International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 05 May-2026 | Impact Factor: 3.5

Autoencoder Based Anomaly Detection in IOT Networks

Sharon Shine[*1], Mr. D. Ashok[*2]
[*1]Masters' Student , [*2]Assistant Professor
Department of Computer Science and Artificial Intelligence
Central University of Andhra Pradesh, Ananthapuramu, Andhra Pradesh
Email:sharonshine5768@gmail.com, ashokdhakuri@cuap.edu.in

How to Cite this Article:

Shine, S. (2026). Autoencoder Based Anomaly Detection in IOT Networks. International Journal of Creative and Open Research in Engineering and Management, 02(05). https://doi.org/10.55041/ijcope.v2i5.277

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.

https://doi.org/10.55041/ijcope.v2i5.277

Abstract - With the tremendous growth of the Internet of Things, the demand for intelligent security systems that can effectively detect anomalous network behaviour in real time has risen rapidly. Most traditional methods fail in detecting anomalies in the high-dimensional, dynamic, real-time IoT network traffic. In this paper, we investigate a system for automatically detecting anomalies in the IoT networks by using deep learning and machine learning approaches to develop an Autoencoder based anomaly detection framework.

For evaluating the proposed system we generate a synthetic IoT network traffic dataset with several network relevant features (such as packet size, byte count, packet type, connection information, etc.). After preparing the data with normalization and scaling, we used Autoencoder, Random Forest and Isolation Forest models to detect the network anomalies and evaluated our system using accuracy, precision, recall, F1-score and AUC.

The result of experiments indicates that our proposed Autoencoder model has detected anomalies with an accuracy of 94.7% and provides strong detection performance for anomalies within the network. These results suggest the advantage of using deep learning based models in detecting anomalies in complex IoT networks.

***Key Words*:** IoT Security, Anomaly Detection, Autoencoder

1.INTRODUCTION

Over the past few decades, the unprecedented progress of digital technology has changed radically the interaction between human, machines and their environment. As part of these technologies, the internet of things (IoT) becomes a most promising paradigms that allows interconnection among physical devices via the internet. IoT is composed of a number of devices embedded with sensors, actuators, software, and networks, that are able to detect, transmit, receive, and act on a physical phenomenon via their connection to internet to collect and transmit the data between these devices and to the cloud for data analysis and utilization in real time, such as a smart thermometer, a wearable

sports bracelet, an automated manufacture process system, etc. The goal of IoT is to develop a context-aware smart environment where devices communicate and collaborate without humans' involvement, that has become possible by the integration of various technologies such as wireless communications, cloud computing, big data analytics, artificial intelligence, etc. The benefits and potentials that IoT can offer are huge and make it becoming a core technology for many application domains such as health care, transportation, agriculture, etc.

The rapid expansion of IoT networks has led to an increasing demand for robust security mechanisms to mitigate cyber threats such as DDoS attacks, malware, and network intrusions. The adoption of SDN in IoT environments offers centralized control, programmability, and enhanced network management, making it an attractive solution for anomaly detection. However, the convergence of SDN and IoT introduces critical security vulnerabilities, such as unauthorized access, limited network visibility, and evolving attack patterns, necessitating the development of advanced DL-based AAD systems for SDN-IoT networks.[1]

Anomaly detection is a crucial component of ensuring reliability, safety, and efficiency in IoT systems. The rapid evolution of IoT systems, characterized by the creation of huge volumes of heterogeneous and high-dimensional data, renders anomaly detection even more relevant [2]. Anomalies, or outliers, can be defined as an observation or set of observations which deviate significantly from normal operation of the system.

The variable performance and distributed nature of the underlying resources that the IoT systems are running on complicates the development of these systems. IoT systems are continuously generating streams of data from various devices including sensors, actuators, and communication modules, making manual inspection of such enormous amounts of data impractical. In order for the IoT system to be efficient, an important feature will be to have the capacity to automatically detect anomaly occurring in the system's normal operation [3].

The growth of the Internet of Things (IoT) has enabled more and more devices to be connected over the network from industries to healthcare and smart cities. This has also introduced new challenges to cybersecurity as the variety of devices, communication protocols, and limited resources in IoT systems makes it an ideal target for cyber-attacks [4]. IoT network intrusion could lead to disruption, data breach, and a detrimental impact on connected devices and critical infrastructure. Traditional IDS systems based on signatures or static rules are inadequate to detect new threats and distributed attacks. This leads to the necessity to adopt novel detection methods based on Machine learning (ML) and Artificial Intelligence (AI) [5].

Autoencoder-based anomaly detection has gained considerable attention as an unsupervised approach which can detect anomalies without large volume of labeled data [6]. The application of intelligent detection methods is important to implement a secure, efficient and scalable mechanism to prevent IoT systems from cyber-attacks and unusual behavior [7].IoT systems produce unstructured data that requires a strong pattern recognition tool for anomaly detection to identify and categorize abnormalities. Several data types may be used to train deep learning algorithms. Deep learning algorithms may be effectively implemented to identify abnormal behaviors in various IoT networks, ensuring that data is sent securely and reliably in IoT networks.[8]

A number of studies have rigorously investigated anomaly detection in IoT networks with machine learning, deep learning and hybrid analytical models. Here, this section discusses the capabilities and limitations of these methods with respects to the aims described in this paper.[9]

Apart from real-time requirements, another significant challenge in IoT anomaly detection is handling them as quickly as possible since in applications such as industrial automation, healthcare, automated control systems, etc., timely detection of anomalies is often vital to prevent critical failures and human lives in danger. Late anomalies detection might lead to severe incidents as destruction of equipment, enormous financial damage, even death of people. The ability to make anomaly detection in real-time depends on well-optimized algorithms and efficient data processing mechanisms as well as low-latency communication. The trade-off between accuracy and performance on real-time system is still a complex problem. Constraints on the resources of IoT devices are other concerns on anomaly detection systems. Most IoT devices lack computational power, memory and energy compared to personal computer; thus the machine learning/deep learning algorithms for anomaly detection cannot be directly implemented. Resource constraint pushes people to use lightweight models or implement distributed systems such as edge and cloud. If data has to be sent to a central cloud for processing, latency, network burden and potential privacy issues may rise. Designing systems with efficiency on resources becomes essential for IoT anomaly detection. Security and privacy are two of the most severe challenges for IoT anomaly detection systems. Because of the vast number of devices connected, as well as lack of sufficient security mechanisms, IoT devices are highly vulnerable to attackers. The attackers can exploit various weaknesses of devices, networks, or communication protocol to obtain sensitive information and make false information. The anomaly detection system needs to detect these malicious behaviors. What else, privacy of collected sensitive data needs to be preserved as well, especially for those collected in health applications. For the dataset, the influential features associated with the energy consumption of IoT devices are extracted by analyzing the features of experiments through a covariance matrix and linear regression. Impressively, we verify a strong Protocol-Energy correlation as a first step.[10]

Scalability is one more major challenge in IoT anomaly detection. The rapidly increased number of connected devices, requiring the anomaly detection systems to handle data in massive volume. To overcome this, distributed systems along with suitable communication protocol, data storage technology and scalable algorithms are expected to play an important role.

Final challenge is evaluating and benchmarking anomaly detection algorithms. Because there is no standardized datasets, performance is evaluated on a variety of different criteria for various applications which makes performance comparison more complicated. However, a comprehensive understanding of anomaly detection algorithm performance can be achieved by establishing common benchmarks and evaluating datasets to foster progress in this research field. In addition, data quality is also a vital part for anomaly detection in IoT system. Noisy, missing and incomplete data might cause the detection model inaccurate. So preprocessing data such as normalization, filtering, imputation can greatly improve model's performance in actual applications.

Secondly, interpretation of anomaly detection model can be challenging when using deep learning methods. Although deep learning methods achieves great accuracy, it always works like a black box, that is, it is hard to understand reason behind a detection. However, in sensitive domains like healthcare and industry control system, understanding reason for detected anomalies is important for making correct actions. Thirdly, the implementation of anomaly detection in IoT must take consideration on existing systems and devices. Different communication protocol, heterogeneous devices and traditional systems might be incompatible, making the integration complex. A good designed integration scheme is critical for efficient detection and control. Finally, energy consumption is also one aspect needs to be considered since many IoT devices rely on battery power. If the model needs too much computational power, it will consume energy much quicker. So the balance between performance and energy consumption should be maintained in system design. Additionally, constant updates of anomaly detection system is necessary in the changing IoT environment to maintain the system's effectiveness against emerging types of attacks and anomalies

2. LITERATURE REVIEW

2.1 Foundations of IoT Anomaly Detection

In the past 10 years, rapid development in digital technologies have greatly impacted communication, computing and data processing systems. Internet of Things (IoT) one of the most widely accepted technologies in recent years that makes the interconnecting devices, sensors, and networks perform intelligent operations through communication

with each other, sending data with an intelligent real time manner [11]. Many application areas are the most well known using IoT, including healthcare monitoring, industrial automation, smart cities, transport and environmental monitoring. Because the amount of connected devices is enormous, the amount of generated data streams are also huge, in various heterogeneity and continuously varying ways [12].

However, due to many challenges in big data IoT applications. Some critical issues need to be discussed. The distributed and volatile characteristics of the IoT environments cause serious weakness in their fault tolerance against failures like hardware fault, sensors failures, communication breakdown, environmental impact and malicious attacks and etc. And these kinds of fault is always represented as some abnormal pattern data, which greatly influenced the quality and security of the system. [13]

Anomaly detection technique has been used in detecting such abnormal pattern. The definition of anomaly detection can be interpreted as the process of identifying data instances that are fundamentally different from the rest of the data [14]. By detecting such anomaly, IoT infrastructures can enhance its reliability, efficiency and security. For instance, anomaly can imply network intrusions, equipment failures, etc.

To tackle the aforementioned challenges, an efficient AD framework for IoT needs to be designed. It should take considerations of detection accuracy and computational complexity seamlessly. Hence, a hierarchical AD framework for IoT applications, the HADIoT, is proposed in this article. Three important issues are explored in the framework, i.e., the architecture design, accuracy improvement and reduction of computational complexity.[15]

2.2 Research Gap

The recent surge in IoT technologies has been accompanied by numerous significant issues related to network security, reliability, and real-time monitoring. IoT networks continuously produce massive quantities of heterogeneous and high dimensional data from a multitude of networked devices and sensors. Traditional anomaly detection methods like rule-based systems and statistical methods are ill-suited for a network characterized by constantly changing dynamics and high volumes of traffic as the nature of IoT network traffic is constantly shifting, requiring manual configuration and predefined rules to detect an anomaly. Such methods cannot effectively identify novel or complicated anomalies occurring in a vast IoT network.

With the application of machine learning approaches, anomaly detection methods are now able to learn from the network data itself. However, many supervised learning methods rely on having labelled data available and labelled data in real IoT systems is not easy to obtain. Moreover, a lot of machine learning models perform poorly with dynamically varying and high dimensional network traffic. Deep learning models like Autoencoders have shown promise in being able to learn the underlying patterns in data; however most existing works concentrate on generic data and do not properly consider real-time IoT anomaly detection or efficiency for varying and dynamic traffic data with regard to scalability.

An intelligent, efficient and scalable anomaly detection system that can appropriately handle the complex behaviour of IoT networks is necessary. This research proposes an anomaly detection system that makes use of Autoencoder along with two of the more commonly used models like Random Forest and Isolation Forest.

2.3 Proposed Contribution

The most significant contribution of this work is proposing a novel intelligent framework that uses an Autoencoder for an anomaly detection system that could enhance the security and reliability of IoT networks. In this approach, we combined the strengths of deep and machine learning to enhance abnormal traffic detection in IoT networks beyond simple rules based methods. Our Autoencoder based intelligent framework which coupled with two machine learning algorithms such as Random Forest and Isolation Forest provides a comparative, efficient, and scalable framework for anomalous traffic detection in changing environments of IoT networks.

Another vital contribution of our work is that, by employing pre-processing mechanisms like normalization, scaling and feature extraction for the high dimension IoT traffic data to make the model better. Unlike normal rule based approaches, our approach successfully learns the characteristics of network traffic, detects anomalous data points without relying on large labelled data sets. This attribute of the

proposed framework is beneficial for actual IoT deployments where reliable labelled anomaly data may not be readily available.

Lastly, the work further contributed with comprehensive comparative analysis by using evaluation metrics such as Accuracy, Precision, Recall, F1-score and AUC. Results obtained showed that the proposed Autoencoder based system was able to efficiently detect anomalies with a high degree of accuracy. Thus, providing the best results from the evaluation perspectives, it facilitates to perform scalable and adaptive anomaly detection system which can further be extended with more advanced approaches such as real time monitoring system, edge computing compatible systems, and improved deep learning architectures for the secure IoT systems at a large scale.

3.METHODOLOGY

3.1 Methodological Framework

This article aims to develop an intelligent anomaly detection system in an IoT environment using deep and machine learning. The massive volume, high dimensionality, and heterogeneity of data generated in the IoT network has led to the development of a systematic pipeline-based framework for efficiently processing the data, training, detecting anomalies and evaluating model performance, integrated with Autoencoder, Random Forest and Isolation Forest models to identify abnormal behaviour in the network to enhancing security and reliability in IoT devices. A synthetic IoT network traffic dataset that emulated the characteristics of a typical IoT network by incorporating a range of network features including size of packets, number of bytes transmitted, protocol and connection metrics was used in this study. Pre-processing steps such as data cleaning, normalization, feature scaling and train test split were performed on the dataset to allow better model stability and learning. An Autoencoder model was built as an unsupervised deep learning model for anomaly detection based on reconstruction error while Random Forest and Isolation Forest were built for comparison analysis. Model performance evaluation was done by considering a range of metrics namely Accuracy, Precision, Recall, F1-score and ROC-AUC to evaluate detection performance. The models and the entire framework were built in Python using popular libraries like TensorFlow, Keras, Scikit-learn, Pandas, NumPy and Matplotlib. The framework provides a modular and flexible architecture which can be extended and adaptable to other IoT network and security monitoring tasks.

3.2 System Workflow

The proposed anomaly detection system is designed with a systematic framework for detecting anomalies in an IoT network system. Initially, a synthetic IoT network traffic data set is created and obtained using various network features such as packet size, protocol type, byte count, communication time or duration, and communication details. This acquired data set is then processed using various cleaning and preprocessing steps which include data cleansing, normalization, features scaling, and splitting into train-test data sets in order to enhance the quality and effectiveness of the data.

Once the data has been processed, it is fed into the different anomaly detection systems for training and evaluation of their performance. An Autoencoder is trained to capture the normal behaviour of the IoT network traffic data using a variety of unsupervised deep learning techniques and a high reconstruction error would be calculated for an anomalous traffic in the test data set. Random Forest and Isolation Forest were also included to provide a comparative analysis of the performance. Finally, the results from each of these systems were measured using performance parameters, for example accuracy, precision, recall, F1-score and ROC-AUC. These were then visually interpreted to determine the accuracy of detection, a final comparison was done to identify the most accurate model for IoT anomaly detection. This system is a scalable and flexible solution capable of assisting in various future real time IoT security and monitoring applications.

3.3 Temporal Analysis Module

The Temporal Analysis Module detects variations in time based on analyzing the sequence and temporal aspects of the traffic in IoT network data. Because the network activities in IoT networks are dynamic and consist of continuous streams of data that are generated from sensors and the other IoT devices, it is important to observe variations that occur in the network activities to identify unexpected changes that can be the anomalies, such as increases in traffic. Anomaly

detection with a dynamic system requires considering time-dependent variations of the data for discovering anomalous changes that might not be captured otherwise.

In this system, the temporal analysis is conducted by observing parameters like packet sending rate, connection duration, number of bytes, traffic frequency, and so on in the network activities over a certain period of time. Variations in such parameters is then used by the module in order to describe traffic patterns and learn which ones deviate to an extent to be considered anomalies. A temporal pattern is particularly helpful to distinguish the momentary changes from stable anomalies in the network traffic in IoT networks. The analyzed data are then sent to the anomaly detection models in both the training and the evaluation phase. The Autoencoder is able to capture normal patterns in sequences of traffic and detect abnormalities whenever anomaly occurs resulting in high reconstruction errors due to unusual traffic behaviour.

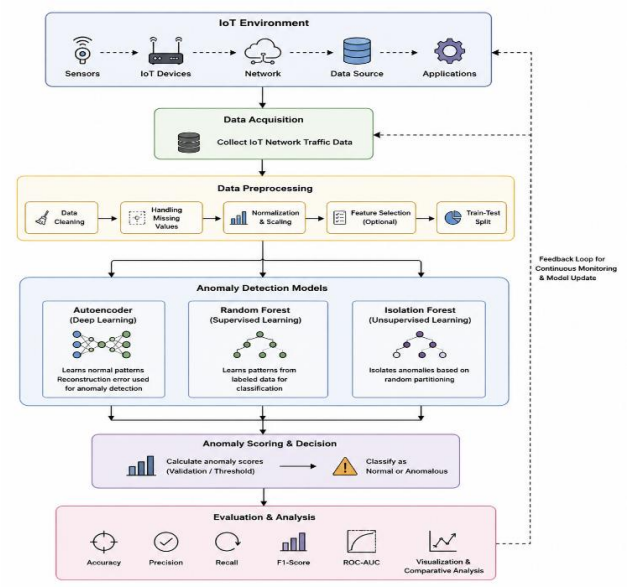


Figure 1: Overall System Architecture

3.4 Data Preprocessing and Model Design

The first step in the framework presented is data preprocessing, because IoT network data usually contains a considerable amount of noise, variety, and is high-dimensional. If data collected from IoT network traffic contain errors or inconsistencies and the scaling of features varies across the network, it can produce a negative effect on model accuracy. Therefore, the preprocessing steps involved in this framework include data cleaning, normalization, feature scaling, and train-test splitting. These steps are taken in order to produce a consistent and trustworthy dataset for the model. The system used an ensemble anomaly detection approach that combines both deep learning and machine learning models.

An Autoencoder model was used as the core unsupervised deep learning algorithm to detect the anomalies in the IoT network traffic. It learns the data (traffic) to compress and reconstruct. In this framework the higher reconstruction error values represent a more anomaly in the traffic within the network during the testing stage. A Random Forest model and an Isolation Forest model were used for comparison with the Autoencoder. A Random Forest model is a supervised machine learning algorithm used to classify network traffic according to certain learned pattern of decision trees. An Isolation Forest model is an unsupervised anomaly detection algorithm designed to efficiently isolate anomalies, based on Random Forests. Finally, accuracy, precision, recall, F1-score, ROC-AUC values were measured to evaluate the models.

4.RESULTS AND DISCUSSION

4.1 Experimental Findings

The experiments were designed and performed in order to analyze the efficiency of the presented framework on anomalous activity detection in IoT network environments. Thus the detection effectiveness of the designed models has been studied in detail and a comparative performance analysis was done utilizing qualitative and quantitative evaluation techniques. Experimental evaluation is considered to be an important part for the validation of a method and study of its capabilities in a real-world system like IoT network, since the network environment in IoT system is inherently dynamic.

For experimentation, a synthetic IoT network traffic dataset which contains both normal and attack traffic was utilized. The traffic data contains network features such as packet size, packet duration, byte count, network protocol, connection stats etc., simulating a typical IoT network system. As high volume of diverse and high dimensional data are produced in IoT systems; the usage of machine learning and deep learning based models are considered for better anomaly detection efficiency and accuracy.

The proposed framework utilizes an Autoencoder deep learning based model and it was compared with the supervised and unsupervised learning based models such as Random Forest, and Isolation Forest respectively. The performed experimental evaluation consists of data pre-processing, data normalization, model training and testing and performance assessment. The proposed framework was evaluated with certain metrics such as accuracy, precision, recall, F1-score and ROC-AUC. The results show that the Autoencoder model have an effective capability in detecting the anomalous activity in IoT network environments.

4.2 Setup of Experiments

The system configuration used in the experiment was developed to assess the efficiency of the proposed IoT anomaly detection framework under controlled conditions. All implementations were performed using the Python programming language, together with specific libraries such as NumPy, Pandas, Scikit-learn, TensorFlow, and Keras for handling and manipulating data and performing various machine and deep learning procedures. The entire experiments were performed on a local machine capable of providing sufficient computational power for model training, testing, and evaluation.

A set of synthetic IoT network traffic data was created for the experiments, representing both normal and abnormal network states. The dataset consisted of various network-related characteristics such as packet size, byte count, protocol information, communication time, and communication rates, to simulate an actual IoT network traffic pattern. For the purpose of adequate model learning and evaluation, the generated data was split into two sets, a training set (80% of the total data) and a testing set (20% of the total data).A number of data preprocessing operations like data cleaning, data normalization, data scaling, and missing value estimation were applied prior to model training. The Autoencoder model was configured for reconstruction-based learning of anomalous network activity, whereas the Random Forest and Isolation Forest models were employed for the sake of comparison. To estimate anomaly detection performance and model reliability in a uniform experimental setup, the models were assessed through the use of numerous performance metrics such as accuracy, precision, recall, F1-score, ROC-AUC, and reconstruction error.

4.3 Implementation and Result Analysis

The implementation of the proposed IoT anomaly detection framework integrated data preprocessing, training, testing, and anomaly detection within a single pipeline. In the beginning, normalization and feature scaling processes were applied to the IoT network traffic data for enhanced consistency and improved performance. The processed data was then passed to the Autoencoder, Random Forest, and Isolation Forest models for training and testing after pre-processing stages.

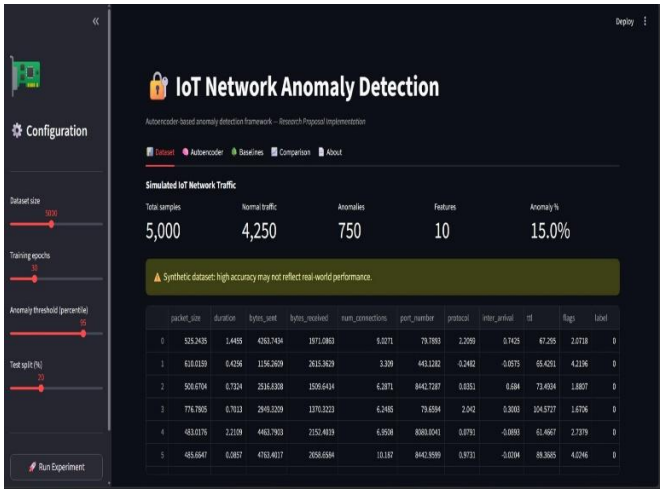
The Autoencoder model was built using a deep neural network structure, comprising an encoder and a decoder network layer. Encoder part compresses the original input data to low-dimensional feature representation and the decoder network rebuilds original input data from low-dimensional representation. The model was trained with the normal network traffic patterns and its key performance was examined using reconstruction error values. Higher reconstruction error was recognized as anomaly during test phase.

Both Random Forest and Isolation Forest were implemented to conduct comparative analysis of anomaly detection efficiency. Random Forest excelled in classification tasks with labeled data available while Isolation Forest accurately identified anomaly without required label data. Through the performance examination, Autoencoder achieved superior effectiveness in detection of intricate abnormal patterns. Using a deep learning and a machine learning models for anomaly detection provides improved robustness, scalability and effectiveness.

4.4 System Interface and Visualization Results

An important component of the proposed IoT anomaly detection framework is the development of an interactive and user-friendly system interface that supports model execution, data analysis, and result visualization. The interface was designed to simplify user interaction with the anomaly detection system while providing clear representation of model performance and detection outcomes. The system enables users to upload datasets, execute anomaly detection models, and visualize the generated results efficiently.

The interface is organized into multiple sections including dataset upload, preprocessing, model



selection, result analysis, and visualization. Users can upload IoT network traffic datasets, after which the system automatically performs preprocessing operations such as normalization and feature scaling before executing the selected anomaly detection model. The framework supports comparative analysis using Autoencoder, Random Forest, and Isolation Forest models to evaluate their performance on similar datasets.

Visualization techniques were incorporated to improve the interpretability of the anomaly detection process and model performance. Graphical outputs such as confusion matrices, feature importance graphs, correlation heatmaps, training loss curves, and comparative performance charts were generated to analyze detection capability and system behavior. These visualizations provide a better understanding of anomaly patterns and help evaluate the effectiveness of the proposed framework in detecting abnormal IoT network activities.

Figure 2: Integrated Dashboard Showing Dataset, Accuracy percentage, normal data and anomalies.

5.CONCLUSION

5.1 Summary of Findings

This research proposes an intelligent anomaly detection framework for IoT based on hybrid deep learning and machine learning approaches. With continuous increase of the number of IoT devices and ever growing network traffic data, security, reliability, and performance are of great concern to the system and require immediate attention. The aim of the proposed framework is to perform efficient abnormal network traffic detection, enhancing the performance for anomaly detection on the IoT environment.

An Autoencoder based deep learning framework was designed, integrating with Random Forest and Isolation Forest for comparison purpose. The Autoencoder was able to perform learning on the complicated patterns in the IoT network traffic data in a deep way and detected anomalies using the reconstruction error of the Autoencoder. Random Forest model exhibited effective classification performance on the labeled data, and Isolation Forest was able to detect anomalies efficiently based on unsupervised learning approach.

A pipeline structure (data pre-processing, feature scaling, model training, anomaly detection and evaluation) was implemented in the framework. Experiments conducted using metrics like accuracy, precision, recall, F1-score, ROC-AUC suggested that Autoencoder models was able to maintain robust anomaly detection performance and exhibited a strong performance for complicated patterns abnormal network traffic detection. Visualization and comparison also added interpretability and effectiveness for IoT anomaly detection system.

5.2 Research Directions For Future

While the proposed anomaly detection framework showed consistent performance for detecting abnormal behavior within the IoT network activities, there are various further improvements that are expected to take place during the subsequent study. One direction of importance is to design lightweight, efficient and computation inexpensive models that can be implemented on limited hardware resources available at IoT and edge devices. Model compression and edge deep learning can both achieve real-time anomaly detection at the same time reducing the computational cost.

Implementation of adaptive, and continuously learning models is the second direction where researchers can contribute in order to tackle the unpredictable IoT traffic nature andconcept drift, and to build more accurate and scalable IoT systems with deep learning. Deep learning architectures like CNNs, RNNs and deep hybrid models would be more promising to efficiently extract spatio-temporal features. These are potential areas to look at when enhancing detection accuracy and scalability of the system.

Utilizing real data-sets rather than the synthetic ones and integrating with various techniques of privacy preservation and security with the support of techniques of distributed computing will definitely enhance the generalization capability of the framework. Interpretable deep learning models by using Explainable Artificial Intelligence can also make the systems understandable by end users especially in those critical applications of the IoT system (e.g. Health-care, industrial automation and security).

REFERENCES

[1] T. Lakshan Yasarathna, M. Liyanage and N. -A. Le-Khac, "Deep Learning-Based Autonomous Anomaly Detection for Security in SDN-IoT Networks," in IEEE Open Journal of the Communications Society, vol. 6, pp. 8007-8048, 2025, doi: 10.1109/OJCOMS.2025.3610365. https://ieeexplore.ieee.org/document/11165121

[2] U. Ahmad, H. Song, A. Bilal, S. Saleem and A. Ullah, "Securing Insulin Pump System Using Deep Learning and Gesture Recognition," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018, pp. 1716-1719, doi: 10.1109/TrustCom/BigDataSE.2018.00258. https://ieeexplore.ieee.org/document/8456126

[3] J. Lee and K. Nam, "A Power Circulation Method Using Two Frequencies in Motor Emulator System," in IEEE Transactions on Energy Conversion, vol. 35, no. 4, pp. 1868-1876, Dec. 2020, doi: 10.1109/TEC.2020.2998090. https://ieeexplore.ieee.org/document/9103022

[4] Gomes, E.; Bertini, L.; Campos, W.R.; Sobral, A.P.; Mocaiber, I.; Copetti, A. Machine Learning Algorithms for Activity-Intensity Recognition Using Accelerometer Data. *Sensors* **2021**, *21*, 1214. https://doi.org/10.3390/s21041214

[5] R. S. Rajkumar, T. Jagathishkumar, D. Ragul and A. G. Selvarani, "Transfer Learning Approach for Diabetic Retinopathy Detection using Residual Network," 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2021, pp. 1189-1193, doi: 10.1109/ICICT50816.2021.9358468. https://ieeexplore.ieee.org/document/9358468

[6] T. T. Pham and Y. S. Suh, "Walking Step Length Estimation Using Waist-Mounted Inertial Sensors With Known Total Walking Distance," in *IEEE Access*, vol. 9, pp. 85476-85487, 2021, doi: 10.1109/ACCESS.2021.3087721. https://ieeexplore.ieee.org/document/9449934

[7] Zhang, T.; Sui, Y.; Wu, S.; Shao, F.; Sun, R. Table Structure Recognition Method Based on Lightweight Network and Channel Attention. *Electronics* **2023**, *12*, 673. https://doi.org/10.3390/electronics12030673

[8] I. Ullah and Q. H. Mahmoud, "A Framework for Anomaly Detection in IoT Networks Using Conditional Generative Adversarial Networks," in IEEE Access, vol. 9, pp. 165907-165931, 2021, doi: 10.1109/ACCESS.2021.3132127. https://ieeexplore.ieee.org/document/9632806

[9] M. M. Mahdi, A. Yousofi, R. Tati and O. Jasim Mohammed Al-Furaiji, "SCF-Net: A Lightweight Multi-Granular Feature Fusion Network for IoT Anomaly Detection," in IEEE Access, vol. 14, pp. 38460-38473, 2026, doi: 10.1109/ACCESS.2026.3671487. https://ieeexplore.ieee.org/document/11422855

[10] A. Shahnejat Bushehri, A. Amirnia, A. Belkhiri, S. Keivanpour, F. G. de Magalhães and G. Nicolescu, "Deep Learning-Driven Anomaly Detection for Green IoT Edge Networks," in IEEE Transactions on Green Communications and Networking, vol. 8, no. 1, pp. 498-513, March 2024, doi: 10.1109/TGCN.2023.3335342. https://ieeexplore.ieee.org/document/1032563

[11] Ayan Chatterjee, Bestoun S. Ahmed, IoT anomaly detection methods and applications: A survey, Internet of Things, Volume 19, 2022, 100568, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.10056

[12] Cook, Andrew & Misirli, Goksel & Fan, Zhong. (2019). Anomaly Detection for IoT Time-Series Data: A Survey. IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2019.2958185. https://www.researchgate.net/publication/340616360_Anomaly_Detection_for_IoT_Time-Series_Data_A_Survey

[13] Bhavsar, M., Roy, K., Kelly, J. *et al.* Anomaly-based intrusion detection system for IoT application. *Discov Internet Things* **3**, 5 (2023). https://doi.org/10.1007/s43926-023-00034-5

[14] Alsoufi, Muaadh & Md Siraj, Maheyzah & Ghaleb, Fuad & Abdulqader, Aya & Ali, Elham & O., Maryam. (2024). An Anomaly Intrusion Detection Systems in IoT Based on Autoencoder: A Review. 10.1007/978-3-031-59707-7_20. https://www.researchgate.net/publication/380630886_An_Anomaly_Intrusion_Detection_Systems_in_IoT_Based_on_Autoencoder_A_Review

[15] H. Chang, J. Feng and C. Duan, "HADIoT: A Hierarchical Anomaly Detection Framework for IoT," in IEEE Access, vol. 8, pp. 154530-154539, 2020, doi: 10.1109/ACCESS.2020.3017763. https://ieeexplore.ieee.org/document/9171239

.