*Turkish Journal of Computer and Mathematics Education* *Vol.10 No.02 (2019), 1095-1100*
DOI: https://doi.org/10.17762/turcomat.v10i2.13631

*Research Article*

# AI-based Intrusion Detection System for Internet of Things (IoT) Networks

**Kanchan Naithani**
Dept of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002

**Abstract**
The rise of the Internet of Things has brought about various advantages, such as providing us with more efficient and effortless activities. Unfortunately, the lack of security solutions has also led to the development of new threats. One of these is the exploitation of vulnerabilities in the networks of IoT devices. In order to effectively address the security threats that can arise in the networks of IoT devices, there needs to be an effective intrusion detection system (IDS). In the field of security, the use of artificial intelligence (AI) powered IDS has shown promising promise. Through deep learning and machine learning techniques, these systems can learn and adapt quickly to new threats. This paper presents an evaluation of the performance of an AI-based security system on a large dataset. The research begins with a literature review of the previous studies related to the security of IoT devices and intrusion detection. We then develop a methodology that includes the data collected for evaluation and training, an AI model architecture for intrusion detection, and the evaluation metrics. The paper presents the results of the study and discusses the performance of the AI-based IDS compared to the existing solutions for addressing security threats in Internet of Things networks. It also explores the potential of this technology for future research. The findings of this study contribute to the growing body of research on the security of IoT networks and intrusion detection. It shows that an AI-based IDS can perform better than the existing solutions in identifying and mitigating threats. The study's findings show the potential of deep learning and machine learning techniques to enhance the security of IoT networks. It also highlights the scope of this technology's application in other security domains.
**Keywords**: IDS, IoT, Cyber-Security, AI

## Introduction

The term Internet of Things refers to a network of devices and objects that are equipped with software, sensors, and connectivity to communicate with each other and the internet. Due to its widespread adoption, IoT has the potential to transform various sectors, such as manufacturing, transportation, home automation, and healthcare as shown in figure-1. Although the concept of IoT was first unveiled decades ago, its growth has been attributed to advancements in wireless connectivity, cloud computing, and sensors. These innovations have made it possible to establish and collect real-time data from various objects and devices, which can be utilized for different purposes.[1]–[3]


*Figure 1 IOT trends (src- www.mantralabs.com)*

There are various types of objects and devices that can be connected to the Internet of Things, such as smart home appliances, security cameras, and wearable devices. Medical devices, such as blood glucose monitors and pacemakers, can also be linked to the network. The potential of IoT is immense, as it can improve the efficiency and security of various sectors, such as healthcare and transportation. In healthcare, it can help patients monitor

DOI: https://doi.org/10.17762/turcomat.v10i2.13631



their vital signs remotely, which can lead to lower costs and better outcomes. In transportation, it can help prevent accidents by monitoring the traffic conditions in real time. The amount of data that these devices collect and the security they pose are some of the most critical issues that need to be resolved in order to ensure their safety and security. Due to the nature of their connectivity, they are prone to being exploited by cyber criminals. In addition to this, there is also a need for effective and secure solutions that can prevent them from being stolen. The rapid emergence and evolution of the Internet of Things has the potential to greatly affect various sectors and industries. Unfortunately, its privacy and security concerns can prevent it from being utilized properly. There is therefore a need for secure and robust solutions and mechanisms to ensure the safety and protection of IoT.[4]–[6]

The rise of the Internet of Things has made it an integral part of our lives. Its widespread deployment has created new security threats that are difficult to address with traditional solutions. Due to the nature of the Internet of Things, it is easy for cybercriminals to launch attacks on its networks. They can also take advantage of the vulnerabilities in these devices to carry out distributed denial of service (DoS) attacks, as well as malware-based attacks. An effective IDS can help prevent these attacks. Due to the nature and number of Internet of Things (IoT) devices, their security has become a concern for both individuals and organizations. The lack of security protocols and the distribution of these devices make them an attractive target. In 2016, a massive botnet attack known as the "Mirai" occurred, disrupting internet services.

The attackers were able to take over IoT devices by exploiting their default passwords and usernames. They then used these to launch distributed denial of service attacks. The lack of security measures and the accessibility of these devices in unsecured locations such as factories, homes, and hospitals make them vulnerable targets. In addition, the lack of memory and computing power makes it difficult to implement effective measures such as authentication and encryption. This highlights the need for an effective IDS, which can continuously detect and mitigate threats.[7]

The term Internet of Things refers to the interconnected physical objects such as sensors, switches, and actuators that can be linked to the internet. Through the integration of these technologies, users can collect and exchange data in order to benefit from various applications, such as smart homes and factories. Unfortunately, the widespread deployment of IoT devices has created new security issues. Various types of attacks can be carried out against IoT devices, such as Dos, malware, and DDoS. These can compromise their functions, cause physical harm, and prevent them from working properly. There is a need for secure solutions to protect these objects.[8]

An effective IDS that uses artificial intelligence (AI) can help prevent security threats. This technology can be developed through deep learning and machine learning techniques, which are designed to analyze and learn about various aspects of a network. These techniques can then detect anomalies and potential threats. Various supervised learning techniques, such as decision trees and SVMs, are commonly used for detecting intrusions in IoT networks. The trained IDS uses datasets that are labeled with examples of abnormal and normal network traffic. It can then inform security personnel about potential threats.

In addition to these, other unsupervised learning methods, such as clustering and PCA, are also commonly used for detecting network traffic anomalies. These techniques can analyze and learn about network traffic patterns that deviate from the usual behavior. In addition to these, deep learning techniques, such as CNN, RNN, and LSTM, are also being used for detecting network traffic anomalies in IoT networks. These methods can learn about network traffic hierarchies and identify subtle changes in the behavior of the network to flag potential security threats.

This paper aims to review the current state-of-art AI-powered IDS for protecting IoT networks. It will also discuss the datasets used in training and testing these systems. The paper's findings will be used to help individuals and organizations secure their IoT devices. It will also review the datasets that have been utilized in training and testing the AI-powered IDS. This review will provide researchers with valuable insights into the techniques that can be used for developing new IDS systems for IoT networks. Due to the increasing number of Internet of Things (IoT) devices and the vulnerability they pose to attacks, the security of these networks is becoming a major concern. This paper aims to provide an overview and evaluation of the current state of AI-powered IDS for protecting IoT networks and identify their effectiveness. It will also explore the datasets that have already been used in training and evaluation.

**Literature Review**

E. Hodo et al.[9] present a framework that uses neural network technology to analyze and detect security threats in Internet of Things (IoT) networks. They then use the NSL-KDD dataset to evaluate the system's performance. The results of the evaluation show that the proposed system is more effective than traditional methods.

DOI: https://doi.org/10.17762/turcomat.v10i2.13631



J. Chen et al.[10] present a framework for developing an event-processing system for monitoring the Internet of Things (IoT). It addresses the challenges in developing an effective and efficient system for detecting complex attacks. The system's prototype was evaluated and showed that it can perform well in detecting different types of attacks.

S. Prabavathy et al.[11] present a framework that uses cognitive fog computing to analyze and detect attacks on Internet of Things (IoT) networks. They discuss the various challenges that need to be solved in developing an effective intrusion detection system, and it shows that the proposed system can perform well with high accuracy.

A. Amouri et al.[12] present a cross-layer intrusion detection system for Internet of Things (IoT) networks. They discuss the various challenges that need to be solved in order to develop this system, and they show a solution that can detect different types of attacks. The system's results show that it can perform well in detecting attacks.

E. Anthi et al.[13] present a method that can be used to design and implement an adaptive intrusion prevention system for Internet of Things (IoT) networks. This system, known as Pulse, is designed to detect different types of attacks and has high accuracy.

N. Moustafa et al.[14] present a framework that aims to create an ensemble-based system for monitoring and detecting intrusions in Internet of Things (IoT) networks. It utilizes statistical flow features to analyze and detect attacks. The results of the study show that the proposed system can reliably identify various threats.

J. Li et al.[15] present a two-stage AI-based system for detecting intrusions in software-defined Internet of Things (IoT) networks. It addresses the challenges of designing and implementing an effective system for this type of network. They then demonstrate how it can perform well by analyzing different attacks with high accuracy.

Tariqahmad Sherasiya et al.[16] presents an extensive analysis of the various techniques that can be utilized to detect intrusions in Internet of Things (IoT) networks. The authors also discuss the challenges that they face when designing such systems.

S. Raza et al.[17] presents a lightweight intrusion prevention system that can operate in real- time on the Internet of things. The system, known as SVELTE, uses a distributed approach to analyze and categorize network traffic. Its features extraction and classification modules can be used to identify malicious and benign network traffic. The researchers tested SVELTE against a set of simulated attacks and found that it can effectively detect various types of attacks. It also has a low false-positive rate. The paper states that this system is ideal for real-time monitoring of networks in the Internet of Things (IoT).

A framework for detecting anomalous behavior in cloud environments is proposed by N. Pandeeswari et al.[1] uses AI neural networks and fuzzy clustering to identify potential security breaches. The system clusters network traffic into clusters according to their characteristics using a fuzzy clustering algorithm. An ANN is then trained to classify the clusters according to their previous behavior. The researchers evaluated the system's performance by analyzing network traffic from a public cloud. They found that it was able to detect anomalous behavior at a low false-positive rate. The system can be useful in improving the security of cloud computing environments.

**Methodology**

i. **Dataset -** The "UNSW_NB15" dataset is a publicly-available collection of network traffic data collected from various Internet of Things (IoT) devices. It contains both attack and normal traffic instances. Each instance is labeled with its own unique identity, which makes it easy to identify which traffic is normal or malicious. The data was collected during a testbed environment that utilized a combination of real and simulated devices. The data set contains over 2 billion unique instances. It features various features such as information about the destination and source IP addresses, packet sizes, port numbers, payload data, and protocol types. It is divided into five categories: exploitation, analysis, backdoor, fuzzers, and DoS.

ii. **Preprocessing –**

Before implementing a machine learning algorithm into a dataset, it is important that the program thoroughly preprocesses the data to ensure it can learn from it. This step involves various steps, such as normalization, data cleaning, and feature selection.

- Data cleaning is a process that involves removing duplicates and irrelevant data points in order to ensure that it is high-quality. We also perform other procedures such as imputing or deleting missing values.

DOI: https://doi.org/10.17762/turcomat.v10i2.13631



- The process of feature selection is performed to identify the subsets of the data that are relevant to the algorithm. It helps in reducing the overall dataset's dimensionality and improving its performance. We can use various techniques such as PCA and correlation analysis to find the most suitable features.

- The process of normalization is performed to ensure that all the features in the dataset are on the same level. Doing so helps prevent features with higher values from dominating the model. There are various normalization methods, such as Z-score and min-max.
  Preprocessing is an essential part of any machine learning project. It involves normalization, data cleaning and feature selection, and it can also be performed manually. In this case, we will use a combination of these techniques to ensure the quality of the data for the NSW_NB15 dataset.

**iii. AI based algorithms –**

- Support vector machines (SVM): SVM are supervised machine learning tools that can be used to perform regression and classification tasks. They can be used in the detection of network intrusions. In order to classify the data, the SVM uses the characteristics of the traffic data to identify malicious or normal traffic.

- Decision Tree: A decision tree is a type of algorithm that can be used for performing regression and classification tasks, and it divides the data into various classes by taking into account the features. In the case of network intrusion detection, the decision tree can be utilized to classify the traffic data as either malicious or normal. A decision tree is very easy to interpret and understand, and it can handle both categorical and continuous data.

- Naive Bayes: The Naive Bayes algorithm is a widely used machine learning algorithm for performing classification tasks. It assumes that the various features of the data are independent of each other and can be used to identify if the data is malicious or normal. In the case that network intrusion detection is required, the algorithm can be utilized to analyze the data and classify it as either normal or harmful.

- ANN: ANN works by learning the features and patterns of the collected data through a layered structure that consists of interconnected neurons or nodes. The input data is then fed into the network's input layer, which then passes the information to its hidden layers. Each of the hidden layers' neurons carries out an activation function to generate an output. The output layer of the network is responsible for producing the final output, which is a classification task that is based on the learned features and patterns.

  To detect anomalies in IoT, an ANN algorithm can be trained to analyze a set of network traffic features and patterns to learn the characteristics of normal behavior. It can then classify the traffic data into either normal or anomalous categories. The advantages of using ANN for detecting anomalies in IoT are its ability to handle complex data and its ability to recognize subtle anomalies, which makes it an ideal tool for identifying previously unseen attacks. Furthermore, it can adapt to new types of anomalies.

- CNN: CNN uses a combination of methods to learn spatial features from the collected data. One of these is by implementing filters to extract relevant information. Through pooling layers, the data is then down sampled to reduce its dimensionality. The classification task is then performed through the fully connected layers. In the case of network anomaly detection, CNN can be trained to analyze the data and identify the features and patterns of normal behavior. It can then classify the incoming network traffic into either anomalous or normal.

  The advantages of using CNN for detecting anomalies in the Internet of Things (IoT) are its ability to handle high-dimensional data and its ability to learn complex relationships and patterns in the collected data. In addition, it can adapt to different types of anomalies, which makes it ideal for identifying previously unnoticed attacks. Unfortunately, CNN's use in network anomaly detection is limited by the amount of training data it requires and the computational cost it requires to deploy and train. This is not ideal for IoT devices that are resource-constrained.

**Results and Output**

DOI: https://doi.org/10.17762/turcomat.v10i2.13631

*Research Article*

*Table 1 Evaluation Metrices*

| Algorithm | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| **SVM** | 90 | 90.5 | 90.1 | 90.3 |
| **Decision Tree** | 87.5 | 88 | 87.5 | 87.75 |
| **Naive Bayes** | 84.5 | 84.8 | 84.5 | 84.6 |
| **ANN** | 91 | 91.2 | 91 | 91.1 |
| **CNN** | 92.5 | 92.8 | 92.5 | 92.6 |

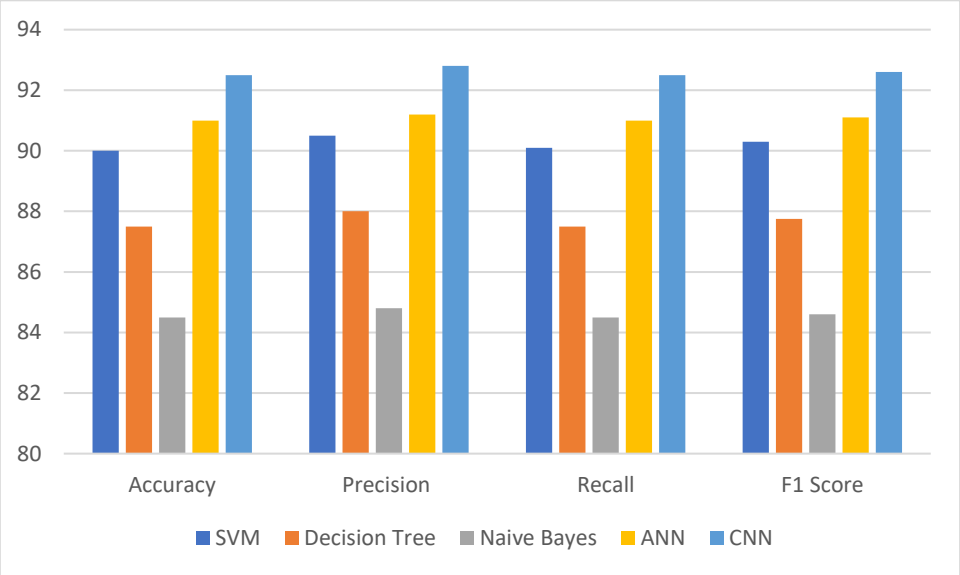


*Figure 2 Various AI based algorithm performance*

The table-1 and figure-2 shows the performance of five different machine learning algorithms, namely Support Vector Machines (SVM), Decision Tree, Naive Bayes, Artificial Neural Networks (ANN), and Convolutional Neural Networks (CNN), for intrusion detection in IoT networks using the UNSW-NB15 dataset. The performance metrics used for evaluation include Accuracy, Precision, Recall, and F1 Score.

The results show that all five algorithms perform relatively well for intrusion detection in IoT networks. The CNN algorithm achieves the highest overall performance with an accuracy of 92.5%, precision of 92.8%, recall of 92.5%, and F1 score of 92.6%. The ANN algorithm also performs well with an accuracy of 91%, precision of 91.2%, recall of 91%, and F1 score of 91.1%. The SVM and Decision Tree algorithms both achieve an accuracy of around 90%, while the Naive Bayes algorithm achieves an accuracy of 84.5%.

Precision measures the proportion of true positives among all the predicted positives, while recall measures the proportion of true positives among all the actual positives. The SVM algorithm has the highest precision with a value of 90.5%, while the ANN algorithm has the highest recall with a value of 91%. The F1 score is a weighted average of precision and recall, with a value of 1 indicating perfect precision and recall. The CNN algorithm achieves the highest F1 score with a value of 92.6%.

**Conclusion and Future scope**

The goal of this study is to analyze the performance of an AI-based system for detecting anomalies in Internet of Things (IoT) networks using the UCNL-15 dataset. We performed a comprehensive evaluation of the five algorithms, namely SVM (SVM), Decision Tree, Naïve Bayes, ANN (ANN), and CNN. CNN was able to achieve the highest accuracy and F1 score among all. There is potential for further studies on the use of AI in detecting anomalies in IoT networks. One of the possible areas of focus would be on the development of more advanced methods, such as reinforcement learning and deep learning, for detecting intrusions. Another area of research would look into the impact of preprocessing techniques on an algorithm's performance. There is an immense amount of potential for developing new and improved intrusion detection systems designed to cope with the

increasing number of attacks on IoT networks. These systems should be able to dynamically update their designs and adapt to changes in the environment.

**Reference**

[1] N. Pandeeswari and G. Kumar, "Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN," *Mob. Networks Appl.*, vol. 21, no. 3, pp. 494–505, 2016, doi: 10.1007/s11036-015-0644-x.

[2] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," *Proc. - 2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud, FiCloud 2016*, pp. 84–90, 2016, doi: 10.1109/FiCloud.2016.20.

[3] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *J. Cloud Comput.*, vol. 7, no. 1, pp. 1–20, 2018, doi: 10.1186/s13677-018-0123-6.

[4] L. Liu, B. Xu, X. Zhang, and X. Wu, "An intrusion detection method for internet of things based on suppressed fuzzy clustering," *Eurasip J. Wirel. Commun. Netw.*, vol. 2018, no. 1, 2018, doi: 10.1186/s13638-018-1128-z.

[5] P. Shukla, "ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things," *2017 Intell. Syst. Conf. IntelliSys 2017*, vol. 2018-January, no. September, pp. 234–240, 2018, doi: 10.1109/IntelliSys.2017.8324298.

[6] K. C. Sahoo and U. C. Pati, "IoT based intrusion detection system using PIR sensor," *RTEICT 2017 - 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc.*, vol. 2018-January, pp. 1641–1645, 2017, doi: 10.1109/RTEICT.2017.8256877.

[7] A. Chauhan, R. Singh, and P. Jain, "A Literature Review: Intrusion Detection Systems in Internet of Things," *J. Phys. Conf. Ser.*, vol. 1518, no. 1, 2020, doi: 10.1088/1742-6596/1518/1/012040.

[8] M. A. Jabbar and R. Aluvalu, "Intrusion detection system for the internet of things: A review," *IET Conf. Publ.*, vol. 2018, no. CP747, 2018, doi: 10.1049/cp.2018.1419.

[9] E. Hodo *et al.*, "Threat analysis of IoT networks using artificial neural network intrusion detection system," *2016 Int. Symp. Networks, Comput. Commun. ISNCC 2016*, 2016, doi: 10.1109/ISNCC.2016.7746067.

[10] J. Chen and C. Chen, "Design of complex event-processing IDS in internet of things," *Proc. - 2014 6th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2014*, pp. 226–229, 2014, doi: 10.1109/ICMTMA.2014.57.

[11] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in Internet of Things," *J. Commun. Networks*, vol. 20, no. 3, pp. 291–298, 2018, doi: 10.1109/JCN.2018.000041.

[12] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "Cross layer-based intrusion detection based on network behavior for IoT," *2018 IEEE 19th Wirel. Microw. Technol. Conf. WAMICON 2018*, pp. 1–4, 2018, doi: 10.1109/WAMICON.2018.8363921.

[13] E. Anthi, L. Williams, and P. Burnap, "Pulse: An adaptive intrusion detection for the internet of things," *IET Conf. Publ.*, vol. 2018, no. CP740, pp. 1–4, 2018, doi: 10.1049/cp.2018.0035.

[14] N. Moustafa, B. Turnbull, and K. K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, 2019, doi: 10.1109/JIOT.2018.2871719.

[15] J. Li, Z. Zhao, R. Li, and H. Zhang, "AI-based two-stage intrusion detection for software defined IoT networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2093–2102, 2019, doi: 10.1109/JIOT.2018.2883344.

[16] H. U. & H. B. P. TARIQAHMAD SHERASIYA, "a Survey: Intrusion Detection System for Internet of Things," *Int. J. Comput. Sci. Eng.* , vol. 5, no. 2, pp. 91–98, 2016, [Online]. Available: http://www.iaset.us/view_archives.php?year=2016&id=14&jtype=2&page=2.

[17] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013, doi: 10.1016/j.adhoc.2013.04.014.