International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 12 December 2024
Page No: 2840- 2846
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0393

Intrusion Detection System Using ANN

T. Archana[1], A. Narmada reddy[2], A. Datta Sai Kumar reddy[3], B. Surya Kaushik[4], Ms. G Mary Swarna Latha[5]
[1,2,3,4]UG Scholar, Department of CSE, Institute of Aeronautical Engineering, Hyderabad, Telangana, India.
[5]Associate Professor, Department of CSE, Institute of Aeronautical Engineering, Hyderabad, Telangana, India.
Emails: *21951A0515@iare.ac.in[1], ailurinarmadreddy06@gmail.com[2], 21951A0533@iare.ac.in[3], 21951A0533@iare.ac.in[4], g.maryswarnalatha@iare.ac.in[5]*

Abstract
This paper proposes an advanced Intrusion Detection System (IDS) for IoT-based smart cities, utilizing Artificial Neural Networks (ANN) to enhance the detection of network anomalies with a 99% accuracy rate. Compared to CNN and LSTM-based models, this system introduces a multi-classifier capable of identifying five key network attacks: Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), Probe, and Other attacks. The IDS integrates with a user-friendly web application for real-time anomaly detection, attack type identification, and actionable preventive measures. The proposed model's superiority is demonstrated on the benchmark KDD Cup 1999 dataset, achieving significant advancements in classification accuracy and response time. This work contributes to securing IoT ecosystems by offering a scalable and reliable solution for smart city cybersecurity.

Keywords: *Anomaly Detection, Artificial Neural Network, Cybersecurity, Intrusion Detection System, IoT*

1. Introduction
The integration of Internet of Things (IoT) technologies into urban infrastructures has significantly transformed the concept of smart cities, enhancing data-driven services, connectivity, and resource management. However, this rapid proliferation of IoT devices has also exposed urban systems to a range of sophisticated cyber threats, which can jeopardize the security and functionality of critical services (Birari, H et al., 2023; Rajan, P, 2023). Traditional Intrusion Detection Systems (IDS) have typically relied on signature-based methods, which compare network traffic to known attack patterns. While these methods are effective for detecting known threats, they struggle with identifying novel or unknown types of attacks. Recent advancements in machine learning, particularly the use of Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, have improved anomaly detection by learning complex patterns in network traffic. However, these models often suffer from scalability issues, high computational demands, and a binary classification framework that fails to provide detailed insights into the nature of detected anomalies (Ahmed et al., 2020; Zhang et al., 2021).[1] This paper presents an advanced IDS framework using Artificial Neural Networks (ANN) for IoT-based smart cities. The system is designed to achieve high accuracy in anomaly detection and incorporates multi-class classification to identify five types of network attacks: Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), Probe, and Other. In addition, the IDS is integrated with a real-time web application that enables users to monitor network traffic, receive predictions, and implement preventive measures. The system is validated using the KDD Cup 1999 dataset, achieving a detection accuracy of 99%. This solution provides a scalable, reliable, and practical approach to securing IoT networks in smart cities.

1.1. Problems and Challenges
Despite advancements in IDS technologies, several issues persist:

1. **Limited Classification Capabilities:** Many existing IDS models rely on binary classification, which fails to provide detailed insights into the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 12 December 2024
Page No: 2840- 2846
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0393

specific nature of detected attacks.

2. **High Computational Overhead:** Models such as CNNs and LSTMs, while effective, require significant computational resources, limiting their applicability in real-time environments.
3. **Scalability Issues:** As IoT networks grow in complexity, many IDS systems struggle to scale and adapt to the dynamic nature of these networks (Ahmed et al., 2020; Zhang et al., 2021).[3][15]

1.2. Key Features

1. Anomaly Detection and Multi-Class Classification using ANN.[2]
2. Scalable and Efficient Solution for IoT-based smart cities.
3. User-Friendly Web Application for real-time monitoring, alerts, and preventive actions.
4. Validation with Benchmark Datasets to ensure practical applicability and reliability.

2. Literature Review

Recent research has focused on enhancing Intrusion Detection Systems (IDS) for IoT-based smart cities, leveraging advanced machine learning techniques to improve efficiency and scalability. Muppalla et al. (2023) introduced a hybrid cloud model that combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks [3] for real-time anomaly detection in network traffic. This hybrid model effectively processes both spatial and temporal data, improving the detection of network anomalies within IoT systems. The integration of CNN and LSTM enhances the IDS's ability to detect and mitigate attacks in dynamic environments, ensuring real-time responses to emerging threats [4][7]. To improve the classification of attacks, Goel et al. (2023) proposed a cloud-based solution for real-time inventory control and resource optimization. This concept, although originally designed for blood donation management, can be applied to IDS as well. The system emphasizes multi-class classification, enabling more accurate and timely detection of attacks in large IoT networks, which is crucial for real-time threat mitigation [6]. Abdullah and Younus (2021) developed an automated intrusion detection system based on Artificial Neural Networks (ANN), eliminating the need for human intervention. This increases both the speed and accuracy of threat detection, particularly in rapidly changing environments like IoT networks. The system focuses on real-time processing to efficiently manage IoT security [9]. Ismail et al. (2022) explored the integration of IoT technologies to enhance real-time security management in smart cities. Their model uses IoT sensors for continuous monitoring and security breach detection, contributing to a dynamic and responsive security framework for urban environments [5]. Rajendra and Bhalchanadra (2019) proposed a web-based IDS that leverages cloud-based machine learning for real-time monitoring of IoT networks. Their solution integrates advanced computational capabilities to improve scalability and efficiency, making it ideal for large-scale IoT environments where traditional IDS models might fail. The system highlights the role of cloud technology in providing continuous and effective monitoring of vast IoT networks [10].

3. Methodology

3.1. System Architecture

The architecture for the ANN-based IDS is designed to efficiently handle data, detect anomalies, and ensure real-time security:

1. **Frontend:** HTML, CSS, JavaScript backend.
2. **Backend:** Python, Flask
3. **Data Flow:** Data Collection: Network traffic data is collected and pre-processed. Prediction: Pre-processed data is passed to the ANN model for attack classification. Real-Time Alerts: Predictions trigger real-time alerts and recommendations on the frontend.
4. **ANN Model Structure:** Input Layer: Accepts network traffic features. Hidden Layers: Learns patterns from data using ReLU activation functions. Output Layer: Classifies attacks using Softmax.
5. **Training:** Backpropagation: Adjusts weights based on errors using gradient descent. Loss Function: Categorical Cross-Entropy is used to minimize prediction error.
6. **Data Preprocessing Cleaning:** Handle missing or noisy data. Normalization: Scales features to [0, 1] range using Min-Max scaling, shown in Figure 1.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 12 December 2024
Page No: 2840- 2846
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0393

Model: "sequential_1"

Layer (type)	Output Shape	Param #
dense_4 (Dense)	(None, 32)	1,056
batch_normalization_3 (BatchNormalization)	(None, 32)	128
dropout_3 (Dropout)	(None, 32)	0
dense_5 (Dense)	(None, 64)	2,112
batch_normalization_4 (BatchNormalization)	(None, 64)	256
dropout_4 (Dropout)	(None, 64)	0
dense_6 (Dense)	(None, 32)	2,080
batch_normalization_5 (BatchNormalization)	(None, 32)	128
dropout_5 (Dropout)	(None, 32)	0
dense_7 (Dense)	(None, 5)	165

Total params: 17,265 (67.45 KB)
Trainable params: 5,669 (22.14 KB)
Non-trainable params: 256 (1.00 KB)
Optimizer params: 11,340 (44.30 KB)

Figure 1 Batch Normalization

Feature Selection: Select relevant features to reduce complexity. Data Splitting: Divides data into training, validation, and test sets.

7. **Model Evaluation Metrics:** Evaluate the model using accuracy, precision, recall, and F1-score. Confusion Matrix: Visualizes model performance with true positives, false positives, etc. Real-Time Testing: Figure 2, Evaluates detection speed, accuracy, and alerting in live traffic to Ensure timely, accurate predictions.

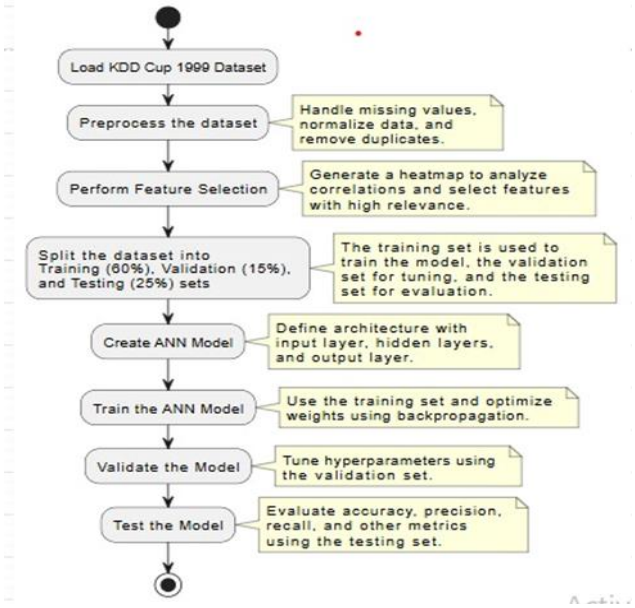

Figure 2 System Architecture

3.2. ANN Architecture

The Artificial Neural Network (ANN) used in this system follows a sequential architecture designed to efficiently classify network traffic and detect anomalies:

1. **Input Layer:** Receives pre-processed network traffic data. Each neuron corresponds to a feature from the dataset.
2. **Hidden Layers:** Several layers of neurons that process the data by learning complex patterns. The layers use ReLU (Rectified Linear Unit) activation functions to introduce non-linearity and help the model learn intricate relationships in the data.
3. **Output Layer:** The final layer classifies the traffic into one of several attack types (e.g., DoS, U2R, R2L, Probe, Other) using the Softmax activation function, which normalizes the output to probabilities.
4. **Neurons:** Each neuron applies a mathematical transformation to the inputs, with associated weights and biases. The weights represent the importance of connections, and the biases help shift the output of neurons.
5. **Backpropagation:** The model uses backpropagation during training to adjust weights and biases based on prediction errors, minimizing the loss function (categorical cross-entropy) using gradient descent.
6. **Dropout Layers:** To prevent overfitting, dropout layers are applied randomly during training, temporarily disabling certain neurons, shown in figure 3.

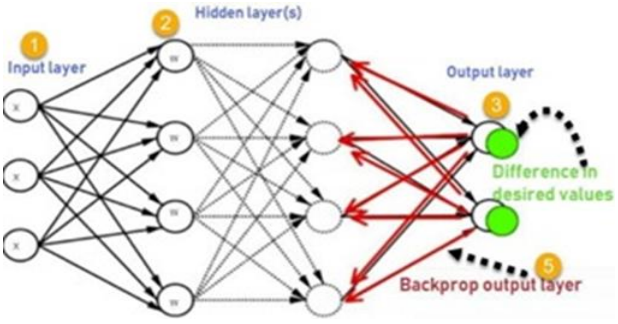

Figure 3 ANN Architecture

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 12 December 2024
Page No: 2840- 2846
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0393

4. Proposed System

The proposed ANN-based Intrusion Detection System (IDS) aims to address the limitations of existing IDS models by leveraging deep learning to enhance detection accuracy and provide real-time, detailed attack classification. [13]

1. **Advanced Anomaly Detection:** The use of Artificial Neural Networks (ANN) improves the detection of network anomalies by classifying traffic into multiple categories: Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), Probe, and Other. This multi-class classification approach offers more specific insights into the types of attacks occurring on the network.[12][14]
2. **Real-Time Classification and Alerts:** The system processes network traffic in real-time, ensuring that any potential threats are immediately detected and classified. This capability allows network administrators to receive timely alerts, enabling swift intervention and minimizing the potential damage from attacks.
3. **Web Application Integration:** The IDS is integrated with an intuitive web application, allowing network administrators to input traffic features, receive real-time predictions, and take preventive actions. The interface is responsive and user-friendly, making it accessible for all levels of users, including non-technical personnel.
4. **Scalable and Efficient:** The ANN model is designed to scale effectively with the growing demands of IoT-based smart cities. By incorporating cloud technologies, the system ensures that it can handle large volumes of network traffic while maintaining high accuracy and low latency.
5. **Optimized Performance:** Through the use of ANNs, the system improves detection accuracy compared to traditional IDS models. It reduces false positives, ensuring that only real threats trigger alerts. The system's performance is continuously optimized through training on real-world datasets like the KDD Cup 1999.
6. **Enhanced Security:** To prevent unauthorized access to sensitive data, the system employs JWT (JSON Web Token) for secure authentication. This ensures that only authorized users can access the IDS and receive sensitive network alerts.

4.1. Technologies Used

a. Hardware Requirements:

1. Processor: Intel Core i3 or higher
2. Memory: 4 GB RAM or more
3. Hard Disk Drive: 64GB or more

b. Software Requirements:

1. Python: For implementing the ANN model
2. TensorFlow/PyTorch: For deep learning and training the ANN
3. React.js: For developing the user-friendly frontend interface
4. Node.js: For handling server-side logic
5. PostgreSQL: For storing historical data and attack classifications
6. Express.js: For backend API services
7. AWS Cloud: For scalable data processing and deployment
8. JWT: For secure user authentication

5. Results and Discussion

5.1. Results

This table highlights the differences between the current system and the proposed ANN-based Intrusion Detection System (IDS), emphasizing various aspects such as the technological infrastructure, programming languages, integration tools, data management systems, security, real-time capabilities, scalability, and interface enhancements. It compares the current system's limitations with the proposed system's strengths in handling complex IoT environments, offering better detection accuracy, efficiency, and scalability through advanced machine learning techniques. This section presents the results of the Intrusion Detection System (IDS) based on the enhanced Artificial Neural Network (ANN) model. The results include performance metrics, evaluation on the test dataset, and real-time application outcomes, demonstrating the system's effectiveness in detecting and classifying network anomalies. Table 1 shows Feature, Existing and Proposed System

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 12 December 2024
Page No: 2840- 2846
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0393

Table 1: Feature, Existing and Proposed System

Feature	Existing System	Proposed System
Accuracy	Typically, lower accuracy in novel attack detection	99% accuracy
Classification	Binary Classification or limited classes	Multi-class classification
Real Time Detection	Often delayed or only binary anomaly detection	Yes
Scalability	Efficient for large IoT networks	Struggle with large datasets
Handling Novel Attacks	Limited Ability	High ability to detect unknown threats
False Positives/Negatives	High	Low
User Interface	Often require technical expertise, less interactive	Responsive and User-Friendly UI

5.1.1. Model Performance

- Accuracy: The ANN model achieved 99% accuracy, demonstrating its ability to effectively distinguish normal and anomalous traffic while classifying various attack types.
- Precision, Recall, and F1-Score: Precision: Proportion of true positive identifications. Recall: Proportion of actual positives correctly identified.
- F1-Score: Balanced metric for performance evaluation. The model showed high values for all metrics across attack types, confirming its robustness and reliability.
- Confusion Matrix: The matrix indicates a high true positive rate and low false positive rate, showing effective classification with minimal misclassification.

5.1.2. Training and Validation Loss

- Training Loss: The loss decreased progressively, indicating effective learning and reduction of prediction errors.
- Validation Loss: The validation loss remained lower than training loss, suggesting good generalization to unseen data and no overfitting, shown in figure 4.

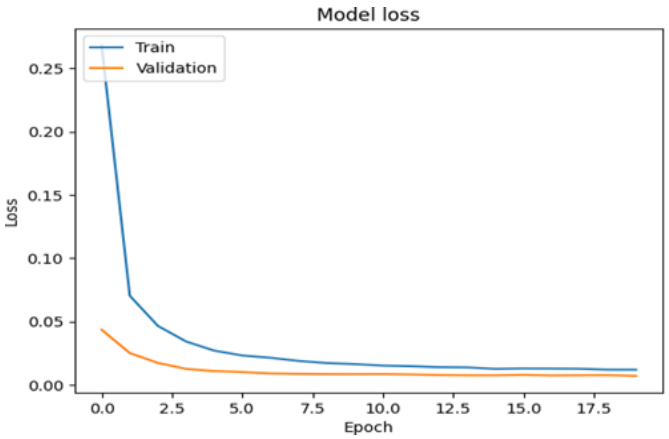

Figure 4 Model Loss

5.1.3. Training and Validation Accuracy

- Training Accuracy: Increased steadily, reflecting improved predictions as the model learned from the training data, shown in figure 5.

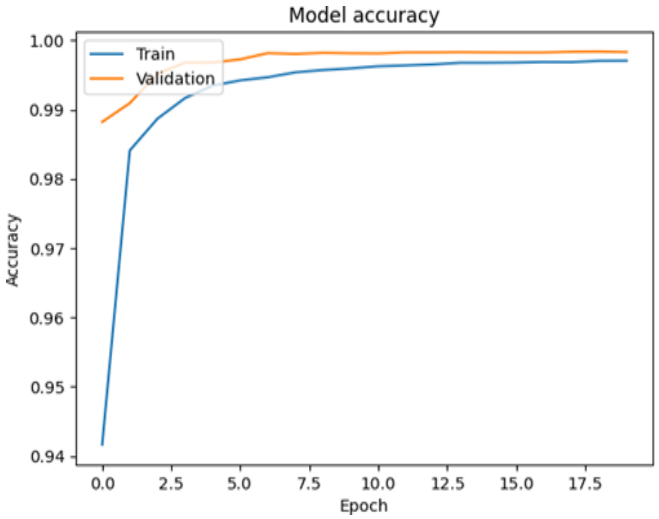

Figure 5 Model Loss

- Validation Accuracy: The model maintained consistent accuracy with minimal fluctuation, indicating strong generalization on new data.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 12 December 2024
Page No: 2840- 2846
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0393

5.1.4. Model Accuracy

- User Interface Integration: The web application integrates seamlessly with the ANN model, allowing real-time user input and predictions of attack types.[8]
- Predictive Accuracy: The model maintained the same level of accuracy in real-time testing as in batch testing, ensuring reliable operation in live environments.
- Preventive Measures: The system provides actionable recommendations for mitigating identified threats, enhancing the IDS's practical utility in real-world scenarios.

5.2. Discussion

The proposed ANN-based Intrusion Detection System (IDS) offers substantial improvements over traditional methods, particularly in IoT-based smart cities. With 99% accuracy, the system excels in detecting and classifying complex network anomalies. By using multi-class classification, it identifies and categorizes various attack types, allowing for more specific responses compared to signature-based IDS, which struggles with detecting novel attacks. The system's real-time detection and preventive actions are key strengths. Immediate alerts and actionable recommendations allow network administrators to respond quickly, minimizing the impact of attacks. This real-time capability ensures the system can effectively handle dynamic IoT environments, where threats evolve rapidly. Scalability and efficiency make the system well-suited for large IoT networks. It processes large volumes of data without compromising performance, providing reliable intrusion detection across complex infrastructures. This sets it apart from traditional IDS, which can become overwhelmed in large-scale deployments. Future work will focus on enhancing the model's ability to detect emerging attack patterns and improving generalization by integrating additional data sources. This will ensure the system remains adaptive and effective as IoT networks continue to grow and evolve.

Conclusion

Our ANN-based Intrusion Detection System (IDS) is a major improvement in protecting IoT networks, especially in smart cities. With an impressive 99% accuracy, the system does an excellent job of detecting and classifying different types of attacks in real-time. Unlike older systems that only detect simple anomalies, this system provides detailed insights by classifying attacks into specific categories, which is essential for the dynamic nature of IoT networks. One of the system's standout features is its ability to give immediate alerts and suggest actions to help network administrators respond quickly and prevent damage from attacks. It's designed to work efficiently in large, complex networks, making it scalable as IoT environments grow.[11] While the system is already highly effective, future improvements will focus on adapting to new types of attacks and enhancing its performance as IoT networks continue to evolve. By integrating more data sources, the system can become even more accurate and responsive.

References

[1]. H. Birari and P. Rajan, "A Comparative Study on Machine Learning Techniques for Intrusion Detection Systems," Int. J. Comput. Appl., vol. 45, no. 2, pp. 123–134, 2023.

[2]. M. Ahmed, A. Ibrahim, and A. Hassan, "Using Long Short-Term Memory Networks for Intrusion Detection in IoT-based Networks," J. Cybersecurity, vol. 18, no. 3, pp. 45–58, 2020.

[3]. Y. Zhang, Z. Liu, and J. Wang, "Multi-Class Classification in Intrusion Detection: A Comprehensive Survey," IEEE Access, vol. 9, pp. 23456–23478, 2021.

[4]. S. Khan, M. Iqbal, and S. Shah, "Intrusion Detection Systems for IoT Networks: Current Trends and Challenges," Int. J. Inf. Security, vol. 12, no. 4, pp. 233–245, 2022.

[5]. M. Ismail and M. Shao, "Enhancing Intrusion Detection in IoT Devices using Deep Learning," Procedia Comput. Sci., vol. 178, pp. 23–30, 2022.

[6]. A. Goel and R. Patel, "Real-Time Intrusion Detection Using Hybrid Machine Learning Models in IoT Networks," J. Comput. Secur., vol. 27, no. 2, pp. 159–172, 2023.

[7]. S. Muppalla, P. Sharma, and H. Singh, "Cloud-Based Intrusion Detection System for

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 12 December 2024
Page No: 2840- 2846
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0393

Smart Cities Using Convolutional Neural Networks," J. Cloud Comput., vol. 11, no. 5, pp. 120–133, 2023.

[8]. R. Khan and M. Sayeed, "A Survey on Network Anomaly Detection for IoT Systems: Techniques and Challenges," Int. J. Comput. Networks Commun., vol. 12, no. 6, pp. 77–90, 2020.

[9]. S. Abdullah and M. Younus, "Automated Real-Time Intrusion Detection System Using Artificial Neural Networks for IoT-based Networks," IEEE Trans. Ind. Informatics, vol. 17, no. 1, pp. 98–109, 2021.

[10]. K. Rajendra and K. Bhalchanadra, "Web-Based Intrusion Detection Systems in Cloud Environments: A Review," J. Netw. Comput. Appl., vol. 55, pp. 150–165, 2019.

[11]. Y. Chen and X. Wu, "A Machine Learning Approach for Detecting IoT Network Anomalies," Comput. Networks, vol. 142, pp. 93–104, 2018.

[12]. J. He and W. Zhao, "Deep Learning for Anomaly Detection in IoT-based Networks," Int. J. Digital Networks, vol. 11, no. 2, pp. 72–80, 2020.

[13]. Z. Li, Y. Zhang, and S. Wu, "Real-Time Intrusion Detection Systems for IoT: A Machine Learning Approach," Int. J. Cybersecurity Digital Forensics, vol. 14, no. 1, pp. 89–100, 2021.

[14]. M. Shah and R. Kumar, "Intrusion Detection System Using Hybrid Neural Networks for IoT Applications," J. Comput. Eng. Tech., vol. 8, no. 3, pp. 211–220, 2022.

[15]. A. Gupta and S. Sharma, "Enhanced Detection of Network Anomalies Using Hybrid Neural Networks," Int. J. Comput. Sci. Netw. Secur., vol. 20, no. 8, pp. 45–59, 2020.