mathematics

MDPI

Article

Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model

Theyazn H. H. Aldhyani [1,*] and Hasan Alkahtani [2]

[1] Applied College in Abqaiq, King Faisal University, P.O. Box 400, Al-Ahsa 31982, Saudi Arabia
[2] College of Computer Science and Information Technology, King Faisal University, P.O. Box 400, Al-Ahsa 31982, Saudi Arabia
* Correspondence: taldhyani@kfu.edu.sa

Abstract: Attackers are increasingly targeting Internet of Things (IoT) networks, which connect industrial devices to the Internet. To construct network intrusion detection systems (NIDSs), which can secure Agriculture 4.0 networks, powerful deep learning (DL) models have recently been deployed. An effective and adaptable intrusion detection system may be implemented by using the architectures of long short-term memory (LSTM) and convolutional neural network combined with long short-term memory (CNN–LSTM) for detecting DDoS attacks. The CIC-DDoS2019 dataset was used to design a proposal for detecting different types of DDoS attacks. The dataset was developed using the CICFlowMeter-V3 network. The standard network traffic dataset, including NetBIOS, Portmap, Syn, UDPLag, UDP, and normal benign packets, was used to test the development of deep learning approaches. Precision, recall, F1-score, and accuracy were among the measures used to assess the model's performance. The suggested technology was able to reach a high degree of precision (100%). The CNN–LSTM has a score of 100% with respect to all the evaluation metrics. We used a deep learning method to build our model and compare it to existing systems to determine how well it performs. In addition, we believe that this proposed model has highest possible levels of protection against any cyber threat to Agriculture 4.0.

Keywords: deep leaning; Agriculture 4.0; food security; intrusion detection system; cybersecurity

MSC: 68Q32

Citation: Aldhyani, T.H.H.; Alkahtani, H. Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics* **2023**, *11*, 233. https://doi.org/10.3390/math11010233

Academic Editors: Todor Tagarev and Xiang Li

Received: 1 December 2022
Revised: 25 December 2022
Accepted: 28 December 2022
Published: 3 January 2023

1. Introduction

Industry 4.0 technology has made it possible to create a setting in which all components are continually and easily connected with one another. All of the devices and functions, such as cyber–physical systems (CPS), are referred to as services. These services are in continuous communication with one another, which allows for a high degree of coordination [1–4]. In this sense, the capability to coordinate activities is essential for improving supply chain management. This is because optimization typically requires the consideration of a large number of factors that are in constant competition with each other [5]; this is where the ability to coordinate activities becomes essential. Figure 1 shows the Industry 4.0 technology for developing agriculture.

According to the findings of the most recent study conducted by the Food and Agriculture Organization of the United Nations [6], in order to sustainably sate Earth's ever-increasing human population, which is projected to approach 9 billion by the year 2050 [7], global food production will need to increase by a factor of 70 percent between now and 2050. As a result of the predicted rise in the number of Internet of Things (IoT) devices used in agriculture, the size of the market for smart agriculture is also likely to expand greatly in the coming years in order to meet these demands [8]. The next technological advance for the agricultural industry that will help ensure the continued production of food in a

sustainable manner is digital agriculture [9]. Desertification is a problem that is now being addressed by a number of nations through initiatives such as the Saudi Green Initiative, which is an expansion of the Saudi Vision 2030. As part of this program, hundreds of millions of plants, including four million lemon trees that are dependent on recycled water for irrigation, are being planted in an effort to alter the climate and make agriculture more manageable. Figure 2 illustrates several applications of artificial intelligence that are based on the Internet of Things (IoT) and are intended to improve the agricultural industry.

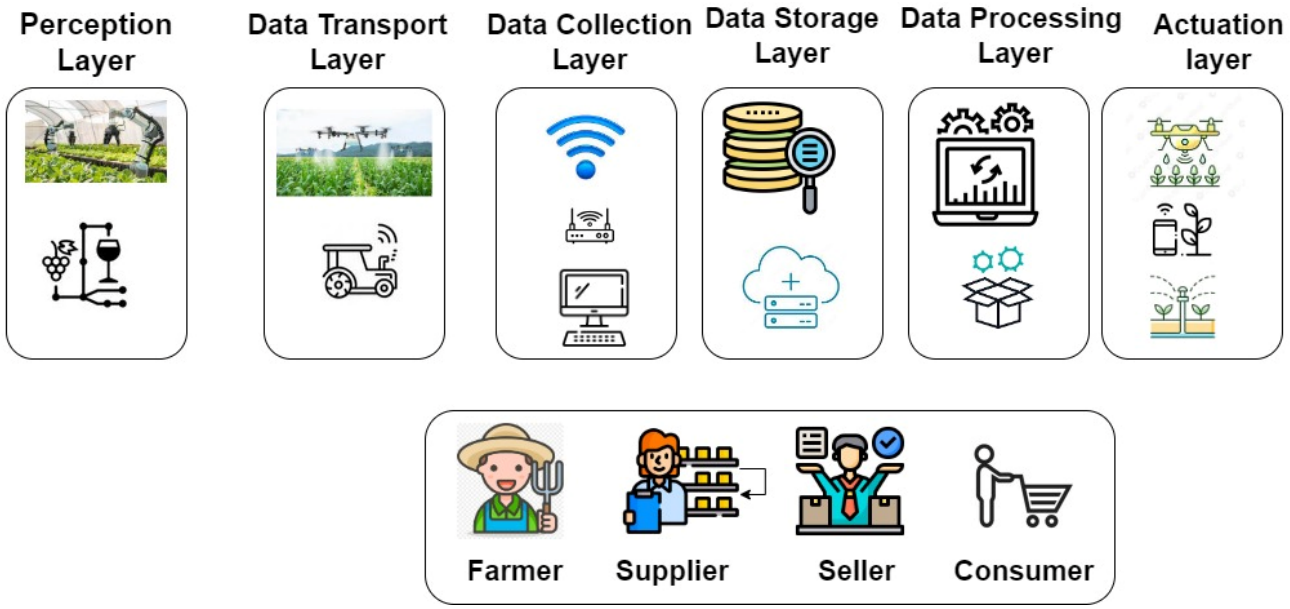

Figure 1. Industry 4.0 technology for developing the agriculture sector.

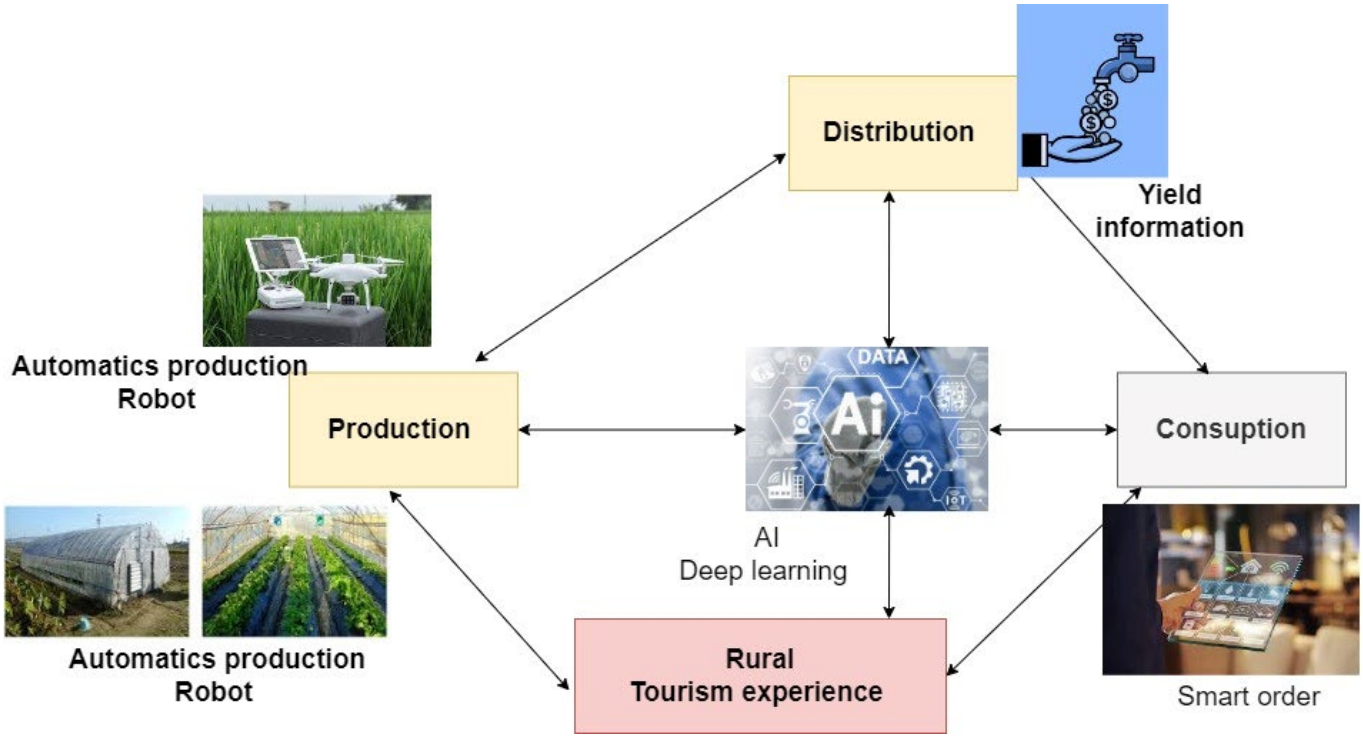

Figure 2. Artificial intelligence based on IoT for improving the agriculture sector.

Advances in information and communication technology (ICT) have supported digitalization, which is a global trend that has transformed various markets and continues to bring up new opportunities across a wide range of industries in economies and communities [10]. This trend is underpinned by advancements in ICT. In recent years, the agricultural industry has engaged a wide array of new information and communication technology (ICT) solutions, which have contributed to the sector's rapid technical expansion. Although Agriculture 4.0 is anticipated to become the industry standard, the presence of physical dangers and hazards in this specific field is a significant aspect that poses a potential barrier to the widespread acceptance and implementation of these innovations. Some of these dangers, such as climate conditions, tend to stay the same over the course of many years, while others are related to the rapid advancement of technological solutions. A number of technologies in digital agriculture, from a vertical farm's heating and ventilation systems to a drone spraying crops, are vulnerable to cyberattacks. The water system in Florida [11], a dairy and beverage company in Australia [12,13], and the world's largest meatpacker, wool Net software, have all recently been the targets of cyberattacks that have made headlines throughout the world. This has brought to light the weaknesses that are present in digital agriculture, as well as the potentially catastrophic repercussions that these vulnerabilities might have on the general population in terms of supply, labor, and cost.

In Agriculture 4.0, however, there are numerous new cybersecurity vulnerabilities since thousands of devices based on IoT are currently being installed in open fields. An adversary seeking to break into the Agriculture 4.0 network will utilize a variety of techniques, including distributed denial-of-service (DDoS) attacks, scanning attacks, and fake data injection attacks, in order to interfere with the normal operation of IoT-based equipment. For instance, if soil pH increases excessively, this suggests that farmers will raise the amount of ammonium added to the soil. If the pH falls, this indicates that the farmer will lower the amount of ammonium added to the soil. With this knowledge, an attacking party may conduct distributed denial-of-service assaults to wreak havoc on the pH parameters. Therefore, it is imperative that sensitive data, such as pH values, be shielded from any potential cyberattacks [14]. In addition to authentication, access control, and integrity procedures, researchers in the field of information security recommend employing an intrusion detection system (IDS) [15,16]. This would protect Agriculture 4.0 from being damaged, altered, tampered with, or accessed by unauthorized parties.

The fourth industrial revolution has made extensive use of these developing technologies, and it should not be difficult to replicate their use in agricultural settings. In this way, the adoption of new developing technologies is not the most significant hurdle to Agriculture 4.0′s development but rather the primary guarantee of security and privacy, given that thousands of IoT devices will be implemented in an open field. Each layer of the IoT's architecture has its own set of privacy and security problems [17], and they are interconnected. Cyberattacks such as distributed denial-of-service (DDoS) attacks might be used by an adversary, for example, to disrupt a service and then insert fraudulent data, which could harm food safety, the efficiency of agri-food supply chain activities, and agricultural production. To ensure the safety of computer networks, intrusion detection systems (IDS) use a method of monitoring system activity in real time and comparing it to historical data to determine if an incursion has occurred. It is recommended that these systems be used by the cybersecurity research community, which uses technology to secure networks. IDS implementation in conjunction with other security measures, such as encryption, authentication, authorization, and blockchain technology, may help protect Agriculture 4.0 against cyberattacks [18–20].

At this time, artificial intelligence (AI) algorithms have been employed to identify attacks on IoT devices with higher levels of assurance. Artificial intelligence technology even has the capacity to recognize variations in the channels and tactics used by attackers. One of the issues that security solutions had to confront when dealing with attacks on the Internet of Things was that hackers would make minute adjustments to their prior attacks, which the security solutions were unable to spot. AI technologies are being

used by researchers and developers to analyze network traffic in order to protect the IoT environment from any potential dangers [21,22]. Deep learning and machine learning are two types of learning that have been integrated into security systems to identify these kinds of threats more effectively. Deep learning is one of the advancements in artificial intelligence that may be seen in many real-life applications for dealing with complicated nonlinear data. This kind of learning is used to manage the data [23–25]. An implementation of a deep recurrent neural network, also known as a DRNN, has been developed to recognize botnet attacks affecting IoT devices.

The main contributions of the development of a system for protecting Agriculture 4.0 based on the deep learning model are as follows:

- We used deep learning models, namely long short-term memory and a convolutional neural network combined with long short-term memory (CNN–LSTM), for detecting various types of attacks that threaten Agriculture 4.0;
- The security system based on Agriculture 4.0 was developed by using a real network traffic dataset: CIC-DDoS2019;
- The developed Agriculture 4.0 system was compared to different security systems;
- We used the Pearson correlation method for selecting important features that can help develop security systems.

This paper's sections are structured as follows: introduction of the research article is presented in Section 1. In Section 2 the background of study is provided. In Section 3, we describe the procedures for collecting data, and methods and experimental design are discussed in Section 4. Section 5 provides a discussion of the results. The last section of the article summarizes the main points.

2. Background of Study

Network security solutions are rare, and artificial intelligence plays a major part in the domain of cybersecurity and Agriculture 4.0 for the creation of an intelligent IoT security system. Researchers have wanted to create a smart model that can help protect smart Agriculture 4.0 infrastructure from outside attacks. IoT-enabled gadgets have transformed the majority of businesses and organizations in recent years.

There are new threats and concerns in terms of IT security in the worldwide market as smart communication technologies rapidly evolve and increase in adoption [26] following IoT integration and the digitalization of businesses. In a dynamic and dispersed cyber-physical environment, a wide range of smart agricultural technologies might be vulnerable to assaults [27]. These kinds of threats and assaults may have a devastating effect on linked firms. Precision agriculture (PA) and smart farming involve cutting-edge technology and remote administration that are unfamiliar to the agriculture industry's stakeholders, and many of the new concerns that have emerged are closely linked to those that are present in other sectors [28], with cybersecurity, data integrity, and data loss being the most common dangers [29]. Because heavy equipment in the PA industry is often linked to the Internet, various new vulnerabilities have opened up that may have potentially fatal results [30,31].

Smart technologies such as the IoT may be used in agriculture to help prevent cybersecurity assaults and threats. Demestichas et al. [32] outlined several strategies for this prevention. An experiment was carried out by Sontowski et al. [33] on a smart farm in which a Raspberry Pi was made to disconnect from the network and stop it from rejoining as part of a denial-of-service (DoS) assault known as a WiFi deauthentication attack.

Using fog nodes, Ng and Selvakumar [34] created a vector convolutional deep learning system for anomaly detection. According to the UNSW's Bot-IoT dataset, the method achieved an accuracy of 99.991% for detecting DDoS attacks, and an accuracy of 99% for detecting DoS attacks. The deep belief network approach was used by Manimurugan et al. [35] to identify cyber threats on the Internet of Medical Things (IMoT). For PortScan attacks and infiltration assaults, the suggested technique has an accuracy of 97.71 percent and 96.37 percent, respectively, according to the CICIDS 2017 dataset. To identify botnets in IoT networks, Popoola et al. [36] developed the LAE–BLSTM hybrid intrusion detection

technique. The LSTM autoencoder and bidirectional long short-term memory (BLSTM) are both used in the LAE–BLSTM mechanism (LAE). It is used for dimensionality reduction, whereas BLSTM is utilized to distinguish botnet assaults from normal network data in IoT networks. The Bot-IoT dataset shows that the LAE–BLSTM mechanism achieved a data reduction ratio of 91.89%.

As our world becomes more connected to the Internet, cybersecurity continues to be an ever-evolving field. Every method of detection is only as powerful as its weakest link, which makes it incredibly difficult to control risks in the supply chains and networks of individual firms [37]. In addition, a third-party application with one or more potential flaws may put the entire adopted system in danger. Companies of all sizes may face recruitment challenges while trying to build an effective intrusion detection system against cyberattacks and threats [38]. Weaknesses in the supply chain are likelier to be discovered as a company grows in size. By exploiting these vulnerabilities, hackers might conduct unlawful attacks on vital infrastructure, including water and electricity systems [39–41].

Security will continue to evolve as our world becomes increasingly linked to the Internet. The supply chain and networks of individual companies are very difficult to regulate in terms of risk. Third-party applications may also pose a risk to the adopted system. Regardless of the size of a company, it may be difficult to hire the right people to guard against cyberattacks and threats. As a firm expands in size, supply chain weaknesses are likelier to be detected. Weaknesses in critical infrastructure, such as water and energy systems, might be exploited by hackers to carry out illegal attacks [42].

Artificial intelligence plays a primary role in building an intelligent system for security in an IoT-based environment. The researchers sought to create a smart model that might help protect IoT devices and infrastructure from outside attacks. IoT has enabled digital changes in the vast majority of businesses and organizations. As a result, fraudsters have discovered new complications and weaknesses that they may easily attack. Some classification methods were developed by Jokar and Leung [43] to identify irregular electricity use, network traffic monitoring in advanced metering infrastructure was performed using clustering technology developed by Alseiari and Aung [44] to identify the IDS, and a support vector machine (SVM) based on a multiclass was used by Vijayanand et al. [45], who found that decision tree techniques were more powerful than the SVM presented by Jindal et al. [46]. IDS detection was evaluated by Boumkheld et al. [47] using a standard machine learning method on top of a naïve Bayesian network. Jokar and Leung [43] developed ZigBee-based Q-learning to guard networks against intrusion and found it to be the most effective technique for monitoring system threats. Finally, the use of a hierarchy to pick relevant features from intrusion detection networks was hypothesized [48–51].

3. Materials and Methods

3.1. Framework of the Proposed System

To identify cyberattacks in Agriculture 4.0, we present deep learning-based IDS models, including one that uses recurrent neural networks, one that uses convolutional neural networks, and LSTM models. The framework of the developing security systems for protecting Agriculture 4.0 is presented in Figure 3.

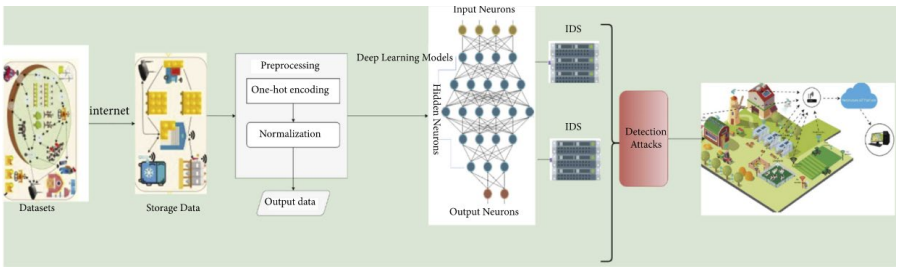

Figure 3. Framework of the proposed method.

CIC-DDoS2019 Dataset

Attacks such as DDoS are a threat to network security, since they are aimed at flooding target networks with malicious traffic, thus rendering them unusable. The construction of a real-time DDoS attack detector with little processing overhead remains a major challenge, despite the development of several statistical methodologies to combat the same.

The CIC-DDoS2019 comprises the most recent and popular DDoS attacks, which are based on real-world information. Data from CICFlowMeter-V3 network traffic analysis, including flow labels based on timestamps and the source and destination IP addresses and ports, protocols, and attack types are also included.

Reflective DDoS attacks such as Portmap, NetBIOS, LDAP, MSSQL, UDP, UDPLag, SYN, NTP DNS, and SNMP are included in this dataset. During this time, a number of attacks occurred. For example, Table 1 shows the DDoS attacks that occurred on the training day, which included NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, and UDPLag. To evaluate the proposed model, no WebDDoS traffic or PortScan results are used because of their low traffic volume and overall lack of PortScan results [52]. The CIC-DDoS2019 dataset has been divided into two portions: 70% training process and 30% testing process, as shown in Table 2.

Table 1. Attacks on CICDDoS2019.

Volume	Attacks CICDDoS2019	#No
7118	Normal	1
7491	NetBIOS	2
7015	Portmap	3
8513	Syn	4
6051	UDPlag	5
1873	UD	6

Table 2. Dataset after dividing into training and testing.

Testing	Training	Attacks
1449	5669	Normal
1518	5973	NetBIOS
1393	5622	Portmap
1688	6825	Syn
1180	4871	UDPlag
385	1488	UD

3.2. Preprocessing

The dataset had a total of 38,061 rows and nine features. Originally, the dataset consisted of 82 features. The preprocessing method is a very important stage for the development of such a system because the network traffic has a very complex format; therefore, we used preprocessing to enhance the deep learning approach to achieve high performance.

3.2.1. One-Hot Encoding Method

By transforming categorical information and label class to numerical values, the one-hot encoding strategy was utilized to enhance the classification process for identifying assaults. This was accomplished through the usage of the one-hot encoding approach.

3.2.2. The Minimum/Maximum Approach

One of the most used methods for normalizing data is called the minimum/maximum approach. The value that is least significant is translated to the number 0; the most

significant value is assigned to the number 1. The following equation is used in the application of the min/max normalization method:

$$z_n = \frac{x - x_{min}}{x_{max - x_{min}}} \quad (1)$$

where x_{min} is the minimum of the data and x_{max} is the maximum of the data.

3.2.3. Feature Selection

In order to select significant features, Pearson's correlation coefficient method was applied to find the features that have a strange relationship with class labels. The nine features that had the highest correlation were selected. The findings of using Pearson's correlation coefficient to determine which characteristics are most relevant are presented in Figure 4.

Figure 4. Selecting features by using the correlation coefficient method.

3.3. Deep Learning Approach

One of the advantages of convolutional neural networks is the ability to recognize, categorize, and analyze certain properties of neural networks. When an input is provided and weights and biases can be learned about it, the method employs a feedforward network to assign priority to its characteristics [53]. There is a convolution layer that results from many kernels or weight matrices coupled to each other in the neighborhood. As it examines an input, the convolution layer performs convolution operations. A feature map or activation map is the name given to the final product. This is followed by a downsampling technique known as pool, which takes the average and maximum values of a certain area and conducts spatial invariance.

In the FC layer, all inputs are coupled to all neurons, and the network reaches its final state. Users then utilize an image vector with contained characteristics to feed the CNN, which then uses this probabilistic approximation to identify the intended target picture at

the end of all of these layers. This approach has a major advantage over other classification algorithms in that it requires less preprocessing on a standard CNN. IDSs often employ a CNN because of the necessity of high accuracy in a given pattern categorization. Using CNN, it is simpler to recognize attacks that follow a given pattern [54–57].

The LSTM network, also known as the long short-term memory network, is a recurrent neural network (RNN) that is often used for the purpose of learning issues involving sequential data prediction. The LSTM neural network, like any other neural network, contains various layers that help it learn and detect patterns for improved performance. It is possible that the fundamental function of LSTM is to save necessary information and to get rid of information that is not necessary or helpful for making more predictions.

The suggested model has an initial LSTM layer as its first hidden component. In the case of the combined DDoS dataset, the input to the first hidden layer is written as (9, 1). The combined DDoS dataset has an output shape of (26642, 9) as training, (7613, 9) as testing, and (7613, 9) as validation. Both shapes are the input for the subsequent layer. LSTM is equipped with several gates that allow for control of the flow of information. For instance, these gates determine how data enters the system, how it is stored, and how it exits the system. In addition, there are two more states, which are referred to as the cell state and the hidden state. A typical LSTM has five activation functions, as well as two ReLU functions, three sigmoid functions (one in each gate), and one ReLU function in each gate. In addition, the LSTM has two ReLU functions in each gate (one in the input gate and the second in the output gate).

As can be seen in Figure 5, the LSTM consists of three gates in its most basic form: the forget, input, and output gates. Equations (2)–(6) provide a mathematical description of the forget, input, and output gates, respectively.

$$\text{Forget gate}: \; f_t = \sigma\left(W_f \cdot X_t + W_f \cdot h_{t-1} + b_f\right) \tag{2}$$

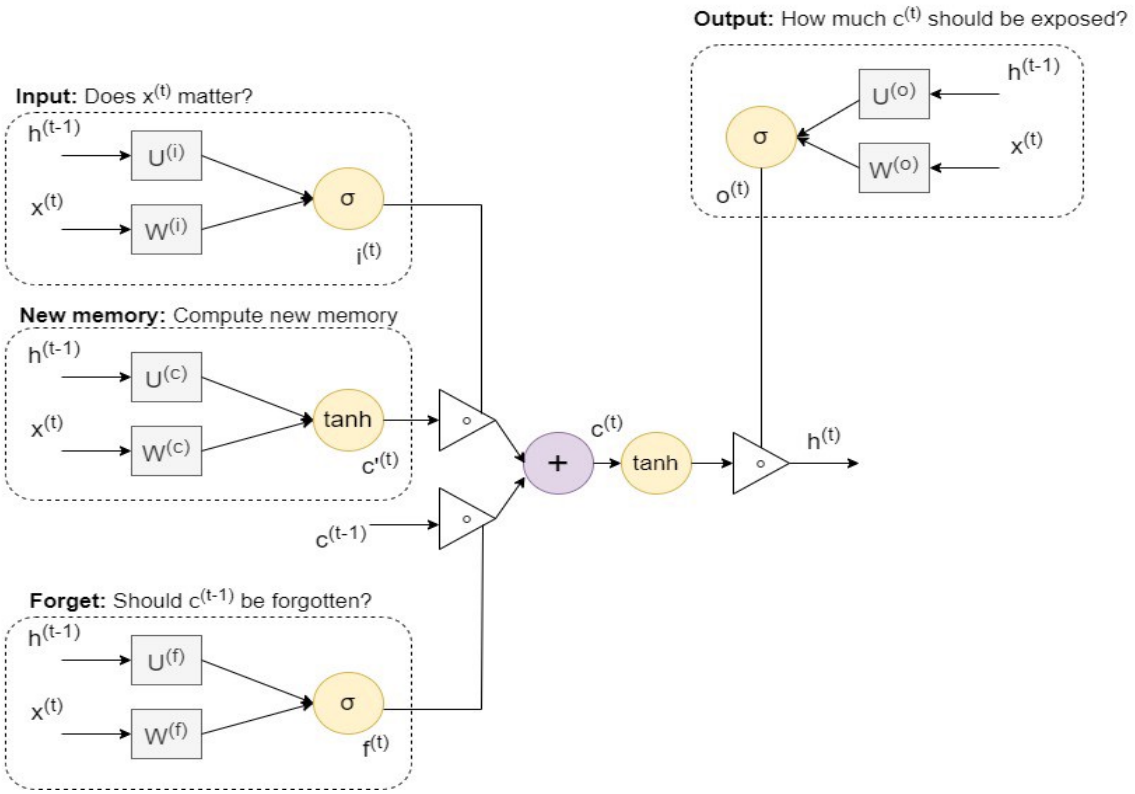

Figure 5. LSTM model.

A forget gate has a weight W_f of that ranges from (0, 1), which is the current layer's input at time t. h_{t-1} is the previous layer's output at time t. The output from the previous run is combined with the input from the current run and fed into the input gate, resulting in the following formulae for the output and the candidate cell output:

$$\text{Input gate}: \quad i_t = \sigma(W_c \cdot X_t + W_i \cdot h_{t-1} + b_i) \tag{3}$$

$$\text{Cell gate}: \quad C_t = (i_t * S_t + f_t * S_{t-1}) \tag{4}$$

W_i represents the weight of the input gate, b_i is the bias of the input gate, W_c is the weight of the candidate gate, and bc is the bias of the candidate gate. These values range from 0 to 1. The following code is used to make a change to the current cell:

$$\text{Output gate}: \quad o_t = \sigma(W_o + X_t + W_o \cdot h_{t-1} + \ V_o \cdot C_t + b_o) \tag{5}$$

$$\text{Cell gate}: \ h_t = o_t + \tan \mathrm{h}(C_t) \tag{6}$$

The LSTM cell output is determined by computing the output gate o_t and cell state as per Formula (11), and h_t represents the hidden layer.

$$\text{Hidden layer}: \ h_t = o_t + \tan \mathrm{h}(C_t) \tag{7}$$

The LSTM cell output is determined by computing the output gate o_t and cell state as per Formula (11), and h_t represents the hidden layer.

To identify intrusions in an IoT network dataset, we suggested a combination of two powerful deep learning algorithms. Figure 6 depicts the suggested structure of a hybrid model that was developed to automatically identify threats. Two deep learning models, CNN and LSTM, were combined to create an architecture that employed the input data on size 9 × 38,061 to extract additional complex features from the important features extracted using the CNN algorithm. To extract these complex features, a convolutional layer with three kernels was utilized, and tanh activation was suggested as a data transmission method. For dimension reduction, we employed a two-kernel maxpool to map features to an LSTM model and to extract additional information about time. To utilize in classification, the fusion features were completely linked after extracting the LSTM time that data attacks on the IoT network might be detected using the softmax algorithm [58,59]. Table 3 presents the CNN–LSTM model's parameter values for your perusal.

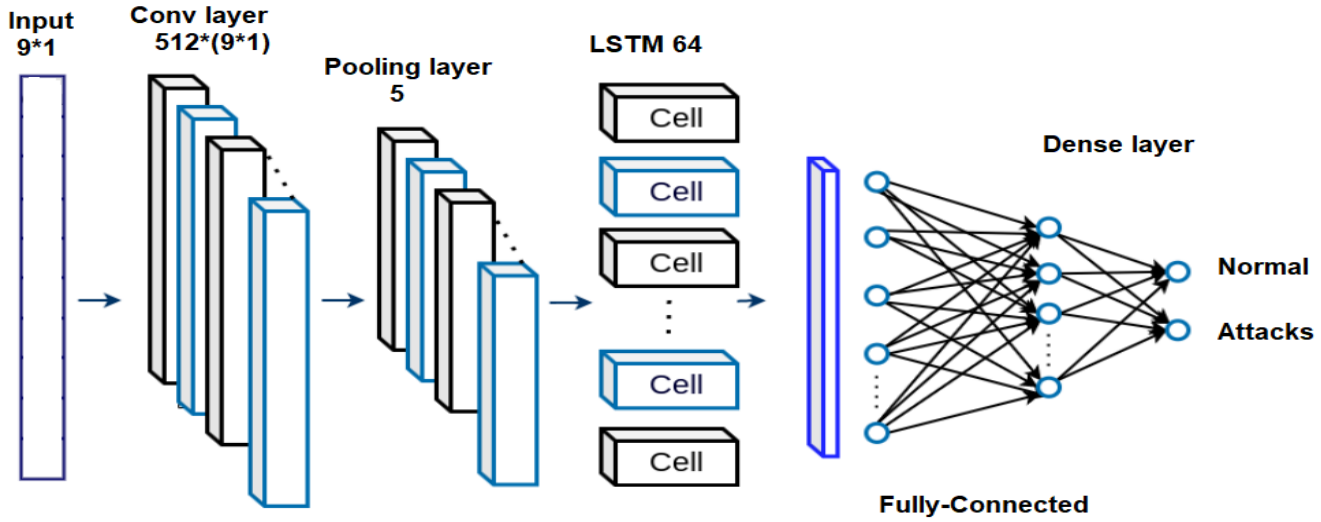

Figure 6. CNN–LSTM model for detecting attacks.

Table 3. Using parameters of CNN–LSTM algorithm for detecting attacks.

#Parameters Indicators	#Values
Convolution layer	512
The size of max pooling	5
Drop out	0.50
The size of the FC layer	64
Activation function	ReLU
Optimizer	RMSprop
Epochs	20
Batch size	150

4. Experiment

All tests were run on the Windows 10 operating system using the open-source software libraries Keras, TensorFlow, and the Python 3 libraries Numpy, Scikits-Learn, and Panda. All models were trained using 8 GB of local GPU memory. We also used Keras to create a variety of CNN models for comparison purposes.

The correlation between characteristics in the dataset and their class labels was determined using Pearson's correlation coefficient. Using a deep learning technique to obtain high performance for detection of attacks on farm systems based on Agriculture 4.0, we selected nine characteristics for further processing. We then used our data to train deep learning models capable of recognizing and learning the right characteristics of the data. Each layer of the network had its own set of criteria, such as input, hidden layer, and output. Our optimal convolution settings were 512 filters, a kernel size of 5, and a batch size of 150, all with the "ReLU" activation. We used a max-pooling strategy with a pooling size of 5 and a stride size of 1 in the pooling layer. The batch size was 150, the activation function was "ReLU," and the dropout was 0.5. For CNN trials, we employed the RMSprop optimizer and a learning rate of 0.001 based on the model's performance at different learning rates, including 0.001, rho = 0.9. On the other hand, recurring models such as LSTM are very much alike. Sequence computation with multiple recurrent blocks and extensive training time consumption caused the models to operate at a learning rate of 0.001. We raised the number of recurrent blocks from 10 to 100 in order to find the ideal performance, but the results were not significantly different. On the other hand, training time consumption rose. As with the single model, the CNN parameters for the combination model were identical to those of the single CNN model, which has 512 filters and a filter size of 5. LSTM models with 32 recurrent blocks were the only ones used, since other recurrent models performed poorly. The LSTM and CNN–LSTM models used RMSprop optimizers with learning rates of 0.001 and 0.001. Additionally, 64 filters with a filter size of 5 were used for convolutional operations. CIC-DDoS2019 was used to assess the system models that have been submitted. For each attack, the system was classed as multiclass, which indicates the system's nth performance. Therefore, we have achieved the following objectives:

1. Finding the significant features that can help to achieve high-performance detection;
2. Using the deep learning approach for detection of attacks to protect agriculture-based IoT;
3. Achieving the highest performance when compared to existing systems.

4.1. Performance Measurements

There are a number of measures that may be used to assess the effectiveness of deep learning. The sensitivity, specificity, precision, recall, F-score metrics, and ROC Curve are the performance indicators we concentrated on in our research.

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \times 100\% \quad (8)$$

$$Sensitivity = \frac{TP}{TP + FN} \times 100\% \quad (9)$$

$$Precision = \frac{TP}{TP + FP} \times 100\% \tag{10}$$

$$Fscore = \frac{2 \times precision \times \text{ Sensitivity}}{precision + \text{ Sensitivity}} \times 100\% \tag{11}$$

False positives and negatives are denoted by the letters FP and FN, respectively. A false positive (FP) or a true negative (TN) was noted for any data that were wrongly identified as an attack. Data that are accurately categorized as an attack are referred to as true positives (TP). Attack data that have been labeled as benign are indicated as false negatives (FN).

4.2. Results

The results of the LSTM model for detecting attacks are summarized in Table 4. It was found that LSTM worked well when we analyzed all datasets with accuracy ratings of 58% to 66%. In Agriculture 4.0, it was discovered that the results obtained from using the LSTM model for cybersecurity intrusion detection were not very satisfactory. The LSTM model successfully attained a detection success rate of one hundred percent for UDP attacks.

Table 4. Results of LSTM for detecting multi-classes.

DDoS Attacks	Precision %	Recall %	F1-Score %
Normal	99	43	60
NetBIOS	55	64	59
Portmap	54	86	67
Syn	76	81	78
UDPLag	50	49	50
UDP	0.00	0.00	0.00
Accuracy%			62
Weighted average	64	62	60
Time		23.05 s	

To improve upon the detection of attacks on Agriculture 4.0 by using the LSTM model, Figure 7 shows the accuracy performance and loss of the LSTM technique. In the testing phase with 20 epochs, the LSTM utilized two processes: training and testing. The training process started from 53.50% and reached 64%, whereas the validation process was passed on a straight line from 52% and reached 60%. The accuracy loss dropped from 1.125 to 0.970 during training, and volitional accuracy rose from 1.100% to 0.950%. Finally, we found that the accuracy of the LSTM model is high; additionally, we found that the model accuracy was at a very low 62%.

True negative and false positive rates, the valid positive rate, and the false negative rate constitute the indicators of confusion shown in Figure 8. Using the LSTM model, the adjusted normal percentage was found to be 7.83%, but the NetBIOS model scored only 13.16%. The Portmap had a false positive rate of 12.31%, while the Syn attack had a false positive rate of 17.02%. The false positive of the UDPLag attack was 8.00%, and the false positive rate of the UDP attack was 0.00. Overall, we observed that the UDP attack achieved a very low detection rate.

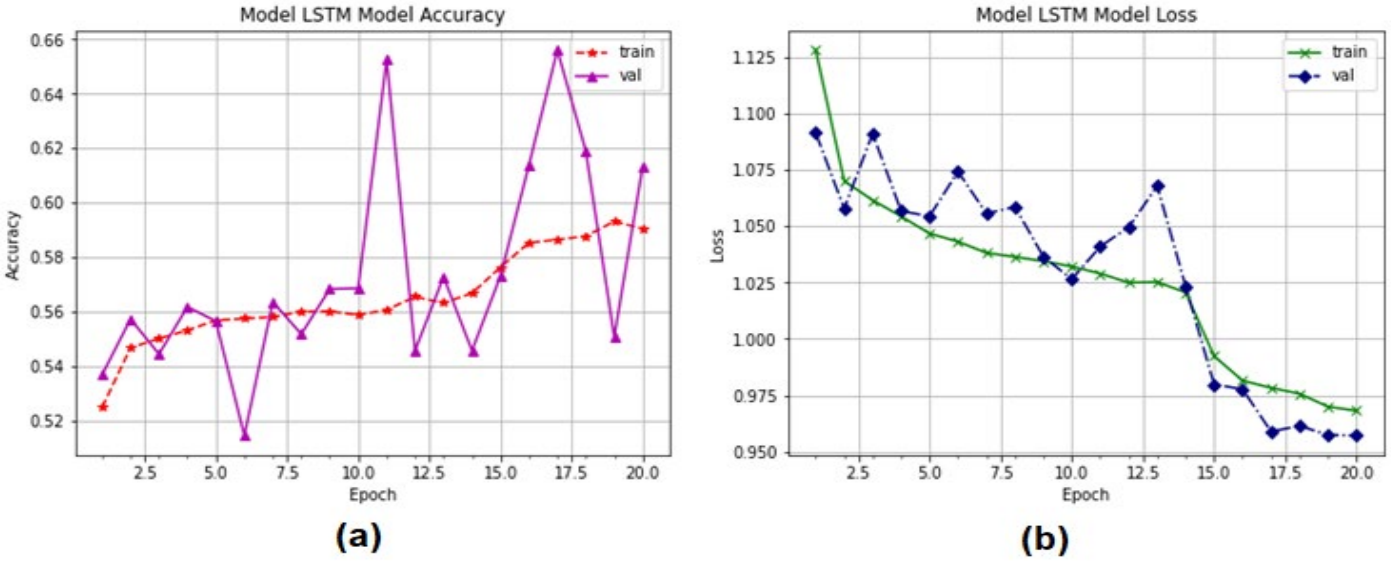

Figure 7. LSTM model performance for detection attacks on Agriculture 4.0. (**a**) Model accuracy; (**b**) model loss.

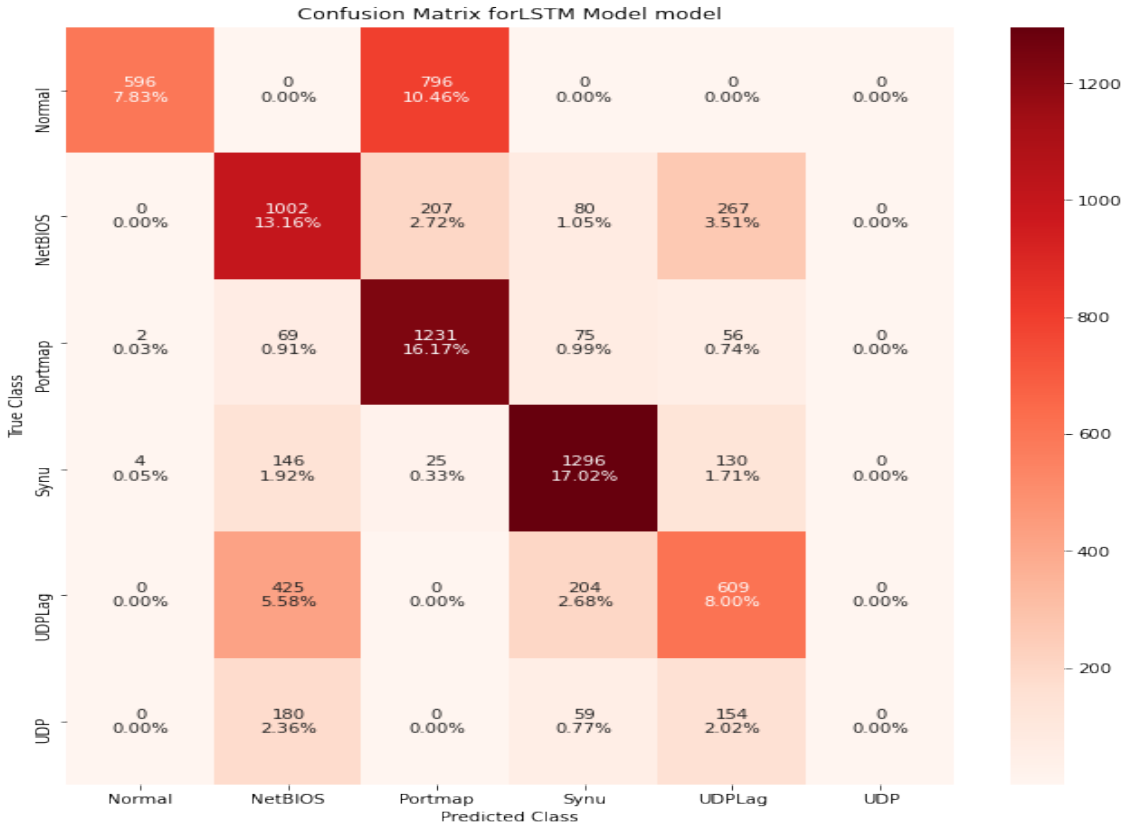

Figure 8. In the LSTM model, confusion metric.

The CNN–LSTM deep learning techniques approach was successful against a variety of types of attacks for securing Agriculture 4.0, according to Table 5. The CNN–LSTM method had the greatest performance (100%) against all types of attacks. Several experiments on binary classification and multiclass classification using deep learning algorithms are shown in Figure 8. Cybersecurity intrusion detection for Agriculture 4.0 may be improved through deep learning.

Table 5. Results of CNN–LSTM for detecting multi-classes.

DDoS Attacks	Precision %	Recall %	F1-Score %
Normal	100	100	100
NetBIOS	100	100	100
Portmap	100	100	100
Syn	100	100	100
UDPLag	100	100	100
UDP	100	100	100
Accuracy%	100	100	100
Weighted average	100	100	100
Time	25.62 s		

For the detection of DDoS attacks on agriculture-based IoT, Figure 9 illustrates the CNN–LSTM technique for predicting multi-attacks, which is a prediction-based deep learning approach. The CNN–LSTM model had an accuracy prediction rate of 100% during training and 100% during testing, where the accuracy performance of the model started from 98.25% and reached 100% at training and validation started from 99.50% and reached 100% at the validation phase. The integrating model is appropriate for detecting attacks on Agriculture 4.0.

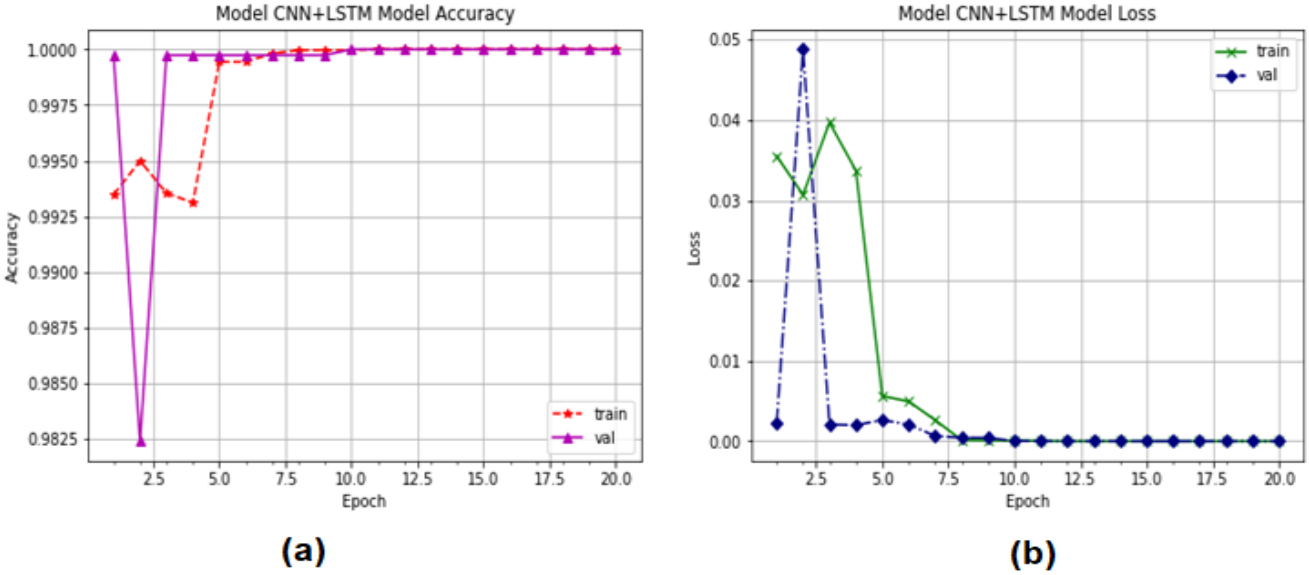

Figure 9. The CNN–LSTM model's performance for detection of attacks on Agriculture 4.0. (**a**) Model accuracy (**b**) Model loss.

The confusion matrix for the CNN–LSTM model can be found in Figure 10. The matrix, which displays the results of using this procedure, contains all of the possible outcomes, including true positives, false negatives, and true negatives. The CNN–LSTM model attained a superior detection rate with all NetBIOS, Portmap, Syn, UDPLag, UDP, and normal. The FP rate is 100% for all classes; therefore, CNN's integration with the LSTM model is an optimal deep learning approach for protecting Agriculture 4.0 from any cyberattacks.

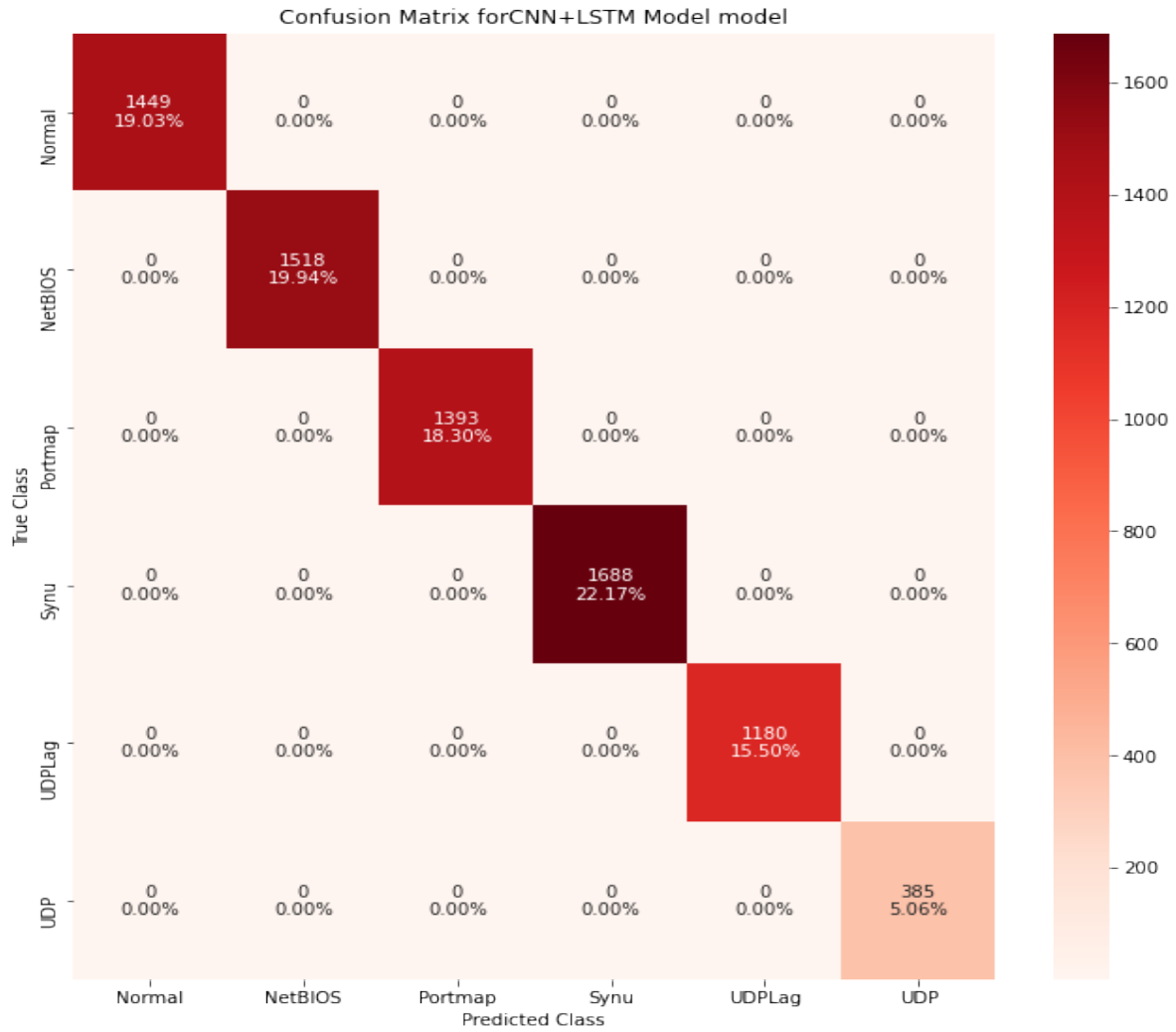

Figure 10. Confusion metrics of the CNN–LSTM model.

5. Discussion

The fourth industrial revolution in agriculture is characterized by the integration of cutting-edge information and communication technology with conventional farming operations. Security experts have become interested in a wide range of cyber dangers associated with this integration. Agriculture 4.0 represents a new age of agriculture that has rapidly emerged as a result of tremendous advancements in agricultural technology. As a consequence of climate change, sicknesses, excessive use of chemicals and resources, and so on, Agriculture 4.0 strives to apply new technology and practices in order to alleviate present problems, limit risks, and lead to more efficient and safer production. This is the goal of Agriculture 4.0. This objective is accomplished through the application of a vast assortment of information and communication technologies (ICTs) that are at the leading edge of their fields. Given that millions of IoT-based devices will be deployed in open fields, the most challenging aspect of building Agriculture 4.0 will not be the deployment of new technology; rather, it will be the assurance of security and privacy. As a consequence of this, each layer of the architecture of the Internet of Things has its own set of problems regarding privacy and safety [6]. Distributed denial-of-service (DDoS) assaults are among the most prevalent types of cyberattacks, and they have the potential to compromise food safety, the effectiveness of agri-food supply chains, and the output of farmers.

We constructed a system that was based on the deep learning model LSTM, and CNN–LSTM models were applied to the system in order to detect any assaults that were made against Agriculture 4.0. For the purpose of evaluating the proposed system, the CIC-

DDoS2019 dataset was utilized. In terms of accuracy, the CNN–LSTM model was the most effective when it came to the categorization of many classes. The outstanding performance of the CNN–LSTM model, taken as a whole, achieved a perfect score of 100 percent when testing against all different kinds of assaults. The receiver operating characteristic curves (ROC) of the deep learning LSTM and CNN–LSTM algorithms are depicted in Figure 11. In Agriculture 4.0, it was found that the CNN–LSTM model performed better than other methods in terms of the recall metric of multiclass classification for the purpose of detecting intrusion. The ROC metric was used to validate the results of the LSTM and CNN–LSTM approaches, where the y-axis represents the recall for classifying the five attacks and the x-axis represents specificity metrics. It was discovered that the CNN–LSTM model was successful in achieving a rating of one hundred percent for identifying five types of attack in addition to normal.

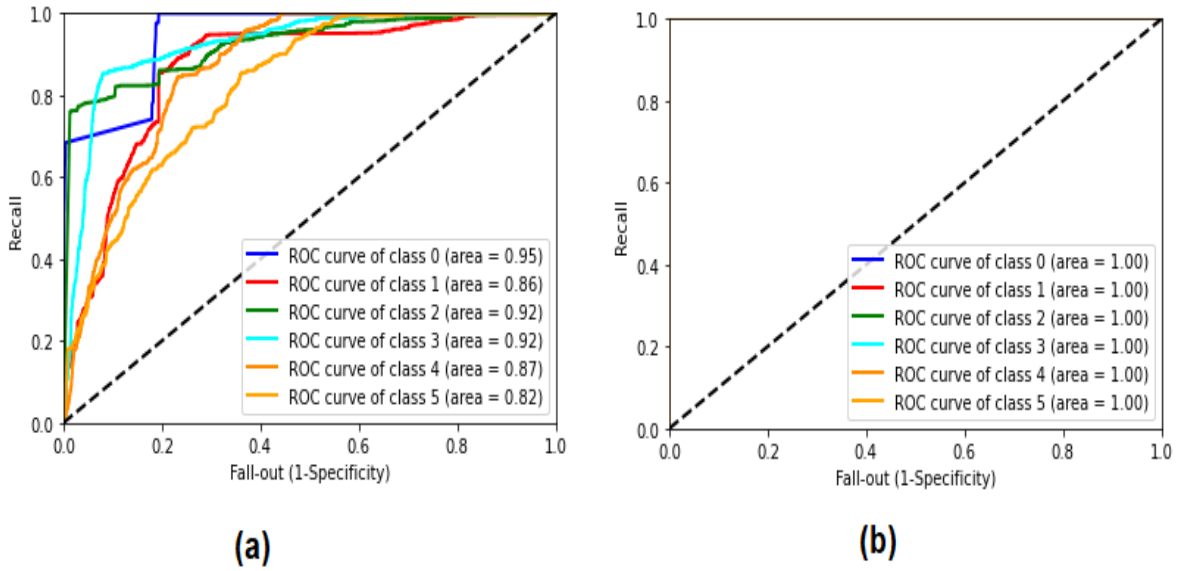

Figure 11. ROC of proposed system: (**a**) LSTM model; (**b**) CNN–LSTM model.

The empirical findings of the suggested deep learning CNN–LSTM algorithm pitted against preexisting security systems that were developed by the system using the dataset are shown in Table 6. A graphical representation of the comparison between the results achieved by our system and those acquired by other existing approaches in terms of accuracy metrics can be seen in Figure 12. In general, the strategy that we suggest provides the highest degree of accuracy among currently accessible strategies.

Table 6. Comparison results between CNN–LSTM model against existing security systems for detecting attacks on Agriculture 4.0.

Ref.	Model	Dataset	Types	Years	Accuracy %
Ref. [60]	LSTM	CIC-DDoS2019	Multi-class	2020	98.9
Ref. [61]	CNN	CIC-DDoS2019	Multi-class	2020	95.4
Ref. [62]	Boosting algorithm	CIC-DDoS2019	Multi-class	2020	91.26
Proposed system	CNN–LSTM	CIC-DDoS2019	Multi-class	2022	100

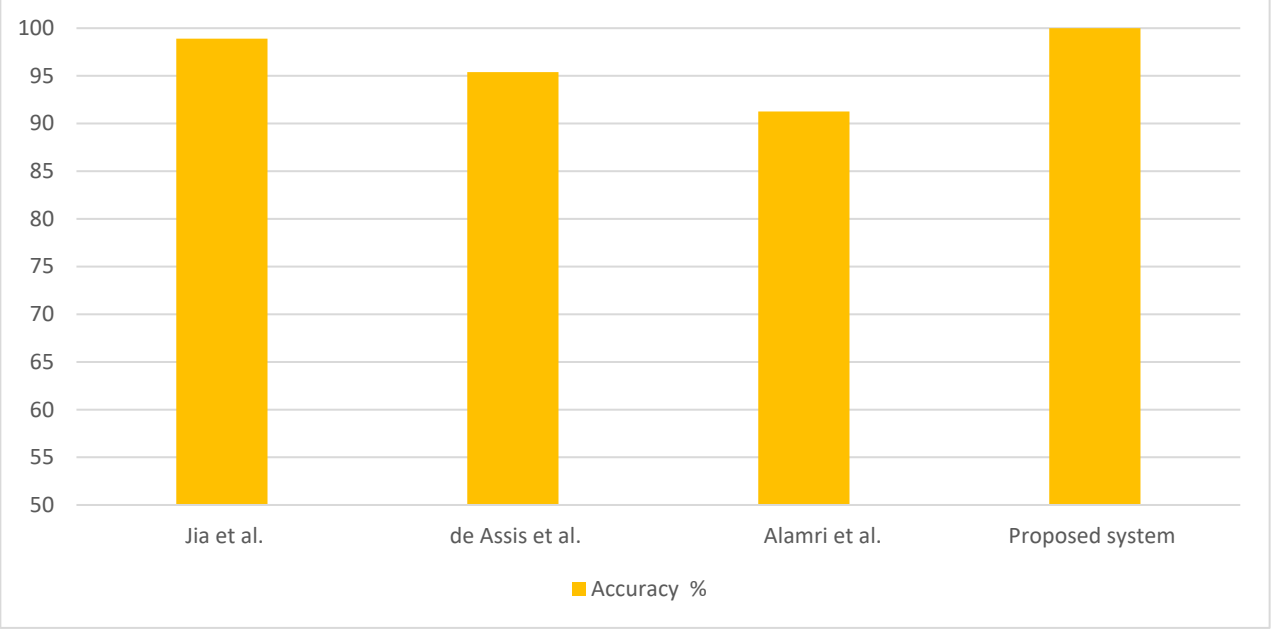

Figure 12. Comparative performance between the CNN–LSTM model and existing approaches to the detection of Agriculture 4.0 attacks.

6. Conclusions

In order to boost both the quality and quantity of agricultural products, it is necessary to implement recently developed technologies into existing farming practices. Internet of Things (IoT), 5G communications, drones, fog/edge computing, cloud computing, artificial intelligence (AI), and software-defined networking are some of the cutting-edge technologies that are presently being investigated.

In this paper, suggestions for intrusion detection models for Agriculture 4.0 that are based on deep learning are offered. These models consist of a convolutional neural network and a long short-term memory, in addition to a recurrent neural network long short-term memory (RNNLSTM) and a combined convolutional neural network and long short-term memory (CNN–LSTM). The current system was designed and built with the help of the real network CIC-DDoS2019 dataset, and approaches based on Pearson's correlation coefficient were applied in order to determine which properties are important. Nine features were chosen because they have a strong association with the classes. This was decided in order to obtain the maximum possible accuracy. The detection rate, the false alarm rate, the precision, the recall rate, the true negative rate, the false accept rate, the ROC, and accuracy are all important metrics to consider when evaluating this system's performance.

Additionally, the LSTM–CNN-based IDS model outperformed the most recent deep learning IDS algorithms. The CIC-DDoS2019 dataset was used to test these approaches. According to the findings, the CNN–LSTM mode achieved a perfect score of 100% when testing its ability to identify attacks. In addition, the IDS model that is based on CNN–LSTM performed significantly better than other deep learning IDS approaches that are considered state of the art. Both percentages reflect an improvement when compared to the most recent deep learning IDS approaches that are available. The limitations of this research are the used standard dataset; researchers can use their own standard data from a real agricultural environment.

Author Contributions: Conceptualization, T.H.H.A. and H.A.; methodology, T.H.H.A.; software, T.H.H.A.; validation, T.H.H.A. and H.A.; formal analysis, T.H.H.A. and H.A.; investigation, T.H.H.A. and H.A.; resources, T.H.H.A.; data curation, T.H.H.A. and H.A.; writing—original draft preparation, T.H.H.A. and H.A.; writing—review and editing, H.A.; visualization, T.H.H.A., H.A. supervision, T.H.H.A.; project administration, T.H.H.A. and H.A.; funding acquisition, T.H.H.A. and H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research and the APC were funded by Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number INST032.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available here: https://www.unb.ca/cic/datasets/ddos-2019.html Accessed Date (accessed on 2 July 2022).

Acknowledgments: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number INST032.

Conflicts of Interest: The authors declare that they have no conflict of interest.

Abbreviations

DL: deep learning; LSTM: long short-term memory; CNN–LSTM: convolutional neural network and long short-term memory; CPS: cyber–physical systems; IoT: Internet of Things; ICT: information and communication technology; DDoS: distributed denial-of-service; IDS: intrusion detection system; AI: artificial intelligence (AI); DRNN: deep recurrent neural network; PA: precision agriculture; DoS: denial-of-service; IMoT: Internet of Medical Things; BLSTM: bidirectional long short-term memory; SVM: support vector machine; FP: false positive; TN: true negative; TP: true positive; FN: false negative

References

1. He, W.; Xu, L. A state-of-the-art survey of cloud manufacturing. *Int. J. Comput. Integr. Manuf.* **2015**, *28*, 239–250. [CrossRef]
2. Lee, J.; Bagheri, B.; Kao, H.-A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
3. Ren, L.; Zhang, L.; Tao, F.; Zhao, C.; Chai, X.; Zhao, X. Cloud manufacturing: From concept to practice. *Enterp. Inf. Syst.* **2013**, *9*, 186–209. [CrossRef]
4. Schlechtendahl, J.; Keinert, M.; Kretschmer, F.; Lechler, A.; Verl, A. Making existing production systems Industry 4.0-ready. *Prod. Eng.* **2015**, *9*, 143–148. [CrossRef]
5. Wiendahl, H. *Auftragsmanagement der Industriellen Produktion: Grundlagen, Konfiguration, Einführung*; Springer: Berlin/Heidelberg, Germany, 2012.
6. Roopaei, M.; Rad, P.; Choo, K.R. Cloud of Things in smart agriculture: Intelligent irrigation monitoring by thermal imaging. *IEEE Cloud Comput.* **2017**, *4*, 10–15. [CrossRef]
7. Karlov, A.A. Cybersecurity of Internet of Things—Risks and Opportunities. In Proceedings of the XXVI International Symposium on Nuclear Electronics & Computing (NEC'2017), Budva, Montenegro, 25–29 September 2017; pp. 182–187.
8. Malavade, V.N.; Akulwar, P.K. Role of IoT in agriculture. *IOSR J. Comput. Eng.* **2016**, *2016*, 56–57.
9. Basso, B.; Antle, J. Digital agriculture to design sustainable agricultural systems. *Nat. Sustain.* **2020**, *3*, 254–256. [CrossRef]
10. Mathews, L. Florida Water Plant Hackers Exploited Old Software and Poor Password Habits. 2021. Available online: https://www.forbes.com/sites/leemathews/2021/02/15/florida-water-plant-hackers-exploited-old-software-and-poor-password-habits/?sh=78dd125c334e (accessed on 2 July 2022).
11. Musotto, R.; Naser, M. Ransomware Attack on Sheep Farmers Shows There's No Room for Woolly Thinking in Cyber Security. 2020. Available online: https://theconversation.com/ransomware-attack-on-sheep-farmers-shows-theres-no-room-for-woolly-thinking-in-cyber-security-132882 (accessed on 13 July 2022).
12. Seselja, E. Cyber Attack Shuts Down Global Meat Processing Giant JBS. 2021. Available online: https://www.abc.net.au/news/2021-05-31/cyber-attack-shuts-down-global-meat-processing-giant-jbs/100178310 (accessed on 5 July 2022).
13. Prasad, R.; Rohokale, V. *Cyber Security: The Lifeline of Information and Communication Technology*; Springer International Publishing: Cham, Switzerland, 2020; ISBN 978-3-030-31702-7.
14. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]

15. Yang, X.; Shu, L.; Chen, J.; Ferrag, M.A.; Wu, J.; Nurellari, E.; Huang, K. A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 273–302. [CrossRef]
16. Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1153–1176. [CrossRef]
17. Tewari, A.; Gupta, B. Security, privacy and trust of different layers in internet-of-things (IoTs) framework. *Future Gener. Comput. Syst.* **2020**, *108*, 909–920. [CrossRef]
18. Zhu, W.J.; Deng, M.L.; Zhou, Q.L. An intrusion detection algorithm for wireless networks based on ASDL. *IEEE/CAA J. Autom. Sin.* **2018**, *5*, 92–107. [CrossRef]
19. Agarwal, M.; Purwar, S.; Biswas, S.; Nandi, S. Intrusion detection system for PS-poll DoS attack in 802.11 networks using real time discrete event system. *IEEE/CAA J. Autom. Sin.* **2017**, *4*, 792–808. [CrossRef]
20. Peppes, N.; Daskalakis, E.; Alexakis, T.; Adamopoulou, E.; Demestichas, K. Performance of Machine Learning-Based Multi-Model Voting Ensemble Methods for Network Threat Detection in Agriculture 4.0. *Sensors* **2021**, *21*, 7475. [CrossRef] [PubMed]
21. Meidan, Y.; Bohadana, M.; Shabtai, A.; Guarnizo, J.D.; Ochoa, M.; Tippenhauer, N.O. ProfilIoT: A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 4–6 April 2017; pp. 506–509.
22. Alkahtani, H.; Aldhyani, T.H.; Al-Yaari, M. Adaptive anomaly detection framework model objects in cyberspace. *Appl. Bionics Biomech.* **2020**, *2020*, 6660489. [CrossRef] [PubMed]
23. Ferrag, M.A.; Maglaras, L. DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1285–1297. [CrossRef]
24. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* **2020**, *50*, 102419. [CrossRef]
25. Alkadi, O.; Moustafa, N.; Turnbull, B.; Choo, K.K.R. A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks. *IEEE Internet Things J.* **2020**, *8*, 9463–9472. [CrossRef]
26. Salam, A. Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends. In *Internet of Things for Sustainable Community Development: Wireless Communications, Sensing, and Systems*; Springer International Publishing: Cham, Germany, 2020; pp. 299–327. ISBN 978-3-030-35291-2.
27. Barreto, L.; Amaral, A. Smart farming: Cyber security challenges. In Proceedings of the 2018 International Conference on Intelligent Systems (IS), Funchal, Portugal, 25–27 September 2018; pp. 870–876.
28. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]
29. European Commission. *Industry 4.0 in Agriculture: Focus on IoT Aspects*; Digital Transformation Monitor; European Commission: Brussels, Belgium, 2017.
30. Window, M. Security in Precision Agriculture: Vulnerabilities and Risks of Agricultural Systems. Master's Thesis, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden, 2019.
31. Boghossian, A.; Linsky, S.; Brown, A.; Mutschler, P.; Ulicny, B.; Barrett, L.; Bethel, G.; Matson, M.; Strang, T.; Ramsdell, K.; et al. *Threats to Precision Agriculture*; 2018 Public-Private Analytic Exchange Program Report; United States Department of Homeland Security and Office of Intelligence and Analysis: Washington, DC, USA, 2020.
32. Demestichas, K.; Peppes, N.; Alexakis, T. Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors* **2020**, *20*, 6458. [CrossRef]
33. Sontowski, S.; Gupta, M.; Chukkapalli, S.S.L.; Abdelsalam, M.; Mittal, S.; Joshi, A.; Sandhu, R. Cyber Attacks on Smart Farming Infrastructure. In Proceedings of the IEEE 6th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 1–3 December 2020; pp. 135–143.
34. Amma, N.G.B.; Selvakumar, S. Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment. *Future Gener. Comput. Syst.* **2020**, *113*, 255–265.
35. Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network. *IEEE Access* **2020**, *8*, 77396–77404. [CrossRef]
36. Popoola, S.I.; Adebisi, B.; Hammoudeh, M.; Gui, G.; Gacanin, H. Hybrid Deep Learning for Botnet Attack Detection in the Internet of Things Networks. *IEEE Internet Things J.* **2021**, *8*, 4944–4956. [CrossRef]
37. Kohl, K.D. The Increase of Cybersecurity Threats to the Food and Agriculture Sector from Smart Agriculture. Master's Thesis, Utica College, New York, NY, USA, 2017.
38. Okupa, H. Cybersecurity and the Future of Agri-Food Industries. Master's Thesis, Department of Agricultural Economics College of Agriculture, Kansas State University, Manhattan, KS, USA, 2020.
39. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
40. Duncan, S.E.; Reinhard, R.; Williams, R.C.; Ramsey, F.; Thomason, W.; Lee, K.; Dudek, N.; Mostaghimi, S.; Colbert, E.; Murch, R. Cyberbiosecurity: A New Perspective on Protecting U.S. Food and Agricultural System. *Front. Bioeng. Biotechnol.* **2019**, *7*, 63. [CrossRef] [PubMed]
41. Manninen, O. Cybersecurity in Agricultural Communication Networks: Case Dairy Farms. Master's Thesis, JAMK University of Applied Sciences, Jyväskylä, Finland, 2018.

42. Alzahrani, A.; Aldhyani, T.H.H. Artificial Intelligence Algorithms for Detecting and Classifying MQTT Protocol Internet of Things At-tacks. *Electronics* **2022**, *11*, 3837. [CrossRef]
43. Jokar, P.; Leung, V. Intrusion Detection and Prevention for ZigBee-Based Home Area Networks in Smart Grids. *IEEE Trans. Smart Grid* **2016**, *9*, 1800–1811. [CrossRef]
44. Alseiari, F.A.A.; Aung, Z. Real-Time Anomaly-Based Distributed Intrusion Detection Systems for Advanced Metering Infrastructure Utilizing Stream Data Mining. In Proceedings of the International Conference on Smart Grid & Clean Energy Technologies, Offenburg, Germany, 14–15 October 2015.
45. Vijayanand, R.; Devaraj, D.; Kannapiran, B. Support Vector Machine Based Intrusion Detection System with Reduced Input Featuresfor Advanced Metering Infrastructure of Smart Grid. In Proceedings of the 4th International Conference on Advanced Computing and Communication Systems, Coimbatore, India, 1–7 January 2017.
46. Jindal, A.; Dua, A.; Kaur, K. Decision Tree and SVM-Based Data Analytics for Theft Detection in Smart Grid. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1005–1016. [CrossRef]
47. Boumkheld, N.; Ghogho, M.; Koutbi, M.E. Intrusion Detection System for the Detection of Blackhole Attacks in a Smart Grid. In Proceedings of the 4th International Symposium on Computational and Business Intelligence, Olten, Switzerland, 5–7 September 2016.
48. Aldhyani, T.H.H.; Alkahtani, H. Artificial Intelligence Algorithm-Based Economic Denial of Sustainability Attack Detection Systems: Cloud Computing Environments. *Sensors* **2022**, *22*, 4685. [CrossRef]
49. Hasan, N.; Toma, R.N.; Nahid, A.-A.; Islam, M.M.; Kim, J.-M. Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach. *Energies* **2019**, *12*, 3310. [CrossRef]
50. Vinayakumar, R.; Soman, K.P.; Poornachandran, P. Applying Convolutional Neural Network for Network Intrusion Detection. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics, Karnataka, India, 13–16 September 2017.
51. Sung, J. The Fourth Industrial Revolution and Precision Agriculture. In *Automation in Agriculture—Securing Food Supplies for Future Generations*; Hussmann, S., Ed.; IntechOpen: London, UK, 2018. [CrossRef]
52. Available online: https://www.unb.ca/cic/datasets/ddos-2019.html (accessed on 10 July 2022).
53. Alkahtani, H.; Aldhyani, T.H.H. Artificial Intelligence Algorithms for Malware Detection in Android-Operated Mobile Devices. *Sensors* **2022**, *22*, 2268. [CrossRef]
54. Mehedi, S.T.; Anwar, A.; Rahman, Z.; Ahmed, K. Deep Transfer Learning Based Intrusion Detection System for Electric Vehicular Networks. *Sensors* **2021**, *21*, 4736. [CrossRef]
55. Alkahtani, H.; Aldhyani, T.H. Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithma. *Complexity* **2021**, *2021*, 5579851. [CrossRef]
56. Aldhyani, T.H.H.; Alkahtani, H. Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors* **2022**, *22*, 360. [CrossRef]
57. Alkahtani, H.; Aldhyani, T.H.H. Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications. *Secur. Commun. Netw.* **2021**, *2021*, 3806459. [CrossRef]
58. Xiaoqiang, Z.; Jingxi, T. Multiple-image encryption algorithm based on genetic central dogma. *Phys. Scr.* **2022**, *97*, 055213.
59. Alzahrani, A.; Aldhyani, T.H.; Alsubari, S.N.; Alghamdi, A.D. Network Traffic Forecasting in Network Cybersecurity: Granular Computing Model. *Secur. Commun. Netw.* **2022**, *2022*, 3553622. [CrossRef]
60. Jia, Y.; Zhong, F.; Alrawais, A.; Gong, B.; Cheng, X. Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks. *IEEE Internet Things J.* **2020**, *7*, 9552–9562. [CrossRef]
61. de Assis, M.V.; Carvalho, L.F.; Rodrigues, J.J.; Lloret, J.; Proença, M.L., Jr. Near real-time security system applied to SDN environments in IoT networks using convolutional neural network. *Comput. Electr. Eng.* **2020**, *86*, 106738. [CrossRef]
62. Alamri, H.A.; Thayananthan, V. Bandwidth Control Mechanism and Extreme Gradient Boosting Algorithm for Protecting Software-Defined Networks Against DDoS Attacks. *IEEE Access* **2020**, *8*, 194269–194288. [CrossRef]