:** Precision is defined as the ratio of a significant instance to a retrieved instance and is expressed as follows:

   \[
   \text{Precision} = \frac{TP}{TP + FP}
   \]

iii. **Accuracy:** This term refers to the proportion of true predictions provided by the model, and it is expressed as follows:

   \[
   \text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN}
   \]

iv. **F1 Score:** This metric measures our recall and precision using the harmonic mean. It is stated as follows:

   \[
   F1\text{Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}
   \]

The tabular representation of the classification report for intrusion detection using multiple ML & DL models is shown in Table 1. Also, the graphical representation for ANN model accuracy is shown in Fig. 4 and the overall results depicted in the Table 1 are graphically represented in Fig. 5 using Bar graphs.
### Table 1
Classification Report for different ML & DL models

<table>
<thead>
<tr>
<th>Algorithms Used</th>
<th>Precision</th>
<th>Recall</th>
<th>f-1 score</th>
<th>Accuracy(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANN</td>
<td>0.999</td>
<td>0.999</td>
<td>0.999</td>
<td>99.61</td>
</tr>
<tr>
<td>Random Forest Classifier</td>
<td>0.998</td>
<td>0.997</td>
<td>0.998</td>
<td>99.58</td>
</tr>
<tr>
<td>Decision Tree</td>
<td>0.997</td>
<td>0.996</td>
<td>0.995</td>
<td>99.52</td>
</tr>
<tr>
<td>KNN</td>
<td>0.996</td>
<td>0.995</td>
<td>0.995</td>
<td>99.49</td>
</tr>
<tr>
<td>Gradient Boosting</td>
<td>0.996</td>
<td>0.992</td>
<td>0.994</td>
<td>99.45</td>
</tr>
<tr>
<td>SVM(Kernel-RBF)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The results have also been visually represented through count-plot, heatmap, and confusion matrix:

**Count Plot** - In order to visualize the distribution of various different one-dimensional values, counts plots are a variation on the strip plot that provide a better view of overlapping data points.

**Heat-Map** - A matrix plot is shown visually as a heatmap. A heatmap collects information in a matrix format. By matrix, we mean that for the data we enter into the cells to be relevant, the index and column names must be similar in some way.

**Confusion Matrix** - An N x N matrix called a confusion matrix is used to assess the effectiveness of a classification model, where N is the total number of target classes. In the matrix, the actual target values are contrasted with those that the machine learning model anticipated.

### 6. Conclusion

As the frequency of security breaches continues to rise, cyber security remains a critical issue for any sector online. Thousands of zero-day attacks are known to emerge regularly due to the addition of multiple protocols, primarily from the Internet of Things (IoT). The majority of these cyber-attacks are minor variations of previously identified cyber-attacks. This suggests that even sophisticated techniques like typical machine learning algorithms have difficulties spotting these small attacks over time. The experiment is conducted on the benchmark NSL-KDD dataset, and the performance of various intrusion detection systems, including Artificial Neural Networks (ANN), Random Forest Classifiers, Decision Trees, KNNs, and Gradient Boosting, is compared. Experimental findings support the suggested model's superior accuracy, precision, recall, and F1-score performance. The suggested hybrid intrusion detection model detects the most attacks in the dataset, with a maximum prediction performance of 99.61%. The success of deep learning (DL) in numerous big data sectors has piqued interest in cyber security. Concatenated Deep Learning architectures can be added to this research study further to expand their use for the detection of multiple attacks. Because of advancements in CPU and neural network techniques, the use of DL has become realistic.
Declarations

Conflict of interest:
On behalf of all authors, the corresponding author states that there is no conflict of interest.

Funding (information that explains whether and by whom the research was supported):
Not Applicable

Conflicts of interest/Competing interests (include appropriate disclosures):
NA

Availability of data and material (data transparency):
Random data set

Code availability (software application or custom code):
NA

References


**Figures**

**Figure 1**

Selective Forwarding attack
Figure 2
The Proposed Model for Intrusion Detection

Figure 3
IDS using a Deep learning model
Figure 4

Model accuracy for ANN
Figure 5

Graphical Representation for classification report of different models
Figure 6

Countplot for different protocol types

Figure 7

Global distribution of attributes
Figure 8

(a) HeatMap  (b) Heat Map
Figure 9

Confusion Matrix