IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15458

Intrusion Detection System for Smart Agriculture Using Deep Learning

Mr. M. Rama Krishna, M Tech[1], P. Keerthi Chandana[2], B. Varshita Lakshmi[3]

Dean of Industrial Relations, Dept. of ECE, ALIET, Vijayawada, Andhra Pradesh, India[1]

Student, Dept. of ECE, ALIET, Vijayawada, Andhra Pradesh, India[2,3]

Abstract: Smart agriculture has rapidly adopted the use of Internet of Things (IoT) technologies that enhance the process of monitoring farm conditions and making decisions based on that. Nevertheless, IoT devices deployed in open and harsh environments are very susceptible to DDoS attacks and other forms of cyber intrusions. This project aims at developing a solution for intrusion detection in smart agriculture systems by applying a deep learning approach. Specifically, this work focuses on the development of an IDS based on a hybrid architecture involving BiGRU and LSTM architectures in order to perform analysis of sequence data and identify malicious operations. To achieve this goal, the intrusion detection system will be built as a web application implemented in Python Flask. The application allows uploading of datasets, training of the model and visualizing the results. TBPTT will be applied to optimize model training process. In this paper, we assess the performance of our model based on metrics such as accuracy, precision, recall and F1-score. Moreover, it should be noted that we calculate mapping between attack severity level and agricultural impact indicators such as water use, fertilizer efficiency and crop risk. Our experiments show promising results regarding accuracy of the model.

Keywords: Smart Agriculture, Internet of Things (IoT), Intrusion Detection System (IDS), Deep Learning, BiGRU, LSTM, TBPTT, Cybersecurity, DDoS Attack Detection, Network Security, Flask Web Application, Time-Series Analysis, Agricultural Impact Analysis

1 INTRODUCTION

The advancement of Internet of Things (IoT) technologies, the development of traditional agriculture to smart agriculture has been greatly facilitated. The technology allows the monitoring and automation process to be improved in the field of agriculture through the usage of sensors for the monitoring of different aspects such as soil, weather, watering, etc. But at the same time, there have emerged serious security concerns due to the use of IoT systems, which are used in an open and harsh environment where cyberattacks like DDoS attacks may happen. Thus, to tackle such problems, an IDS that utilizes deep learning approach with the help of a BiGRU-LSTM neural network architecture to detect any malicious activity has been proposed in the project. The application developed using the Flask framework enables uploading datasets, training models, and visualizing performance of the IDS.

2 LITERATURE SURVEY

Recently, a lot of attention has been focused on protecting IoT-enabled smart agricultural networks from various cyber-attacks since the system is vulnerable to different kinds of attacks. Various machine learning algorithms like Random Forest, SVM, and Decision Trees have been extensively employed to detect intrusions; however, there have been many problems encountered when using them to analyze massive datasets and sequential information. Therefore, more attention has been paid to using deep learning techniques that include DNN, CNN, and RNN. It was observed that these methods perform better in detecting sophisticated attack patterns. Furthermore, RNN is best suited to process temporal information, which is ideal for intrusion detection.

Advanced IDS solutions have involved the use of hybrid deep learning systems that integrate the benefits of different types of neural network architectures. Hybrid neural networks that integrate GRU and LSTM architectures have been proposed to analyze short- and long-term dependency relationships in the data stream. TBPTT algorithms have also been developed to optimize training time and minimize computational requirements. Modern IDS solutions can be enhanced by leveraging edge computing in intrusion detection systems to perform real-time analysis close to IoT devices. Such IDS innovations have yielded impressive results in terms of accuracy, precision, and performance, prompting further innovations in IDS systems designed for intelligent agriculture.

3 PROPOSED SYSTEM

This paper proposes an IDS that leverages the power of deep learning in providing more secure IoT-enabled smart agriculture systems. This system consists of a hybrid architecture involving the use of Bidirectional Gated Recurrent Units (BiGRUs) and Long Short -Term Memories (LSTMs). In this case, BiGRU works by processing the network traffic data in both forward and backward directions for maximum context. The LSTM, on the other hand, is utilized to overcome

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.15458

the vanishing gradient issue since it helps to retain the dependencies of the sequences being considered. It is important to note that this combination will help the IDS to be more effective when detecting several cyberattacks such as DDoS attacks. A softmax classifier is used in the output layer to classify the traffic.

In order to increase the computational efficiency and performance of the system during training, the system uses Truncated Backpropagation Through Time (TBPTT) that breaks down a long sequence into short parts in order to minimize memory requirements and increase speed. The IDS described in this work is developed as a web-based solution by utilizing the Flask library. It allows for uploading datasets, their preprocessing, training, and visualization of results. Metrics for evaluating the performance of the system include accuracy, precision, recall, and F1-score. Moreover, this system implements an original mapping between attack severity and impact on the agricultural system by calculating the usage of water, fertilizers, and risks for crops.

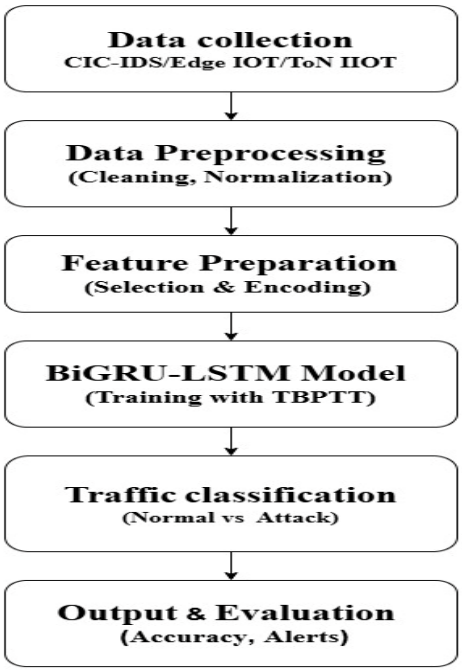

Figure 1: Proposed System Block Diagram

4 METHODOLOGY

4.1 Data Collection and Preprocessing:

Data sets related to network traffic are obtained from trusted sources. Data cleansing includes eliminating data having missing values and infinity values, besides handling irrelevant features. Normalization procedures like min-max normalization ensure that all values fall within the same range.

4.2 Data Splitting and Transformation:

The prepared data set is split into training and testing data in the ratio of 80:20, respectively. It is further reshaped to make it compatible with a deep learning network, enabling the system to detect the sequence dependency.

4.3 Model Design and Development:

Deep learning-based architecture uses two types of neural networks, namely Bidirectional Gated Recurrent Unit (BiGRU) and Long Short-Term Memory (LSTM). While BiGRU helps in capturing bidirectional dependencies, LSTM deals with long term memory issues as well as avoids vanishing gradient issue. A Softmax function acts as classifier for normal and attack data.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.15458

4.4 Model Training Using TBPTT:

Model training is carried out via TBPTT that breaks down long sequences into short chunks. This technique helps minimize memory consumption, increase training speed, and optimize learning. This way, the model can learn to detect patterns of both normal and malicious behaviors.

4.5 Evaluation and Deployment:

The developed system is created as a Flask application enabling uploading of datasets, model training, and results visualization. Performance evaluation is done via accuracy, precision, recall, and F1-scores, while attack level detection is used for mapping agricultural impact factors including water consumption, fertilizer efficacy, and plant risks.

5 BiGRU-LSTM MODEL

The proposed model for this project combines a BiGRU and LSTM to create a hybrid architecture which uses both techniques in one model to efficiently detect network intrusions. A combination of BiGRU and LSTM in this application will enable the system to have a better understanding of both short-term and long-term sequential data patterns that are involved in attacks. The bidirectional GRU processes data in two opposite directions (forward and backward), thereby creating an efficient process to learn context information. On the other hand, LSTM enables the system to store information for long periods.

This model is highly effective in applications involving time-series data. As a result, it is possible to easily distinguish between malicious behaviour and legitimate user activity based on the learned patterns. Besides being accurate in detecting network anomalies, another advantage of this model involves the utilization of TBPTT that significantly reduces training computational and memory complexity. Therefore, the model creates an appropriate balance between computational efficiency and high accuracy in real-time intrusion detection.

6 INTRUSION DETECTION SYSTEM

An Intrusion Detection System is a security mechanism that monitors the network traffic for any kind of intrusion or violation of security policies. It is very important for the security of computer networks as well as for IoT-based systems because it monitors the activities in order to detect any kind of attack. The IDS can be classified into two categories, namely signature-based IDS that use predefined patterns to recognize an attack and anomaly-based IDS that recognize deviation from a set pattern in data. IDS can be applied in smart agriculture systems which incorporate IoT components such as sensors and controllers in order to protect against DDOS, botnets, and other types of attacks.

In IDS has been developed using deep learning algorithm along with BiGRU-LSTM hybrid architecture. The machine learning algorithm takes input in the form of network traffic data and learns the pattern of the data to predict any deviation from the usual pattern which indicates an intrusion. This approach enables detection of intrusions by capturing the long-term dependencies present in sequence data. Furthermore, the detected results can be analysed in order to estimate the risk level and the threat to agricultural resources.

6.1 Risk Level Module

After Prediction, the system calculates the attack ratio (percentage of attack samples in the uploaded database) and defines the risk level as follows:

- Low Risk (attack_ratio < 0.3): Stable system – regular operations unaffected.
- Moderate Risk (0.3 ≤ attack_ratio < 0.7): Monitoring recommended – possibility of sensor malfunction.
- High Risk (attack_ratio ≥ 0.7): Actions needed immediately – danger to critical systems.

6.2 Agricultural Resource Impact Module

The agricultural resources affected by the attack are calculated based on the percentage of the attack ratio:

- Water usage disrupted: attack_ratio × 100%
- Fertilizer supply disrupted: attack_ratio × 80%
- Power consumption affected: attack_ratio × 70%

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15458

- Crops losses expected: attack_ratio × 60%

7 EXPERIMENTAL RESULTS

In order to evaluate the proposed deep learning intrusion detection approach, experiments were conducted on a network traffic dataset in which the capability of the IDS to detect cyber attacks in smart agriculture environment was tested. The used dataset was preprocessed and split into training, validation, and test sets. The hybrid BiGRU-LSTM neural network architecture was trained using TBPTT technique. The obtained experimental results indicated that the proposed system can detect attacks in a network with high accuracy and learn patterns in the network traffic dataset.

Evaluation metrics used to measure the performance of the system include accuracy, precision, recall, and F1 score. High accuracy values achieved by the proposed system indicate that attacks are detected with high precision and recall. Furthermore, the proposed IDS computes the attack ratio and categorizes its outputs into low, medium, and high risk attack types. Finally, the agricultural impact module calculates the effect of these attacks on various resources like water usage, fertilizer utilization, power consumption, and crop loss.

Figure 2: Admin Login page

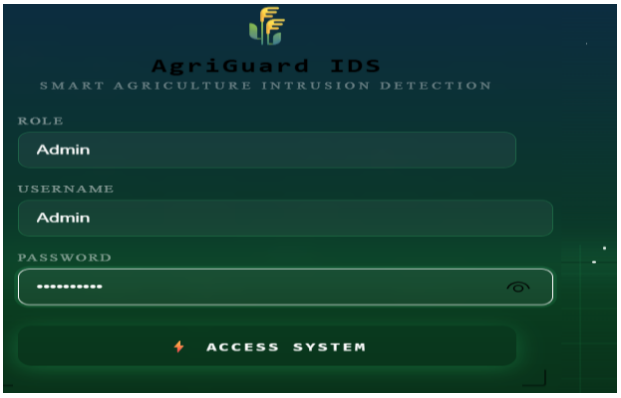

Figure 3: User Login page

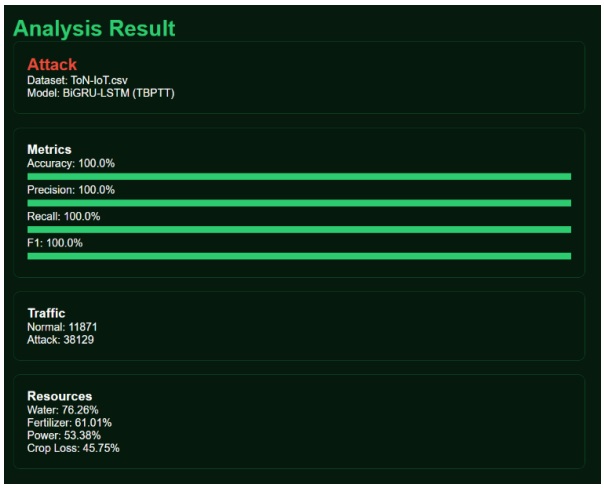

Figure 4: Analysis Results of ToN-IoT Data set

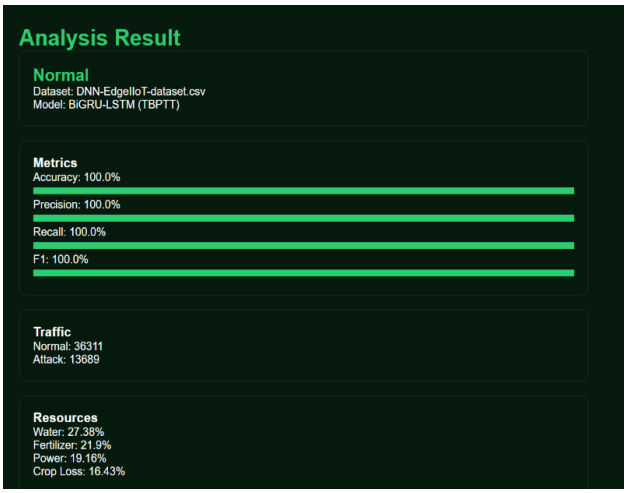

Figure 5: Analysis Results of EdgeIIoT Data set

8 RESULTS AND DISCUSSION

The results obtained from the implementation of the proposed IDS indicate that the biGRU-LSTM hybrid model effectively identifies network intrusion with high accuracy, precision, recall, and F1-score in smart agriculture networks. The incorporation of TBPTT enhances training effectiveness while reducing computational complexity, making the system fast and efficient. The proposed IDS classifies traffic data into normal and attacks and evaluates the level of attack based on attack ratio to determine the risk level, which may be low, medium, or high. Moreover, incorporating the

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15458

agricultural impact module offers insightful information by quantifying resource disruptions including water utilization, fertilizer effectiveness, energy utilization, and crop production losses. The results indicate that the proposed IDS can not only detect network intrusion effectively but is also useful as it links cyberattacks to agricultural consequences.

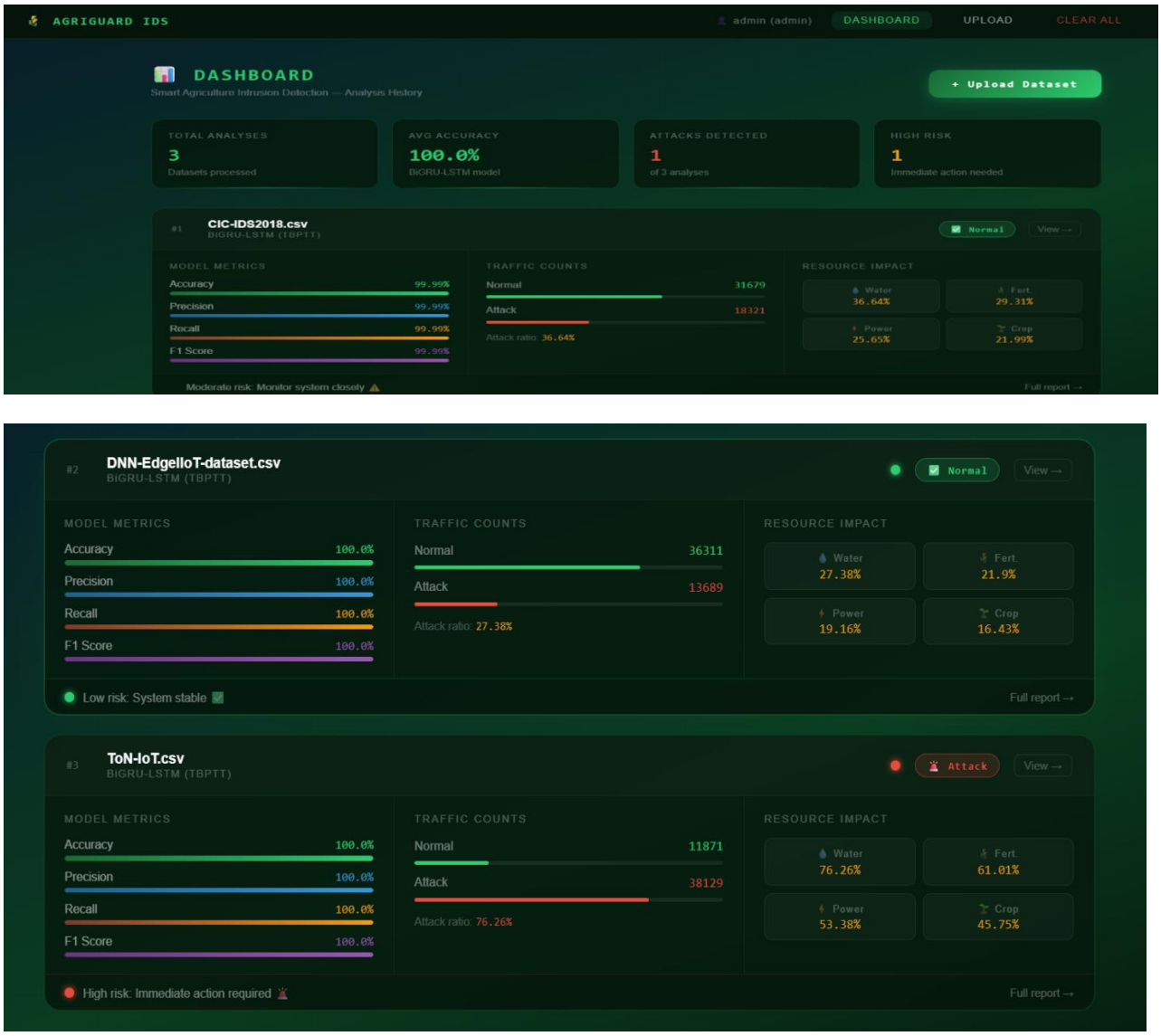

Figure 6: Dashboard Page

9 CONCLUSION

The paper described an IDS based on deep learning for ensuring better security in smart agriculture applications utilizing IoT. The proposed method employed a hybrid model that combined BiGRU and LSTM to ensure effective analysis of the network traffic sequences for detecting any malicious activities. The use of TBPTT ensured better training time and lower computational complexity. The implementation of the IDS was done using Flask, which provided an easy-to-use interface for data analysis, modeling, and visualizations.

The experiments showed that the IDS is capable of delivering good performance in terms of accuracy, precision, recall, and F1-score. In addition, the risk level classification and its impact on agriculture showed how harmful a particular attack could be by analyzing water usage, the effect of fertilizers, power consumption, and crop loss, among others. Thus, the IDS can be considered reliable and practical enough, providing room for further development.

10 FUTURE SCOPE

There are various ways in which the Intrusion Detection System for smart agriculture can be made better in terms of performance and practicality. First, the use of real-time monitoring of data through live streams of data from IoT sensors

DOI: 10.17148/IJARCCE.2026.15458

instead of static datasets can help in making this model work even better as it will be possible to respond immediately to any cyber threat detected by the system. The accuracy of the model can be greatly enhanced if a greater amount of data was used in training it along with advanced deep learning techniques like attention mechanisms and transformers.

One key area of future research is implementing this model on edge computing systems for faster results. Other technologies that can be considered to increase the security provided by this model include technologies like blockchain for the secure transfer of data. In addition to binary classifying attacks into benign or malicious, a better approach would be to classify attacks according to multiple classes. Finally, creating an easy-to-use mobile or web dashboard for the system can also greatly enhance its utility and ease of use.

REFERENCES

[1] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent edge computing for IoT-based energy management in smart cities," *IEEE Network*, vol. 33, no. 2, pp. 111–117, 2019.
[2] I. A. Kandhro et al., "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures," *IEEE Access*, vol. 11, pp. 9136–9148, 2023.
[3] G. C. Amaizu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Investigating network intrusion detection datasets using machine learning," in *Proc. ICTC*, 2020, pp. 1325–1328.
[4] S. Seth, G. Singh, and K. Kaur, "Smart intrusion detection system using deep neural network gated recurrent unit technique," in *Proc. Int. Conf. Communication and Cyber Physical Engineering*, 2022, pp. 285–293.
[5] X. Luo, W. Zhou, W. Wang, Y. Zhu, and J. Deng, "Attention-based relation extraction with bidirectional GRU," *IEEE Access*, vol. 6, pp. 5705–5715, 2017.
[6] R. C. Staudemeyer and E. R. Morris, "Understanding LSTM—A tutorial into long short-term memory recurrent neural networks," arXiv:1909.09586, 2019.
[7] C. Tallec and Y. Ollivier, "Unbiasing truncated backpropagation through time," arXiv:1705.08209, 2017.
[8] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," *IEEE Access*, vol. 7, pp. 167529–167540, 2019.
[9] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems using UNSW-NB15 dataset," *IEEE*, 2015.
[10] H. Hindy et al., "A taxonomy of network threats and intrusion detection systems," *Future Generation Computer Systems*, vol. 88, pp. 130–143, 2018.
[11] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proc. EAI ICST*, 2016.
[12] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
[13] K. Cho et al., "Learning phrase representations using RNN encoder–decoder for statistical machine translation," arXiv:1406.1078, 2014.
[14] M. Abadi et al., "TensorFlow: Large-scale machine learning on heterogeneous systems," 2016.
[15] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," arXiv:1412.6980, 2015.

