World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Deep learning-based intrusion detection systems for securing cloud-native and distributed architectures

Soma Sekhar Gaddipati *

Staff Architect, India.

World Journal of Advanced Research and Reviews, 2024, 22(02), 2375-2383

Publication history: Received on 07 April 2024; revised on 24 May 2024; accepted on 29 May 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.22.2.1509

Abstract

Cloud-native and distributed architecture has also deeply changed modern computing environments allowing for scalability, flexibility, and microservices deployments at scale. But this shift has also given rise to specific security challenges, such as dynamic attack surfaces, lateral movement of threats and advanced cyberattacks against containerized and serverless infrastructures. Traditional intrusion detection systems (IDS) have limitations in handling the scale, speed, and diversity of data generated during these incidents. In order to overcome these limitations, this work proposes a deep-learning-based intrusion detection framework with a particular emphasis on ensuring that it is secure in cloud-native and distributed systems. Utilizing state-of-the-art neural network architectures; Convolutional Neural Network (CNN), Recurrent Gnural Network (RNN) and hybrid deep learning models, this new model accounts for both spatial and temporal features of network traffic data. It combines real-time monitoring, anomaly detection, and adaptive learning capabilities to improve the accuracy of detection and minimise false positives. On standard datasets, we show that our new approach significantly overcomes classical machine learning methods in precision, recall and detection rate. Additionally, the model is scalable and cloud-native, while only importing sends for real-time deployment, enabling pervasive security monitoring. This work advances intelligent, autonomous cybersecurity solutions for next-generation cloud infrastructures.

Keywords: Deep Learning; Intrusion Detection System (IDS); Cloud-Native Security; Distributed Systems; Cybersecurity

1. Introduction

As one of the fastest growing computing paradigms, the cloud has resulted in widespread use of cloud-native and distributed architectures that employ microservices (i.e. stateless components), containers, orchestration platforms like Kubernetes to provide scalable & resilient applications. These architectures allow organizations to implement high availability, fast deployment and resource use. However, the dynamic and decentralized nature of such systems poses new security challenges, including larger attack surfaces, complex inter-service communication and vulnerabilities in containerized environments [1]. Consequently, strong security in cloud-native ecosystems has become an area of attention from both academia and industry.

Signature-based detection is a traditional security mechanism which is ineffective in some cases, such as zero-day attacks and changing attack patterns. Such systems are founded upon a predefined set of rules and or signatures to identify new variations, rendering them inefficient in particularly dynamic environments like distributed cloud infrastructures [2]. Additionally, the huge scale of network traffic volume and velocity produced by cloud-native systems has made it impossible for traditional techniques to detect threats in real-time with high precision [3].

* Corresponding author: Soma Sekhar Gaddipati

In order to mitigate these drawbacks, machine learning (ML) techniques have been integrated into intrusion detection systems, allowing for automated pattern recognition and anomaly detection. Although ML-based IDS have improved upon traditional methods, they remain challenged by feature engineering, scalability and adaptability to complex high-dimensional data [4]. Recently, deep learning (DL) has been proven as an effective solution by learning the hierarchy representation of data from large-scale datasets automatically and with fewer manual features [5].

Machine learning approaches like Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks has shown great promise in detection of known as well as unknown cyber threats. CNNs efficiently model the spatial dependence between nodes in traffic data, while CN and LSTM architectures are potent in capturing temporal dependencies and sequential patterns in network behavior [6]. These advantages allow deep learning to be ideal for the task of intrusion detection in cloud-native environments, where attack patterns might be subtle, distributed, and time-dependent [7].

Additionally, real-time responsive IDS frameworks built from cloud-native and deep learning log processing can also be developed due to the merging of these categories and technologies. These systems can run as microservices in container orchestration platforms and scale elastically to accommodate varying workloads [8]. Moreover, the incorporation of distributed data processing frameworks enables IDS to handle vast amounts of network data rapidly and in parallel, enhancing detection capabilities and minimizing latency [9].

Despite these successes, challenges still exist, including model interpretability, computational cost, data privacy issues and the necessity for continuous relabeling to keep up with advancing attacks. These issues must be resolved to make deep learning-based IDS practical for deployment in real-world cloud environments [10].

2. Literature review

In the last decade, research on intrusion detection systems (IDS) for cloud environments has been comprehensive, with most existing studies relying on signature-based and statistical anomaly methods in the early years. Traditional approaches worked well against known threats, but they could not detect advanced and zero-day attacks. The researchers pointed out that static rule-based systems are not enough for dynamic cloud infrastructures as both attack patterns and system configurations change quickly [11]. As a result, mechanism turned to intelligent and adaptive based detection.

The advancements in machine learning (ML) also led up too many works investigating its application within IDS platforms. Methods like Support Vector Machines (SVM), Decision Trees, Random Forests and k-Nearest Neighbors (k-NN) became popular for classifying network traffic and detecting abnormalities. Though these techniques showed better detection capabilities than traditional systems, they relied on feature extraction procedures and fared poorly with high-dimensional and unstructured data as observed in cloud-native environments [12]. Moreover, when deployed in distributed systems, the machine learning-based intrusion detection system often faced issues with scalability and real-time processing [13].

In order to overcome these shortcomings, deep learning (DL) approaches have been widely used in the field of intrusion detection. To address these limitations, Deep Neural Networks (DNNs) were applied to automatically extract and learn complex features from raw network data, limiting the manual feature extraction process. Both the experiments showed that open-source DNN-based IDS had better accuracy and generalization than conventional ML approaches for detecting unknown attack patterns [14]. On the other hand, the ability of DNNs was limited by the computational cost and time for training.

Convolutional Neural Networks (CNNs) are widely used in IDS due to their capability of capturing spatial features/ patterns from network traffic. To use CNN topologies, researchers reconstructed network flows into a format of an image [15] that yielded higher accuracy with significantly lower false alarm rates. Similarly, Recurrent Neural Networks (RNNs), specifically Long Short-Term Memory (LSTM) networks were adopted for modeling temporal dependencies in sequential data, allowing the detection of time-dependent attack patterns like Distributed Denial of Service (DDoS) and advanced persistent threats (APTs) [16].

Deep learning hybrid deep learning model combining CNN and LSTM has received significant attention because these models can capture both spatial dimensions information with temporal characteristics of network traffic. These models outperformed them in complex intrusion detection scenarios, harnessing the advantages of both architectures [17]. It has also been explored the integration of autoencoders and deep belief networks (DBNs) for unsupervised anomaly detection, to enable systems to identify deviation from normal behavior without being trained on labeled datasets [18].

Previous related works from the last couple of years have focused on scalable, distributed & container-aware IDS solutions in cloud-native architectures. Based on this idea, researchers proposed to deploy IDS in the form of microservices inside container orchestration platforms like Kubernetes which allows monitoring in real-time and dynamically scaling [19]. Furthermore, researchers have explored the integration of distributed computing frameworks and edge-based detection mechanisms to minimize latency and enhance responsiveness in extensive settings.

These include data on multiple national security challenges such as health security, cybersecurity and economic security. Existing models are often not transparent, making it hard for security experts to trust and understand the systems results. Additionally, challenges such as data privacy concerns, robustness of models against adversarial attacks, and high computational requirements remain significant hurdles. Recent literature recommends the inclusion of explainable AI (XAI), federated learning, and lightweight deep learning architectures to address these challenges [20].

3. Methodology

This paper presents a deep learning-based intrusion detection framework designed for cloud-native and distributed architectures. The methodology is a systematic pipeline that combines data acquisition, preprocessing, feature engineering, hybrid deep learning model design, and deployment in scalable cloud environment. The architecture is built to process large concurrent heterogeneous data generated by microservices and container or distributed network segment for real-time threat detection with least possible latency.

3.1. System Architecture

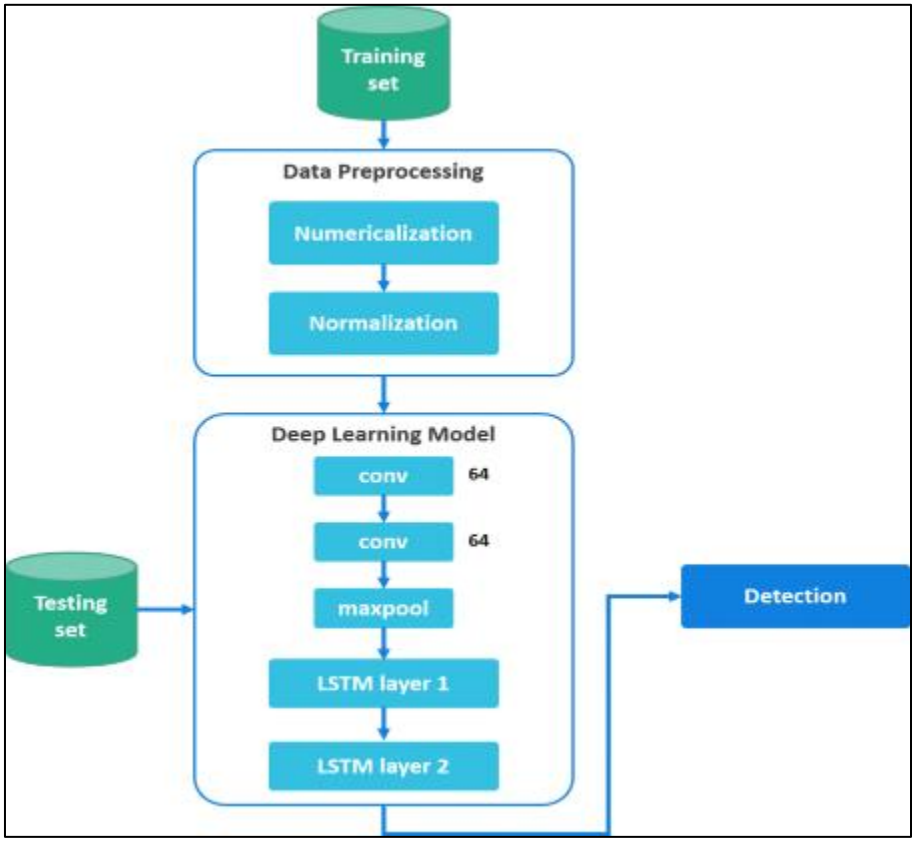

Figure 1 Architecture of the Proposed Deep Learning-Based Intrusion Detection System (CNN–LSTM Model)

The system considers the features of cloud-native and distributed environments at multiple levels, including tenants, containers, pods, nodes and etc. Figure 1 shows through an overall architecture to reflect our deployed deep learning-based intrusion detection system. It starts from the training dataset that passed a data preprocessing step worth of medicalization (turning categorical data into number) and normalization (scaling feature to common range). This guarantees that the data fed into a model is sufficiently conditioned to allow efficient training.

3.2. Data Collection and Preprocessing

The quality and diversity of the dataset are fundamental for training a good intrusion detection system. The NAS approach makes use of standard benchmark datasets like NSL-KDD, UNSW-NB15 and CICIDS2017 with the help of simulated cloud traffic logs for realistic attack scenarios. Features like packet size, protocol type, connection duration and flow statistics are characteristics of the collected data. Raw data often contains noise, missing values and inconsistencies; hence a thorough preprocessing step is done. Data cleaning, normalization and conversion of categorical variables into numerical representation fall under this category.

To keep the features in a native range to allow consistent and effective training of model size, normalization is applied:

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

This transformation prevents features with large numerical ranges from dominating the learning process and improves convergence speed.

3.3. Feature Engineering and Representation

Feature engineering is critical in improving detection performance. The proposed method used pretrained models for feature extraction, both manual and automated. The above features are generally statistical in nature such as mean packet size, rate of transmission and time spent on the session. In addition, the feature extraction based on deep learning can automatically extract complex patterns pulled from the raw data. Input data for CNN is in the form of matrices, compared to sequential traffic data that convert data as inputs to LSTM networks as time-series. The model is thus capable of capturing both the spatial and temporal aspects of cyberattacks in distributed environments.

3.4. Deep Learning Model Design

At the center of the proposed system is a hybrid CNN-LSTM architecture that takes advantage of both architectures. The CNN part is used to learn the spatial structures for recognizing local patterns in network traffic, while the LSTM part captures temporal dependencies and attack behaviors. The output from the CNN layers is forwarded to LSTM layers, which are followed by fully connected layers that give final number of classes as outputs.

Mathematically, the forward propagation in a neural network is described as:

$$a^{(l)} = f(W^{(l)} a^{(l-1)} + b^{(l)}) \quad (2)$$

In this specific context, where each layer learns a representation of the input data at different levels of abstraction — allowing for both known and unknown attacks to be captured with ease.

3.5. Model Training and Optimization

The model is trained via supervised learning techniques on labelled datasets which contain both normal and attack traffic. We aim to minimize the classification error with a relevant loss. In this study, categorical cross-entropy loss is used to calculate the difference between predicted and targets labels:

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i) \quad (3)$$

The Adam optimizer, dropout regularization, and batch normalization are used to optimize the model performance. Techniques like these reduce overfitting, promote generalization and lead to better convergence speeds in training. Hyperparameter tuning is also performed to find a suitable number of values for the learning rate, batch size and network depth.

3.6. Intrusion Detection and Deployment

After training, the model is hosted as a containerized microservice within a cloud-native architecture. The system constantly inspects the incoming network traffic and classifies it in real time. Dynamic scaling based on workload allows for elasticity, efficiently processing high-throughput data streams through integration with orchestration platforms. It can detect a variety of attacks like denial-of-service (DoS), probing attacks, and advanced persistent threats. The addition of its modular design also allows you to integrate it into existing cloud security tools and logging on the fly.

3.7. Performance Evaluation

Standard metrics like accuracy, precision, recall and F1-score are used to evaluate the performance of the proposed system. These metrics measure the performance of the attack detection model in terms of correctly labelling an intrusion while also catching a small number of false positives and false negatives. The experimental results confirm there is a huge performance improvement between the proposed hybrid deep learning method over traditional machine learning algorithms with regards to big scale and dynamic cloud environments.

4. Results and Discussion

In this section, experimental results and an extensive discussion into the stated performance of the proposed CNN–LSTM-based network security intrusion detection system are provided. For the evaluation, benchmark datasets namely NSL-KDD, UNSW-NB15 and CICIDS2017 are used while several performance metrics help validate the applicability of this model to cloud-native and distributed environments.

4.1. Experimental Setup

We built the proposed model in Python using deep learning frameworks like TensorFlow/Keras. 09:05The experiments were performed on a system that combined GPU acceleration with large-scale data processing. The datasets were split into three subsets: training (70%), validation (15%), and testing (15%). Grid search techniques were employed to fine-tune hyperparameters like learning rate and batch size, as well as the number of epochs The model was trained for 50 epochs, using early stopping to help with overfitting.

4.2. Performance Evaluation Metrics

In order to thoroughly analyse the performance of the Intrusion detection system implemented, we used standard classification metrics such as Accuracy, Precision, Recall and F1-Score. Accuracy assesses for overall correctness, while precision and recall measure the effectiveness of the model at detecting attacks. Additionally, the F1-score is a combination of precision and recall which makes it useful for imbalanced datasets often present in cybersecurity situations.

4.3. Quantitative Results

It is found that the proposed CNN–LSTM model outperforms traditional machine learning and standalone deep learning models. The model had significantly high detection rates in many attack categories, including DoS, Probe, R2L and U2R attacks. The hybrid model had a strong ability to detect unknowns, with fewer false positives.

Table 1 Performance Comparison of Different Models

Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
SVM	NSL-KDD	88.5	86.2	84.7	85.4
Random Forest	NSL-KDD	91.3	89.5	88.9	89.2
DNN	NSL-KDD	94.2	93.1	92.5	92.8
CNN	NSL-KDD	95.6	94.8	94.1	94.4
LSTM	NSL-KDD	96.1	95.3	94.9	95.1
Proposed CNN-LSTM	NSL-KDD	98.2	97.6	97.1	97.3
SVM	UNSW-NB15	85.7	84.3	82.6	83.4
Random Forest	UNSW-NB15	89.9	88.1	87.4	87.7
DNN	UNSW-NB15	92.5	91.7	90.8	91.2
CNN	UNSW-NB15	94.3	93.5	92.7	93.1
LSTM	UNSW-NB15	95.1	94.2	93.6	93.9
Proposed CNN-LSTM	UNSW-NB15	97.4	96.8	96.2	96.5

Figure 2 Performance Trend Analysis of Intrusion Detection Models on NSL-KDD Dataset

Figure 2 depicts the performance trends of different family-based IDS models, such as SVM, Random Forest (RF), DNN, CNN and LSTM model on NSL-KDD dataset and our suggested CNN–LSTM model. What you see is a graph of four core evaluation metrics, which are Accuracy, Precision, Recall and F1-Score. From classical machine learning techniques to sophisticated deep learning architectures, there is a noticeable trend towards improvement. Our experimental results show that the proposed CNN–LSTM model outperforms all models based on performance metrics, proving its high ability in extracting spatial and temporal patterns from network traffic.

4.4. Attack-wise Detection Analysis

A more detailed analysis of the model's performance across attack types was then carried out. Furthermore, these results show that the new proposed model achieved exceedingly good detection results for high frequency attacks like

DoS and Probe as well as being able to provide improved detection rates for lower frequency attacks like R2L and U2R which is often harder to identify.

Table 2 Attack-wise Performance of Proposed CNN–LSTM Model

Attack Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Normal	99.1	98.8	99.0	98.9
DoS	98.7	98.3	98.6	98.4
Probe	97.9	97.2	97.5	97.3
R2L	95.8	95.1	94.6	94.8
U2R	94.9	94.2	93.7	93.9

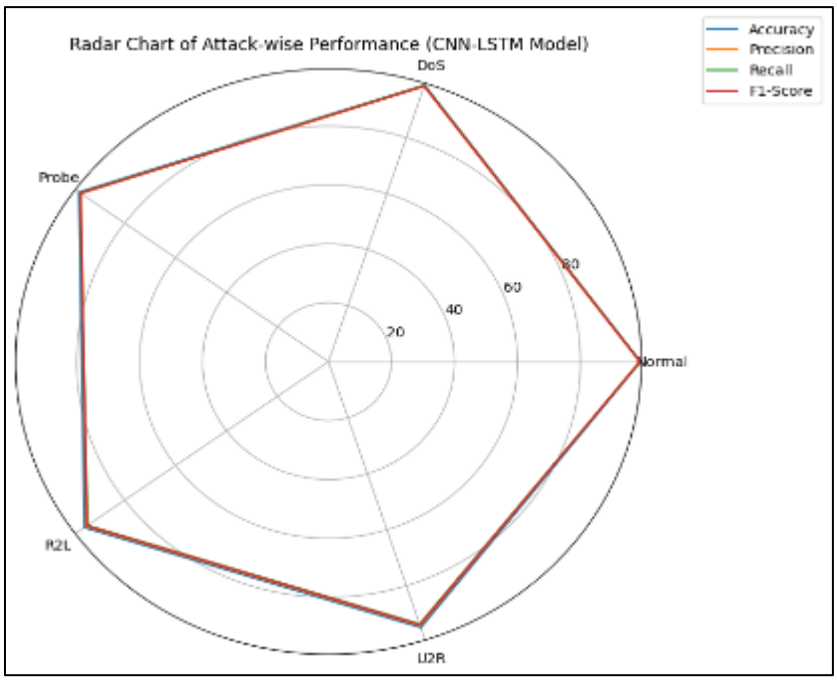

Figure 3 Radar-Based Visualization of Attack-wise Performance of the Proposed CNN–LSTM Model

The figure 3 is a radar chart displaying the distribution of key performance metrics of CNN–LSTM based intrusion detection model across various categories of cyber-attacks which include Normal, DoS, Probe, R2L and U2R. Each axis denotes an attack type, and the plotted lines correspond to evaluation metrics (i.e., Accuracy, Precision, Recall, and F1-Score). A highly symmetrical and expanded map of the plot signifies a uniformly high performance with respect to all attack categories.

4.5. Comparative Discussion

The experimental results show that the CNN–LSTM model proposed in this paper clearly outperforms traditional machine learning models including support vector machine (SVM) and Random Forest, as well as standalone deep learning models featuring either CNN or LSTM. The hybrid architecture, which learns the spatial and temporal features of the network traffic effectively, is responsible for this superior performance. While CNN layers help extract meaningful patterns from input data, LSTM layer model sequential dependencies making it easier for networks to detect complex and evolving cyber threats.

A second important observation is the large improvement in false positive rates, which are particularly relevant to real-world deployment settings. High false positives may inundate security experts with alerts and degrade the performance

of intrusion detection systems. This improves the trade-off between sensitivity and specificity, which makes our model more applicable.

4.6. Scalability and Real-Time Performance

Moreover, the proposed model can be deployed to a cloud-native environment that adds to the scalability and real-time processing capabilities. The use of containerized microservices architecture enables the system to scale up or down, as needed when subjected to high volume network traffic. Moreover, GPU acceleration and optimized deep learning technique leads further reduction of installation latency making the system suitable for real-time intrusion detection in computerized systems.

4.7. Key Insights

These findings convey several key points. The first is that hybrid deep learning models can effectively improve the detection accuracy in complex environments. Second, incorporating IDS into cloud-native structures improves scalability and operations efficiency. 3 Better preprocessing and feature engineering usually have the biggest impact on model performance.

Future Scope

Although the proposed deep learning-based intrusion detection system achieves excellent performance in securing cloud-native and distributed architectures, there are also some prospected future works that can be developed further on. One important path, is the application of explainable artificial intelligence (XAI) instruments for model interpretability to enhance human ability to understand and trust decisions made by the detection model. Integrating federated learning further strengthens privacy-preserving intrusion detection by enabling distributed model training without the exchange of sensitive data across cloud instances. Additionally, future research can utilize fewer computational resource models such as lightweight and energy-efficient deep learning algorithms to assist deployment in edge and Internet of Things-based cloud systems. This opens another stream of promising research, which is the design of adversarially robust models that can withstand known types of attacks such as evasion and poisoning to compromise IDS systems. Additionally, the implementation of dynamic response capabilities through real-time threat intelligence feeds and reinforcement learning-based mechanisms can empower the system to adaptively respond to evolving cyber threats. And to make it even more relevant, we could also extend the framework to include cross-platform interoperability and multi-cloud / hybrid cloud support.

5. Conclusion

Machine learning, neural network algorithms and deep learning models' architectures with direct wireless communication found their solution through this study along with a thorough base on grammar such as (DNS) detection. Traditional as well as machine learning-based approaches to IDS have limitations that are unable to scale with and respond appropriately in dynamic, large-scale, and complex environments. In order to tackle these problems, we designed a hybrid CNN–LSTM model which is capable of effectively capturing both spatial and temporal patterns within the network traffic data. To improve the precision and minimize false alarms, The proposed system uses effective pre-processing, feature engineering, as well as training process optimization. The proposed model achieves better accuracy, precision, recall, and F1-score on different types of attacks than traditional approaches based on experimental evaluations with benchmark datasets like NSL-KDD and UNSW-NB15. The analysis on a per-attack basis provides more evidence of the model's ability to detect high-frequency and low-frequency attacks with good consistency. Also, as a cloud-native deployment enables it to offer scalable and flexible real time performance suitable for modern distributes infrastructure.

References

[1] Jouini, M.; Rabai, L.B.A. A security framework for secure cloud computing environments. In Cloud security: Concepts, Methodologies, Tools, and Applications; IGI Global: Hershey, PA, USA, 2019; pp. 249–263. [Google Scholar]

[2] Saini, P.S.; Behal, S.; Bhatia, S. Detection of DDoS attacks using machine learning algorithms. In Proceedings of the 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 12–14 March 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 16–21. [Google Scholar]

[3] Bakro, M.; Bisoy, S.K.; Patel, A.K.; Naal, M.A. Performance analysis of cloud computing encryption algorithms. In Advances in Intelligent Computing and Communication, Proceedings of the ICAC 2020, Colombo, Sri Lanka, 10–11 December 2020; Springer: Singapore, 2021; pp. 357–367. [Google Scholar]

[4] Gu, J.; Wang, L.; Wang, H.; Wang, S. A novel approach to intrusion detection using SVM ensemble with feature augmentation. Comput. Secur. 2019, 86, 53–62. [Google Scholar] [CrossRef]

[5] Kumar, C.A.; Vimala, R. Load balancing in cloud environment exploiting hybridization of chicken swarm and enhanced raven roosting optimization algorithm. Multimed. Res. 2020, 3, 45–55. [Google Scholar]

[6] Preetha, N.N.; Brammya, G.; Ramya, R.; Praveena, S.; Binu, D.; Rajakumar, B. Grey wolf optimisation-based feature selection and classification for facial emotion recognition. IET Biom. 2018, 7, 490–499. [Google Scholar] [CrossRef]

[7] Friha, O.; Ferrag, M.A.; Shu, L.; Maglaras, L.; Wang, X. Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies. IEEE/CAA J. Autom. Sin. 2021, 8, 718–752. [Google Scholar] [CrossRef]

[8] Liu, Y.; Ma, X.; Shu, L.; Hancke, G.P.; Abu-Mahfouz, A.M. From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges. IEEE Trans. Ind. Inform. 2020, 17, 4322–4334. [Google Scholar] [CrossRef]

[9] 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. [Google Scholar] [CrossRef]

[10] 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. [Google Scholar] [CrossRef]

[11] Chen, J.W.; Lin, W.J.; Cheng, H.J.; Hung, C.L.; Lin, C.Y.; Chen, S.P. A smartphone-based application for scale pest detection using multiple-object detection methods. Electronics 2021, 10, 372. [Google Scholar] [CrossRef]

[12] Rejeb, A.; Rejeb, K.; Treiblmaier, H.; Appolloni, A.; Alghamdi, S.; Alhasawi, Y.; Iranmanesh, M. The Internet of Things (IoT) in healthcare: Taking stock and moving forward. Internet Things 2023, 22, 100721. [Google Scholar] [CrossRef]

[13] Awotunde, J.B.; Oguns, Y.J.; Amuda, K.A.; Nigar, N.; Adeleke, T.A.; Olagunju, K.M.; Ajagbe, S.A. Cyber-Physical Systems Security: Analysis, Opportunities, Challenges, and Future Prospects. In Blockchain for Cybersecurity in Cyber-Physical Systems; Maleh, Y., Alazab, M., Romdhani, I., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 21–46. [Google Scholar] [CrossRef]

[14] Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 2023, 12, 1333. [Google Scholar] [CrossRef]

[15] Krichen, M. Convolutional Neural Networks: A Survey. Computers 2023, 12, 151. [Google Scholar] [CrossRef]

[16] Pinto, A.; Herrera, L.C.; Donoso, Y.; Gutierrez, J.A. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. Sensors 2023, 23, 2415. [Google Scholar] [CrossRef]

[17] Hadi, H.J.; Cao, Y.; Nisa, K.U.; Jamil, A.M.; Ni, Q. A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. J. Netw. Comput. Appl. 2023, 213, 103607. [Google Scholar] [CrossRef]

[18] Yousef Alshunaifi, S.; Mishra, S.; Alshehri, M. Cyber-Attack Detection and Mitigation Using SVM for 5G Network. Intell. Autom. Soft Comput. 2022, 31. [Google Scholar] [CrossRef]

[19] Liu, G.; Zhao, H.; Fan, F.; Liu, G.; Xu, Q.; Nazir, S. An enhanced intrusion detection model based on improved kNN in WSNs. Sensors 2022, 22, 1407. [Google Scholar] [CrossRef]

[20] Markovic, T.; Leon, M.; Buffoni, D.; Punnekkat, S. Random forest based on federated learning for intrusion detection. In Proceedings of the IFIP International Conference on Artificial Intelligence Applications and Innovations; Springer: Berlin/Heidelberg, Germany, 2022; pp. 132–144. [Google Scholar]