

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

List Of Contents

Chapter 1: Introduction	3
1.1 Introduction	3
1.2 Background	4
1.3 Problem Statement.....	5
1.4 Research Objectives	6
1.5 Scope of the study.....	7
Chapter 2 : Literature review	8
Chapter 3: Research Methodology	15
3.1 Research Methodology	15
3.2 Expected Results	16
3.3 Gantt Chart (Timeline).....	17
Reference	18

Chapter 1: Introduction

1.1 Introduction

The fast development of the Internet of Things (IoT) has dramatically altered the contemporary technological space by ensuring smooth connectivity of devices in different fields including healthcare, industry and smart cities. Nevertheless, this growth has not only come with significant security concerns, with the number of connected devices growing, so has the number of hackers and network attacks. The rise in the number of intrusion attempts is a direct consequence of the development of IoT ecosystems, and the issue of security is a crucial concern in these networks (Jayalaxmi et al., 2022).

Intrusion Detection Systems (IDS) have become indispensable in the process of tracking network traffic and detecting malicious actions. Such systems are critical in identifying unauthorized access and notifying administrators about possible threats. In addition, Intrusion Prevention Systems (IPS) enhance this feature by actively preventing attacks after they are identified (Jayalaxmi et al., 2022). Although they are vital, conventional IDS methods are limited to identify advanced and changing cyberattacks especially in dynamic IoT systems.

To address these constraints, in recent years, there has been a growing interest in the use of machine learning and deep learning methods in intrusion detection. Such methods are more accurate and flexible, as they acquire network behavior patterns using vast amounts of data and detect network behavior changes as anomalies. As an example, machine learning models, like the Random Forest, and deep learning models, like the Long Short-Term Memory (LSTM), have shown good results in cyberattack detection, obtaining high accuracy rates in IoT systems (Ali & Al-Sharafi, 2025).

Beyond this, comparative research has shown that deep learning models generally have a higher ability to detect complex and unknown threats than conventional machine learning methods, but issues like the cost of computation and deployment limitations persist (Ali et al., 2025). Thus, there is an increased necessity to create effective and scalable intrusion detection solutions to the peculiarities of IoT networks.

1.2 Background

The Internet of Things (IoT) concept describes a system of interconnected gadgets that interact and provide information with little human participation, allowing the automation and wise choice-making in various fields. IoT has major advantages, but this technology also brings various vulnerabilities because it is distributed, has limited resources of the device, and has heterogeneous network structures (Baich et al., 2022).

The deployment of intrusion detection systems is one of the main solutions in order to deal with these security issues. IDS are mostly divided into two major categories including signature-based detection systems (SIDS) and anomaly-based detection systems (AIDS). The signature-based systems are also good in identifying known attacks with minimal false alarms, but they cannot identify new or unknown attacks. Conversely, anomaly-based systems can recognize zero-day attacks by identifying abnormal behavior, but they might have more false positives (Rakine et al., 2024).

As artificial intelligence evolves, two methods of machine learning (ML) and deep learning (DL) have gained a wide following to enhance the performance of IDS. These methods have demonstrated better qualities of identifying different forms of cyberattacks, such as DDoS and zero-day attacks, as well as enhancing detection rates and minimizing false alarm rates (Almohaimed et al., 2025).

The effectiveness of these techniques is also supported by experimental studies. Indicatively, machine learning models like Decision Trees have presented very high accuracy with feature selection methods (Baich et al., 2022). Likewise, state-of-the-art deep learning models, including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) have shown high performance in both the analysis of complex network traffic and identification of sophisticated threats (Ali et al., 2025).

These developments notwithstanding, there are a number of challenges. The models of deep learning are also resource-intensive and therefore not easy to execute on the resource-constrained IoT devices. Also, problems like data imbalance, privacy and non-standardized evaluation structures remain barriers to the effective adoption of such systems (Almohaimeed et al., 2025).

1.3 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.

1.4 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.

1.5 Scope of the study

The current research is aimed at improving intrusion detection systems (IDS) in Internet of Things (IoT) networks by implementing machine learning and deep learning. The study is particularly aimed at comparing and assessing various artificial intelligence-based solutions in identifying cyber threats in IoT settings.

This paper will not discuss hardware-based security measures but only software-based intrusion detection techniques. It focuses on the usual forms of cyberattacks in the IoT networks, including DDoS, denial-of-service (DoS), and man-in-the-middle (MitM) attacks. Anomaly-based methods of detection are also highlighted in the study because they are effective in detection of unknown and zero-day attacks.

Moreover, the study will involve benchmark datasets to model the propagation of the IoT network traffic and test the performance of the chosen models. Standard evaluation measures are used in measuring performance; these measures include accuracy, detection rate, precision and false alarm rate.

The paper contrasts the classical machine learning algorithms, e.g., Decision Trees, Random Forest, and Support Vector Machines, with deep-learning models, e.g., Artificial Neural Networks (ANN) and Long Short-Term Memory (LSTM). Nonetheless, it is only implemented within controlled experimental settings, and does not involve real-time use within real-life IoT systems.

Also, this study is aimed at enhancing the efficiency of detection and taking into account the computational limitations of IoT devices. The concerns of privacy, encryption, and network infrastructure design are out of the scope of this study.

Chapter 2 : 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, IootID20 and Ioot 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.

Jayalaxmi et al. (2022) give a detailed overview of machine learning and deep learning solutions to intrusion detection and prevention systems in IoT environments. The main aim of the research was to review existing models of IDS and IPS and point out the weaknesses in them and suggest a hybrid model as a way of enhancing security. The methodology was oriented on the review of AI-based techniques, such as machine learning and deep learning, and their feasibility, compatibility, and real-time performance evaluation. The results suggest that hybrids between IDS and IPS features can contribute to IoT system detection and prevention abilities significantly. The main advantage of this research is the incorporation of risk factors analysis and a suggested hybrid model. But, just like any other survey-based research, it has not been experimentally validated, which restricts its practical usage.

The other study of interest is the one conducted by Ali & Al-Sharafi (2025), the researchers aim to identify Man-in-the-Middle (MitM) attacks in IoT networks with the help of machine learning and deep learning. The research was to compare the efficiency of models like Random Forest, Support Vector machine (SVM) and Long Short-Term Memory (LSTM). The experimental findings revealed Random Forest had the best accuracy of 94 percent whereas LSTM was good at working with sequential data with an accuracy of 92 percent. This study is strong because it

provides an experimental comparison of various algorithms when it comes to attack situations. The limitation however is that the study does not investigate other forms of cyber threats but only the MitM attacks, limiting its use in generalizing other types of cyber threats.

Rakine et al. (2024) review machine learning-based and deep learning-based intrusion detection systems in IoT networks in their conference paper. The intention of the research was to examine various IDS methods, such as signature-based and anomaly-based methods of detection. The results indicate that signature based systems can identify known attacks with a low number of false alarms, whereas anomaly based systems are more appropriate in identifying unknown attacks and zero-day attacks. The key strength of this research is that it categorizes the IDS strategies in a clear manner and describes the research obstacles. The research is, however, theoretical and does not have empirical validation.

Likewise, Baich et al. (2022) study is a comparative study of machine learning in intrusion detection in IoT networks. The study was focused on determining the best machine learning algorithms through experimentation with a popular data set. It was found that Decision Tree with Fisher Score feature selection had an accuracy of 99.26% and required minimum time to make predictions. This work has strength as it was supported by experiments and compared with performance. But, the weakness is that it primarily concentrates on machine learning methods without giving much attention to deep learning methods.

Moreover, the study by Almohaimeed et al. (2025) offers a recent overview of machine learning and deep learning applications to detect intrusion of the IoT. The paper examined various contemporary frameworks, such as hybrid frameworks, federated frameworks, and LSTM-based frameworks. These results suggest that the novel methods are more accurate, scalable, and detectable than the conventional

ones. The research also highlights the significance of applying the IDS with fog computing to detect in real-time. Its attention to recent developments and real-life issues is one of its main strengths. Nonetheless, some challenges like the complexity of the computations, privacy, and the absence of standard benchmarks are unsolved.

Lastly, the article by Ali et al. (2025) compares the deep learning and conventional machine learning methods of intrusion detection in large scale networks. The study was aimed at testing various models, such as CNN, LSTM, Random Forest, and K-Nearest Neighbors, and dealing with the problem of class imbalance with the help of such methods as SMOTE. The findings indicated that deep learning models had a high accuracy (up to 98%), and Random Forest was the best model with an accuracy of 99.9. The rigor of this study is that it is a full-scale experimental design with optimization on performance. Nevertheless, it emphasizes the accuracy vs. computational cost tradeoff that still is a significant issue with IDS implementation in IoT.

Discussion of Previous Studies

The overviewed research papers all indicate that machine learning (ML) and deep learning (DL) methods are relevant when enhancing intrusion detection systems (IDS) in internet of things (IoT) networks. The majority of the research findings suggest that the deep learning models, including LSTM, CNN, and deep neural networks, are more accurate in identifying complex and unknown cyberattacks than the traditional machine learning algorithms. As an example, such studies as (Islam et al., 2021) and (Ali et al., 2025) emphasize the effectiveness of deep learning models to work with large and complex data sets.

Conversely, a number of articles highlight the performance of machine learning models like Random Forest and Decision Trees to obtain high accuracy at a reduced

cost of computation as demonstrated in (Ali and Al-Sharafi, 2025) and (Baich et al., 2022). It means that even though deep learning has a more promising detection abilities, the traditional machine learning models remain helpful in terms of efficiency and deployment.

In addition, survey-based research like (Rahman et al., 2025), (Jayalaxmi et al., 2022), and (Almohaimeed et al., 2025) offer general descriptions of the IDS methods and underline such key issues as high false alarm rates, dataset constraints, and unstandardized evaluation frameworks. These researches help in the comprehension of the research environment, but not in practical application and experimental confirmation.

There are also studies which specialize in certain types of attacks, like DoS or MitM attacks, like (Susilo and Sari, 2020) and (Ali and Al-Sharafi, 2025), and hence are not applicable to a wider scope of IoT security. Other reports, like (Awajan, 2023), have been proved to be highly accurate, but they are mostly tested in regulated laboratory settings, which casts doubt on their applicability in the field.

On balance, although the current literature supports the ability of ML and DL solutions, it also demonstrates some shortcomings in the evaluation systems, the lack of practical testing, and the deficit in the balance between performance and computational efficiency.

Chapter 3: Research Methodology

3.1 Research Methodology

The research paper will employ an experimental and analysis research approach to explore how machine learning (ML) and deep learning (DL) can be used to boost intrusion detection systems (IDS) of Internet of Things (IoT) networks. The methodology is oriented to provide a systematic review of various models and respond to the challenges of the IoT environments, including limited computational resources and types of attacks.

The study starts with data gathering on benchmark datasets that are popular in intrusion detection studies, including NSL-KDD and IoT-based datasets. The data sets are used to train and test IDS models by having different types of network traffic both normal and malicious. The datasets comprise various categories of attacks like Denial of Service (DoS), Distributed Denial of Service (DDoS), and botnet attacks, making sure that they cover all real-life situations.

The preprocessing of data is done to enhance the quality of the data that is inputted. This process entails cleaning data, normalization and feature selection. Unnecessary and redundant elements are eliminated in order to minimize the computational complexity and improve the model performance. In IoT settings, especially with device resource constraints, feature selection techniques are of need.

After the preprocessing stage, several machine learning models are used, including Decision Tree, Random Forest, and Support Vector Machine (SVM). Simultaneously, deep learning networks such as Artificial Neural Networks (ANN) and Long Short-Term Memory (LSTM) are developed as well. The trained models are optimized by tuning the parameters to the best possible performance using the prepared datasets.

The models are evaluated based on various performance measures, such as accuracy, precision, recall (detection rate), and false alarm rate. These measures give a clear picture of the effectiveness of each model in identifying cyber threats but with minimal false categorizations. A comparative analysis is then carried out to determine the strengths and weaknesses of each approach.

3.2 Expected Results

The projected outcomes of this research are that both machine learning and deep learning methods will significantly enhance the performance of intrusion detection systems in IoT network. Deep learning models, especially LSTM, are expected to succeed in identifying more complex and novel cyberattacks because of their capabilities to capture the time-varying patterns of network traffic.

Simultaneously, machine learning models like the Random Forest are likely to show good performance at a reduced computational cost, and therefore, it is more appropriate to be used in resource-constrained IoT devices. Thus, there is a belief that a hybrid solution between ML and DL-based techniques will bring the most optimal balance between the accuracy of detection and computational efficiency.

Also, the model proposed is likely to show less false alarms than the conventional IDS systems, a vital consideration in enhancing the reliability of the system. The research also foresees the enhancement of detection rates of different categories of attacks, known and unknown threats.

On the whole, the findings will confirm that incorporating smart algorithms into IDS can help to strengthen the security of the IoT networks and overcome the current constraints of the existing systems.

3.3 Gantt Chart (Timeline)

Task	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6
Literature Review	✓	✓				
Data Collection		✓	✓			
Data Preprocessing			✓	✓		
Model Development (ML & DL)				✓	✓	
Model Evaluation					✓	✓
Results Analysis					✓	✓
Report Writing						✓
Final Review & Submission						✓

Reference

- Ali, M. A., & Al-Sharafi, S. A. H. (2025). Intrusion detection in IoT networks using machine learning and deep learning approaches for MitM attack mitigation. *Discover Internet of Things*, 5, Article 48.
- Ali, M. L., Thakur, K., Schmeelk, S., Debellio, J., & Dragos, D. (2025). Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study. *Applied Sciences*, 15(4), 1903. <https://doi.org/10.3390/app15041903>
- 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.
- Almohaimeed, M., Alyoubi, R., Aljohani, A., Alhaidari, M., Albalwy, F., Ghabban, F., Alfadli, I., & Ameerbakhsh, O. (2025). Use of machine learning and deep learning in intrusion detection for IoT. *Advances in Internet of Things*, 15(2). <https://doi.org/10.4236/ait.2025.152002>
- Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. *Computers*, 12(2), 34.
- Baich, M., Hamim, T., Sael, N., & Chemlal, Y. (2022). Machine learning for IoT-based networks intrusion detection: A comparative study. *Procedia Computer Science*, 215, 742–751. <https://doi.org/10.1016/j.procs.2022.12.076>
- 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.

- Jayalaxmi, P., Saha, R., Kumar, G., Conti, M., & others. (2022). Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. *IEEE Access*, 10, 1–1. <https://doi.org/10.1109/ACCESS.2022.3220622>
- 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.
- Rakine, I., El Guemmat, K., Ouahabi, S., Atouf, I., & Talea, M. (2024). IoT intrusion detection: A review of ML and DL-based approaches. In *2024 4th International Conference on...* IEEE.
- 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.