

Enhanced smart farming security with class-aware intrusion detection in fog environment

Selvaraj Palanisamy¹, Radhakrishnan Rajamani¹, Prabakaran Pramasivam², Mani Sumithra³,
Prabu Kaliyaperumal¹, Rajakumar Perumal⁴

¹School of Computer Science and Engineering, Galgotias University, Greater Noida, India

²Department of Electrical and Electronics Engineering, Chennai Institute of Technology, Chennai, India

³Department of Information Technology, Panimalar Engineering College, Chennai, India

⁴Department of Computer Science and Applications, Sharda School of Computing Science and Engineering, Sharda University, Greater Noida, India

Article Info

Article history:

Received Nov 25, 2024

Revised Jun 21, 2025

Accepted Aug 6, 2025

Keywords:

Agriculture 4.0

Anomaly detection

Autoencoder

IoT

Multi-class classification

SoftMax classifier

ABSTRACT

The adoption of the internet of things (IoT) in smart farming has enabled real-time data collection and analysis, leading to significant improvements in productivity and quality. However, incorporating diverse sensors across large-scale IoT systems creates notable security challenges, particularly in dynamic environments like Fog-to-Things architectures. Threat actors may exploit these weaknesses to disrupt communication systems and undermine their integrity. Tackling these issues necessitates an intrusion detection system (IDS) that achieves a balance between accuracy, resource optimization, compatibility, and affordability. This study introduces an innovative deep learning-driven IDS tailored for fog-assisted smart farming environments. The proposed system utilizes a class-aware autoencoder for detecting anomalies and performing initial binary classification, with a SoftMax layer subsequently employed for multi-class attack categorization. The model effectively identifies various threats, such as distributed denial of service (DDoS), ransomware, and password attacks, while enhancing security performance in environments with limited resources. By utilizing the Fog-to-Things architecture, the proposed IDS guarantees reliable and low-latency performance under extreme environmental conditions. Experimental results on the TON_IoT dataset reveal excellent performance, surpassing 98% accuracy in both binary and multi-class classification tasks. The proposed model outperforms conventional models (convolutional neural network (CNN), recurrent neural network (RNN), deep neural network (DNN), and gated recurrent unit (GRU)), highlighting its superior accuracy and effectiveness in securing smart farming networks.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Prabu Kaliyaperumal

School of Computer Science and Engineering, Galgotias University

Greater Noida, Delhi NCR, India

Email: mega.prabu@gmail.com

1. INTRODUCTION

The internet of things (IoT) has brought significant changes to traditional network communication methods by facilitating coordinated connections among diverse devices. The expanding range of IoT applications highlights its promising impact on enhancing communication efficiency, paving the way for various scientific breakthroughs [1], [2]. Smart farming represents a modern method of agricultural production that combines data technology, informed decision-making, and intelligent control systems to

enhance both the productivity and quality of farming [3]. However, deploying IoT in smart farming covering areas like water, soil, and air management is often challenged by extreme environmental conditions, such as strong winds, snowfall, flooding, and diverse landscapes [4]. These implementations form the foundation for various smart farming applications, such as monitoring water quality, precision farming, livestock health, and climate conditions, facilitating real-time data collection and analysis [5]. Fog computing is seen as an ideal solution for enabling efficient communication in IoT systems used within the challenging environments of smart farming. The primary goal of fog computing is to handle data processing as close as possible to the source of data generation [6], [7]. By minimizing the amount of data sent over the network, the Fog-to-Things approach helps lower latency and conserves network resources. In large-scale, centralized extreme environments, it is necessary to store data at a central site for monitoring and future use [6]. Fog computing can also play a role by storing data at an appropriate local site that is accessible to all participating nodes. In the challenging conditions of smart agriculture, edge computing can enhance communication efficiency, load distribution, and network reliability, marking a significant step toward more dependable operations [8], [9].

El-Ghamry *et al.* [10] introduces a convolutional neural network (CNN) based intrusion detection system (IDS) for smart farming, leveraging deep learning techniques to secure agricultural IoT networks. Evaluated using the NSL-KDD dataset, the system emphasizes data pre-processing, feature selection, and hyperparameter optimization to achieve over 99% detection accuracy, precision, and F1-scores. While it showcases the importance of machine learning (ML) for securing smart farming, class imbalance in the dataset may impact detection performance for rarer attack types. Alanazi and Alrashdi [11], a smart agriculture system integrating deep learning methods like CNN and long short-term memory (LSTM) is developed to detect anomalies in real-time. Designed to operate at the network edge, it reduces latency and enables timely interventions for crop health and resource management. The study highlights distributed denial of service (DDoS) attack prevention, which could disrupt agricultural operations, but it acknowledges that other cybersecurity threats exist, though they are not deeply explored. Aldhyani and Alkahtani [12] discusses using deep learning, particularly CNN and LSTM, for cyber threat detection in Agriculture 4.0. It stresses the need to protect IoT networks from DDoS attacks. The models aim to enhance agricultural output quality and quantity through AI and cloud computing, while addressing cybersecurity risks. However, challenges like false alarms or missed detections could impact the system's efficiency and security. Zwayed *et al.* [13] presents a hybrid feature selection approach with BiLSTM for intrusion detection in fog computing environments, handling the complexities of high-dimensional IoT data. With accuracy rates of 98.42% on the TON_IoT dataset and 98.7% on the BoT-IoT dataset, this method improves both efficiency and accuracy, showcasing deep learning's role in securing IoT networks. Dash *et al.* [14] introduces a deep learning framework for anomaly detection in IoT networks using BiLSTM and gated recurrent unit (GRU), optimized by the JAYA algorithm. The models, JAYA-BiLSTMIDS and JAYA-GRUIDS, achieved accuracy rates of 99.65% and 99.42%, respectively, with minimal false alarms. A fog computing framework for Unmanned aerial vehicle (UAV) assisted smart farming, as discussed in [15], addresses energy-related attacks, focusing on DDoS and unauthorized access. By using ML for intrusion detection, the system aims to secure UAV operations, enhancing data reliability and agricultural productivity. Finally, Lawall *et al.* [16], a framework for mitigating DDoS attacks in IoT networks via fog computing combines signature- and anomaly-based detection. ML enables rapid attack detection, improving resource efficiency and security. The methodology includes comparing the k-NN classifier's performance to other models, demonstrating enhanced accuracy in network traffic anomaly detection. The studies highlight deep learning's potential in IoT security, urging solutions for class imbalance, real-time scalability, and evolving threats.

The integration of diverse sensors in smart farming communication brings forth numerous security challenges. This is particularly significant in expansive networks, where the presence of heterogeneous sensors can potentially compromise the system's integrity. In a Fog-to-Things architecture, establishing a robust communication framework is critical to facilitating seamless interactions [17]. Malicious actors within the network may disrupt the communication infrastructure, leading to erratic and unpredictable interactions [18]. These complex scenarios necessitate effective security measures to address the evolving challenges. An effective IDS can reduce the likelihood of attacks by identifying malicious entities within the network promptly [19]. In recent years, deep learning (DL)-based IDS have become increasingly popular due to their rapid anomaly detection capabilities [20]. Additionally, DL-based IDS yield more precise outcomes compared to traditional ML methods [21]. In these systems, the model is initially trained on an extensive dataset that reflects potential attacks within the specific application area. Subsequently, the system is implemented in a real-time smart farming environment, where it detects similar attack patterns. While DL-based IDS offers robust monitoring of potential threats, developing an appropriate IDS remains a complex challenge [22], [23]. Before developing a DL-based IDS, various factors, including resource usage, compatibility, security requirements, system flexibility, latency and cost, must be considered [24].

This paper presents an effective DL-driven IDS designed for fog-assisted smart farming in challenging IoT environments. This IDS utilizes a hybrid approach, incorporating an autoencoder neural network for anomaly detection and initial binary classification. The encoded features in the latent space are further analyzed using a SoftMax classifier to achieve multi-class attack classification, which is crucial for improved prevention and detecting threats at the network edge. The proposed model effectively detects a wide range of attack types in smart farming, including backdoor, DDoS, injection, password attacks, ransomware, scanning, XSS, and others. This approach utilizes a class-aware autoencoder that combines a reconstruction objective with an integrated classification layer. During training, the model optimizes both reconstruction and classification errors, allowing it to learn the structure of each class while carrying out direct classification. To address the challenges of cloud-based deployment in extreme environments, we propose a Fog-to-Things deployment architecture for the IDS. Evaluations on the TON_IoT [25] datasets demonstrate the model's strong performance across standard evaluation metrics, reinforcing its suitability for such environments. Furthermore, to establish the effectiveness of the proposed IDS, we compare it against baseline models and recent state-of-the-art methods.

The structure of this article is as follows: section 2 outlines the proposed DL-based attack detection framework. In section 3 presents the evaluation of the proposed IDS and compares its performance with state-of-the-art methods. Lastly, section 4 concludes the paper and discusses potential future research directions.

2. RESEARCH METHOD

This section proposes a class-aware autoencoder framework for anomaly detection and attack classification in an IoT-enabled smart farming environment, using both binary and multi-class approaches for effective attack identification. The TON_IoT dataset serves as the data source for model input. As illustrated in Figure 1, the method employs an autoencoder neural network for anomaly detection, performing an initial binary classification. The encoded representation in the latent space is then processed by a SoftMax classifier, enabling multi-class classification of attacks—an essential step for enhanced prevention. The framework is implemented within the smart farming system, which consists of three layers: sensor, fog, and cloud. This approach specifically targets the intermediary fog layer within the smart farming architecture.

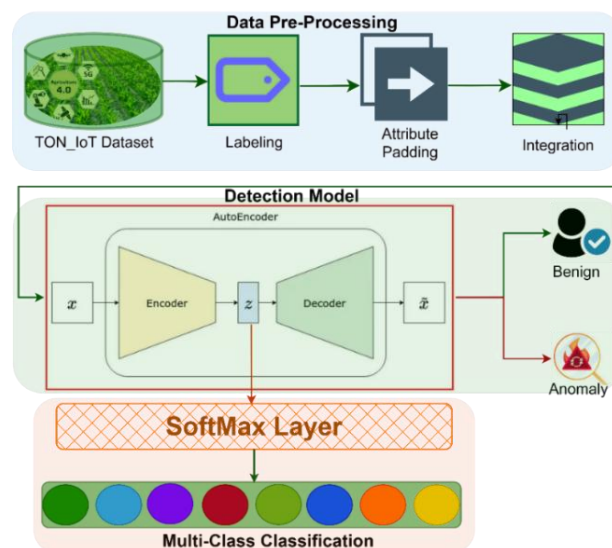


Figure 1. Architecture of the proposed class-aware autoencoder with multi-class classifier for smart farming

2.1. TON_IoT dataset

The TON_IoT dataset serves as a recent testbed for an IIoT network, providing three distinct types of data: network data, operating system data, and telemetry data. In this study, the telemetry datasets from IoT and IIoT sensors, organized across seven files, are utilized. The seven files in the telemetry dataset represent data observations from seven sensors associated with weather, fridge, garage door, GPS tracker, Modbus, motion light, and thermostat. These sensors provide data points such as temperature, humidity, pressure, door open/close status, latitude and longitude, and light on/off status. It includes eight classes:

seven attack types—backdoor, DDoS, injection, password, ransomware, scanning, and XSS—as well as a normal class. It has 3,270,022 normal instances and 527,311 attack instances, totaling 3,797,333 data points.

2.2. Data preprocessing

The data preprocessing stage involves labeling, attribute padding, and integrating seven data files into a single source dataset. To create a common feature space, attribute padding with a zero label is applied for any missing attributes. Z-score normalization (Z-scaling) is used to standardize the values by transforming the data, as shown in (1), shifting the mean to 0 and scaling it to have a standard deviation of 1. This optimized dataset (oDATA), then serves as input to the detection model.

$$Z_i = \frac{(x_i - \mu)}{\sigma} \quad (1)$$

2.3. Anomaly detection using the autoencoder

The autoencoder, a neural network architecture based on an unsupervised learning approach, is utilized for anomaly detection in this experiment. It extracts hierarchical features to improve binary anomaly detection [26]. The normalized data from the preprocessing module serves as input to the autoencoder. This autoencoder is trained solely on benign data, which helps address the data imbalance issue. The architecture, as shown in Figure 2, consists of an input layer, a hidden layer with 12 neurons, and a latent layer with 4 neurons, mirrored by the decoder. The latent layer represents the encoded representation of the entire dataset (${}_L\text{DATA}$). During the training phase, both the encoder and decoder use backpropagation to adjust weights, while the input data passes through the network in a feedforward manner. This network model utilizes the rectified linear unit (ReLU) and Sigmoid activation functions, along with the Adam optimizer, to enhance the optimization process. The hidden layers in the encoder use ReLU, while the decoder uses Sigmoid. ReLU activates by applying $\max(0, \text{oDATA})$, whereas Sigmoid activates as shown in (2). During the training phase, the Autoencoder model processes batches (1024) of normal traffic data to minimize the reconstruction error. The detection threshold is dynamically adjusted according to the accumulated loss. This process is repeated for a predefined number of epochs (31), and at the end, the trained Autoencoder model, along with the detection threshold (0.02625), is returned as the output of the training phase. In the detection phase, the trained Autoencoder model is tested on the dataset to identify any anomalies. The reconstruction error for each data point is computed by comparing the original and reconstructed data. If the error exceeds the detection threshold, the data point is classified as anomalous; otherwise, it is considered normal traffic. The output generated provides a classification for each data point, identifying it as either normal or anomalous traffic. This testing process is crucial for evaluating the effectiveness of the trained detection model on unseen data, helping to identify potential anomalies.

$$\text{Sigmoid} = \frac{1}{(1 + e^{-(\text{oDATA})})} \quad (2)$$

$$x' = g((W' * {}_L\text{DATA}) + b') \quad (3)$$

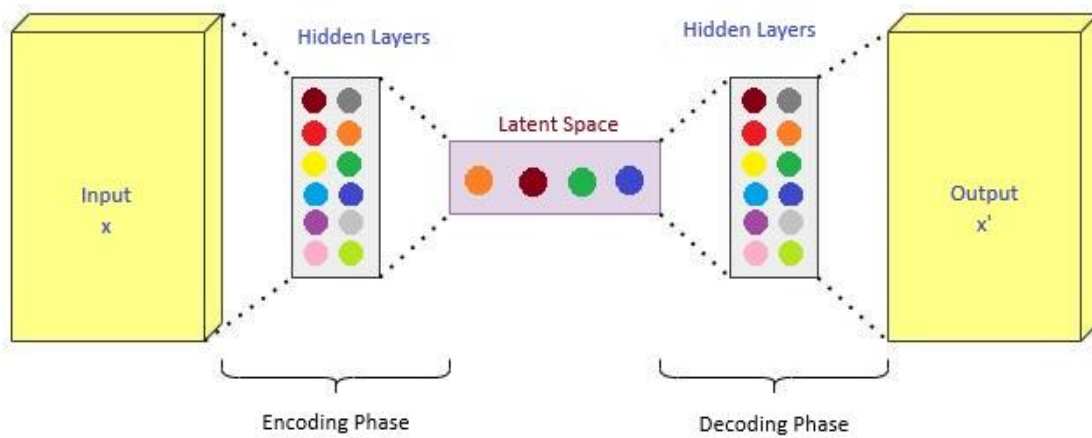


Figure 2. The autoencoder operational architecture

2.4. Multi-class classification with SoftMax layer

After training the autoencoder on normal data, a second phase of training is conducted to optimize the integrated SoftMax layer within the latent space. During this phase, both normal and attack data are introduced, enabling the SoftMax classifier to categorize samples using latent features. The dimensionality reduction capability of the autoencoder enhances its effectiveness in multi-class classification. The data in the latent space are labeled using one-hot encoding for each class. The classifier is trained using both normal and attack data, with the SoftMax layer leveraging the 2D latent representation from the bottleneck to output the probability distribution, classifying each sample as normal, backdoor, DDoS, injection, password, ransomware, scanning, or XSS. This approach utilizes a class-aware autoencoder that combines a reconstruction objective with an integrated classification layer. During training, the model optimizes both reconstruction and classification errors (0.02628), allowing it to learn the structure of each class while carrying out direct classification. This simultaneous optimization enables the adjustment of the weight factors for both reconstruction error and classification loss, as shown in the total loss (4).

$$Total\ Loss = (\alpha * Reconstruction\ Loss) + (\beta * Classification\ Loss) \quad (4)$$

In this context, α and β are weighting factors that determine the relative importance of each loss component in the overall objective function. This allows the model to detect anomalies (via reconstruction error) and classify attack types (using the SoftMax output) as part of an integrated, end-to-end system.

3. RESULTS AND DISCUSSION

The evaluation of the proposed class-aware autoencoder framework is conducted on both binary and multi-class classification using the TON_IoT dataset. For binary classification, performance is assessed using a confusion matrix along with standard evaluation metrics. In the multi-class classification, the framework is tested across eight classes, with performance measured using standard metrics. Additionally, the proposed method is compared with established approaches. The data samples used in this research experiment are listed in Table 1 and the hyper parameters used to fine tune the model is shown in Table 2.

Table 1. Overview of experimental data for the proposed class-aware autoencoder method

| Category | Description |
|----------------------------|---|
| Dataset | TON_IoT |
| Autoencoder training class | Normal |
| SoftMax training class | Normal, backdoor, DDoS, injection, password, ransomware, scanning, and XSS. |
| Testing classes | Normal, backdoor, DDoS, injection, password, ransomware, scanning, and XSS. |
| Number of benign instances | 3,270,022 |
| Number of attack instances | 527,311 |
| Number of attack class | 7 |
| Train and test split | 70:30 |

Table 2. Hyper parameter configuration

| Hyperparameters | Values |
|-----------------------|---------|
| Optimizer | Adam |
| Threshold | 0.02625 |
| Batch size | 1024 |
| Epochs | 31 |
| Learning rate | 0.001 |
| Hidden layers / Nodes | 2/16 |

3.1. Performance metrics

The performance of the proposed method is evaluated using standard metrics, including precision, recall, specificity, F-measure, and accuracy. Recall, shown in (5), indicates the model's effectiveness in correctly identifying positive instances. Precision, defined in (6), reflects the accuracy of positive predictions made by the model. The F-score, outlined in (7), provides a balanced measure that combines both precision and recall. Specificity, as shown in (8), offers insights into the model's ability to accurately recognize negative class instances. Accuracy, shown in (9), represents the overall proportion of correctly classified instances by the model.

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (5)$$

$$Precision = \frac{True\ Positive}{Predicted\ Positives} \quad (6)$$

$$F - Measure = \frac{2 * (Precision * Recall)}{Precision + Recall} \quad (7)$$

$$Specificity = \frac{True\ Negative}{True\ Negative + False\ Positive} \quad (8)$$

$$Accuracy = \frac{True\ Positive + True\ Negative}{Predicted\ Positive + Predicted\ Negative} \quad (9)$$

3.2. Training and testing of class aware autoencoder model

Figure 3 shows the mean squared error (MSE) loss trends for both training and testing phases of the autoencoder and SoftMax classifier, as well as the combined joint loss function. The autoencoder training Loss (green bars) steadily decreases, indicating the model's improving ability to reconstruct training data. The autoencoder testing loss (brown bars) follows a similar downward trend, suggesting good generalization to unseen data. The SoftMax training loss (represented by the orange line) decreases as the classifier becomes more effective at distinguishing between normal and attack classes, while the SoftMax testing loss (represented by the blue line) follows a similar trend, indicating improved performance on unseen data. The joint loss (indicated by the purple area), which integrates both losses, decreases progressively, reflecting the model's ongoing learning process.

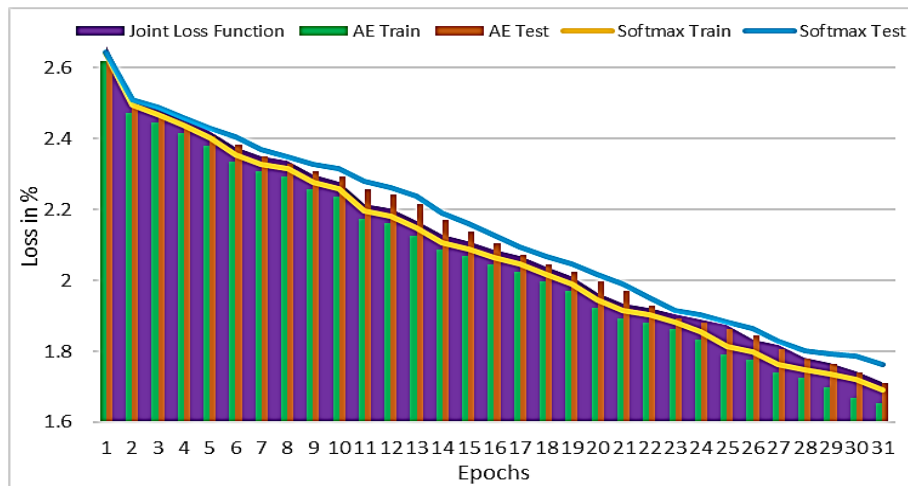


Figure 3. Loss functions of the proposed model: autoencoder loss, SoftMax loss, and joint loss

3.3. Evaluation on the binary class classification module

The overall performance of the proposed models is illustrated in Figure 4, which contains results for both binary and multi-class classification tasks. The autoencoder model demonstrates excellent performance across various metrics, as shown in Figure 4(a), particularly excelling in precision and recall, which makes it highly effective for anomaly detection in smart farming applications. Elevated values in precision, recall, and F1-score suggest that the model successfully differentiates between normal and anomalous data, whereas high specificity and accuracy demonstrate its reliability in minimizing both false positives and false negatives. The SoftMax multi-class classifier shows excellent performance on all metrics, as illustrated in Figure 4(b), consistently achieving values greater than 0.97. Its high precision, recall, and F1-score highlight the model's reliability in accurately identifying the correct classes and minimizing false positives. The classifier's high accuracy demonstrates its overall effectiveness across various classes, making it an ideal choice for multi-class classification tasks, such as anomaly detection, intrusion detection, or smart farming, especially when working with datasets like TON_IoT.

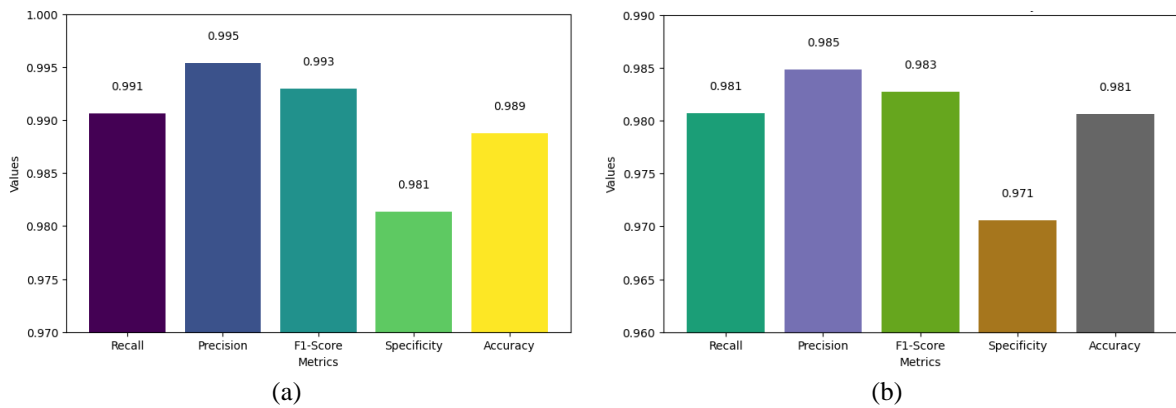


Figure 4. Performance metrics of (a) autoencoder and (b) SoftMax classifier

3.4. Evaluation on multi-class classification module

The SoftMax classifier model excels at identifying the normal class, accurately predicting over 3 million instances, as shown in Figure 5, demonstrating its effectiveness in recognizing non-anomalous traffic. The model performs well in detecting attack categories such as backdoor and password, although there are occasional misclassifications.

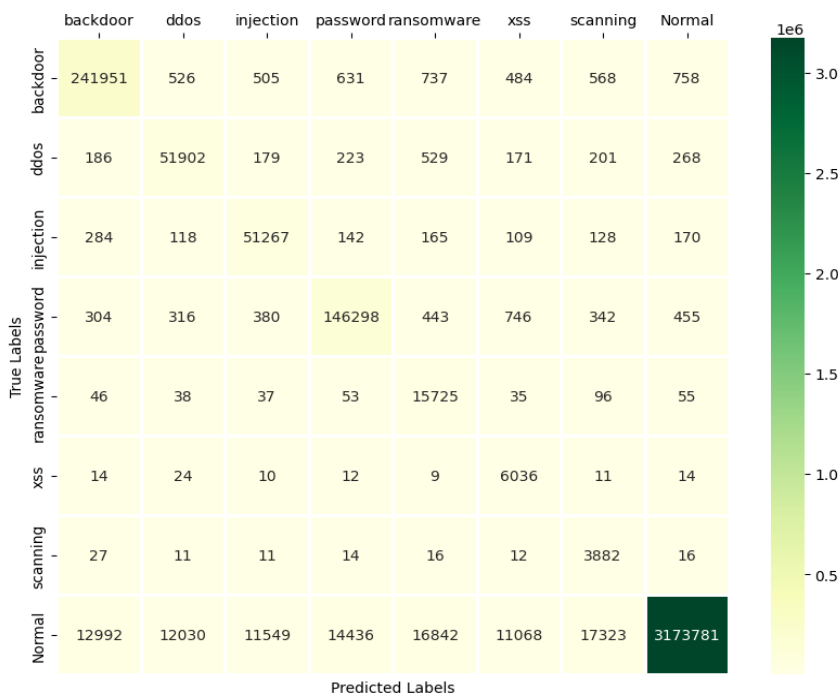


Figure 5. Confusion matrix for multi-class classifier

3.5. Discussion

Overall, the binary classification accuracy tends to outperform the multi-class classification accuracy across all models. The proposed model surpasses all other models in both binary and multi-class classifications, as shown in Figure 6, suggesting that its architecture contributes to its enhanced classification performance. In both binary and multi-class tasks, the proposed model exhibits superior performance, demonstrating a significant accuracy advantage over standard models (CNN, recurrent neural network (RNN), DNN, GRU), particularly in binary classification. The loss function graph demonstrates a general decline in loss across all components—autoencoder and SoftMax losses for both training and testing, along with the joint loss—suggesting effective training and steady progress. The near alignment of training and testing losses for both the autoencoder and SoftMax classifier indicates strong generalization, suggesting that

the model is not overfitting and can effectively handle unseen data. The SoftMax classifier demonstrates strong performance, establishing it as a dependable option for multi-class classification in this context. The model achieves strong precision and recall across classifications, demonstrating high reliability and accuracy, making it well-suited for anomaly detection tasks.

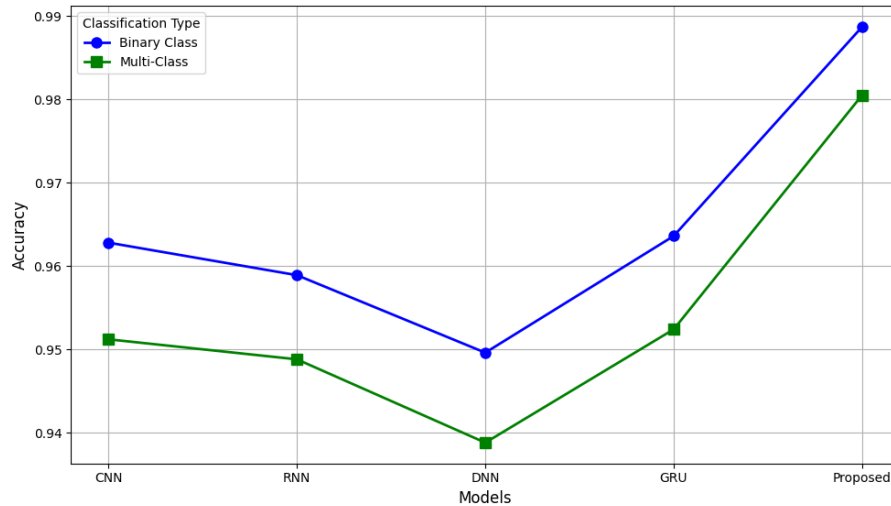


Figure 6. Accuracy comparison of binary class vs multi-class with exiting models

4. CONCLUSION

The proposed deep learning-driven IDS provides an effective approach to address the security issues encountered in IoT-based smart farming environments. The system utilizes the Fog-to-Things architecture alongside a hybrid autoencoder design, enabling effective detection of diverse cyberattacks while optimizing resource efficiency and reducing latency. Experimental evaluations conducted on the TON_IoT dataset reveal the system's high efficacy, achieving over 98% accuracy in both binary and multi-class classifications, highlighting its capability to detect and mitigate security threats effectively, while ensuring its adaptability for deployment in extreme and resource-constrained environments. Incorporating deep learning for anomaly detection and multi-class attack classification offers a reliable approach to enhancing the security and reliability of IoT-driven smart farming systems. Future studies could investigate scalability and optimization strategies for managing larger and more diverse networks in smart farming applications.

FUNDING INFORMATION

Authors state no funding is involved

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

| Name of Author | C | M | So | Va | Fo | I | R | D | O | E | Vi | Su | P | Fu |
|------------------------|---|---|----|----|----|---|---|---|---|---|----|----|---|----|
| Selvaraj Palanisamy | ✓ | | | ✓ | | ✓ | ✓ | | | ✓ | ✓ | ✓ | | |
| Radhakrishnan Rajamani | | ✓ | | | | ✓ | ✓ | | | ✓ | ✓ | | ✓ | |
| Prabakaran Pramasivam | ✓ | | | | ✓ | | ✓ | | | ✓ | | ✓ | | |
| Mani Sumithra | ✓ | | ✓ | | ✓ | | | ✓ | ✓ | | | ✓ | | |
| Prabu Kaliyaperumal | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | | ✓ | |
| Rajakumar Perumal | | ✓ | | ✓ | | ✓ | | ✓ | ✓ | | ✓ | | | |

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.





DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [P.K], upon reasonable request.





REFERENCES

- [1] C. S. kumar and R. V. Anand, "Security in IoT-enabled smart agriculture systems," in *Internet of Things*, vol. Part F2482, Springer Nature Singapore, 2024, pp. 279–300.
- [2] B. Isong, O. Kgote, and A. Abu-Mahfouz, "Insights into modern intrusion detection strategies for internet of things ecosystems," *Electronics (Switzerland)*, vol. 13, no. 12, p. 2370, Jun. 2024, doi: 10.3390/electronics13122370.
- [3] S. Kiruthika *et al.*, "Smart agriculture land crop protection intrusion detection using artificial intelligence," *E3S Web of Conferences*, vol. 399, p. 4006, 2023, doi: 10.1051/e3sconf/202339904006.
- [4] S. Padhy *et al.*, "AgriSecure: A fog computing-based security framework for agriculture 4.0 via blockchain," *Processes*, vol. 11, no. 3, p. 757, Mar. 2023, doi: 10.3390/pr11030757.
- [5] H. T. Bui *et al.*, "Agriculture 4.0 and beyond: evaluating cyber threat intelligence sources and techniques in smart farming ecosystems," *Computers and Security*, vol. 140, p. 103754, May 2024, doi: 10.1016/j.cose.2024.103754.
- [6] J. Miao, D. Rajasekhar, S. Mishra, S. K. Nayak, and R. Yadav, "A fog-based smart agriculture system to detect animal intrusion," in *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, Dec. 2023, pp. 2523–2530, doi: 10.1109/ICPADS60453.2023.00336.
- [7] X. Yang *et al.*, "A survey on smart agriculture: development modes, technologies, and security and privacy challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 273–302, Feb. 2021, doi: 10.1109/JAS.2020.1003536.
- [8] M. A. Ferrag, L. Shu, O. Friha, and X. Yang, "Cyber security intrusion detection for agriculture 4.0: machine learning-based solutions, datasets, and future directions," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 407–436, Mar. 2022, doi: 10.1109/JAS.2021.1004344.
- [9] M. A. Alahe *et al.*, "Cyber security in smart agriculture: threat types, current status, and future trends," *Computers and Electronics in Agriculture*, vol. 226, p. 109401, Nov. 2024, doi: 10.1016/j.compag.2024.109401.
- [10] A. El-Ghamry, A. Darwish, and A. E. Hassanien, "An optimized CNN-based intrusion detection system for reducing risks in smart farming," *Internet of Things (Netherlands)*, vol. 22, p. 100709, Jul. 2023, doi: 10.1016/j.iot.2023.100709.
- [11] B. Alanazi and I. Alrashdi, "Anomaly detection in smart agriculture systems on network edge using deep learning technique," *Sustainable Machine Intelligence Journal*, vol. 3, Jun. 2023, doi: 10.61185/smij.2023.33104.
- [12] T. H. H. Aldhyani and H. Alkahtani, "Cyber security for detecting distributed denial of service attacks in agriculture 4.0: deep learning model," *Mathematics*, vol. 11, no. 1, p. 233, Jan. 2023, doi: 10.3390/math11010233.
- [13] F. A. Zwayed *et al.*, "An efficient intrusion detection systems in fog computing using forward selection and BiLSTM," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 13, no. 4, pp. 2586–2603, Aug. 2024, doi: 10.11591/eei.v13i4.7143.
- [14] N. Dash, S. Chakravarty, and A. K. Rath, "Deep learning model for elevating internet of things intrusion detection," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 5, pp. 5874–5883, Oct. 2024, doi: 10.11591/ijece.v14i5.pp5874-5883.
- [15] J. Sajid, K. Hayawi, A. W. Malik, Z. Anwar, and Z. Trabelsi, "A fog computing framework for intrusion detection of energy-based attacks on UAV-assisted smart farming," *Applied Sciences (Switzerland)*, vol. 13, no. 6, p. 3857, Mar. 2023, doi: 10.3390/app13063857.
- [16] M. A. Lawall, R. A. Shaikh, and S. R. Hassan, "A DDoS attack mitigation framework for IoT networks using fog computing," *Procedia Computer Science*, vol. 182, pp. 13–20, 2021, doi: 10.1016/j.procs.2021.02.003.
- [17] P. Pirozmand, M. A. Ghafary, S. Siadat, and J. Ren, "Intrusion detection into cloud-fog-based IoT networks using game theory," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–9, Nov. 2020, doi: 10.1155/2020/8819545.
- [18] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, and G. Srivastava, "P2TIF: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6358–6367, Sep. 2022, doi: 10.1109/TII.2022.3142030.
- [19] D. Manivannan, "Recent endeavors in machine learning-powered intrusion detection systems for the Internet of Things," *Journal of Network and Computer Applications*, vol. 229, p. 103925, Sep. 2024, doi: 10.1016/j.jnca.2024.103925.
- [20] M. Sajid *et al.*, "Enhancing intrusion detection: a hybrid machine and deep learning approach," *Journal of Cloud Computing*, vol. 13, no. 1, Jul. 2024, doi: 10.1186/s13677-024-00685-x.
- [21] S. Konde and S. B. Deosarkar, "A novel intrusion detection system (ids) framework for agricultural iot networks," *Journal of Theoretical and Applied Information Technology*, vol. 15, no. 21, 2023, [Online]. Available: www.jatit.org.
- [22] K. Kethineni and G. Pradeepini, "Intrusion detection in internet of things-based smart farming using hybrid deep learning framework," *Cluster Computing*, vol. 27, no. 2, pp. 1719–1732, Jun. 2024, doi: 10.1007/s10586-023-04052-4.
- [23] I. Ullah and Q. H. Mahmood, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.
- [24] R. Y. Aburasain, "Enhanced black widow optimization with hybrid deep learning enabled intrusion detection in internet of things-based smart farming," *IEEE Access*, vol. 12, pp. 16621–16631, 2024, doi: 10.1109/ACCESS.2024.3359043.
- [25] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustainable Cities and Society*, vol. 72, p. 102994, Sep. 2021, doi: 10.1016/j.scs.2021.102994.
- [26] Y. Ren, K. Feng, F. Hu, L. Chen, and Y. Chen, "A lightweight unsupervised intrusion detection model based on variational auto-encoder," *Sensors (Basel, Switzerland)*, vol. 23, no. 20, p. 8407, Oct. 2023, doi: 10.3390/s23208407.





BIOGRAPHIES OF AUTHORS

Selvaraj Palanisamy     assistant professor in School of Computer Science and Engineering at Galgotias University, holds 15 years of teaching experience. With an M.E. from Anna University, he has published 3 patents and 4 research papers, specializing in machine learning, networks, cloud computing, and cyber security. He can be contacted at email: selvajkf@gmail.com.







Radhakrishnan Rajamani     assistant professor in School of computer science and engineering at Galgotias University, holds 16 years of teaching experience with an M.Tech. from Anna University, he has published 4 patents and 8 research papers, specializing in networks, cloud computing, and machine learning. He can be contacted at email: prof.rrk8@gmail.com.







Prabakaran Pramasivam     assistant professor in Department of Electrical and Electronics Engineering at Chennai Institute of Technology, holds 14 years of teaching experience. With an M.E. from Anna University, currently pursuing a Ph.D., he has published 3 patents and 4 research papers, specializing in computer networks, telecommunications, cybersecurity in communication systems and machine learning. He can be contacted at email: prabakaranp@citchennai.net.







Dr. Mani Sumithra     is a professor in the Department of Information Technology at Panimalar Engineering College. With 20 years of teaching experience, she holds a Ph.D. and has authored 4 patents, 3 book chapters, and has published 15 research papers in renowned international journals and 30 papers in international conferences. Her areas of expertise include image processing, data mining applications, and machine learning. She can be contacted at email: msumithra@panimalar.ac.in.



Prabu Kaliyaperumal     assistant professor in School of Computer Science and Engineering at Galgotias University, has 16 years of teaching experience. Currently pursuing a Ph.D., he holds an M.Tech. in CSE from SRM University and MBA from Anna University. He has published 4 patents and 12 research papers in international journals and conferences. His expertise includes cyber security, networks, cloud computing and machine learning. He can be contacted at email: mega.prabu@gmail.com.



Rajakumar Perumal     assistant professor in School of Computer Science and Engineering at Galgotias University, holds 22 years of teaching experience and is pursuing a Ph.D. in Computer Science and Engineering at Shri Venkateshwara University. With an M.E. CSE from Anna University, he has published 4 patents and 8 research papers, specializing in networks, cloud computing, software engineering, and machine learning. He can be contacted at email: rajkumar.jcet@gmail.com.