Array 31 (2026) 101072

Contents lists available at ScienceDirect

Array

journal homepage: www.sciencedirect.com/journal/array

An intelligent and secure IoT-based framework for crop price prediction in smart agriculture

R. Nithya *, N. Narmadhavarshini

Department of CSE, Vivekanandha College of Engineering for Women, Tiruchengode, 637205, India

ARTICLE INFO

Keywords:
Crop price prediction
Rural farmers
Internet of things
Smart agriculture
Information gain
Rectified adam
Graph convolutional network

ABSTRACT

Internet of Things (IoT) has become a revolutionary technology that links sensors, devices, farm machinery, and stakeholders to enhance efficiency and decision-making in farming. Smart agriculture will allow cost savings, increase in yields, optimization of resources, and remote monitoring. Nonetheless, the extensive implementation of IoT systems presents security risks of cyber attacks that can undermine the integrity of data and farm activities. At the same time, climate variability, market demand, and uncertainty in the supply chain lead to economic risks to rural farmers due to fluctuation in crop prices. This study proposes a Crop Price Prediction and Recommendation System for Rural Farmers (CPP-RSRF) approach. The major intention of this paper is to present a secure IoT-based system for accurate crop price prediction. The proposed model implements dual stages, namely, predicting crop prices and the attack detection process. For the crop price prediction stage, the proposed CPP-RSRF technique primarily pre-process the input data using min-max scaling normalization to enhance further investigation. Following that, a temporal convolutional network and transformer with a self-attention module are employed to predict crop price. Along with that, the rectified adam is utilized for tuning parameters and boosting the model's performance. For the attack classification stage, an information gain is used for selecting features and determining the most informative features. In addition, the graph convolutional network is used for securing IoT in the agricultural section via intrusion detection process. Experimental findings indicate that CPP-RSRF had higher forecasting accuracy and intrusion detection performance than recent baseline models, and thus can be used in secure smart agriculture applications.

1. Introduction

Internet of Things (IoT) denotes the device network that has the capability to collect, connect and exchange data to external devices across the Internet. IoT is a transformative technology that has significant applications in several domains of engineering and sciences like traffic, logistics, and healthcare, agriculture and gas and oil industries [1]. In the agricultural segment, the farmer still use traditional agriculture techniques, resulting in lower-crop and fruit yields. The incorporation of IoT in the traditional agriculture approach has led to important changes in the agriculture domain. Various sensors and IoT devices are providing the services to automate agricultural accuracy and to track crop conditions [2]. These IoT devices are applied in agricultural fields to improve the yields production through creating smart farming decisions and to gather crops temperature data, humidity level and irrigation infrastructure. Farm-based commodities are traded in world-wide marketplaces [3]. This associated with potential risks and benefits for all stakeholders involved. By the side of, market mechanisms could support implementing fair prices via enabling farmers and agribusinesses to “lock” costs by futures agreements and decisions, stabilize their income levels, and help long-range planning [4]. On the other hand, the commodity exchanges could be affected by conjectural activity and that make prices extremely volatile and detached from fundamental factors. In addition, small-scale farmers in several developing countries might lack the necessary infrastructure, data, or financial expertise to employees and advantages from the trade network [5]. The price variation in agricultural fields poses important challenges for traders, farmers, policymakers, and consumers similarly. Unexpected and unpredictable variations in costs could disrupt income, destabilize planning for farmers, and lead to inflation, social unrest, and food insecurity [6].

Machine learning (ML) has been utilized in farming for many years. Crop yield forecast is a major challenging concern in agricultural accuracy, and few methods have been presented and examined so far. This

* Corresponding author.
E-mail addresses: nithyaravicse@gmail.com (R. Nithya), narmadhavarshini6@gmail.com (N. Narmadhavarshini).

https://doi.org/10.1016/j.array.2026.101072
Received 11 February 2026; Received in revised form 24 June 2026; Accepted 6 July 2026
Available online 8 July 2026
2590-0056/© 2026 The Authors. Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

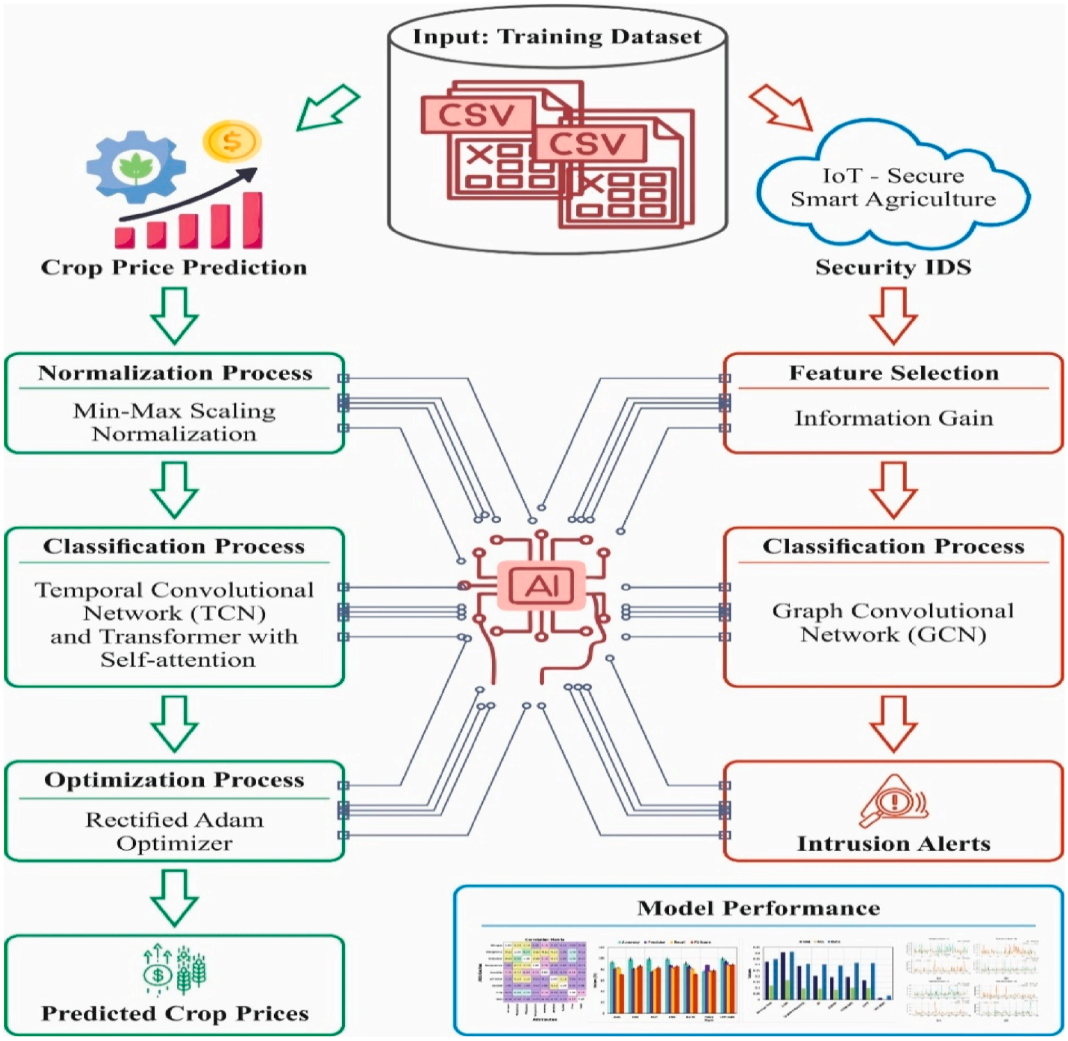


Fig. 1. Entire workflow of proposed CPP-RSRF technique.

concerns the demand for the usage of many datasets as crop yield depends on several aspects like weather, climatic conditions, soil-type, use of fertilizer, and variety of seed [7]. This specifies that the crop yield estimation is not an easy task; rather, it involves several complex procedures. Recently, crop yield prediction methods could predict the real yield reasonably, but a further improvement in yield estimation is still needed [8]. ML is a subset of Artificial Intelligence (AI) concentrating on learning, that can be a feasible method and delivered great yield prediction on the basis of many features. ML can conclude the correlations and patterns and extract knowledge from datasets [9]. The approaches must be trained utilizing datasets, where the results are characterized on the basis of previous experience. The predictive method is developed using many features, and like parameters of the techniques are determined employing historical data during the training process. During the testing phase, a subset of the historical data that doesn't applied for training is utilized for the performance evaluation [10].

The latest developments in smart agriculture have shown that IoT technology can be used to create effective monitoring systems, machine learning-based crop forecasting models, and deep learning-based intrusion detection systems. Currently, most of the related studies are dedicated to either cyber security protection tasks or agricultural prediction tasks separately. Thus, this subject of how crop price forecasting and IoT security interact has been largely unexplored. Some of the traditional crop price prediction methods have limitations in both temporal characteristics and long time scale dependency in agricultural market data which cause less accuracy in prediction. Likewise, existing IDSs used in the agricultural IoT networks often lack feature representation and fail to leverage graph-structured network relationships. This study proposes a Crop Price Prediction and Recommendation System for Rural Farmers (CPP-RSRF) approach. The primary aim of this paper is to develop a secure IoT-based system for precise crop price prediction. The proposed method follows two processes like crop price prediction and enabling secure smart agriculture.

Novelty and Contribution.

- Integrate the temporal convolutional network (TCN) and transformer with a self-attention module for predicting crop price, together with the rectified adam (Radam) optimizer for tuning hyperparameters and improving the performance of the model.
- Utilize information gain (IG) for selecting relevant features, and a graph convolutional network (GCN) for classifying and acquiring graph-based data, thereby enhancing secure smart agriculture.
- Validate the performance of the proposed CPP-RSRF method on dual benchmark datasets namely crop price prediction and TON_IoT datasets.

2. Literature survey of crop price prediction

This section briefly reviews previous research works of crop price prediction. Sizan [11] presented an innovative algorithm combining ML,

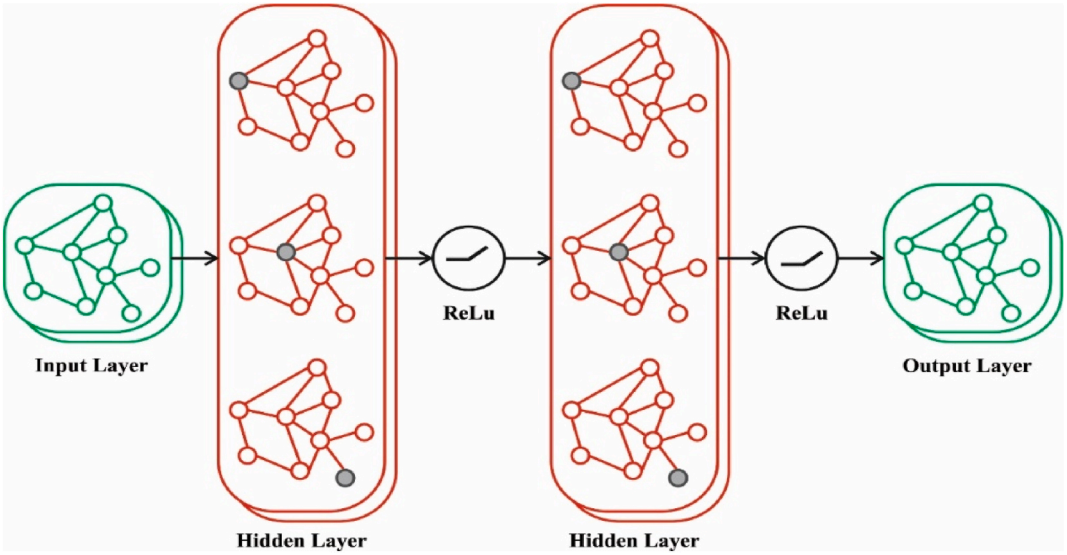


Fig. 2. Structure of the GCN approach.

Table 1
Dataset description.

Dataset	Source	Samples	Features	Purpose
Crop Price Dataset	Kaggle	Historical Records	Price, Crop, Weather	Forecasting
ToN-IoT	UNSW Canberra	119,957	43	Intrusion Detection

Table 2
Experimental setup hyperparameter settings.

Parameter	Value
TCN Layers	3
Kernel Size	3
Filters	64
Transformer Layers	2
Attention Heads	4
Hidden Units	128
Batch Size	32
Epochs	50
Learning Rate	0.001
Optimizer	RAdam

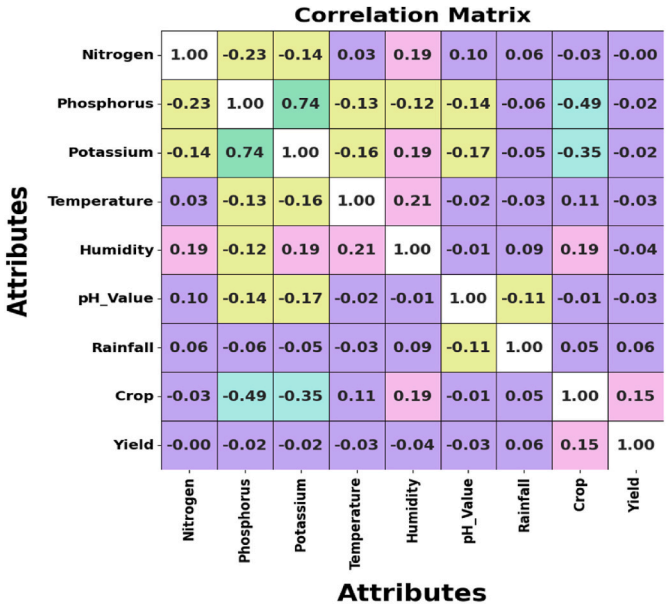


Fig. 3. Correlation matrix of CPP-RSRF model.

IoT, and blockchain (BC) methods. Utilizing IoT, real-life data from the sensor networks constantly monitoring the ecological factors and fertility of soils, considerably increasing this comprehension of crop growing strategies. To assure the integrity and security of the sensor data employed for such predictions, the author combines the Ethereum BC, which gives a secure and efficient framework. It allows the predicted data remain reliable and protected. Addanki [12] developed an approach for incorporating drones, IoT, and AI within Agriculture 4.0, which converts standard farming techniques, improving sustainability and efficiency. Though the combination of IoT devices in wide fields gives significant cybersecurity concerns, a tendency towards Distributed Denial of Service (DDoS) threats and the capable to data manipulation. Such attacks impair the dependability, safety, and integrity of agricultural methods, highlighting the imperative requirement for serious security measures. The current study emphasizes the effectiveness of IDSs in identifying and mitigating such threats.

Mohy-eddine et al. [8] developed a network IDSs (NIDSs) for moderating the smart agriculture security attacks. The author enhances the architecture employing radial basis function neural networks (RBFNNs) for detecting and classifying the interruptions in the IoT system. The author used a collective intellect tree-driven ML models for selecting related features in the datasets. The author utilized 1 class support vector machine (1-CSVM) for identifying and removing the outliers. Kethineni and Pradeepini [13] introduced an innovative and efficient DL-based architecture is improved for detecting the intrusions in smart agricultural techniques. This framework is 3 types with the initial tier existence of the sensor layer that includes the assignment of sensors in farming fields. Then, another type is the Fog Computing Layer (FCL) that includes Fog nodes, and the presented IDS can be applied in every Fog node. The collected data is transmitted to this fog layer for more data examination. The final type is the cloud computing layer (CCL) that gives comprehensive services and data storage. This approach consists of a hybrid CNN system with the bidirectional gated recurrent unit (Bi-GRU) technique for identifying and classifying the attackers.

Aldhyani and Alkahtani [14] proposed NIDSs that may be used in Agriculture 4.0 systems, and efficient DL techniques were recently utilized. An adjustable and effectual IDS could be applied by employing the frameworks of a convolutional neural network (CNN) integrated with

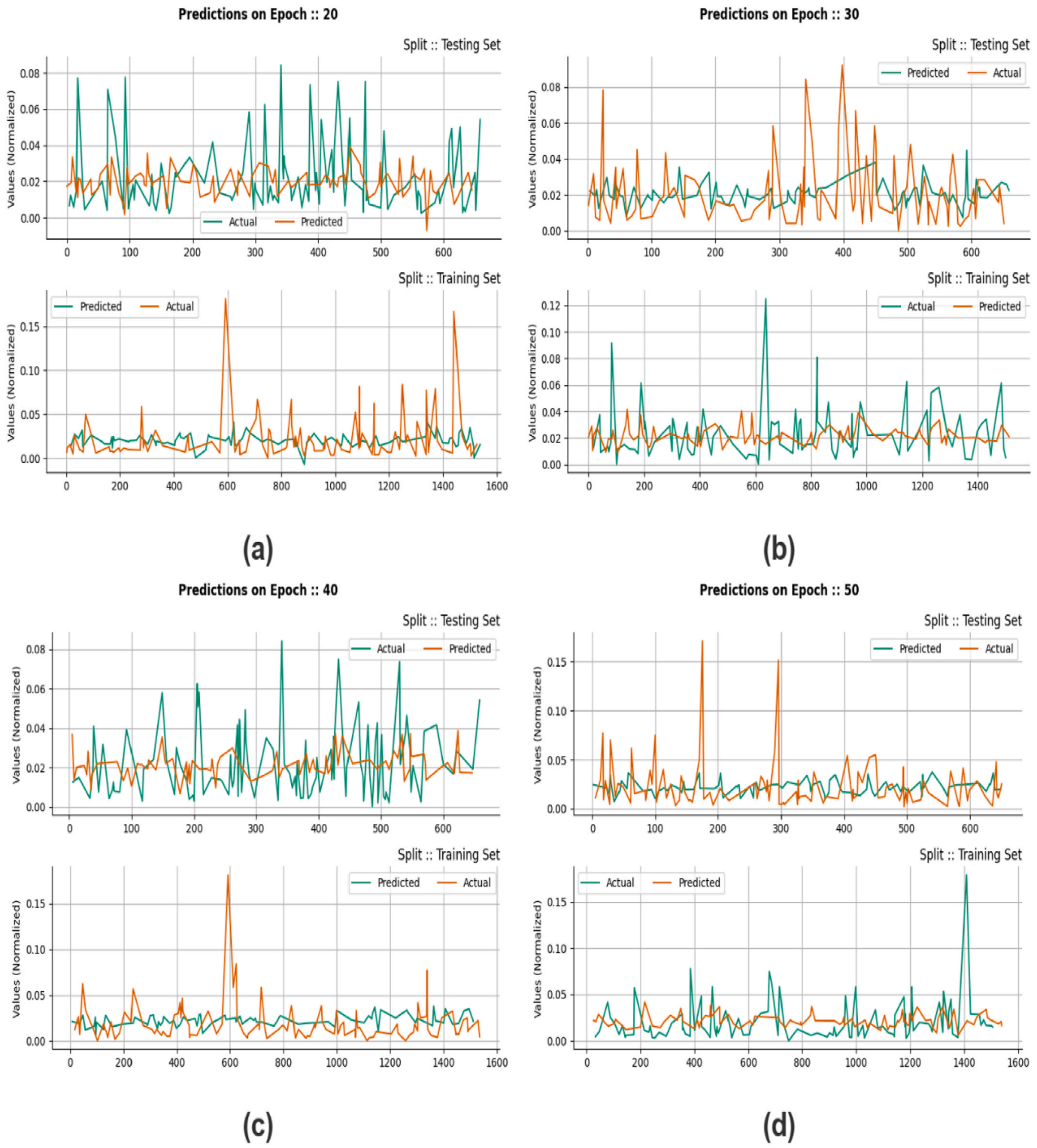


Fig. 4. Actual and predicted of CPP-RSRF model.

Table 3
Training and testing sets of the CPP-RSRF model with different metrics.

Metrics	Training Set	Testing Set
MSE	0.00115	0.00040
RMSE	0.03386	0.01994
MAE	0.01550	0.01395
MAPE	9.09164	6.57797

long short-term memory (CNN–LSTM) to detect DDoS threats. This approach has been capable of attaining a higher degree of accuracy. El-Ghamry et al. [15] presented an advanced context that identifies intrusions in IoTs employed in agriculture. The smart farming on the environment improved due to the dependency of IoT systems, they develop more vulnerable to cyber-attacks. This is the cause, the IoT systems contain vast number of nodes with some resources obtainable, creation securing them a stimulating concern. Consequently, the require

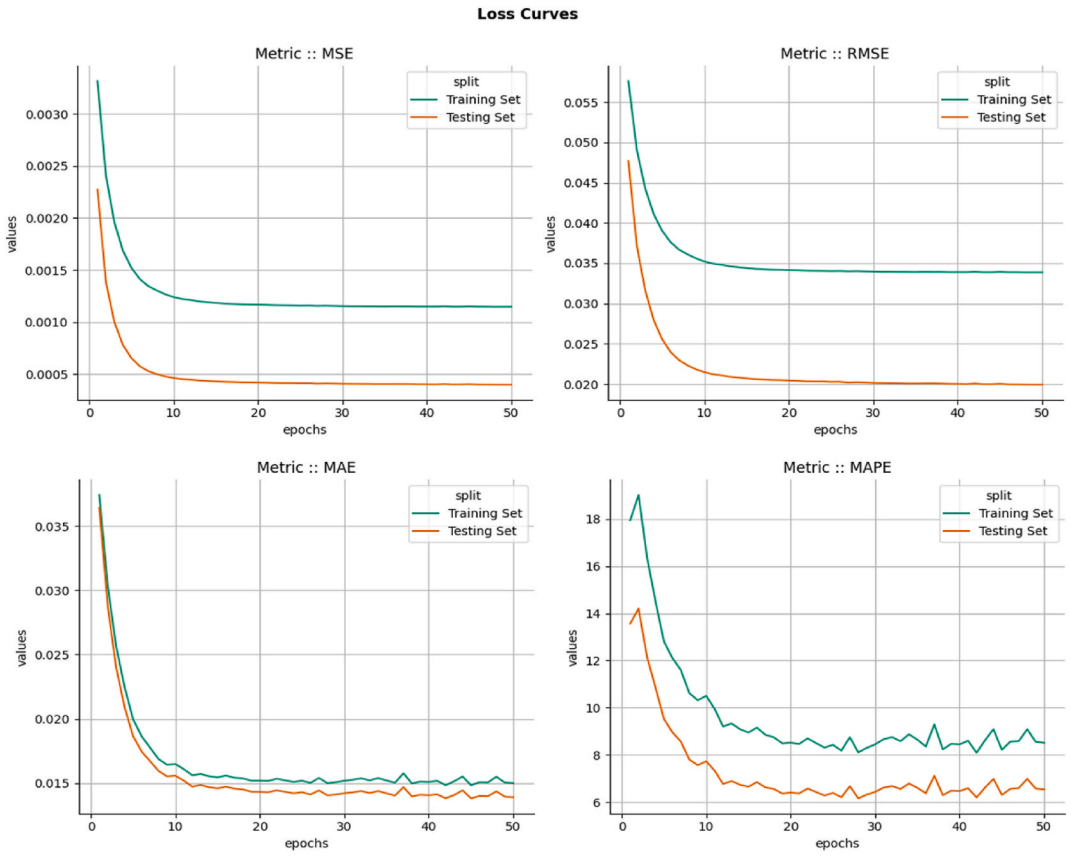


Fig. 5. Loss curve of CPP-RSRF model.

Table 4
Comparative study of CPP-RSRF method with existing models.

Algorithms	MAE	MSE	RMSE
Decision Tree	0.3260	0.1210	0.3479
k-NN	0.4060	0.1690	0.4111
Gradient Boosting	0.2860	0.0950	0.3082
RF	0.2030	0.0930	0.3050
1DCNN	0.1930	0.0850	0.2915
LSTM-DBN	0.1940	0.1010	0.3178
CYPA	0.1660	0.0990	0.3146
CPP-RSRF	0.0155	0.0012	0.0339

Table 5
Details of dataset.

Classes	No. of Count
Normal	78369
MiTM	336
DoS	5440
DDoS	5987
Password	6016
Injection	5867
XSS	5951
Ransomware	5976
Backdoor	6015
Total Count	**119957**

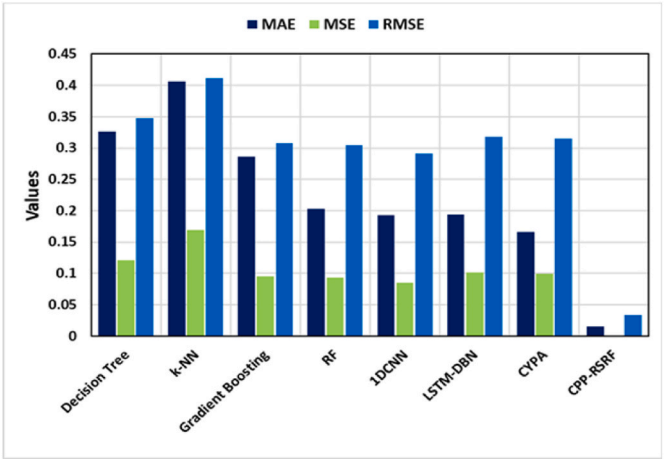


Fig. 6. Comparison outcomes of the CPP-RSRF model.

for an IDS that can adapt to these problems is the main significance. Kethineni. and Gera [16] proposed an IoT-driven privacy-enhancing abnormality detection method for smart farming. The intention of this technique is twofold. Initially, securing data privacy in IoT-driven agriculture is among the main significance because of the capacities of sensitive data gathered by IoT systems, including crop health, environmental factors, and resource use data. Another one, the accurate identification of abnormalities in smart agricultural techniques, is crucial for allowing active involvements, like avoiding, optimizing resource allocation, crop impairment, and securing sustainable farming methods.

Morchid et al. (2026) suggested a smart irrigation system based on Internet of Things (IoT) and cloud computing to achieve sustainable farming. The system used sensors to measure the temperature, air humidity, soil humidity, and water level, and an ESP32 microcontroller sent the information to the ThingsBoard cloud service to be analyzed in real-time. The automated algorithm used sensor readings to regulate irrigation pumps to make best use of water. The experimental outcomes revealed less water waste, and more accurate irrigation, as well as

Table 6
Confusion matrices and classifier outcomes of the CPP-RSRF method with 70:30 split.

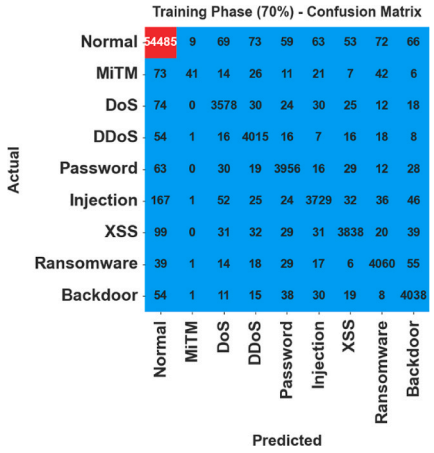
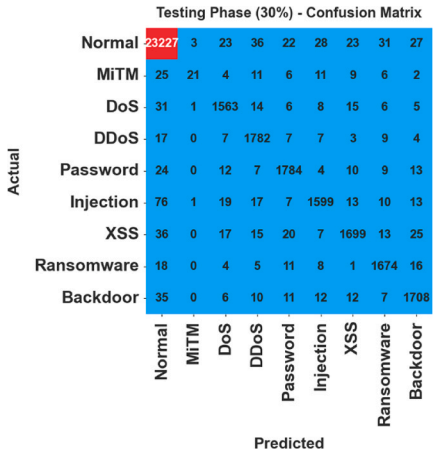
Confusion Matrix	Classes	$Accur_y$	$Preci_n$	$Recal_l$	F_{score}	MCC
	Normal	98.71	98.87	99.16	99.01	97.14
	MiTM	99.75	75.93	17.01	27.80	35.87
	DoS	99.46	93.79	94.38	94.08	93.80
	DDoS	99.55	94.40	96.72	95.55	95.32
	Password	99.49	94.51	95.26	94.88	94.61
	Injection	99.29	94.55	90.69	92.58	92.23
	XSS	99.44	95.35	93.18	94.25	93.97
	Ransomware	99.52	94.86	95.78	95.32	95.07
	Backdoor	99.47	93.82	95.82	94.81	94.54
	Average	**99.41**	**92.90**	**86.44**	**87.59**	**88.06**
	Normal	98.74	98.88	99.18	99.03	97.22
	MiTM	99.78	80.77	22.11	34.71	42.19
	DoS	99.51	94.44	94.78	94.61	94.35
	DDoS	99.53	93.94	97.06	95.47	95.24
	Password	99.53	95.20	95.76	95.48	95.23
	Injection	99.33	94.95	91.11	92.99	92.66
	XSS	99.39	95.18	92.74	93.95	93.63
	Ransomware	99.57	94.84	96.37	95.60	95.38
	Backdoor	99.45	94.21	94.84	94.52	94.23
	Average	**99.43**	**93.60**	**87.10**	**88.49**	**88.90**

Table 7
Comparison outcomes of CPP-RSRF method with existing models.

Models	$Accur_y$	$Preci_n$	$Recal_l$	F_{score}
ADA	92.96	81.52	82.96	70.81
KNN	98.50	81.09	81.50	86.00
MLP	98.54	76.13	79.54	83.12
CNN	98.32	86.91	82.32	85.16
LSTM	90.94	85.09	80.94	71.26
Naïve Bayes	76.98	88.07	76.98	77.83
CPP-RSRF	99.43	93.60	87.10	88.49

flexibility to other crops and land conditions [17]. Goswami et al. (2022) demonstrated that neural network-driven secure resource allocation models in IIoT settings can greatly enhance communication efficiency and cybersecurity resilience, inspiring combined AI-driven smart agriculture systems [18].

3. System architecture and methodology

This study is followed a systematic methodology for the prediction of crop prices and enables secure smart agriculture. The entire workflow of the proposed CPP-RSRF system is displayed in Fig. 1. The presented method follows dual processes namely crop price prediction and assuring secure smart agriculture.

Before the models were trained, a lot of data preprocessing was done to enhance the efficiency of learning and the quality of the data. Appropriate imputation techniques were used to investigate and analyze missing data. To prevent data duplication, duplicate records were removed. To ensure the uniform distribution of features, numerical attributes were normalized by using Min-Max Scaling and to prevent the domination of the attributes with larger numerical range.

The normalized feature value is calculated as:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

where X represents the original feature value, X_{min} denotes the minimum value of the feature, and X_{max} indicates the maximum value.

Using a ratio of 70:30, the crop price data set was split into a training and test set. Likewise, the ToN-IoT dataset was divided in order to assess the intrusion detection ability of a framework in realistic deployment scenarios.

3.1. Stage I: crop price prediction

Primarily, the min-max scaling normalization has been utilized for preprocessing, the TCN and transformer with a self-attention module are utilized for predicting long-range sequential data and RAdam for parameter tuning.

3.1.1. Data scaling

Min-Max Scaling: Measuring the data to a particular ranges for preserving the comparative relation among feature values [19].

$$x' = \frac{x - \min(\max_n - \min_n)}{\max - \min} + \min_n \quad (1)$$

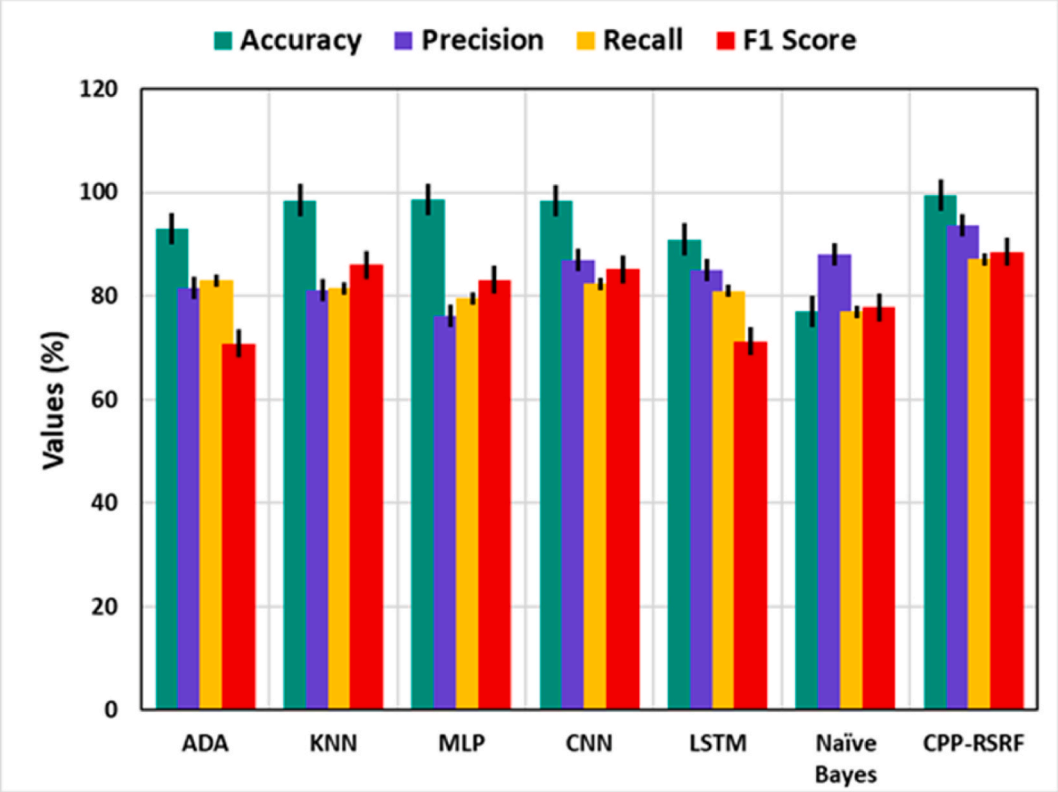


Fig. 7. Comparison outcomes of CPP-RSRF model.

Here, the parameter x represents the primary input value, x' refers to the standardized values, min and max are the maximum and minimum feature values, correspondingly. Min-max data normalization is a technique that can be utilized for equalizing the weight of various features and causes to have a similar result on the decision- making process for ML and data analysis.

3.1.2. *Modeling of TCN and transformer with attention*

The presented hybrid framework integrates the capacities of TCN and Transformers using a sensibly designed combination mechanism [20]. The TCN module processes the input data employing enlarged convolutions for capturing the local temporal relations, producing features that encode short-term patterns. Concurrently, the Transformer component employs self-attention mechanisms to model global dependences and relations over several time steps. To allow expressive combination, the temporal responsive field of the TCN is associated with the Transformers attention mechanism, ensuring that both components concentrate on reciprocal temporal features of the data. The results of the TCN and Transformer are focused on forming a combined feature extraction that is consequently penetrated a fully associated layer for producing the last outputs. This design allows the hybrid system to use both long-term and short-term dependences efficiently though maintaining computational scalability and efficiency.

TCN: The TCN employs basic convolutions for ensuring that the predictions for time step t are only affected by earlier time steps, thus preventing information leakage from future data. For every input sequence $x = [x_1, x_2, \ldots, x_T]$, the TCN uses a series of 1D intricacies with enlargements for capturing the long- range dependences. Let the input sequence be signified as $x = [x_1, x_2, \ldots, x_T]$, Now, T refers to the distance of the input sequence and the term x_t denotes the input value at time step t. The convolutional process for a layer with dilation d and filter size k is specified by:

$$h_t^{(l)} = \sum_{i=0}^{k-1} W_i^{(l)} x_{t-d \cdot i}^{(l-1)} + b^{(l)} \tag{2}$$

The term $h_t^{(l)}$ remain the output in time step t for layer 1, $W_i^{(l)}$ signifies the convolution filter weights, and $b^{(l)}$ is a bias term. The dilation factor d handles the space among the input values, enabling the network to capture the extensive dependences. The last output of the TCN penetrates the Transformer component.

Transformer with self-attention: The Transformer component acquires the global dependences over various time steps employing a self-attention (SA) mechanism. The SA mechanism estimates the weighted sum of the input value order, where the weights are resolute depend on the significance of every time step to the present outcome. For a given input order $x = [x_1, x_2, \ldots, x_T]$, the SA mechanism initially estimates the keys K, queries Q, and values V with linear transformations as follows:

$$Q = W_q x, K = W_k x, V = W_v x \tag{3}$$

Where the terms W_q, W_k, and W_v describes the learned weight matrices for keys, values, and queries, correspondingly. The attention scores were measured as the dot product between the keys and queries, followed by a soft-max function for obtaining the attention weights as given in mathematical form,

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{4}$$

Where d_k is the key's dimensionality and, the given output of the SA mechanism is a weighted sum of the valuesV that acquire the dependences over the complete series. This attention-based illustration is penetrated by many layers of the Transformer, with every layer containing a multi-head attention mechanism (AM) and a positional-wise anticipate system. The SA mechanism acquires dependences over diverse time steps, emphasizing the roles of keys, values, and queries in

estimating attention values. The diagram supports understanding the relation among multi-head attention and the position-wise feedforward system in the Transformer layers.

Hybrid architecture: The combined framework integrates the Transformer and TCN outputs for creating a unified representation for predicting challenges. The TCN processes the input order for generating the features encoding short-term sequential dependences, when the Transformer utilizes SA for acquiring the global interactions over the series. Such outputs have been focused to form a complex feature extraction that can be penetrated by a FC layer for the last outcomes. For a given input series $X = [x_1, x_2, \ldots, x_T]$, the TCN process X to get H_{TCN}:

$$H_{TCN} = TCN(X) \tag{5}$$

Encoding local dependences over many time steps. Simultaneously, the Transformer controls on X to calculate

$$H_{Trans} = Transformer(X) \tag{6}$$

Where SA mechanisms acquire extensive dependences. Such outputs are focus to form the composite feature extraction:

$$H_{combined} = [H_{TCN}, H_{Trans}] \tag{7}$$

This hybrid representation is then penetrated by a fully associated layer for generating the last outcome:

$$\widehat{Y} = W_{fc} H_{combined} + b_{fc} \tag{8}$$

Where b_{fc} and W_{fc} are the bias term and weight matrix. The temporal responsive field of the TCN supports with the AM in the Transformer, assuring complementary feature extraction. This incorporation improves the model's capability for using both long-term and short-term dependences while handling computational efficacy. The model features are enhanced constantly, updating the Transformer and TCN components cooperatively to attain efficient predicting.

3.1.3. Radam optimizer

In Adam, the learning level changing adaptably, and the modification is high enough in the initial phases of maximization [21]. Rectified Adam (Radam), as a form of Adam, is intended for solving the variance difficulties of the learning level. Radam handles the change by calculating a correction parameter that validates the learning score. The rectification term drives the constant optimization at the initial phases of the training method.

Initially, Radam describes the degree of freedom (ρ_t) for the systematic form of variation as

$$P\tau = \frac{2}{1-\beta_2} - 1 - \frac{2t\beta_2^{\tau}}{1-\beta_2^{\tau}} \tag{9}$$

and the variance rectification factor (r_t) is given by,

$$r_t = \sqrt{\frac{(\rho_t - 4)(\rho_t - 2)\rho_{\infty}}{(\rho_{\infty} - 4)(\rho_{\infty} - 2)\rho_t}} \tag{10}$$

Where $\rho_{\infty} = 2/(1-\beta_2) - 1$. Later, when the variance can be manipulable, i.e., $\rho_t > 4$, Radam is updated the weights utilizing the variance rectification factor as represented by,

$$w_{t+1} = w_t - \frac{\eta_t r_t}{\sqrt{\widehat{\nu}_t}} \widehat{m}_t = w_t - \eta_t r_t l_t \widehat{m}_t, \tag{11}$$

Where l_t is declared as the adaptive learning rates, $l_t = 1/\sqrt{\widehat{\nu}_t}$.

Then, the weights can be restructured by employing the 1st moment that evaluates without adaptation as given below

$$w_{t+1} = w_t - \eta_t \widehat{m}_t \tag{12}$$

Consequently, dual different update methods are combined into a one update procedure for reducing the unnecessary volatility. In the Radam optimizer, the same hyper-parameter sceneries could be utilized as in Adam.

3.2. Stage II: attack detection

In this stage, the IG is implemented to select relevant features, and GCN is employed to acquire and categorize graph-based data.

3.2.1. Feature reduction using MI model

The IG is a significant feature selection (FS) technique broadly used by research workers for regulating the consequence threshold of features [22]. The value of data gain is acquired through removing the entropy values previously segregation after detachment. Mainly, the calculation is used as a first stage to regulate that attribute could be reserved for classification techniques. The procedure of FS employing IG contains of 3 phases:

1. Estimate IG for Every Attribute in the Original Dataset: In this phase, the IG value is calculated for every attribute in the original dataset.
2. Control the Desired Threshold: research workers set a boundary, enabling attributes with a weight equivalent to or bigger than the threshold to be engaged, while attributes lower than the threshold are rejected.
3. Improve the Dataset by decreasing Attributes: This phase includes reducing the dataset by eliminating attributes. The attributes measurement is defined as:

$$info(D) = -\sum_{i=1}^{m} pi \log_2(pi) \tag{13}$$

Now, the term D represents the sets of conditions, M indicates the count of divisions ofD, and *pi* denotes the amount of Di corresponding to D. *pi* signifies the possibility of a tuple in *D* appropriate to class *Ci* and is assessed by $|Ci,D|/|D|$. The logarithmic function employed as the data is encoded like bits. The estimation of the entropy values and then it could be accomplished utilizing the above mathematical expression:

$$inf\ o_A(D) = -\sum_{j=1}^{v} \frac{|D_j|}{|D|} \times I(D_j) \tag{14}$$

Here, $|Dj|$ indicates the number of cases in separation *j*, the term D indicates the types of conditions, A represents the attribute. *v* is the count of divisions of attribute *A*. $|D|$ denotes the entire number of cases in *D*. $I(Dj)$ represents the whole entropy.

$$Gain(A) = I(D) - I(A) \tag{15}$$

Now, the term $I(D)$ denotes the entire entropy, $Gain(A)$ implies the attribute of information *A*, and $I(D,A)$ indicates the attribute entropy *A*.

3.2.2. GCN based attack classification process

The GCN is an essential system in GNN, intended to effectively performs the graph- structured information [23]. Derived from CNNs that can be extracted spatial features in the grid-structured data, like GCNs, encompass this perception to non-Euclidean fields, images, wherever data points (nodes) have been related in arbitrary model. The main concept in GCNs is collecting the data within the adjacent nodes in an efficient method, enabling every node's representation as efficient depending on the local graph structure features. It makes GCNs mainly well appropriate for processes like links prediction, graph classification, and node classification, where acquiring the relations among entities is critical. Fig. 2 implies the architecure of the GCN method.

A GCN operating on an input graph containing of edges, nodes, and a related feature matrix. Every node begins with a first feature vector that is continually sophisticated with numerous layers of the network. Every GCN layer achieves a message-passing process, where nodes collecting

data from their instant neighbors, converting their feature extractions. The above procedure is precisely formulated as given below,

$$H^{(l+1)} = \sigma\left(\widetilde{D}^{-\frac{1}{2}}\widetilde{A}\widetilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)}\right) \quad (16)$$

Here, the term $\widetilde{A}$ is the adjacent matrix, $\widetilde{D}$ refers to the related degree matrix, $W^{(l)}$ is the learning weight matrix, $H^{(l)}$ signifies the node-feature matrix in layer l, and σ indicates a non-linear stimulation function (generally ReLU). The above process regularizes and disseminates information with the graph when preserving consistency in the learnable method. Utilizing many nodes, layers collect data from gradually higher neighborhoods, allowing the algorithm to acquire both global and local graph models. The last layer produces task-specific embeddings, which acquire the relevant representations tailor-made to the learnable objective. Such embeddings could be efficiently used in different downstream applications, namely semi-supervised node classification—it can be an inadequate sub-set of nodes is considered, and the intention is to gather labels for the remaining nodes and graph categorization, where the system allocates a classified label to a whole graph depending on its features and complete architecture. Related to alternative GNN frameworks, GCNs give a scalable, efficient, and comprehensible method for learning from graph-structured data, leads a fundamental technique within GNN-based DL.

4. Performance validation

In this part, the experimental outcomes of the CPP-RSRF method is demonstrated below the Crop Price Prediction Dataset [24], shown in Table 1.

This dataset comprises historical crop cost logs from different platforms, beneficial for developing models that predict future crop prices using previous data. It's generally used in ML for analysis of price trend and agricultural market intelligence. The proposed framework for CPP-RSRF was designed in Python and tested on workstation with Intel Core i9 processor, NVIDIA RTX-series GPU and RAM of 32 GB. The TensorFlow and Scikit-Learn libraries were used for model development and evaluation. The settings of the major parameters used in the experiments are outlined in Table 2.

Fig. 3 demonstrates the correlation matrix of the CPP-RSRF method for soil, atmosphere, crop, and yield characteristics in the dataset. A robust positive correlation is identified between phosphorus and potassium concentrations. Moderate negative correlations are present among crop type and key nutrients like phosphorus and potassium. Most other characteristics comprising humidity, pH value, rainfall, temperature, and yield show weak correlations, signifying a complex and non-linear relation between the factors.

Fig. 4 exemplifies the comparative analysis of actual and predicted normalized values of the CPP-RSRF approach at various training epochs (20, 30, 40, and 50) for both training and testing splits. As the epochs count increases, the predictable values progressively aligned with the definite values, signifying enhanced learning and method integration. Small deviations and occasional peaks recommends the existence of complex patterns and variability in the data.

Table 3 denotes the training and testing sets of CPP-RSRF method with diffident metrics. With training set, the CPP-RSRF approach gives results with MSE, RMSE, MAE, and MAPE of 0.00115, 0.03386, 0.01550, and 9.09164, correspondingly. Meanwhile, testing set, the CPP-RSRF techniques deliver results with MSE, RMSE, MAE, and MAPE of 0.00040 0.01994, 0.01395, and 6.57797, accordingly.

Fig. 5 demonstrates the training and validation loss curves of the CPP-RSRF method with a training–testing split over 50 epochs. Both losses reduced sharply during the initial epochs, representing rapid learning, and then progressively stabilized and smoothly, showing effective integration. The close alignment among training and testing loss, with only a small constant gap, recommends minimal overfitting and strong generalization ability. Generally, the stable reduction in loss ensures the efficiency and stability of the training process.

The comparison outcomes of the CPP-RSRF method with the present methodologies are validated in Table 4 and Fig. 6 [25]. These simulation result displays that the CPP-RSRF model outperformed grater performances. According to MAE, the CPP-RSRF model has least results with MAE of 0.0155 during the Decision Tree, k-NN, Gradient Boosting, RF, 1DCNN, LSTM-DBN and CYPA techniques have higher results with MAE of 0.3260, 0.4060, 0.2860, 0.2030, 0.1930, 0.1940, and 0.1660, correspondingly. Lastly, based upon MSE, the CPP-RSRF method has minimal performance with MSE of 0.0012 during the Decision Tree, k-NN, Gradient Boosting, RF,1DCNN, LSTM-DBN and CYPA techniques includes greater performance with MSE of 0.1210, 0.1690, 0.0950, 0.0930, 0.0850, 0.1010, and 0.0990, correspondingly.

The performance measurements of the CPP-RSRF technique is conducted using the ToN-IoT dataset [26]. This higher-scale, varied cybersecurity dataset from UNSW Canberra is created to examine AI and ML–driven intrusion identification in IoT and IIoT settings. It includes telemetry, operating system, and network traffic data gathered under normal and multiple attack conditions. The datasets includes 43 features, of which 27 are chosen for examination, and contains 9 classes with a total of 119,957 records, as summarized in Table 5.

Table 6 illustrates the confusion matrices and classification results of the CPP-RSRF techniques utilizing a 70:30 split of TRAP/TESP. From the confusion matrices, the CPP-RSRF model validates effective identification and accurate detection of all classes. For the 70% TRAP, the CPP-RSRF approaches obtain average performance with an $accur_y$ of 99.41%, $preci_n$ of 92.90%, $recal_l$ of 86.44%, F_{score} of 87.59% and MCC of 88.06%, respectively. In the meantime, for the 30% TESP, the CPP-RSRF model attains average results with an $accur_y$ of 99.43%, $preci_n$ of 93.60%, $recal_l$ of 87.10%, F_{score} of 88.49% and MCC of 88.90%, respectively

Table 7 and Fig. 7 denotes the comparison analyses of the CPP-RSRF model with previous approaches in terms of various measures [27]. The Naïve Bayes approach has validate minimal performances with $accur_y$ of 76.98%, $preci_n$ of 88.07%, $recal_l$ of 76.98%, and $F1_{score}$ of 76.98%. Additionally, the LSTM and ADA approaches have outperformed reasonable and closer results. Therefore, the KNN, MLP, and CNN approaches have moderately results. Lastly, the CPP-RSRF model has depicted higher performances with $accur_y$ of 99.43%, $preci_n$ of 93.60%, $recal_l$ of 87.10%, and $F1_{score}$ of 88.49%.

From the detailed results and discussion, it is assured that the CPP-RSRF model has demonstrated superior performance over other models.

5. Discussion

The experimental results illustrate the efficiency of the proposed CPP-RSRF to crop price prediction and intrusion detection problem. This better accuracy in forecasting is due to the complementary capacities of the TCN and Transformer modules. The TCN captures the temporal dependencies in the local data with dilated convolutions, whereas the Transformer component captures the long-range relationships between past price observations by using a self-attention mechanism. Moreover, training with the RAdam optimizer brings about better convergence stability and helps to reduce variation changes during the training process, which leads to improved prediction accuracy. The IG approach is effective in removing irrelevant attributes and dimensional reduction, while the GCN approach is capable of learning structural relationships between IoT entities, which are useful for intrusion detection. The IG approach is useful for removing irrelevant attributes and dimensional reduction, and the GCN approach can learn the structural relationship between IoT entities for intrusion detection. As a result, the proposed framework has better detection performance than the traditional machine learning and deep learning methods.

6. Conclusion

This study presents a CPP-RSRF methodology for enabling secure smart agriculture. The primary intention of this paper is to develop a secure IoT-based system for precise crop price prediction. The proposed technique applies dual stages such as predicting crop prices and attack detection process. For crop price prediction stage, the proposed CPP-RSRF approach initially pre-process the input data utilizing min-max scaling normalization to improve further analysis. To accomplish that, a TCN and transformer with a self-attention module are leveraged to predict crop price. Together with, the Radam is leveraged for tuning parameters and upgrading the execution of the model. For attack classification stage, an IG is leveraged for selecting features and determining the most informative features. Additionally, the GCN is applied to categorize the attack in smart agriculture application. To evaluate the boosted classification performance of the CPP-RSRF methodology, the widespread outcomes take place on standard datasets. The wide-ranging comparative results guaranteed the betterment of the CPP-RSRF methodology through recent techniques.

Funding statement

No Funding

CRediT authorship contribution statement

R. Nithya: Data curation, Formal analysis, Project administration, Resources, Supervision, Validation, Writing – review & editing. **N. Narmadhavarshini:** Conceptualization, Investigation, Methodology, Software, Visualization, Writing – original draft.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] Saadouni R, Gherbi C, Aliouat Z, Harbi Y, Khacha A, Mabed H. Securing smart agriculture networks using bio-inspired feature selection and transfer learning for effective image-based intrusion detection. Internet Things 2025;29:101422.
[2] Zangana HM, Luckyardi S, Mustafa FM, Li S. Enhancing agricultural cybersecurity: leveraging deep learning and large language models for smart farming protection. In: Revolutionizing cybersecurity with deep learning and large language models. IGI Global Scientific Publishing; 2025. p. 307–38.
[3] Prashanth JS, Krishna GB, Prasad AV, Rao PR. Smart farming revolution: a cutting-edge review of deep learning and IoT innovations in agriculture. Operations Research Forum 2025, March;6(1):1–39. Springer International Publishing.
[4] Kaushik I, Prakash N, Jain A. An AI-blockchain-assisted smart agriculture framework for enabling secure and efficient data transaction: a hybrid approach. Knowl Inf Syst 2025;67(11):10087–135.
[5] Selvam P, Krishnamoorthy N, Kumar SP, Lokeshwaran K, Lokesh M, Syamala M, Vidhya RG. Internet of things integrated deep-learning algorithms monitoring and predicting abnormalities in agriculture land. Internet Technol Lett 2025;8(5):e607.
[6] Prathap C, Sivaranjani S, Sathya M. ML-Based yield prediction in smart agriculture systems using IoT. In: 2024 5th international conference on innovative trends in information technology (ICITIIT). IEEE; 2024, March. p. 1–7.
[7] Rahman W, Hossain MM, Hasan MM, Iqbal MS, Rahman MM, Hasan KF, Moni MA. Automated detection of harmful insects in agriculture: a smart framework leveraging IoT, machine learning, and blockchain. IEEE Transactions on Artificial Intelligence 2024;5(9):4787–98.
[8] Mohy-eddine M, Guezzaz A, Benkirane S, Azrour M. Malicious detection model with artificial neural network in IoT-based smart farming security. Clust Comput 2024;27(6):7307–22.
[9] Palei S, Lenka RK, Mallick SR, Sinha A, Biswal SS, Rath SS, Srivastava A, Saxena S. Secure and decentralized apple leaf disease identification using DL integration models. In: 2024 international conference on emerging systems and intelligent computing (ESIC). IEEE; 2024, February. p. 68–73.
[10] Mahalingam N, Sharma P. An intelligent blockchain technology for securing an IoT-based agriculture monitoring system. Multimed Tool Appl 2024;83(4):10297–320.
[11] Sizan NS, Layek MA, Hasan KF. A secured triad of IoT, machine learning, and blockchain for crop forecasting in agriculture. In: International conference on innovative computing and communication. Singapore: Springer Nature Singapore; 2025, February. p. 187–99.
[12] Addanki UK, Devareddi RB, Kamarajugadda KK, Pavani M, Gera P. Machine learning-powered intrusion detection system for agriculture 4.0: securing the next generation of farming. International Journal of Innovative Research and Scientific Studies 2025;8(1):1964–78.
[13] Kethineni K, Pradeepini G. Intrusion detection in internet of things-based smart farming using hybrid deep learning framework. Clust Comput 2024;27(2):1719–32.
[14] Aldhyani TH, Alkahtani H. Cyber security for detecting distributed denial of service attacks in agriculture 4.0: deep learning model. Mathematics 2023;11(1):233.
[15] El-Ghamry A, Darwish A, Hassanien AE. An optimized CNN-Based intrusion detection system for reducing risks in smart farming. Internet Things 2023;22:100709.
[16] Kethineni K, Gera P. IoT-based privacy-preserving anomaly detection model for smart agriculture. Systems 2023;11(6):304.
[17] Morchid A, Qjidaa H, Alami RE, et al. Smart irrigation-based internet of things and cloud computing technologies for sustainable farming. Sci Rep 2026;16:5293. https://doi.org/10.1038/s41598-026-35810-0.
[18] Goswami P, Mukherjee A, Maiti M, Tyagi SKS, Yang L. A neural-network-based optimal resource allocation method for secure IIoT network. IEEE Internet Things J 2021;9(4):2538–44.
[19] Kim YS, Kim MK, Fu N, Liu J, Wang J, Srebric J. Investigating the impact of data normalization methods on predicting electricity consumption in a building using different artificial neural network models. Sustain Cities Soc 2025;118:105570.
[20] Rafi MA, Rodrigues GN, Mir MNH, Bhuiyan MSM, Mridha MF, Islam MR, Watanobe Y. A hybrid temporal convolutional network and transformer model for accurate and scalable sales forecasting. IEEE Open Journal of the Computer Society 2025.
[21] Altınel D. Development of deep learning optimizers: approaches, concepts, and update rules. 2025. arXiv preprint arXiv:2509.18396.
[22] Hasdyna N, Dinata RK. A hybrid optimization of supervised learning models using information gain-based feature selection. 2025.
[23] Nguyen TT, Park M. El-gnn: a continual-learning-based graph neural network for task-incremental intrusion detection systems. Electronics 2025;14(14):2756.
[24] https://www.kaggle.com/datasets/varshitanalluri/crop-price-prediction-dataset.
[25] Abdel-salam M, Kumar N, Mahajan S. A proposed framework for crop yield prediction using hybrid feature selection approach and optimized machine learning. Neural Comput Appl 2024;36(33):20723–50.
[26] https://research.unsw.edu.au/projects/toniot-datasets.
[27] Yaras S, Dener M. IoT-based intrusion detection system using new hybrid deep learning algorithm. Electronics 2024;13(6):1053.