

Course title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Assignment Report: Machine Learning and Deep Learning Solutions on Intrusion Detection Systems in IoT Networks.

student ID: 221000769

Student Name: Fares Ashraf Abdulghani

Problem Statement

The Internet of Things (IoT) technologies have been rapidly developed which has greatly enlarged the number of devices connected and traffic of networks. Although there are numerous advantages to IoT systems in various domains like healthcare, smart houses and industrial robots, there are severe security risks. Conventional security solutions and rule-based intrusion detection system solutions are not very useful in identifying sophisticated and dynamic cyber threats in IoT setup.

Recent studies have addressed how machine learning and deep learning methods may be used to improve intrusion detection systems. Researchers like Rahman et al. (2025) emphasized that AI-enabled intrusion detection systems may enhance the level of accuracy in detection and the minimization of false alarms in contrast to the conventional methods. Equally, Awajan (2023) proved that deep learning models are effective in identifying various forms of cyberattacks within the IoT networks with a high degree of accuracy. These findings were corroborated by other researchers like Islam et al. (2021) who assert that the deep learning models are more effective than the traditional machine learning algorithms in classification of advanced cyber threats.

Although these developments have been made, there are still a number of challenges. Most suggested systems have large computational complexity and need substantial processing power which is challenging to execute using resource-limited IoT devices. Moreover, other studies are restricted to laboratory experiments or particular types of attacks, which limits their practical use. As an example, Susilo & Sari (2020) concentrated primarily on DoS attacks, whereas Almiani et al. (2020) tested their model with the use of a single dataset.

Thus, it is necessary to create more effective intrusion detection systems that will consolidate high detection rates with lower computational demands to become suitable to the real-life IoT settings. This gap can be addressed in order to bring positive changes in the security and reliability of the IoT networks.

Research Objectives

The primary goal of the study is

- To assist intrusion detection systems in IoT networks with machine learning and deep learning methods.

The particular aims of this research are:

- To examine the current machine learning and deep learning methods in the context of intrusion detection systems of IoT networks.

- To find out the primary difficulties and drawbacks of existing IDS models, specifically regarding the complexity of the computations and the detection rate.
- To develop a better intrusion detection model that will be effective in detecting cyberattacks within the IoT.
- To assess the performance of the proposed model with the help of proper datasets and the performance indicators like accuracy, detection rate, and false alarm rate.
- To compare the proposed model with those in the literature of IDS so as to compare the gains in the performance of detection and efficiency.

Literature review

The paper of Rahman, Shakil, and Mustakim (2025) is a thorough survey of intrusion detection systems of the IoT networks. The aim of the research was to discuss the available IDS methods, specifically machine learning and deep learning algorithms. The authors examined the various datasets, assessment measures, and algorithm models applied in earlier researches. Their results show that AI-assisted IDS systems are highly effective to detect cyber threats and lower the false positives in comparison with conventional security systems. The advantages of this study are the fact that it embraces the IDS models, datasets and methods of evaluation comprehensively. Nevertheless, being a survey study, it does not have an experimental implementation and a given IDS model to be applied in practice. However, the paper is useful as it states the existing research problems of computational complexity and high false alarm rates of the IoT IDS systems.

Awajan (2023) has developed another significant study by suggesting an intrusion detection system built on deep learning, and it is designed specifically to work in an IoT environment. The primary goal of the study was the construction of an intelligent IDS that could identify malicious traffic to the IoT devices within real-time. The methodology concerned construction of a four-layered fully connected neural network that is used in analyzing network traffic to detect various kinds of attacks including: Distributed Denial of Service (DDoS), Blackhole, Sinkhole, Opportunistic Service, and Workhole attacks. The results of the experiment showed good performance in terms of detection, with the average accuracy of 93.74 percent and a detection rate of 93.21. The merit of the study is that the authors were able to develop a practical deep learning architecture that can identify different attacks successfully. The first weakness, however, is that the model has been tested mostly under laboratory conditions and its functionality in the real-world IoT conditions is still unknown.

The systematic review by Sharma, Kumar, and Dutta (2024) dwells on multi-objective optimization algorithms in intrusion detection of internet of things networks. The study aimed at studying the application of optimization methods to improve the performance of IDS systems by balancing various contradictory goals, which include detection, relevance of a feature, reduction of redundant features, and false alarms. The researchers conducted a review of numerous

algorithms and datasets employed in the literature of the study of the intrusion of IoT. Based on their results, they believe that multi-objective optimization methods can be used to enhance the IDS performance in the complex IoT setting. The key advantage of this study is that it is a comparative study of optimization algorithms and their efficiency. Nevertheless, the lack of experimental confirmation of the suggested methods is the limitation of the study because it is mainly based on the review of literature that is already existing.

The other applicable research is the one put forward by Islam et al. (2021), the study that examines machine learning-based intrusion detecting systems in IoT networks. The study will seek to compare shallow and deep machine learning algorithms in the detection of IoT attacks. The paper employed a number of benchmark data such as the NSL-KDD, IoTDevNet, DS2OS, lootID20 and loot Botnet data. The findings have shown that the deep-learning architecture including LSTM, Bi-LSTM, and deep neural networks is better than the conventional machine-learning-based algorithms like decision trees, random forests, support-vector-machines in identifying advanced cyberattacks. The comparison of various ML and DL models on a variety of datasets is the greatest asset of the present research as it offers an extensive picture of the performance of IDS. Nevertheless, another major challenge highlighted in the research is that deep learning model consumes a lot of computational power, and this may not be well-fit on resource constrained IoT devices.

On the same note, Susilo and Sari (2020) examined how deep learning algorithms can be used to detect denial-of-service (DoS) attacks in IoT networks. The aim of the study was to enhance security of IoT systems with the application of machine learning and deep learning algorithms. The researchers used Python based models like TensorFlow and Scikit-learn to implement their model. The results showed that the deep learning algorithms can achieve a significant increase in the effectiveness of the attack detection and overall performance of the IoT networks in terms of security. One of the key strengths of the research is the fact that the model offered is practically implemented on the basis of popular machine learning frameworks. Nevertheless, the research is predominantly DoS attacks, which restricts its use to other categories of cyber attacks.

Almiani et al. (2020) also provide another important contribution, suggesting a deep recurrent neural network-based intrusion detection system in the framework of IoT and fog computing setting. The purpose of the study was to develop an automated IDS, which will identify cyberattacks on cloud and fog computing infrastructures related to the IoT systems. The procedure entailed the introduction of a multi-layer recurrent neural network and its testing in the NSL-KDD data. The outcomes were found to perform well and be strong in a number of evaluation measures, such as accuracy, Mathew correlation coefficient, and Cohen Kappa. The main advantage of the study is its developed neural network design and evaluation measures.

Nevertheless, a single dataset is used, which can be seen as one of the limitations because it might influence the extrapolation of the results.

Comparing the results of the chosen studies, it is possible to outline a number of connections. The majority of the papers concur that machine learning and deep learning approaches are effective in enhancing the operation of intrusion detection systems in IoT networks. Specifically, deep learning models are always more accurate than the conventional machine learning algorithms are. The research carried out by Islam et al. (2021), Susilo, and Sari (2020), and Awajan (2023) is highly supportive of the idea that deep neural networks were used to identify sophisticated cyber threats. Nevertheless, certain contradictions are also presented about the real life implementation of these models. Although deep learning methods are more accurate, various reports point to issues such as complexity and resource usage, which can be difficult to realize in small devices in the IoT. Additionally, survey studies such as Rahman et al. (2025) and Sharma et al. (2024) emphasize the need for more efficient IDS models that balance detection performance with computational efficiency.

Summary Table of Reviewed Papers

Year	Authors	Methodology	Key Findings	Weaknesses / Limitations
2025	Rahman, Shakil & Mustakim	Survey of ML/DL-based IDS techniques	AI-based IDS improves detection accuracy and reduces false positives	No experimental implementation
2023	Awajan	Deep learning fully connected neural network	Achieved 93.74% accuracy in detecting multiple IoT attacks	Limited real-world evaluation
2024	Sharma, Kumar & Dutta	Systematic review of multi-objective optimization algorithms	Optimization techniques improve IDS performance and feature selection	Lack of experimental validation
2021	Islam et al.	Comparative ML and DL models using multiple datasets	Deep learning models outperform traditional ML algorithms	High computational requirements
2020	Susilo & Sari	Deep learning model for DoS attack detection	Improved accuracy and security in IoT networks	Focused only on DoS attacks

2020	Almiani et al.	Deep recurrent neural network IDS	Demonstrated robust performance using advanced evaluation metrics	Tested on limited datasets
------	----------------	-----------------------------------	---	----------------------------

Reference

Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory*, 101, 102031.

Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. *Computers*, 12(2), 34.

Islam, N., Farhin, F., Sultana, I., Kaiser, M. S., Rahman, M. S., Mahmud, M., Hosen, A. S. M. S., & Cho, G. H. (2021). Towards machine learning based intrusion detection in IoT networks. *Computers, Materials & Continua*, 69(1), 123–142.

Rahman, M. M., Al Shakil, S., & Mustakim, M. R. (2025). A survey on intrusion detection system in IoT networks. *Cyber Security and Applications*, 3, 100082.

Sharma, S., Kumar, V., & Dutta, K. (2024). Multi-objective optimization algorithms for intrusion detection in IoT networks: A systematic review. *Internet of Things and Cyber-Physical Systems*, 4, 258–267.

Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning algorithm. *Information*, 11(5), 279.