Convolutional Neural Network-Gated Recurrent Units with SelectKBest Model for Detecting Distributed Denial of Service Threats in Smart Farming System

Lateef Caleb Umoru
Dept. of Cyber Security Science
Federal University of Technology
Minna, Nigeria
umorulc@custech.edu.ng

Joseph Adebayo Ojeniyi
Dept. of Cyber Security Science
Federal University of Technology
Minna, Nigeria
ojeniyija@futminna.edu.ng

John Kolo Alhassan
Dept. of Computer Science
Federal University of Technology
Minna, Nigeria
jkalhassan@futminna.edu.ng

Solomon A. Adepoju
Dept. of Computer Science
Federal University of Technology
Minna, Nigeria
solomon.adepoju@futminna.edu.ng

Bello L. Yunusa
Dept. of Crop Production
Federal University of Technology
Minna, Nigeria
b.yunusa@futminna.edu.ng

***Abstract*—This research focuses on developing and evaluating optimized deep learning frameworks for effective detection of Distributed Denial-of-Service (DDoS) intrusions across various benchmark datasets. The study implemented three hybrid models: (1) a Gated Recurrent Unit enhanced through a Genetic Algorithm (GRU+GA), (2) a Convolutional Neural Network integrated with GRU and SelectKBest feature selection (CNN+GRU+SelectKBest (proposed)), and (3) an Autoencoder-based classifier optimized with a Genetic Algorithm (Autoencoder+GA). These models were tested on the NSL-KDD, and CIC-DDoS2019 datasets, utilizing metrics such as accuracy, precision, recall, F1-score, AUC-ROC, and error rates. The proposed CNN+GRU+SelectKBest model consistently outperformed the other two models. For instance, on the NSL-KDD dataset, it achieved the highest accuracy at 0.9817 along with the lowest Type I error rate of 0.0192. On the NSL-KDD dataset, it recorded the highest true positives (TP) of 2643 and true negatives (TN) of 2304, surpassing both GRU+GA and Autoencoder+GA. In the case of the CIC-DDoS2019 dataset, the model attained perfect classification metrics (accuracy, precision, recall, and F1-score of 1.0000) with no false positives or negatives, while the GRU+GA and Autoencoder+GA models achieved accuracies of 0.9856 and 0.9992, respectively. When compared to alternative architectures, the CNN+GRU+SelectKBest model exhibited superior detection accuracy, lower error rates, and enhanced generalization capabilities, demonstrating its effectiveness and adaptability for advanced DDoS intrusion detection systems.**

Keywords—smart farm, intrusion detection, deep learning, DDoS, hyperparameters tuning, feature selection, CNN, GRU, SelectKBest, data integrity, internet of things

I. INTRODUCTION

Agriculture has been a fundamental aspect of human progress. Its development ensured that there was enough food to satisfy essential subsistence requirements. Improvements in both the quantity and quality of agricultural output were vital in averting famines and maintaining societal stability. However, various pressing challenges in the real world necessitate more efficient agricultural practices. Around 500 million people globally are still undernourished, with 821 million facing hunger, a situation that is likely to worsen as the population continues to grow. Additionally, the overuse of land and water pollution have adversely affected crop production. The rise of urbanization has led to a reduction in both arable land and agricultural workers, significantly impacting the efficiency and scale of agricultural output [1].

For developing nations with high population density, expanding land for agricultural use and implementing effective crop protection methods can be challenging. In such scenarios, the best approach is to enhance agricultural practices by leveraging advanced technologies like the Internet of Things (IoT) and artificial intelligence (AI) [2]. IoT has greatly broadened its scope across various sectors such as business, smart home technology, healthcare, agriculture, and numerous global services. IoT devices can be interconnected to manage and track environmental factors in applications like weather stations, smart cities, agro-industry, and human activity recognition. A recent report by Allied Market Research indicates that the IoT device market, which generated $77.8 billion in 2021, is projected to grow at a compound annual growth rate (CAGR) of 18.6% from 2022 to 2031, potentially reaching $413.7 billion. Additionally, the report forecasts a surge in the number of connected IoT devices, estimating an increase from 27 billion in 2017 to over 125 billion by 2030 [3] [4].

The agricultural industry has undergone a significant transformation, largely due to the rise of the IoT, which seeks to address the substantial annual losses ranging from 20% to 40% caused by inadequate monitoring of crop conditions. This technological progress has greatly enhanced agricultural management by enabling data-driven decision-making through the seamless integration of various devices and equipment. As the dependence on Agricultural IoT (AG-IoT) increases, concerns regarding the security and privacy of these devices have become prominent. Protecting the integrity and confidentiality of the data that flows between AG-IoT devices and central servers is crucial for maintaining both the security and functionality of the IoT ecosystem. To mitigate these risks, implementing cybersecurity measures, such as intrusion detection systems (IDS), is essential to safeguard against unauthorized access and potential data breaches [5].

The rise in connected devices and online services has led to a substantial increase in network traffic, heightening the importance of availability and security. However, DDoS attacks represent a serious risk to the availability of IoT networks. These attacks utilize extensive botnets to inundate a target's resources, rendering them incapable of serving legitimate users. Notable recent DDoS incidents affecting Google and AWS, which reached peak traffic levels exceeding 2 Tbps, underscore the escalating scale of this issue [6]. DDoS attacks are particularly concerning for agricultural IoT, given the sector's broader attack surface and the vital role of timely operations in farming. In recent years, we have seen unprecedented DDoS attacks achieving terabit levels, with recorded peaks of 1.7 Tbps and 2.3 Tbps [7].

The research conducted by Ref [8] supports previous findings by indicating that the steady rise of approximately 5.03 billion internet users globally poses a significant risk to cybersecurity. In the third quarter of 2022, there was a remarkable 90% increase in DDoS attacks when compared to the same timeframe the previous year. These attacks result in substantial losses affecting infrastructure, various industries, government operations, and the overall economy. Notably, around 65% of these DDoS attacks are classified as volumetric. This means they involve sending a massive amount of irrelevant data to overwhelm the targeted computational resources or the capacity of nearby network connections. DDoS attacks represent a distinct form of assault aimed at disrupting the online services of a particular web server with malicious intent.[8].

The foundation of smart farming initiatives lies in the IoT, which plays a significant role in agricultural systems. However, the design and implementation of smart farms often face challenges related to security breaches and risks associated with data collection, storage, transmission, and manipulation. IoT-based farming systems lack adequate security measures across various agricultural value chains, particularly in the face of rising cyber-physical threats. Additionally, poor network connectivity has further compromised the security of smart farming and its components, leading to both logical and physical disruptions [9]. To achieve this goal, it is essential to establish a dependable security framework that protects farms, farmers, and their valuable assets, including data. This will enable them to fully experience the advantages of technology and device-driven agriculture.

This paper makes several important contributions: First, it aims to minimize redundancy in the features of the smart farm intrusion dataset through the application of the SelectKBest algorithm. Second, it focuses on optimizing the hyperparameters of the CNN model by utilizing the GRU algorithm. Lastly, it assesses the effects of feature selection and hyperparameter tuning on the performance of the CNN model.

II. Related Studies

Ref. [10] initiated an intrusion detection system aimed at identifying DDoS attacks through the use of convolutional neural networks, deep neural networks, and recurrent neural networks. They examined the performance of individual models across two types of classification—binary and multiclass—by utilizing two novel real traffic datasets: the CIC-DDoS2019 dataset and TON_IoT, which encompass various DDoS attack types. The results demonstrated remarkable accuracy rates of 99.95% for binary traffic classification and 99.92% for multiclass traffic classification within a smart farming context. However, it is noteworthy that the study did not incorporate any proactive defense mechanisms, such as encryption algorithms.

Ref. [11] explored a framework called DDoSViT aimed at enhancing detection and alert systems for attacks. This framework, which is based on Vision Transformers (ViT), transforms attack flows into images and trains the Vision Transformers using a dataset of attack images. They utilized the CICIoT2023 and CICIoMT2024 datasets, which encompass real-world attack scenarios and multi-vector attacks, for both training and validation purposes. The findings revealed that the model achieved impressive metrics: an accuracy of 99.50%, precision of 99.53%, recall of 99.50%, and an F1-score of 99.50% in multi-class classification across 23 distinct variants of DDoS and DoS attacks, surpassing the performance of existing models. This framework also minimizes false positives and ensures reliable alerts during firmware updates for IoT-edge devices. However, there is potential to simplify the feature complexity to enhance the model's robustness and efficiency.

Ref. [12] examined the application of various ML methods for detecting DoS attacks and reducing their impact. The authors evaluated the effectiveness of both hard and soft ensemble techniques using two datasets: the Wireless Sensor Network Dataset (WSN-DS) and the Wireless Sensor Network Blackhole, Flooding, and Selective Forwarding (WSN-BFSF) datasets. The ensemble models combined outputs from several models to enhance overall accuracy, achieving a notable 98.12%. Among the results, the soft ensemble method slightly surpassed the hard ensemble method for the WSN-DS dataset, which recorded an accuracy of 97.97%. Conversely, the hard ensemble technique recorded an impressive accuracy of 99.967% on the WSN-BFSF dataset, whereas the soft ensemble technique reached an exceptional accuracy of 100%. This highlights the necessity of extending generalization of the model.

Ref. [13] introduced the Multi-Layer Deep Autoencoder (M-LDAE), which is specifically designed for detecting threats across different layers of IoT systems, addressing various challenges in this area. This study presents the M-LDAE as a solution for detecting IoT attacks that span multiple layers. By leveraging the hierarchical simplification capabilities of deep autoencoders, M-LDAE can extract latent representations that encompass both global and local characteristics. This technology provides robust protection against a range of cyber threats, such as Man-in-the-Middle attacks at the network layer and DDoS attacks at the transport layer within IoT networks. To enhance detection capabilities and adapt to new attack techniques, the M-LDAE integrates Recurrent Neural Networks (RNNs), Graph Neural Networks (GNNs), and Temporal Convolutional Networks (TCNs). The model demonstrates impressive performance with an accuracy of 92.5%, a sensitivity of 90.8%, a specificity of 94.8%, F1 scores of 89.4%, and a Jaccard index of 89.4%. However, it is important to note that the M-LDAE model faces challenges related to overhead, generalization, and scalability.

Ref. [14] presented a deep learning-based intrusion detection system (IDS) that combines CNN with principal

component analysis (PCA) and examines the use of vision transformers (ViT). The hybrid model was evaluated using the CICDDoS2019 dataset, demonstrating a significant enhancement in detection accuracy. Initially, the CNN-based model detected DDoS attacks with an accuracy of 99.72%. After incorporating ViT, the accuracy rose to an impressive 99.99%. This groundbreaking approach represents a substantial leap forward in DDoS attack detection capabilities and highlights the potential benefits of integrating advanced deep learning models into cybersecurity strategies. Future research could explore the use of additional deep learning classifiers, alternative dimensionality reduction techniques, addressing class imbalance, and optimizing hyper-parameters across different datasets.

Ref. [15] created a DDoS detection framework utilizing the CNN-BiLSTM model, designed for implementation in a distributed network and featuring comprehensive pre-processing. The effectiveness of this model surpasses that of other approaches, including CNN, BiLSTM, and RNN, achieving an accuracy of 99.625%, precision of 99.015%, recall of 99.132%, and an F1-score of 99.059. However, the findings lack generalizability since they rely on a single dataset.

A multi-stage learning approach that employs a one-dimensional convolutional neural network (1D-CNN) alongside decision tree classification to effectively identify DDoS attacks within SDN-based SCADA systems by [16]. To support the training and evaluation of this model, a new dataset was developed, featuring a range of attack scenarios tailored to a specific experimental network topology. The experimental findings indicated that the proposed model reached an impressive accuracy rate of 97.8% in detecting DDoS attacks. This multi-stage learning approach demonstrates the potential for achieving high performance in recognizing DDoS threats targeting SDN-based SCADA systems. Future research could explore the scalability and performance of this model with the newly created dataset.

Ref. [17] proposed a robust Intrusion Detection System (IDS) that integrates both rule-based and machine learning methods to identify DDoS attacks that threaten the infrastructure of Cyber-Physical Production Systems (CPPS). The system's training and validation were conducted using real-time network traffic from a practical industrial environment known as the Farm-to-Fork (F2F) supply chain system. In this process, both attack traffic and normal traffic were recorded, and bidirectional features were extracted utilizing CIC-FLOWMETER. The authors employed eight supervised and unsupervised machine learning techniques to identify malicious flows. Subsequently, a rule-based detection mechanism was implemented to assess the frequency of these malicious flows and assign varying severity levels based on the calculated frequency. The results indicated that supervised models significantly outperformed their unsupervised counterparts, achieving an impressive accuracy of 99.97% and a True Positive Rate (TPR) of 99.96%. When tested and deployed in a real-time setting, the overall weighted accuracy reached approximately 98.71%. Future research should address the model's limitations regarding generalization and scalability.

Ref. [18] introduced IoTShield, a dual-stage defensive framework based on Software Defined Networking (SDN), aimed at countering various flow-based attacks aimed at IoT systems. Drawing on recent advancements in programmable networks, this framework assigns each programmable switch within the network's connectivity layer the task of identifying a specific category of prevalent attacks. To effectively manage the spread of these threats, the network controller classifies detected attacks, allowing for timely updates to the defensive rules in the data plane. The authors demonstrated, using the CICIoT2023 dataset, that implementing distinct detectors for DDoS and web-based attack categories on programmable data planes leads to a significant reduction in false alarms—by 58% and 97%, respectively. Additionally, a lightweight Decision Tree (DT) model serving as a single DDoS attack detector in the data plane achieves an impressive accuracy rate of 80-99% for identifying various types of attack flows. The more detailed classification is handled by a CNN classifier in the control plane, which boasts a 99% accuracy rate. Moreover, IoTShield effectively minimizes latency and reduces the load on the controller during attack detection, resulting in 0.14 milliseconds increase in median queuing delay. Although IoTShield does not classify the type of attack, it does confirm the occurrence of attacks across the network.

Ref. [19] presented a novel IoT-enabled hybrid model aimed at enhancing smart agriculture by combining machine learning and artificial intelligence algorithms to create an efficient and dependable decision-making framework. The authors designed a strong anomaly detection system that utilized the features of Multilayer Perceptron (MLP), Naïve Bayes, and Support Vector Machine (SVM) with a dataset focused on dry beans. They employed hybrid deep learning models, specifically combining InceptionV3 with Long Short-Term Memory (LSTM) and VGG16 paired with fully connected dense layers. This research utilized two distinct datasets: the dry beans dataset from 2021 and a soil type dataset from 2024. Findings indicated that the MobileNetV2 model achieved impressive accuracy and recall rates of 97% in detecting soil types. Additionally, the hybrid model integrating random forest and neural networks reached an accuracy of 92%, while the SVM model recorded an accuracy of 93%. The combination of InceptionV3 and LSTM layers also demonstrated a notable accuracy of 91%. It is essential for future research to address data access methods to ensure data integrity and to implement data augmentation strategies to enhance the efficiency and reliability of these models.

Ref. [20] introduced an innovative approach to improve the performance of machine learning-based DDoS detection systems by integrating MLP and CNN methodologies. By employing a Bayesian optimizer along with the Shapley Additive feature-selection technique, their model showcases an impressive overall accuracy of 99.95% and 99.98% on the CICDDoS-2019 and InSDN datasets, respectively. The findings indicate that this model is exceptionally effective in identifying DDoS attacks within SDN environments. Moreover, these models hold potential for extension to enhance network security in IoT-based systems.

III. Research Methodology

A. Architecture of the Proposed Model

The architecture of the proposed intrusion detection model for detecting threats and preserving smart sensor data using data encryption scheme as shown in Fig. 1. From Fig. 1, the

main components of the architecture of the proposed model include the smart devices (sensors) and sensed dataset as the input to the proposed model. Secondly, the data scrutiny and detection using enhanced CNN model with GRU optimization and SelectKBest feature selection algorithms serving as the process component of the model. And the output component provides threats classification with deep learning algorithms.

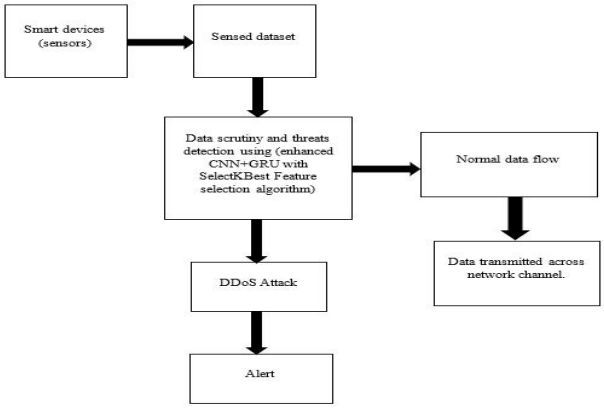

Fig. 1. he architecture of the proposed model

From Fig. 1, the main components of the architecture of the proposed model include the smart devices (sensors) and sensed dataset as the input to the proposed model. Secondly, the data scrutiny and detection using enhanced CNN model with GRU optimization and SelectKBest feature selection algorithms serving as the process component of the model. And the output component provides threats classification with deep learning algorithms.

B. Data Collection and Preprocessing

The NSL-KDD dataset was obtained from the Kaggle repository, containing 25,192 entries and 42 attributes. Within this dataset, there are 13,449 instances of normal data flow and 11,743 instances of anomalous data flow. On the other hand, the CIC-DDoS2019 dataset offers a comprehensive collection of Distributed Denial of Service (DDoS) attacks, many of which utilize some type of amplification through reflection techniques. This dataset includes crucial feature sets essential for identifying various DDoS attacks, along with their respective weights. [21]. For data preparation, preprocessing steps were applied to eliminate any empty records and non-scalar columns using Python functions. Categorical columns were converted into numerical values, while the target column was transformed into binary format, consisting of 0s and 1s, to facilitate the training of the proposed model.

C. CNN-GRU-SlectKBest Model's Algorithm

The main objective is to identify DDoS and normal traffic in smart-farm IoT networks by (1) selecting the most informative features with SelectKBest, (2) learning spatial patterns with a 1-D CNN, and (3) learning temporal dependencies with GRU as defined by Algorithms 1 and 2.

Algorithm 1: SelectKBest_DDoS
Input: D_raw, k, train_val_test_split
Output: F_sel,

1. Data Load and Cleaning
   D := load(D_raw)
   Remove duplicates, handle missing values (impute or drop)
   Convert categorical fields -> numeric (one-hot or ordinal as needed)
   Ensure timestamps are monotonic and synchronized
2. Feature Engineering
   If data is packet-level = aggregate into flow windows (like 5s) to create features:
   - pkt_count, byte_count, duration, avg_pkt_size, pkts_per_second, interarrival_mean, entropy_payload, src_unique_count, ...
   Add domain features (protocol, port categories, device_type) as needed
3. Label and Balance
   y := labels (0/1)
   If class imbalance is severe: compute class_weights = {w0, w1}
4. Train/Val/Test Split
   X_train, X_temp, y_train, y_temp := stratified_split(X, y, train_size)
   X_val, X_test, y_val, y_test := stratified_split(X_temp, y_temp, val_size/(val+test))
5. Scaling
   scaler := fit StandardScaler or MinMaxScaler on X_train
   X_train_s := scaler.transform(X_train)
   X_val_s := scaler.transform(X_val)
   X_test_s := scaler.transform(X_test)
6. Feature Selection (SelectKBest)
   selector := SelectKBest(score_func=f_classif, k=k)
   selector.fit(X_train_s, y_train)
   X_train_sel := selector.transform(X_train_s)
   X_val_sel := selector.transform(X_val_s)
   X_test_sel := selector.transform(X_test_s)
7. Return F_sel := indices or names of selected features

Algorithm 2: CNN_GRU_SelectKBest_DDoS
Input: F_sel, k, train_val_test_split, hyperparameters
Output: M_cnn_gru, evaluation_metrics
1. Reshape for CNN-GRU
   7.1 Decide timesteps T:
   - If sequence data exists, set T = sequence length and reshape accordingly
   - If single-row per window, set timesteps = 1
   7.2 Reshape X_*_sel into shape [samples, timesteps, num_features] for Keras
2. Build CNN+GRU Model
   model := Sequential()
   model.add(Conv1D(filters=64, kernel_size=3, activation='relu', padding='same', input_shape=(T, num_features)))
   model.add(MaxPooling1D(pool_size=1))
   model.add(Dropout(0.3))
   model.add(GRU(128, return_sequences=False))
   model.add(Dropout(0.3))
   model.add(Dense(64, activation='relu'))
   model.add(Dense(1, activation='sigmoid'))
   model.compile(optimizer = Adam(lr = 1e-3), loss = 'binary_crossentropy', metrics=['accuracy'])
9. Train
   callbacks := EarlyStopping(monitor='val_loss', patience=5, restore_best_weights=True)
   model.fit(X_train_sel, y_train, validation_data=(X_val_sel, y_val),
   epochs=epochs, batch_size=batch_size, class_weight=class_weights, callbacks= [callbacks], verbose=1)
10. Evaluate
   y_proba := model.predict(X_test_sel)
   y_pred := threshold(y_proba, 0.5)
   Compute metrics: accuracy, precision, recall, f1, auc = AUC(y_test, y_proba)
   ConfMat := confusion_matrix(y_test, y_pred)
   TypeI := FP / (FP + TN)
   TypeII := FN / (FN + TP)

11. Save and Export
Save model weights and scaler and selector (pickle/hdf5)
Save F_sel list and metadata (feature names, hyperparameters, experiment log)
12. Return model, F_sel, metrics

D. Performance Metrics

The suggested model underwent assessment to determine its security and resilience based on standard datasets that were gathered. The primary evaluation criteria consist of accuracy, precision, recall, and F1-score, as outlined in Equations 1, 2, 3, and 4[22].

$$Acc = \frac{TP + TN}{TP + FP + FN + TN} \times 100\% \quad (1)$$

$$Pre = \frac{TP}{TP + FP} \times 100\% \quad (2)$$

$$Sen = \frac{TP}{TP + FN} \times 100\% \quad (3)$$

$$F1 = \frac{2 \times Pre \times Sen}{Pre\ Sen} \times 100\% \quad (4)$$

where, Acc is the accuracy, Pre is the precision, Sen is the sensitivity, $F1$ is the F1-score, TP is the true positives, FP is the false positives, FN is the false negative, and TN is the true negatives.

IV. Results and Discussion

This section provides the outcomes and implications of the proposed intrusion detection models using two forms of processed datasets.

A. CNN Mode with GRU and SelectKBest Feature Selection Methods

The model that integrates CNN with GRU, enhanced through the SelectKBest feature selection technique, demonstrated remarkable effectiveness in identifying intrusions within IoT network datasets. A comparative evaluation of three intrusion detection models utilized on the NSL-KDD dataset is displayed in Table 1.

TABLE I. DDoS Detection Models' Performances with NSL-KDD Dataset

Parameter	GRU+GA Model	CNN + GRU + SelectKBest Model	Autoencoder + Classifier + GA Model
Accuracy	0.9734	0.9817	0.9786
Precision	0.9736	0.9833	0.9787
Recall	0.9734	0.9825	0.9786
F1-Score	0.9734	0.9829	0.9786
AUC-ROC	0.0069	0.9983	0.9973
Type I Error	0.0406	0.0192	0.0321
Type II Error	0.0142	0.0175	0.0120

From the observations in Table 1, these conclusions can be drawn. The GRU+GA model is effective for sequential intrusion pattern learning, utilizing Genetic Algorithms for optimizing hyperparameters and features. It performs well in identifying temporal attack patterns, although it may have a slightly higher rate of false positives. The CNN+GRU+SelectKBest model represents a hybrid deep learning approach where CNN is responsible for extracting spatial and local dependency features, while GRU focuses on capturing temporal dependencies. SelectKBest conducts statistical feature selection, which helps in minimizing redundancy and noise. This combination results in the highest accuracy and precision among the models tested, indicating an effective balance between feature extraction and time-sequence modelling.

The Autoencoder+Classifier+GA Model employs an Autoencoder for unsupervised feature reduction and the reconstruction of normal patterns. The features produced are then classified using a supervised classifier, such as MLP, with Genetic Algorithms fine-tuning crucial parameters. This model shows improved performance over GRU+GA but is slightly outperformed by CNN+GRU, suggesting it has strong reconstruction abilities, albeit with less discriminative power. In terms of performance metrics, accuracy reflects the fraction of correctly classified samples, including both attacks and normal instances.

The CNN+GRU+SelectKBest model achieved an impressive accuracy of 0.9817, indicating it accurately classified 98.17% of the total samples. The GRU+GA model followed closely with an accuracy of 0.9734, while Autoencoder+GA recorded a moderate 0.9786. Thus, the hybrid feature extraction and selection approach of CNN+GRU+SelectKBest leads to more precise detection. Precision assesses the proportion of identified intrusions that are genuine threats, highlighting the rate of false positives. The CNN+GRU+SelectKBest model exhibited the highest precision at 0.9833, showcasing its reliability in reducing false alarms. This is particularly significant in smart farm or IoT environments, where fewer false alerts can lead to less unnecessary responses to typical traffic. Recall, or sensitivity, indicates how many actual attacks were accurately detected. Again, CNN+GRU+SelectKBest excelled with a recall of 0.9825, followed by Autoencoder+GA at 0.9786. A higher recall is crucial for ensuring the integrity of IoT network security by minimizing missed attacks.

The F1-Score, which represents the harmonic mean of precision and recall, was highest in the CNN+GRU+SelectKBest model at 0.9829, confirming its optimal balance between attack detection and false alarm reduction. The AUC-ROC measures the model's capability to differentiate between attack and normal instances. All three models achieved an AUC above 0.99, indicating excellent classification efficacy, with CNN+GRU+SelectKBest reaching a near-perfect score of 0.9983.

In analyzing error rates, Type I Error (False Positive Rate) reflects the frequency of normal instances incorrectly categorized as attacks. The CNN+GRU+SelectKBest model had the lowest rate at 0.0192, equating to about 1.9% false alarms, while the GRU+GA model had a higher rate at 0.0406, indicating a greater likelihood of triggering false alerts. The hybrid structure of CNN-GRU+SelectKBest effectively mitigates over-sensitivity to normal variations, which is essential for minimizing false alerts in smart farm

systems. Conversely, Type II Error (False Negative Rate) measures missed attacks that are classified as normal. The Autoencoder+GA model recorded the lowest rate at 0.0120, excelling at detecting hidden or stealthy attacks. The CNN+GRU+SelectKBest model had a slightly higher rate at 0.0175 yet remained low. This suggests that the Autoencoder's latent representation is adept at capturing subtle anomalies, thus reducing the chances of missed detections.

Table 2 presents the confusion matrices corresponding to the three intrusion detection models, detailing True Negatives (TN), False Positives (FP), False Negatives (FN), and True Positives (TP). Each matrix illustrates the performance metrics of the models in relation to these key terms.

TABLE II. CONFUSION MATRICS OF THE DDOS DETECTION MODELS WITH NSL-KDD DATASET

Model	TN	FP	FN	TP
GRU+GA	2269	96	38	2636
CNN+GRU+SelectKBest	2304	45	47	2643
Autoencoder+GA	2289	76	32	2642
Model	TN	FP	FN	TP
GRU+GA	2269	96	38	2636
CNN+GRU+SelectKBest	2304	45	47	2643
Autoencoder+GA	2289	76	32	2642

In Table 2, the combination of CNN+GRU+SelectKBest exhibits the lowest false positives (FP) at 45, indicating that it seldom misidentifies normal traffic as attacks. On the other hand, Autoencoder+GA records the fewest false negatives (FN) at 32, thereby identifying a greater number of attacks. Meanwhile, GRU+GA delivers reasonable performance but demonstrates a slightly higher FP count, reflecting an increased Type I Error rate.

Table 3 presents a comparative performance assessment of three deep learning-based models for intrusion detection: GRU+GA, CNN+GRU+SelectKBest, and Autoencoder+Classifier+GA. These models were evaluated using the CIC-DDoS2019 dataset, which includes a variety of real-world Distributed Denial-of-Service (DDoS) attack patterns alongside normal traffic flows. This dataset serves as an excellent benchmark for assessing security measures in smart farming networks.

TABLE III. CONFUSION MATRICS OF THE DDOS DETECTION MODELS WITH CIC-DDOS2019 DATASET

Model	TN	FP	FN	TP
GRU+GA	2269	96	38	2636
CNN+GRU+SelectKBest	2304	45	47	2643
Autoencoder+GA	2289	76	32	2642
Model	TN	FP	FN	TP
GRU+GA	2269	96	38	2636
CNN+GRU+SelectKBest	2304	45	47	2643
Autoencoder+GA	2289	76	32	2642

According to the comparison presented in Table 3, the CNN+GRU+SelectKBest model demonstrated the best overall performance, surpassing both the GRU+GA and Autoencoder-based approaches. The Autoencoder+GA method was a close runner-up, exhibiting minimal detection errors and slightly lower complexity when compared to CNN+GRU. Although the GRU+GA model remains competent, it revealed some minor shortcomings in its rates of false positives and false negatives.

Table 4 illustrates the confusion matrices for the three intrusion detection models, detailing True Negatives (TN), False Positives (FP), False Negatives (FN), and True Positives (TP).

TABLE IV. CONFUSION MATRICES COMPARISIONS OF THE DDOS DETECTION MODELS WITH CIC-DDOS2019 DATASET

Parameter	GRU+GA Model	CNN + GRU + SelectKBest Model	Autoencoder + Classifier + GA Model
Accuracy	0.9856	1.0000	0.9992
Precision	0.9845	1.0000	0.9992
Recall	0.9886	1.0000	0.9992
F1-Score	0.9877	1.0000	0.9992
AUC-ROC	0.98766	1.0000	0.9999
Type I Error	0.0016	0.0000	0.0007
Type II Error	0.0062	0.0000	0.0010

In Table 4, the CNN+GRU+SelectKBest model shows a zero false positive rate, indicating it seldom misclassifies normal traffic as attacks. In contrast, the Autoencoder+GA model records the lowest false negative rate at 19, successfully identifying a greater number of attacks. The performance of CNN+GRU+SelectKBest is notable, reflecting flawless Type I and Type II error rates. These findings highlight the effectiveness of deep hybrid models that merge feature selection with sequential learning for detecting DDoS attacks in IoT-driven smart farming settings, where traffic patterns are constantly changing and varied. The CNN+GRU+SelectKBest framework offers real-time adaptability, scalability, and resilience against network-layer threats, making it an excellent choice for implementation on smart farm gateways or edge devices.

Table 5 details the performance of each intrusion detection model, evaluating standard metrics such as accuracy, precision, recall, AUC-ROC, Type I error, and Type II error.

TABLE V. THE OVERALL BREAKDOWN OF THE MODELS'PERFORMANCES

Criterion	Best Model	Implications
Accuracy	CNN+GRU+Select KBest	Highest overall detection rate
Precision	CNN+GRU+Select KBest	Fewest false alarms
Recall	CNN+GRU+Select KBest	Detects most attacks
AUC-ROC	CNN+GRU+Select KBest	Near-perfect separability

Type I Error	CNN+GRU+Select KBest	Lowest false positive rate
Type II Error	Autoencoder+GA	Best in detecting stealthy attacks

According to Table 5, the CNN+GRU+SelectKBest model achieves the optimal balance among detection accuracy, false alarm rates, and overall robustness. It successfully identifies spatial-temporal attack patterns within IoT and smart farm data while effectively reducing both Type I and Type II errors. The Autoencoder+GA model also shows impressive performance, especially in minimizing undetected attacks (Type II errors), which makes it particularly useful for anomaly detection in unsupervised or zero-day situations. On the other hand, the GRU+GA model is dependable but falls short in terms of feature discrimination and sensitivity to normal fluctuations.

V. Conclusion

This paper provides a comparative analysis of three enhanced deep learning models (GRU+GA, CNN+GRU+SelectKBest (proposed), and Autoencoder+GA) specifically for detecting Distributed Denial-of-Service (DDoS) intrusions. Extensive testing was conducted using the NSL-KDD and CIC-DDoS2019 datasets. The results revealed that the proposed CNN+GRU+SelectKBest model consistently surpassed the others, achieving remarkable outcomes in detection accuracy, precision, recall, and F1-score.

Notably, it demonstrated flawless classification on the CIC-DDoS2019 dataset, with no false positives or negatives, showcasing its adaptability, reliability, and resilience against intricate cyberattack strategies. By integrating convolutional and recurrent layers, the model effectively captured both spatial and temporal features. Additionally, the incorporation of SelectKBest for feature selection, along with GA optimization, significantly improved learning efficiency and minimized misclassification.

The findings indicate that hybrid models that merge evolutionary optimization with deep learning can greatly enhance the performance of Intrusion Detection Systems (IDS) across various datasets.

The proposed CNN+GRU+SelectKBest model presents a viable approach to improving network security in practical settings such as smart farming systems, IoT infrastructures, and corporate networks. Its impressive accuracy, minimal false alarm rate, and efficient computational performance make it an ideal candidate for implementation in intrusion prevention systems (IPS) and security information and event management (SIEM) solutions. By adopting this model, organizations can enhance their proactive threat detection capabilities, minimize system downtime, and bolster their defences against extensive DDoS attacks and various forms of network intrusions.

Future research will aim to apply the CNN+GRU+SelectKBest framework within real-time intrusion detection settings, utilizing streaming network data from smart farm environments. There will be a strong focus on enhancing computational efficiency to facilitate deployment in large-scale and resource-limited systems. Further investigations will also include the integration of explainable AI (XAI) techniques to improve the interpretability, trust, and transparency of detection outcomes. Additionally, expanding this framework to detect multi-vector and zero-day attacks will be essential for developing a more adaptive and resilient cybersecurity infrastructure that can dynamically address evolving network threats.

Acknowledgment

Authors wish to thank TETFUND for providing funds for the research and all authors whose work were cited.

References

[1] Z. Wei et al., "CatBoost-based Intrusion Detection Method for the Physical Layer of Smart Agriculture," in ITM Web of Conferences, AISS 2023, 2024, pp. 1–8. doi: https://doi.org/10.1051/itmconf/20246000009 attacks.

[2] S. Mandal, A. Yadav, F. A. Panme, K. Monika, and S. K. S. M, "Smart Agricultural Technology Adaption of smart applications in agriculture to enhance production," Smart Agric. Technol., vol. 7, no. March, p. 100431, 2024, doi: 10.1016/j.atech.2024.100431.

[3] J. H. Park, S. Yotxay, S. K. Singh, and J. H. Park, "PoAh-Enabled Federated Learning Architecture for DDoS Attack Detection in IoT Networks," Human-centric Comput. Inf. Sci., vol. 14, no. 03, pp. 1–24, 2024, doi: https://doi.org/10.22967/HCIS.2024.14.003.

[4] E. I. Elsedimy and S. M. M. Abohashish, "An intelligent hybrid approach combining fuzzy C-means and the sperm whale algorithm for cyber attack detection in IoT networks," Sci. Rep., vol. 15, no. 1005, 2025, doi: https://doi.org/10.1038/s41598-024-79230-4 1.

[5] R. Ferreira, I. Bispo, C. Rabadão, L. Santos, and R. L. de C. Costa, "Farm-flow dataset: Intrusion detection in smart agriculture based on network flows," Comput. Electr. Eng., vol. 121, p. 109892, 2025, doi: 10.1016/j.compeleceng.2024.109892.

[6] M. R. Minhas et al., "F-OSFA: A Fog Level Generalizable Solution for Zero-Day DDOS Attacks Detection," IEEE Access, vol. 13, pp. 75157–75170, 2025, doi: 10.1109/ACCESS.2025.3557822.

[7] E. M. Pasca, D. Delinschi, R. Erdei, I. Baraian, and O. D. Matei, "A Vulnerable-by-Design IoT Sensor Framework for Cybersecurity in Smart Agriculture," Agriculture, vol. 15, p. 1253, 2025, doi: https://doi.org/10.3390/ agriculture15121253.

[8] D. P. Kumar and R. Nithya, "Improving DDoS Detection Capabilities with Machine Learning Techniques," Junikhyat, vol. 14, no. 01, pp. 21–32, 2024.

[9] A. R. Riaz, S. M. M. Gilani, S. Naseer, S. Alshmrany, M. Shafiq, and J. Choi, "Applying Adaptive Security Techniques for Risk Analysis of Internet of Things (IoT)-Based Smart Agriculture," Sustainability, vol. 14, p. 10964, 2022.

[10] M. A. Ferrag, L. Shu, D. Hamouda, and K.-K. R. Choo, "Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0," Electronics, vol. 10, p. 1257, 2021, doi: 10.3390/electronics10111257.

[11] M. Ali, Y. Saleem, S. Hina, and G. A. Shah, "Internet of Things DDoSViT: IoT DDoS attack detection for fortifying firmware Over-The-Air (OTA) updates using vision transformer," Internet of Things, vol. 30, p. 101527, 2025, doi: 10.1016/j.iot.2025.101527.

[12] G. Al Sukkar and S. Al-Sharaeh, "Enhancing Security in Wireless Sensor Networks: A Machine Learning-based DoS Attack Detection," Eng. Technol. Appl. Sci. Res., vol. 15, no. 1, pp. 19712–19719, 2025, doi: https://doi.org/10.48084/etasr.7191.

[13] K. Saranya and A. Valarmathi, "A multilayer deep autoencoder approach for cross layer IoT attack detection using deep learning algorithms," Sci. Rep., vol. 15, p. 10246, 2025, doi: https://doi.org/10.1038/s41598-025-93473-9 1.

[14] J. Shaikh, T. A. Syed, S. A. Shah, S. Jan, Q. U. Ain, and P. K. Singh, "Advancing DDoS attack detection with hybrid deep learning: integrating convolutional neural networks, PCA, and vision transformers," Int. J. Smart Sens. Intell. Syst., vol. 17, no. 1, pp. 1–16, 2024, doi: 10.2478/ijssis-2024-0040.

[15] W. A. Silas, L. Nderu, and D. Ndirangu, "A distributed framework for distributed denial-of-service attack detection in internet of things environments using deep learning A distributed framework for distributed denial-of-service attack detection in internet of things environments using deep lear," Int. J. Web Eng. Technol., vol. 19, no. 1, pp. 67–87, 2024, doi: 10.1504/IJWET.2024.10062503.

[16] O. Polat et al., “Multi-Stage Learning Framework Using Convolutional Neural Network and Decision Tree-Based Classification for Detection of DDoS Pandemic Attacks in SDN-Based SCADA Systems,” Sensors, vol. 24, p. 1040, 2024, doi: https://doi.org/10.3390/s24031040.

[17] A. Hussain, E. M. Tordera, X. Masip-Bruin, and H. C. Leligou, “Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS),” IEEE Access, vol. 12, pp. 114894–114911, 2024, doi: 10.1109/ACCESS.2024.3445261.

[18] M.-R. Fida, A. H. Ahmed, and A. S. Arsalaan, “IoTShield: Defending IoT Systems Against Prevalent Attacks Using Programmable Networks,” IEEE Access, vol. 13, pp. 136446–136457, 2025, doi: 10.1109/ACCESS.2025.3594580.

[19] M. Aldossary, H. A. Alharbi, C. Anwar, and U. Hassan, “Internet of Things (IoT)-Enabled Machine Learning Models for Efficient Monitoring of Smart Agriculture,” IEEE Access, vol. 12, pp. 75718–75734, 2024, doi: 10.1109/ACCESS.2024.3404651.

[20] S. Mehmood, R. Amin, J. Mustafa, M. Hussain, F. S. Alsubaei, and M. D. Zakaria, “Distributed Denial of Services (DDoS) attack detection in SDN using Optimizer-equipped CNN-MLP,” PLoS ONES, vol. 20, no. 1, p. e0312425, 2025, doi: 10.1371/journal.pone.0312425.

[21] M. A. Talukder and M. A. Uddin, “CIC-DDoS2019 dataset,” Mendeley Data, vol. VI, 2023, doi: https://doi.org/10.17632/ssnc74xm6r.1.

[22] 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, p. 233, 2023.