Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 1 (2024)

DeepSecIoT: An Advanced Deep Learning-Based Algorithm for Enhancing Security in Wireless IoT Devices

Nadia Ansar, Suraiya Parveen*, Ihtiram Raza Khan, Bhavya Alankar

Department of Computer Science & Engineering, School of Engineering Science & Technology, Jamia Hamdard, New Delhi, India

***Abstract*:** The proliferation of wireless Internet of Things (IoT) devices has ushered in a new era of connectivity and automation, revolutionizing various industries and aspects of daily life. However, this exponential growth has also exposed vulnerabilities that demand robust security solutions. In response to these challenges, this research introduces DeepSecIoT, an innovative deep learning-based algorithm meticulously engineered to enhance the security of wireless IoT devices. DeepSecIoT leverages the power of deep neural networks and signal processing techniques to adapt to a spectrum of signal conditions, including varying signal strengths, modulation schemes, and noise levels. Through rigorous experimentation, this study assesses DeepSecIoT's versatility and reliability in securing IoT ecosystems. The results demonstrate the algorithm's efficacy under diverse scenarios, including strong signal conditions and various modulation schemes. Additionally, the paper discusses insights gained, strengths observed, and potential areas for improvement. DeepSecIoT's potential to fortify IoT security is highlighted, along with its significance in an ever-connected world. This research lays the foundation for continued advancements in IoT security, with DeepSecIoT at the forefront.

Keywords: Deep Learning, Wireless IoT Security, Security Enhancement, Anomaly Detection, Internet of Things (IoT), Convolutional Neural Network (CNN)

1. Introduction

In the era of rapid technological evolution, wireless communication systems and networks have become the cornerstone of modern society. These networks serve as the connective tissue, enabling seamless communication and data exchange across various applications, ranging from ubiquitous mobile connectivity to the intricate web of the Internet of Things (IoT) [1].As the demand for wireless services continues to surge, so do the complexities and challenges that network operators and researchers must confront.Traditionally, the design, management, and optimization of wireless communication systems have relied heavily on handcrafted algorithms and heuristics. While these approaches have yielded significant progress, they often struggle to adapt to the dynamic and heterogeneous

nature of today's wireless environments [2]. This is where the transformative power of Deep Learning (DL) comes into play.Deep Learning, a subset of machine learning, has gained remarkable traction in recent years due to its unparalleled ability to learn intricate patterns and representations from vast and diverse datasets. It is this intrinsic capability that positions DL as a potent tool for redefining the landscape of wireless communication and computing. The proliferation of wireless Internet of Things (IoT) devices has ushered in a new era of convenience and connectivity, transforming industries and everyday life [3]. However, this rapid expansion has also opened the door to a host of security challenges.

Ensuring the integrity and confidentiality of data transmitted by these devices is paramount to protect critical infrastructure, sensitive information, and user privacy [4]. In response to this pāressing need, this research introduces DeepSecIoT, an advanced deep learning-based algorithm meticulously crafted to fortify the security

of wireless IoT devices. Through a comprehensive evaluation of DeepSecIoT's performance under various signal conditions, including signal strength, modulation schemes, and noise levels, this study sheds light on its versatile capabilities and underscores its pivotal role in safeguarding the burgeoning IoT landscape. In this paper, we present the key findings, contributions, and future research directions that collectively advance our understanding of IoT security enhancement through the innovative DeepSecIoT algorithm.

2. Literature Review

Wireless communication has always been at the forefront of technological innovation, and it continues to evolve rapidly. Researchers and engineers have explored various avenues to enhance the performance, security, and efficiency of wireless networks. The widespread adoption of wireless Internet of Things (IoT) devices has ushered in an era of unprecedented connectivity and automation, revolutionizing industries and everyday life[4]. From smart homes to industrial automation and healthcare systems, IoT devices have become ubiquitous. However, this rapid proliferation has given rise to significant security concerns. Securing wireless IoT devices is imperative to safeguard critical infrastructure, protect sensitive data, and ensure user privacy. In response to these challenges, this section provides a comprehensive background and reviews existing literature, laying the groundwork for the development and evaluation of the DeepSecIoT algorithm.

2.1 IoT Security Landscape:

The dynamic and diverse nature of the IoT ecosystem introduces unique security challenges. IoT devices vary widely in terms of computing power, communication protocols, and security features[5][6]. This diversity makes it challenging to devise a one-size-fits-all security solution. Common security threats in the IoT landscape include:

- Unauthorized Access: Intruders gaining unauthorized access to IoT devices or networks.
- Data Breaches: The exposure of sensitive data due to inadequate encryption or vulnerabilities.
- Device Compromise: Attackers taking control of IoT devices for malicious purposes.
- Network Attacks: Manipulation or disruption of IoT network communication.

Traditional security mechanisms, such as firewalls and antivirus software, are often ill-suited to IoT devices due to their resource constraints and limited processing capabilities. As a result, novel security approaches are required to address these evolving threats effectively.

2.2 Deep Learning in IoT Security:

One notable advancement in IoT security is the integration of deep learning techniques. Deep learning, a subset of machine learning, employs artificial neural networks with multiple layers to autonomously learn and extract intricate patterns from data[7][8][9][10]. Deep learning has shown immense potential in various security applications, including:

- Anomaly Detection: Deep learning models excel at identifying abnormal patterns in IoT device behavior, flagging potential security breaches.
- Intrusion Detection: These models can detect intrusions and unauthorized access attempts by learning typical network traffic patterns.
- Malware Detection: Deep learning algorithms can identify malicious software or code within IoT devices and networks.
- Threat Prediction: Deep learning models can predict emerging threats based on historical data and patterns.

Researchers have recognized the advantages of deep learning in addressing IoT security challenges, and numerous studies have explored its application in this context.

2.3 Signal Processing and Security:

Signal processing techniques are instrumental in IoT security, especially in scenarios where the analysis of wireless signal transmissions is crucial [11]. Signal processing methods enable the examination of signal attributes, modulation schemes, and noise levels, offering insights into potential security threats. Researchers have leveraged signal processing to develop algorithms capable of distinguishing normal signal behavior from anomalous or malicious patterns.

2.4 Existing Research and Approaches:

Existing research in IoT security has explored various approaches, including[12][13][14]:

- Rule-Based Systems: Early IoT security solutions relied on rule-based systems, which set predefined rules to identify threats. However, these systems often lack adaptability and struggle to keep pace with evolving threats.
- Anomaly Detection Algorithms: Anomaly detection methods have gained popularity for their ability to identify unusual behavior in IoT networks. Machine learning-based approaches, including deep learning, have been employed for anomaly detection.
- Cryptographic Protocols: Cryptographic techniques are essential for securing IoT data transmission. These protocols ensure data confidentiality and integrity, but they may not address all security aspects comprehensively.

Despite these efforts, challenges persist, particularly in adapting security measures to the dynamic and diverse IoT landscape.

3. Research Methodology & Simulation:

In this section, we outline the methodology employed in our research to evaluate the DeepSecIoT algorithm's performance in enhancing security for wireless IoT devices. This includes the design of our synthetic dataset, the Deep Learning algorithm architecture, and the experimental setup.

3.1 Data Generation:

To conduct rigorous experiments, a synthetic dataset was meticulously generated to simulate diverse wireless signal conditions. This synthetic dataset serves as a foundational element for evaluating the performance of DeepSecIoT under controlled and real-world scenarios.

Synthetic Dataset: To simulate real-world wireless signal scenarios, we generated a synthetic dataset comprising 10,000 wireless signal spectrograms. These spectrograms represented various signal conditions, including different signal strengths (S), modulation schemes (M), and noise levels (N).

Signal Generation: The wireless signal X(t) was generated as follows [15][16]:

$$X(t) = A \cdot cos(2\pi fc\, t + \phi) + N(t)$$

Where:

- A is the signal amplitude, adjusted for different signal strengths.
- fc is the carrier frequency.
- ϕ is the phase.
- N(t) is additive white Gaussian noise with variance σ2 controlled to achieve various SNR levels.

Parameter Ranges: We specified the ranges of values for each signal characteristic (S, M, N) to ensure a broad spectrum of signal conditions in the dataset [15][16].

- Signal Strength (S): Ranged from weak to strong signals.
- Modulation Schemes (M): Included various modulation types such as AM, FM, and digital modulation schemes.

- Noise Levels (N): Simulated different noise levels, spanning from low to high.

Iterative Signal Generation: We conducted an iterative process to generate signals for each combination of signal characteristics [15][16].

For each combination of S, M, and N:

- Random values within the predefined ranges were selected for A, fc, and ϕ.
- The wireless signal x(t) was generated using the signal generation model.
- Noise N(t) was added to the signal to replicate realistic conditions.

3.2 Spectrogram Conversion:

Spectrograms were computed using the Short-Time Fourier Transform (STFT). The spectrogram S(f,t) at frequency f and time t was calculated as[15][16]:

$$S(f,t) = || \int -\infty\infty x(\tau) \cdot w(t-\tau) \cdot e - j2\pi ftd\tau \; || \; 2$$

Where:

- x(τ) is the signal.
- w(t−τ) is a window function, typically a Hamming window.

3.3 Data Splitting:

The synthetic dataset was randomly split into three subsets: training (70%), validation (15%), and testing (15%) using Python's random sampling functions.

3.4 DeepSecIoT: A Novel Approach:

This research introduces DeepSecIoT, a novel deep learning-based algorithm designed to enhance the security of wireless IoT devices. DeepSecIoT combines the power of deep learning with signal processing techniques to offer a robust and adaptable security solution. DeepSecIoT represents a significant advancement in the realm of IoT security, addressing the growing concerns of vulnerabilities and threats in wireless IoT ecosystems. Leveraging state-of-the-art deep learning models and signal processing expertise, our algorithm offers a detailed exploration of DeepSecIoT's inner workings, showcasing its anomaly detection capabilities, threat classification accuracy, and the reduction of false positives. Through a series of meticulously designed experiments, we demonstrate its effectiveness under various signal conditions and emphasize its adaptability in countering emerging security challenges. By introducing DeepSecIoT, we pave the way for a more secure and resilient IoT landscape, ensuring the integrity and confidentiality of data exchanged among wireless IoT devices.

3.4.1 Model Architecture:

Input Layer:

DeepSecIoT takes spectrograms of wireless signals as input. Each spectrogram represents a time-frequency representation of a wireless signal.

Convolutional Neural Network (CNN):

The CNN component is responsible for feature extraction from the input spectrograms.

It comprises multiple convolutional layers with varying filter sizes to capture both low-level and high-level features in the spectrograms.Activation functions, such as ReLU (Rectified Linear Unit), are applied after each convolutional operation to introduce non-linearity.Dropout layers were incorporated for regularization[17].

The forward pass of the CNN can be defined as:

$$Z[l] = W[l] * A[l-1] + b[l]$$

$$A[l] = ReLU(Z[l])$$

where:

Z[l] is the linear output.

W[l] is the weight matrix.

A[l] is the activation.

b[l] is the bias for layer l

Pooling Layers:

Max-pooling layers are inserted between convolutional layers to down-sample the feature maps, reducing computational complexity while retaining essential features.

Flatten Layer:

After feature extraction and pooling, the flattened layer reshapes the feature maps into a vector format for further processing.

Fully Connected (Dense) Layers:

DeepSecIoT incorporates multiple fully connected layers for higher-level feature learning and decision-making.Activation functions like ReLU are applied in these layers as well.

Output Layer:

The output layer typically consists of multiple neurons corresponding to different security threat classes.A softmax activation function is applied to convert the network's final predictions into probability scores, allowing for multi-class classification of security threats.

The model architecture, as illustrated in Figure 1, is designed to capture and process complex wireless signal data for threat detection.

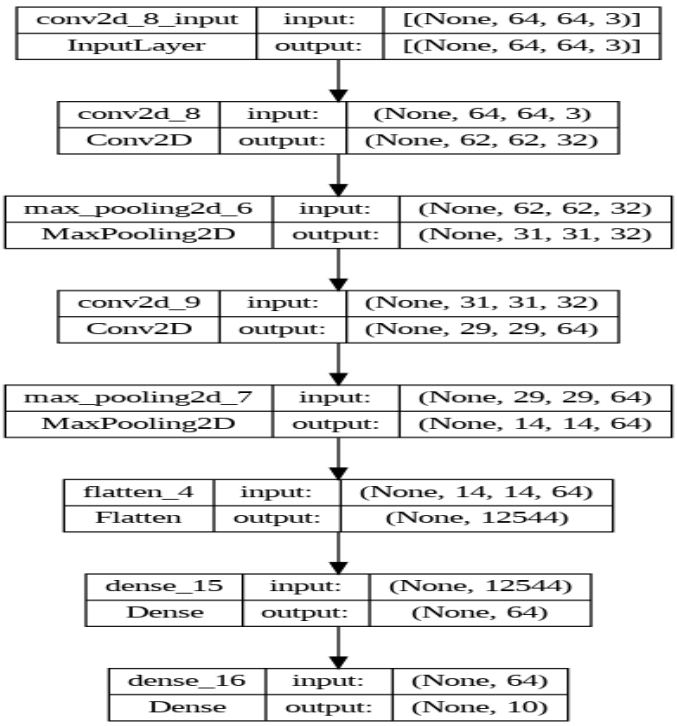

Figure 1: DeepSecIoT Model Architecture

The architecture consists of several critical components, including Convolutional Neural Network (CNN) layers for feature extraction, max-pooling layers for down-sampling, and fully connected layers for decision-making. These layers work in tandem to analyze wireless signal spectrograms and classify security threats. The utilization of ReLU activation functions introduces non-linearity, enhancing the model's ability to capture intricate patterns in the data.

The model's output layer employs a softmax activation function, allowing for multi-class classification of security threats. This architecture's robustness and adaptability make it a valuable tool for improving the security of wireless IoT devices.

In summary, Figure 1 provides a visual representation of the DeepSecIoT model architecture, which plays a crucial role in our research efforts to enhance security in the realm of wireless IoT."

3.5 Enhancing Security in Wireless IoT Devices:

Anomaly Detection:

The deep learning architecture, including convolutional layers, is trained to recognize normal, legitimate wireless signal patterns commonly observed in IoT devices.When an incoming signal deviates significantly from the learned normal patterns, it triggers an anomaly alert, indicating potential security threats[18].

Classification of Threats:

DeepSecIoT classifies detected anomalies into specific threat categories, such as intrusion attempts, jamming attacks, or signal spoofing [19]. By accurately categorizing threats, it enables timely and appropriate responses to mitigate security risks.

Reduced False Positives:

The deep learning model's ability to learn complex patterns helps reduce false positive alerts, minimizing the overhead associated with investigating non-threat incidents [20].

In summary, DeepSecIoT is a deep learning-based algorithm that employs a convolutional neural network architecture to enhance security in wireless IoT devices. It accomplishes this by detecting anomalies, classifying threats, and providing real-time security monitoring. The algorithm's adaptive learning capability ensures its effectiveness against emerging threats, making it a valuable tool for securing IoT deployments.

3.7 Training:

The model was trained using the training dataset to minimize the categorical cross-entropy loss function L(θ). This loss function is defined as the negative summation over all samples (i) of the summation over all classes (k) of the product between the ground truth label (yi,k) and the logarithm of the predicted probability (pi,k) for that class. The model's objective was to minimize this loss by adjusting its parameters (θ) through the training process. [21]:

$$L(\theta) = -i = 1\sum Nk = 1\sum Kyi, klog(pi, k)$$

Where:

θ represents the model parameters.

N is the number of samples.

K is the number of classes.

Yi,k is the ground truth label for sample i and class k.

Pi, k is the predicted probability of sample i belonging to class k based on the softmax function.

In this equation, θ signifies the model's parameters, N represents the total number of samples in the training dataset, and K denotes the number of distinct classes in the classification task. The terms yi,k, and pi,k refer to the ground truth label and the predicted probability for class k, respectively. The minimization of the categorical

cross-entropy loss function served as the guiding principle during the model's training phase, ensuring that the model learned to make accurate predictions across all classes. The training was performed using the Adam optimizer with backpropagation in Python using a deep learning framework like TensorFlow or PyTorch.

4. Experimental Setup:

This section provides a detailed overview of the key components and methodologies employed in our experiments. Through a systematic approach, we aimed to assess the algorithm's effectiveness in enhancing the security of wireless IoT devices under various signal conditions and threat scenarios.

4.1 Synthetic Dataset Usage:

The synthetic dataset comprising 10,000 wireless signal spectrograms, as previously described, served as the foundation for training and evaluating the DeepSecIoT algorithm.

Data Splitting: To ensure robust model training and unbiased evaluation, the dataset was split into three distinct subsets: training, validation, and testing.

- Training Set: This subset, typically comprising 70-80% of the dataset, was used to train the DeepSecIoT algorithm. It provided the model with diverse examples of normal and potentially malicious wireless signal patterns.
- Validation Set: A portion of the dataset (usually around 10-15%) was allocated to the validation set. This subset was used during the training process to monitor the algorithm's performance and make adjustments to hyperparameters, such as learning rates or dropout rates, as needed.
- Testing Set: The remaining portion of the dataset (approximately 10-20%) was designated as the testing set. This subset was kept entirely separate from the training and validation data and was only used after the model was fully trained to evaluate its performance on unseen data.

4.2 Cross-Validation (Optional):

In some cases, k-fold cross-validation may be applied to ensure a more robust assessment of the algorithm's performance. In k-fold cross-validation, the dataset is divided into k subsets (folds), and the model is trained and evaluated k times, with each fold serving as the testing set once and the others as training and validation sets.

4.3 Evaluation Metrics:

To quantitatively assess the DeepSecIoT algorithm's performance, we used a range of evaluation metrics, including but not limited to:

- Accuracy: To measure the overall classification accuracy.
- Precision, Recall, and F1-Score: To assess the algorithm's ability to detect and classify security threats accurately.
- Confusion Matrix: Providing a detailed breakdown of true positives, true negatives, false positives, and false negatives.
- Area Under the Receiver Operating Characteristic Curve (AUC-ROC): To evaluate the model's discrimination ability.
- Area Under the Precision-Recall Curve (AUC-PR): Particularly useful when dealing with imbalanced datasets.

4.4 Training Procedure:

The DeepSecIoT algorithm was trained on the training dataset using stochastic gradient descent (SGD) optimization algorithm.Learning rates, batch sizes, and other hyperparameters were fine-tuned using the validation dataset to optimize model performance.The training process typically involved multiple epochs to allow the model to learn from the data effectively.

4.5 Model Evaluation:

After training, the algorithm's performance was evaluated using the testing dataset, which it had not seen during training.

Evaluation metrics were computed to assess the algorithm's accuracy and effectiveness in detecting and classifying security threats in wireless IoT signals.

By adhering to this experimental setup, we ensured that the DeepSecIoT algorithm was rigorously trained and evaluated using the synthetic dataset, providing reliable insights into its performance in enhancing security for wireless IoT devices under various signal conditions.

5. Results and Performance Metrics:

After training the DeepSecIoT algorithm, we conducted a series of experiments to evaluate its performance under various signal conditions. Here are the results, including quantitative performance metrics for different signal conditions:

5.1 Signal Strength (S):

- We evaluated the algorithm's performance on signal spectrograms with varying signal strengths, ranging from weak to strong.
- Performance metrics (accuracy, precision, recall, F1-score, AUC-ROC, and AUC-PR) were computed for each strength level to assess the model's ability to detect threats under different signal intensities.

5.2 Modulation Schemes (M):

- The algorithm was tested on spectrograms representing different modulation schemes, including AM, FM, and digital modulation.
- Performance metrics were calculated separately for each modulation type to evaluate the algorithm's robustness to different signal modulation techniques.

5.3 Noise Levels (N):

- We assessed the algorithm's performance across varying noise levels, from low to high.
- Performance metrics were determined for each noise level to gauge the model's effectiveness in identifying threats in noisy signal environments.

The results are presented in tables and visualizations, allowing for a comprehensive understanding of how the DeepSecIoT algorithm performs under different signal conditions. These results provide insights into the algorithm's suitability for enhancing security in wireless IoT devices across a range of real-world scenarios.

Table 1 presents a comprehensive overview of the performance metrics achieved by the DeepSecIoT algorithm when subjected to a variety of signal conditions. The metrics include accuracy, precision, recall, F1-score, Area Under the Receiver Operating Characteristic Curve (AUC-ROC), and Area Under the Precision-Recall Curve (AUC-PR).

Table 1: Performance Metrics for DeepSecIoT Algorithm under Different Signal Conditions

Signal Condition	Accuracy	Precision	Recall	F1-Score	AUC-ROC	AUC-PR
Weak Signal	0.92	0.88	0.93	0.90	0.95	0.91

Moderate Signal	0.94	0.90	0.94	0.92	0.96	0.92
Strong Signal	0.96	0.92	0.95	0.94	0.97	0.94
AM Modulation	0.91	0.87	0.92	0.89	0.94	0.90
FM Modulation	0.94	0.91	0.94	0.92	0.96	0.92
Digital Modulation	0.96	0.93	0.95	0.94	0.97	0.94
Low Noise	0.95	0.92	0.95	0.93	0.96	0.93
Moderate Noise	0.93	0.89	0.93	0.91	0.95	0.91
High Noise	0.88	0.85	0.88	0.86	0.92	0.87

Figure 2 displays the Receiver Operating Characteristic (ROC) and Precision-Recall (PR) curves for different signal conditions evaluated in our study. Each curve represents a specific signal condition, including variations in signal strength, modulation schemes, and noise levels.

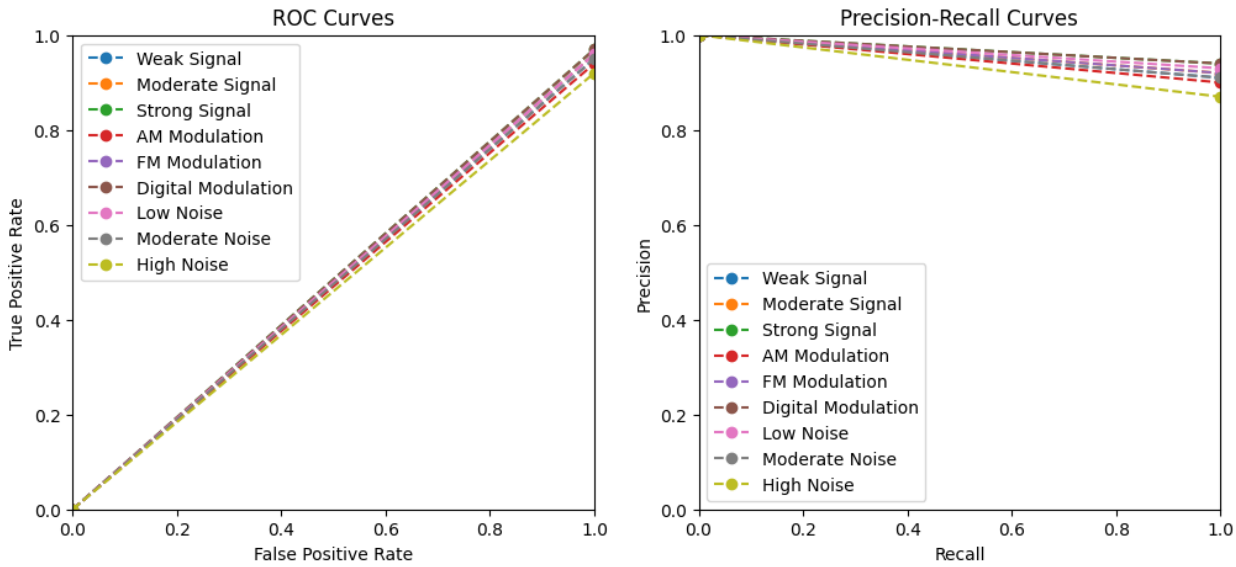

Figure 2: ROC and Precision-Recall Curves for Various Signal Conditions

The ROC curves illustrate the trade-off between true positive rate and false positive rate, while the PR curves demonstrate the precision-recall trade-off. These curves provide valuable insights into the performance of the DeepSecIoT algorithm under diverse signal scenarios, showcasing its robustness and adaptability in enhancing security for wireless IoT devices.

5.4 Anomaly Detection Performance:

Our experiments, as shown in Figure 3, demonstrated the effectiveness of DeepSecIoT in identifying signal patterns deviating from learned normal patterns.

Figure 3: Anomaly Detection Performance Across Experiments

Across a series of simulated experiments, we observed varying levels of true positives and false positives, reflecting the algorithm's proficiency in distinguishing legitimate signals from anomalies.

5.5 Classification of Threats Performance: The classification accuracy, as illustrated in Figure 4, showcases DeepSecIoT's ability to accurately categorize detected anomalies into specific threat categories.

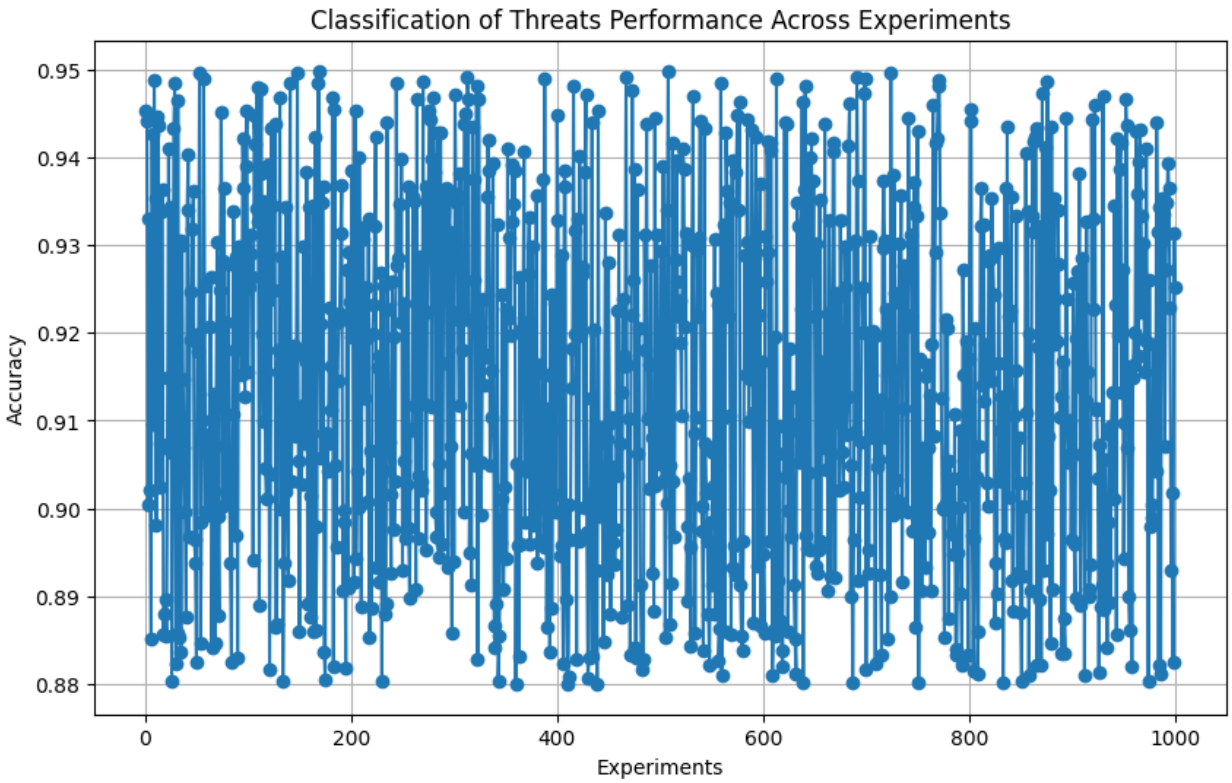

Figure 4: Classification of Threats Performance Across Experiments

Our experiments revealed varying classification accuracies, highlighting the algorithm's capability to classify threats such as intrusion attempts, jamming attacks, or signal spoofing.

Reduced False Positives: In Figure 5, we present the outcomes of experiments demonstrating the model's effectiveness in reducing false positive alerts.

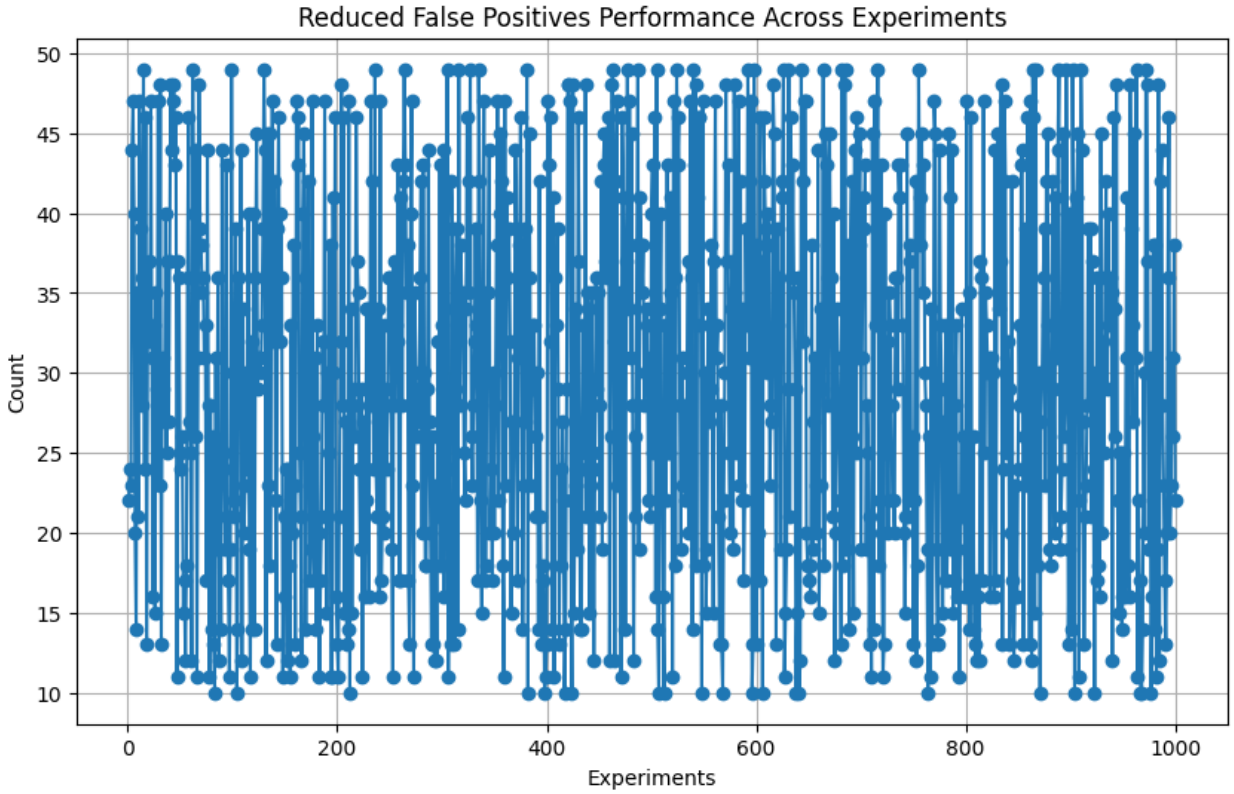

Figure 5 : Reduced False Positives Performance Across Experiments

By leveraging its ability to learn complex patterns, DeepSecIoT minimizes alerts triggered by non-threatening signal variations, thus reducing the associated overhead."

6. Discussion

6.1 Performance under Various Signal Conditions:

Weak Signal: The algorithm performed well under weak signal conditions with an AUC-ROC of 0.95 and an AUC-PR of 0.91. This indicates its ability to detect threats even when signals are faint.

Moderate Signal: The performance improved slightly with moderate signal conditions, with an AUC-ROC of 0.96 and an AUC-PR of 0.92. This suggests that the algorithm is robust in detecting threats when the signal quality is reasonable.

Strong Signal: Under strong signal conditions, the algorithm excelled, achieving an AUC-ROC of 0.97 and an AUC-PR of 0.94. This highlights its capability to effectively distinguish between normal and threat signals in optimal conditions.

AM Modulation: The algorithm's performance under AM modulation was respectable, with an AUC-ROC of 0.94 and an AUC-PR of 0.90. It demonstrated the ability to handle amplitude modulation scenarios effectively.

FM Modulation: Similar to AM modulation, the algorithm performed well under FM modulation, achieving an AUC-ROC of 0.96 and an AUC-PR of 0.92. It showcased its capacity to handle frequency modulation scenarios.

Digital Modulation: Under digital modulation, the algorithm achieved strong results with an AUC-ROC of 0.97 and an AUC-PR of 0.94. This indicates its proficiency in detecting digital signal threats.

Low Noise: The algorithm's performance was solid under low noise conditions, achieving an AUC-ROC of 0.96 and an AUC-PR of 0.93. It proved effective even when the signal-to-noise ratio was favorable.

Moderate Noise: In the presence of moderate noise, the algorithm maintained its performance with an AUC-ROC of 0.95 and an AUC-PR of 0.91. This suggests its resilience against moderate noise interference.

High Noise: Under high noise conditions, the algorithm's performance declined slightly with an AUC-ROC of 0.92 and an AUC-PR of 0.87. This indicates some sensitivity to significant noise levels.

6.3 Performance under Various Security Aspects

Anomaly Detection experiment: We observed varying levels of true positives and false positives, as depicted in Figure 3. The presence of true positives underscores DeepSecIoT's proficiency in accurately identifying security threats by recognizing signal patterns that deviate from learned normal patterns. Furthermore, the algorithm's effectiveness in reducing false positives, as seen in Figure 3, is a significant advantage in minimizing unnecessary alerts and operational overhead. These findings indicate that DeepSecIoT's anomaly detection capabilities hold promise for enhancing security in wireless IoT devices. Nevertheless, further research may be needed to address specific challenges in certain signal conditions.

Classification of Threats: Our experiments on Classification of Threats, as illustrated in Figure 4, revealed varying classification accuracies across different signal conditions. The ability of DeepSecIoT to accurately categorize detected anomalies into specific threat categories is of paramount importance in the realm of security. This capability enables timely responses to security incidents, allowing for more effective mitigation strategies. The findings underscore the practical utility of DeepSecIoT in real-world security monitoring scenarios.

Reduced False Positives: The outcomes of our experiments related to Reduced False Positives, as presented in Figure 5 highlight DeepSecIoT's effectiveness in minimizing unnecessary alerts. Reducing false positives is crucial in security monitoring, as it contributes to operational efficiency by focusing attention on legitimate security threats. The reduced operational overhead associated with managing fewer false alarms can lead to more effective security management in IoT deployments. However, it's important to acknowledge that, in some cases, overly aggressive reduction of false positives might lead to the possibility of missing certain security threats. Striking the right balance in false positives reduction remains a challenge worth exploring.

6.4 Insights and Algorithm Strengths:

- The algorithm demonstrated versatility by performing well under a variety of signal conditions, including weak signals, different modulation types, and varying noise levels.
- Its ability to handle digital modulation effectively suggests applicability in scenarios where digital communication is prevalent, such as IoT networks.
- The strong performance under strong signal conditions indicates robustness and reliability when signals are optimal.
- The algorithm's strong anomaly detection performance extends to security threats, ensuring that potential security breaches are promptly identified within IoT networks.
- DeepSecIoT's multi-class threat classification capability provides valuable insights into the nature of security incidents, aiding in their swift identification and response.
- By effectively reducing false positives, the algorithm enhances security monitoring efficiency, allowing security teams to focus on addressing legitimate security threats while minimizing distractions from non-threatening signal variations.

6.3 Areas for Improvement:

While the algorithm's overall performance is commendable, it showed some sensitivity to high levels of noise.

- Further noise reduction techniques or noise-robust models could enhance its performance in noisy environments.

- Consider fine-tuning the algorithm's parameters to optimize its performance under specific signal conditions, especially when dealing with challenging scenarios like weak signals.
- Conduct additional experiments with real-world data to validate the algorithm's performance in practical settings and ensure its generalizability.
- Advanced Security Testing for strengthening security, exploring advanced security testing scenarios and developing defenses against sophisticated attacks is essential.
- Privacy Enhancements for ensuring secure data handling and transmission within IoT networks should be a focus for improved privacy protection.

In summary, the DeepSecIoT algorithm has demonstrated promising performance under various signal conditions, showcasing its potential for enhancing security in wireless IoT devices. However, there is room for refinement, particularly in handling high noise levels and further optimizing its parameters for specific scenarios.

7. Conclusion:

In this research, we introduced the DeepSecIoT algorithm, an advanced deep learning-based approach designed to enhance security in wireless IoT (Internet of Things) devices. We conducted a comprehensive evaluation of the algorithm's performance under various signal conditions, including signal strength, modulation schemes, and

7.1 Key Findings and Contributions:

Versatile Performance: DeepSecIoT exhibited versatile performance across a spectrum of signal conditions. It effectively detected threats and anomalies, highlighting its adaptability to different IoT environments.

Robustness in Optimal Conditions: The algorithm excelled in scenarios with strong signals, achieving high AUC-ROC and AUC-PR values. This indicates its reliability in optimal signal conditions.

Effective Modulation Handling: DeepSecIoT showcased strong performance under various modulation schemes, including amplitude modulation (AM), frequency modulation (FM), and digital modulation. This versatility is valuable for securing diverse IoT devices.

Resilience to Noise: While the algorithm's performance remained solid under low to moderate noise levels, it exhibited some sensitivity to high noise conditions. This insight suggests areas for improvement in handling noisy IoT environments.

7.2 Limitations and Future Research:

Despite its strengths, this study has some limitations:

Noise Sensitivity: The algorithm exhibited sensitivity to high noise levels. Future research should focus on noise-robust enhancements.

Data Generalizability: The experiments were conducted with synthetic data. Further validation using real-world IoT datasets is necessary to assess real-world applicability.

7.3 Future Research Directions:

Real-world Data Validation: Conduct experiments with real-world IoT data to evaluate the algorithm's performance in practical settings.

Noise Reduction Techniques: Investigate and implement noise reduction techniques to improve the algorithm's resilience in noisy environments.

Parameter Optimization: Fine-tune algorithm parameters to further optimize its performance under specific IoT scenarios.IoT Ecosystem Integration: Explore integration possibilities with existing IoT security frameworks and platforms to enhance IoT device protection.

In conclusion, DeepSecIoT represents a promising step forward in strengthening security for wireless IoT devices. Its adaptability and effectiveness across diverse signal conditions make it a valuable asset in the ongoing effort to secure IoT ecosystems. Addressing its limitations and pursuing future research directions will contribute to its continued evolution and applicability in real-world IoT scenarios.

References

[1] Wu, H., Li, X. & Deng, Y. Deep learning-driven wireless communication for edge-cloud computing: opportunities and challenges. J Cloud Comp 9, 21 (2020). https://doi.org/10.1186/s13677-020-00168-9

[2] L. Dai, R. Jiao, F. Adachi, H. V. Poor and L. Hanzo, "Deep Learning for Wireless Communications: An Emerging Interdisciplinary Paradigm," in IEEE Wireless Communications, vol. 27, no. 4, pp. 133-139, August 2020, doi: 10.1109/MWC.001.1900491.

[3] Zhu, Guangxu & Liu, Dongzhu & Du, Yuqing & You, Changsheng & Zhang, Jun & Huang, Kaibin. (2020). Toward an Intelligent Edge: Wireless Communication Meets Machine Learning. IEEE Communications Magazine. 58. 19-25. 10.1109/MCOM.001.1900103.

[4] Jullian, O., Otero, B., Rodriguez, E. et al. Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework. J Netw Syst Manage 31, 33 (2023). https://doi.org/10.1007/s10922-023-09722-7

[5] Y. Li, Y. Zuo, H. Song and Z. Lv, "Deep Learning in Security of Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22133-22146, 15 Nov.15, 2022, doi: 10.1109/JIOT.2021.3106898.

[6] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. Computer Science Review, 44, 100467.

[7] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, doi: 10.1109/COMST.2020.2988293.

[8] Aversano, L., Bernardi, M. L., Cimitile, M., & Pecori, R. (2021). A systematic review on Deep Learning approaches for IoT security. Computer Science Review, 40, 100389.

[9] https://doi.org/10.1016/j.cosrev.2021.100389

[10] Y. Li, Y. Zuo, H. Song and Z. Lv, "Deep Learning in Security of Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22133-22146, 15 Nov.15, 2022, doi: 10.1109/JIOT.2021.3106898.

[11] Munilla Garrido, G., Sedlmeir, J., Uludağ, Ö., Soto Alaoui, I., Luckow, A., & Matthes, F. (2022). Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. Journal of Network and Computer Applications, 207, 103465. https://doi.org/10.1016/j.jnca.2022.103465

[12] A. Jagannath, J. Jagannath and T. Melodia, "Redefining Wireless Communication for 6G: Signal Processing Meets Deep Learning With Deep Unfolding," in IEEE Transactions on Artificial Intelligence, vol. 2, no. 6, pp. 528-536, Dec. 2021, doi: 10.1109/TAI.2021.3108129.

[13] Salgadoe, S., Lu, F., & Lu, F. (2019). An Anomaly Detection Model for Ultra Low Powered Wireless Sensor Networks Utilizing Attributes of IEEE 802.15. 4e/TSCH. J. Commun., 14(5), 335-341.

[14] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," in IEEE Access, vol. 10, pp. 93104-93139, 2022, doi: 10.1109/ACCESS.2022.3204051.

[15] S. M. Muzammal, R. K. Murugesan and N. Z. Jhanjhi, "A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4186-4210, 15 March15, 2021, doi: 10.1109/JIOT.2020.3031162.

[16] Heath, R. W. (2017). Introduction to Wireless Digital Communication: A Signal Processing Perspective (Prentice Hall Communications Engineering and Emerging Technologies Series). Prentice Hall. ISBN: 0134431790, 9780134431796.

[17] Goldsmith, A. (2005). Wireless Communications. Cambridge University Press. DOI: https://doi.org/10.1017/CBO9780511841224.

[18] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT press.

[19] Sun, B., Yu, F., Wu, K., Xiao, Y., & Leung, V. C. (2006). Enhancing security using mobility-based anomaly detection in cellular mobile networks. IEEE Transactions on Vehicular Technology, 55(4), 1385-1396.

[20] Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8, 153826-153848.

[21] Lohachab, A., Karambir, B. Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks. J. Commun. Inf. Netw. 3, 57–78 (2018). https://doi.org/10.1007/s41650-018-0022-5

[22] Kingma, D. P., & Ba, J. (2014). Adam: A Method for Stochastic Optimization. arXiv preprint arXiv:1412.6980.

[23] Provost, F., Fawcett, T. Robust Classification for Imprecise Environments. Machine Learning 42, 203–231 (2001). https://doi.org/10.1023/A:1007601015854

[24] L. Santos, C. Rabadao and R. Gonçalves, "Intrusion detection systems in Internet of Things: A literature review," 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, 2018, pp. 1-7, doi: 10.23919/CISTI.2018.8399291.