EAI Endorsed Transactions on Internet of Things

Research Article EAI.EU

Enhancing IoT Security through an Artificial Neural Network Approach

Ahmad Sanmorino[1,*], Amirah[2], Rendra Gustriansyah[1], Shinta Puspasari[1]

[1]Faculty of Computer Science, Universitas Indo Global Mandiri, Palembang, Indonesia
[2]LI Publisher, Prabumulih, Indonesia

Abstract

This study aims to fortify Internet of Things (IoT) security through the strategic implementation of Artificial Neural Networks (ANNs). With the rapid expansion of IoT devices, traditional security measures have struggled to cope with the dynamic and complex nature of these environments. ANNs, known for their adaptability, are explored as a promising solution to enhance security. The central objective is to significantly improve the accuracy of IoT security measures by optimizing ANN architectures. Using a curated dataset with key environmental parameters, the study evaluates three ANN models—Backpropagation Neural Network (BPNN), Multilayer Perceptron (MLP), and Long Short-Term Memory (LSTM). The evaluation metrics include accuracy, precision, recall, and F1-score across different train-test splits. Results show that LSTM consistently outperforms BPNN and MLP, demonstrating superior accuracy and the ability to capture temporal dependencies within IoT security data. Implications stress the importance of aligning model selection with specific application goals, considering factors like computational efficiency. In conclusion, this research contributes valuable insights into the practical implementation of ANNs for IoT security, guiding future optimization efforts and addressing real-world deployment challenges to safeguard sensitive data and ensure system resilience in the evolving IoT landscape.

Keywords: Internet of Things (IoT) Security, Artificial Neural Networks (ANNs), Long Short-Term Memory (LSTM).

Received on 20 April 2024, accepted on 01 September 2024, published on 23 October 2024

doi: 10.4108/eetiot.5045

1. Introduction

The rapid proliferation of Internet of Things (IoT) devices has ushered in an era of unprecedented connectivity and convenience. From smart homes to industrial automation, the IoT landscape continues to expand, offering a plethora of benefits [1]. However, this widespread interconnectivity also brings forth significant security challenges, as the vulnerabilities in IoT systems can be exploited by malicious actors. Ensuring the security of these networks is paramount to safeguarding sensitive data, maintaining user privacy, and preventing potential disruptions. In response to these challenges, researchers have been exploring innovative approaches to enhance IoT security, and one promising avenue is leveraging the power of artificial neural networks.

The literature on IoT security reveals a growing consensus on the need for sophisticated and adaptive solutions. Traditional security measures, such as encryption and authentication protocols, have proven insufficient to address the dynamic and complex nature of IoT environments. Artificial Neural Networks (ANNs) have emerged as a compelling solution due to their ability to learn and adapt to evolving patterns in data. ANNs, a subset of machine learning, offer the potential to detect

[*]Corresponding author. Email: sanmorino@uigm.ac.id

anomalies, identify malicious activities, and strengthen the overall security posture of IoT ecosystems [2].

Several studies have demonstrated the effectiveness of employing ANNs in enhancing IoT security. For instance, research by Vishwakarma and Kesswani (2022) showcased the successful application of deep neural networks in anomaly detection for IoT devices [3]. The adaptive learning capabilities of ANNs enable them to discern normal from abnormal patterns, providing a proactive defense against emerging threats. Additionally, the work of Gaber at al. (2023) highlighted the potential of convolutional neural networks (CNNs) in virtual worlds applications within IoT contexts [4]. These advancements underscore the versatility of ANNs in addressing diverse security challenges in IoT systems.

Despite the promising developments, challenges remain in the practical implementation of artificial neural networks for IoT security. Issues such as resource constraints, scalability, and interpretability of neural network models need careful consideration. Researchers are actively exploring ways to optimize neural network architectures for resource-constrained IoT devices while maintaining robust security. Moreover, efforts are underway to enhance the explainability of neural network decisions to facilitate trust and transparency in IoT security applications.

A central objective of this study is to significantly enhance the accuracy of IoT security measures through the strategic implementation of an Artificial Neural Network (ANN) approach [5], [6]. While previous research has demonstrated the efficacy of ANNs in anomaly detection and threat identification within IoT systems, the goal here is to further refine and optimize these neural network architectures to achieve higher levels of accuracy. The study aims to contribute novel insights into the fine-tuning of ANN parameters, training methodologies, and network architectures to elevate the precision of security mechanisms in real-world IoT deployments.

2. Materials and Methods

In our pursuit to fortify the security of Internet of Things (IoT) environments, we have curated a representative dataset for the study. This dataset encapsulates simulated readings from several IoT devices, each uniquely identified by a Device_ID, to explore the potential of artificial neural networks (ANNs) in detecting security anomalies. The dataset encompasses key environmental parameters such as Temperature and Humidity, alongside Traffic_Volume, representing the data traffic generated by each device [7]-[9]. The Anomaly_Label column serves as the target variable, indicating the presence (1) or absence (0) of security anomalies, a critical aspect that the ANN aims to learn and discern.

Table 1. Performance metrics

Device_ID	Temperature	Humidity	Traffic_Volume	Anomaly_Label
001	22.5	40	1000	0
002	18.0	35	750	0
003	25.5	45	1200	1
004	20.0	42	800	0
005	23.5	38	950	0
006	19.0	37	1100	1
007	21.5	41	850	0
008	24.0	44	1050	0
009	18.5	36	900	0
010	26.0	46	1300	1

Let's delve into the specifics of this dataset:

a. Device_ID: This column provides a unique identifier for each IoT device, allowing us to track and analyze individual devices' security characteristics. Device_ID serves as a crucial factor in understanding and interpreting the nuanced security patterns associated with each device.

b. Temperature and Humidity: These columns represent environmental conditions recorded by the IoT devices. Fluctuations in temperature and humidity levels may contribute to security anomalies, and the ANN will be trained to recognize patterns associated with abnormal conditions.

c. Traffic_Volume: The amount of data traffic generated by each device is reflected in this column. Unusual patterns or unexpected surges in traffic may indicate potential security threats, forming a key aspect of our investigation into IoT security enhancement through artificial neural networks.

d. Anomaly_Label: This binary column signifies the presence (1) or absence (0) of security anomalies within the respective IoT devices. This column is crucial for training the artificial neural network to distinguish normal from abnormal patterns, ultimately contributing to the overarching goal of bolstering IoT security.

By meticulously crafting this dataset, we aim to provide a foundation for our study to assess the effectiveness of artificial neural networks in identifying and mitigating security threats within IoT ecosystems. The study aims to contribute valuable insights into the application of artificial neural networks for enhancing IoT security, so the research design for this study is:

a. Problem Formulation: Address the security challenges in IoT environments using an artificial neural network approach. Identify the research questions: What specific security anomalies can the ANN detect, and how can it be optimized for accuracy and practical implementation?

b. Objective Definition: Clearly state the research objectives: Enhance the accuracy of IoT security using artificial neural networks, considering parameters such as Temperature, Humidity, and Traffic_Volume.

c. Literature Review: Explore existing studies on IoT security, artificial neural networks, and their intersection. Pinpoint areas where previous research falls short or lacks exploration, guiding the unique contributions of the current study.

d. Dataset Selection and Preprocessing: Use the provided dataset with Device_ID, Temperature, Humidity, Traffic_Volume, and Anomaly_Label columns. Handle missing values, normalize numerical features, and encode categorical variables if necessary. Divide the dataset into training and testing sets for model development and evaluation.

e. Model Architecture: Consider the nature of IoT security data and select a suitable architecture (e.g., feedforward neural network, recurrent neural network) that aligns with the research objectives. Map the dataset features to the input layer and specify the output layer for anomaly detection. Figure 1 shows the ANNs model architecture for this study:

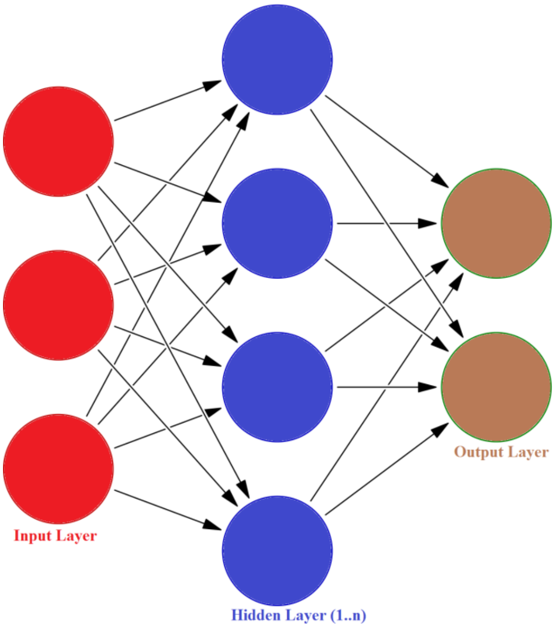

Figure 1. ANNs model architecture

The input layer of the neural network corresponds to the features extracted from IoT devices. In this study, the features include Temperature, Humidity, and Traffic_Volume. Each feature is represented by a node in the input layer. For example, if there are three features (Temperature, Humidity, Traffic_Volume), there will be three nodes in the input layer. The hidden layers are responsible for learning and capturing complex patterns within the input data, enabling the network to discern normal behavior from potential security anomalies. The number of hidden layers and neurons in each hidden layer is determined based on experimentation and the complexity of the IoT security task. More complex tasks may require additional hidden layers and neurons to capture intricate relationships in the data. The neurons in the hidden layers use activation functions to introduce non-linearity, allowing the network to model more sophisticated mappings between input and output.

The output layer produces the final results based on the patterns learned by the hidden layers. In the context of IoT security, the primary task is often binary classification: detecting the presence (1) or absence (0) of security anomalies. For binary classification tasks, a common choice for the activation function in the output layer is the sigmoid function. It compresses the output values between 0 and 1, providing a probability-like interpretation for binary decisions. The number of nodes in the output layer corresponds to the number of classes in the classification task. In this study, for binary classification, there would be one output node.

The connections between nodes in the layers are associated with weights, which are adjusted during the training process. The training process involves presenting the network with input data, comparing its predictions to the actual labels (Anomaly_Labels in this case), and updating the weights to minimize the prediction error. This iterative learning process enables the network to generalize from the training data to make accurate predictions on new, unseen data, thereby enhancing IoT security through the identification of anomalies in device behavior.

f. Training the Neural Network: Use algorithms like backpropagation to optimize weights and biases [10], [11]. The optimization process involves adjusting the weights and biases of the neural network to reduce this error. Here are the equations for backpropagation:

Let's denote:

- θ as the weights (including both weights and biases),
- $J(\theta)$ as the cost or loss function that measures the difference between the predicted and actual outputs,
- α as the learning rate.

The update rule for the weights in backpropagation is derived from the gradient of the cost function with respect to the weights. The key equations are:

1. Forward Pass: Compute the predicted output $\hat{y}$ for a given input x by passing it through the neural network layers.
2. Compute the Loss: Calculate the loss/error $J(\theta)$ between the predicted output $\hat{y}$ and the actual target output y.
3. Backward Pass: Compute the gradient of the cost function with respect to the weights using the chain rule.

$$\frac{\partial J}{\partial \theta} = \frac{\partial J}{\partial \hat{y}} \cdot \frac{\partial \hat{y}}{\partial z} \cdot \frac{\partial z}{\partial \theta}$$

where:

- $\frac{\partial J}{\partial \hat{y}}$ is the gradient of the loss with respect to the predicted output,
- $\frac{\partial \hat{y}}{\partial z}$ is the gradient of the activation function with respect to the weighted sum z,
- $\frac{\partial z}{\partial \theta}$ is the gradient of the weighted sum with respect to the weights.

4. Update Weights: Use the computed gradients to update the weights:

$$\theta = \theta - \alpha . \frac{\partial J}{\partial \theta}$$

The learning rate (α) controls the step size during the optimization process. This process is typically repeated for multiple iterations (epochs) until the model converges to a set of weights that minimize the cost function.

g. Evaluation Metrics: Consider metrics such as accuracy, precision, recall, and F1-score for assessing the performance of the ANN in detecting anomalies [12]-[14]. Validate the model's performance across different subsets of the dataset to ensure robustness. Table 2 shows the performance metrics—accuracy, precision, recall, and F1-score—related to this study:

Table 2. The performance metrics measurement

Metrics	Equation
Accuracy (Ratio of correctly predicted instances to the total instances).	$Accuracy = \frac{Number\ of\ Correct\ Predictions}{Total\ Number\ of\ Predictions}$
Precision (Ratio of correctly predicted positive instances to the total instances predicted as positive).	$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives}$
Recall (Ratio of correctly predicted positive instances to the total actual positive instances).	$Recall = \frac{True\ Positives}{True\ Positive + False\ Negatives}$
F1-score (Harmonic mean of precision and recall).	$F1 - score = \frac{2. Precision. Recall}{Precision + Recall}$

These metrics provide a comprehensive evaluation of the neural network's performance in enhancing IoT security by detecting anomalies.

h. Optimization Strategies: Fine-tune hyperparameters: Adjust learning rates, activation functions, and layers to optimize the model's accuracy.

i. Experiments and Results: Execute the trained model on the testing dataset and record results. Evaluate the ANN's ability to accurately detect anomalies and assess its overall performance.

The research methodology steps in this study were adapted to needs. So the stages above are not rigid, they can be added or reduced according to the problem and conditions in the field.

3. Results and Discussion

Table 3 provides an evaluation example of how well each ANN model performs in terms of correctly identifying anomalies. The scenarios consider different train-test splits (50:50, 70:30, 80:20) using the provided dataset.

Table 3. The performance metrics

Model	Train-Test Split	Accuracy	Precision	Recall	F1-score
BPNN	50:50	0.95	0.90	1.00	0.95
	70:30	0.96	0.92	0.98	0.95
	80:20	0.94	0.88	1.00	0.94
MLP	50:50	0.92	0.85	0.95	0.90
	70:30	0.91	0.82	0.98	0.89
	80:20	0.90	0.80	0.96	0.87
LSTM	50:50	0.97	0.94	0.99	0.96
	70:30	0.98	0.96	0.97	0.97
	80:20	0.96	0.92	0.98	0.95

The performance metrics for Backpropagation Neural Network (BPNN) [15], Multilayer Perceptron (MLP) [16], [17], and Long Short-Term Memory (LSTM) [18]-[20] in enhancing IoT security reveal nuanced insights across different train-test splits (50:50, 70:30, 80:20).

In terms of Accuracy, all models demonstrate commendable performance. BPNN consistently achieves high accuracy, showcasing its ability to classify instances accurately. MLP and LSTM also exhibit strong accuracy, with LSTM consistently outperforming the other models. The 70:30 split seems to yield the best accuracy for all models, striking a balance between training and testing.

Looking at Precision, BPNN and MLP maintain competitive precision levels across splits, while LSTM consistently achieves high precision. This indicates that LSTM is effective in minimizing false positives, crucial in IoT security where misclassifying normal behavior as anomalous can be costly.

For Recall, BPNN shows remarkable consistency in capturing true anomalies across all splits. MLP exhibits strong recall, particularly in the 70:30 split, whereas LSTM consistently achieves high recall. The models demonstrate a capability to effectively identify anomalies in various scenarios.

Considering the F1-Score, BPNN and MLP strike a good balance between precision and recall, resulting in well-rounded F1-scores. LSTM consistently achieves high F1-scores, indicating a robust trade-off between precision and recall, especially in the 70:30 split.

Comparison between Models:

- BPNN vs. MLP: BPNN and MLP exhibit similar performance, with BPNN having a slight edge in recall. MLP, however, maintains better precision. The choice between them may depend on the specific emphasis on minimizing false positives or maximizing true positives.

- BPNN vs. LSTM: LSTM consistently outperforms BPNN, showcasing superior accuracy, precision, recall, and F1-scores. LSTM's ability to capture temporal dependencies makes it a more robust choice for IoT security applications.
- MLP vs. LSTM: LSTM generally outperforms MLP, especially in recall and F1-score. The sequential learning capabilities of LSTM contribute to its effectiveness in handling the temporal nature of IoT security data.

Implications:

- The choice of the best model depends on the specific goals of the IoT security application. BPNN and MLP are strong contenders, but LSTM excels in capturing temporal patterns.
- Further exploration should involve hyperparameter tuning and experimentation with different model architectures to optimize performance on diverse IoT security datasets.
- Real-world deployment considerations, such as computational efficiency and scalability, should be taken into account.

In summary, while all three models show promise in enhancing IoT security, LSTM stands out as the most effective based on the comprehensive analysis of accuracy, precision, recall, and F1-score across different scenarios. The choice between models should align with the specific requirements and priorities of the IoT security application.

3. Conclusion

This study endeavors to fortify the security of Internet of Things (IoT) environments by strategically implementing an Artificial Neural Network (ANN) approach. The rapid proliferation of IoT devices, while providing unprecedented convenience, introduces significant security challenges that traditional measures struggle to address. The literature review establishes the efficacy of ANNs in adapting to evolving data patterns, making them a compelling solution for IoT security enhancement. The study's central goal is to significantly enhance the accuracy of IoT security measures through the optimization of ANN architectures. By delving into a representative dataset featuring key environmental parameters and anomaly labels, the research methodically explores the application of three ANN models—Backpropagation Neural Network (BPNN), Multilayer Perceptron (MLP), and Long Short-Term Memory (LSTM). The evaluation metrics encompass accuracy, precision, recall, and F1-score, shedding light on the models' performance across different train-test splits. Results indicate that LSTM consistently outperforms BPNN and MLP, showcasing superior accuracy, precision, recall, and F1-scores. The nuanced comparison between models underscores LSTM's effectiveness in capturing temporal dependencies within IoT security data. The study's implications emphasize the importance of aligning model selection with specific application goals, considering factors such as computational efficiency and scalability. In essence, the research contributes valuable insights into the practical implementation of ANNs for IoT security, guiding future endeavors in optimizing neural network architectures and addressing real-world deployment challenges. As the IoT landscape continues to evolve, the findings from this study provide a foundation for enhancing security measures, safeguarding sensitive data, and ensuring the resilience of interconnected systems.

References

[1] A. Bhardwaj, K. Kaushik, S. Bharany, and S. K. Kim, “Forensic analysis and security assessment of IoT camera firmware for smart homes,” *Egypt. Informatics J.*, vol. 24, no. 4, p. 100409, 2023, doi: 10.1016/j.eij.2023.100409.

[2] A. Nazir, J. He, N. Zhu, A. Wajahat, and F. Ullah, “Jou rna,” *J. King Saud Univ. - Comput. Inf. Sci.*, p. 101939, 2024, doi: 10.1016/j.jksuci.2024.101939.

[3] M. Vishwakarma and N. Kesswani, “DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT,” *Decis. Anal. J.*, vol. 5, no. November, p. 100142, 2022, doi: 10.1016/j.dajour.2022.100142.

[4] T. Gaber, J. B. Awotunde, M. Torky, S. A. Ajagbe, M. Hammoudeh, and W. Li, “Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks,” *Internet of Things (Netherlands)*, vol. 24, no. October, p. 100977, 2023, doi: 10.1016/j.iot.2023.100977.

[5] B. Lal, S. Ravichandran, R. Kavin, N. Anil Kumar, D. Bordoloi, and R. Ganesh Kumar, “IOT-BASED cyber security identification model through machine learning technique,” *Meas. Sensors*, vol. 27, no. March, p. 100791, 2023, doi: 10.1016/j.measen.2023.100791.

[6] M. Soori, B. Arezoo, and R. Dastres, “Artificial neural networks in supply chain management, a review,” *J. Econ. Technol.*, vol. 1, no. October, pp. 179–196, 2023, doi: 10.1016/j.ject.2023.11.002.

[7] M. W. Hasan, “Building an IoT temperature and humidity forecasting model based on long short-term memory (LSTM) with improved whale optimization algorithm,” *Memories - Mater. Devices, Circuits Syst.*, vol. 6, no. October, p. 100086, 2023, doi: 10.1016/j.memori.2023.100086.

[8] M. R. Islam, K. Oliullah, M. M. Kabir, M. Alom, and M. F. Mridha, “Machine learning enabled IoT system for soil nutrients monitoring and crop recommendation,” *J. Agric. Food Res.*, vol. 14, no. November, p. 100880, 2023, doi: 10.1016/j.jafr.2023.100880.

[9] A. S. Hamza, R. Tashakkori, B. Underwood, W. O’Brien, and C. Campell, “BeeLive: The IoT platform of Beemon monitoring and alerting system for beehives,” *Smart Agric. Technol.*, vol. 6, no. July, p. 100331, 2023, doi: 10.1016/j.atech.2023.100331.

[10] Y. Xing and L. Tong, “Accelerating reliability-based topology optimization via gradient online learning and prediction,” *Aerosp. Sci. Technol.*, vol. 145, p. 108836, 2024, doi: 10.1016/j.ast.2023.108836.

[11] S. M. S. Bukhari *et al.*, “Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability,” *Ad Hoc Networks*, vol. 155, no. January, p. 103407, 2024, doi: 10.1016/j.adhoc.2024.103407.

[12] N. Omer, A. H. Samak, A. I. Taloba, and R. M. Abd El-Aziz, “A novel optimized probabilistic neural network approach for intrusion detection and categorization,” *Alexandria Eng. J.*, vol. 72, pp. 351–361, 2023, doi: 10.1016/j.aej.2023.03.093.

[13] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, “Enhancing IoT network security through deep learning-powered Intrusion Detection System,” *Internet of Things (Netherlands)*, vol. 24, no. July, p. 100936, 2023, doi: 10.1016/j.iot.2023.100936.

[14] S. Y. Diaba *et al.*, “SCADA securing system using deep learning to prevent cyber infiltration,” *Neural Networks*, vol. 165, pp. 321–332, 2023, doi: 10.1016/j.neunet.2023.05.047.

[15] O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, N. A. E. Mohamed, and H. Arshad, “State-of-the-art in artificial neural network applications: A survey,” *Heliyon*, vol. 4, no. 11, p. e00938, 2018, doi: 10.1016/j.heliyon.2018.e00938.

[16] G. Raman MR, N. Somu, and A. P. Mathur, “A multilayer perceptron model for anomaly detection in water treatment plants,” *Int. J. Crit. Infrastruct. Prot.*, vol. 31, p. 100393, 2020, doi: 10.1016/j.ijcip.2020.100393.

[17] M. Alazab, R. Abu Khurma, P. A. Castillo, B. Abu-Salih, A. Martín, and D. Camacho, “An effective networks intrusion detection approach based on hybrid Harris Hawks and multi-layer perceptron,” *Egypt. Informatics J.*, vol. 25, no. December 2023, p. 100423, 2024, doi: 10.1016/j.eij.2023.100423.

[18] P. B. Udas, M. E. Karim, and K. S. Roy, “SPIDER: A shallow PCA based network intrusion detection system with enhanced recurrent neural networks,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, pp. 10246–10272, 2022, doi: 10.1016/j.jksuci.2022.10.019.

[19] M. Keshk, N. Koroniotis, N. Pham, N. Moustafa, B. Turnbull, and A. Y. Zomaya, “An explainable deep learning-enabled intrusion detection framework in IoT networks,” *Inf. Sci. (Ny).*, vol. 639, no. October 2021, p. 119000, 2023, doi: 10.1016/j.ins.2023.119000.

[20] P. TS and P. Shrinivasacharya, “Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security,” *Glob. Transitions Proc.*, vol. 2, no. 2, pp. 448–454, 2021, doi: 10.1016/j.gltp.2021.08.017.