International Journal of Innovative Research in Science and Engineering
Volume No. 12, Issue No. 03, Year 2026
ISSN : 2454-9665

SPAM DETECTION FOR IOT DEVICES USING DEEP LEARNING TECHNOLIGES

1. Mr.S.ANIL KUMAR M.Tech.,Ph.D.
Associate Professor,
Department of CSE, TEC,
sakmba.k@gmail.com

2. P .TEJA HARIKA
tejaharikapadala@gmail.com

3. J.NAGA POOJITHA
puji.jinka@gmail.com

4. K.SHYNI
kampashyni@gmail.com

5. K.DEBORA
karapatidebora333@gmail.com

Abstract— The rapid growth of Internet of Things (IoT) networks has significantly increased the volume of connected devices, making them vulnerable to spam traffic and malicious activities. IoT spam not only degrades network performance but also poses serious security and privacy risks[5]. Early detection and accurate classification of spam traffic are therefore essential for maintaining secure and reliable IoT ecosystems. This project presents a deep learning–based IoT spam detection system using a Deep Neural Network (DNN) model to analyze and classify IoT network datasets effectively.

The proposed system integrates data preprocessing, feature normalization, and classification to distinguish between spam and non-spam traffic patterns[19]. Traditional spam detection techniques rely on rule-based methods and manual feature engineering, which often fail to adapt to evolving attack patterns and large-scale IoT data[1]. In contrast, the DNN-based framework automatically learns complex relationships within the dataset, improving detection accuracy and robustness. The model is trained on structured IoT traffic datasets containing both legitimate and spam records.

Keywords— IoT Spam Detection, Deep Neural Network, Network Security, Data Preprocessing, Classification, Cybersecurity, IoT Traffic Analysis, Spam Filtering, Web-Based Application, DNN Mode

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has led to the widespread deployment of interconnected smart devices across various domains such as smart homes, smart cities, healthcare, and industrial automation[19]. IoT enables seamless communication between physical devices through wired and wireless networks, generating massive volumes of real-time data. While this technological advancement improves efficiency and automation, it also introduces significant security challenges, particularly in the form of spam, malicious traffic, and unauthorized data transmission[7].

As IoT networks expand, traditional spam detection mechanisms based on rule-based filtering and conventional machine learning techniques become insufficient[9]. These methods often rely on manual feature extraction and struggle to adapt to dynamic and evolving spam patterns[2]. Additionally, IoT devices typically operate with limited computational resources, making real-time detection of malicious activities more challenging.

To address these limitations, deep learning techniques have emerged as powerful tools for intelligent threat detection[23]. Deep learning models can automatically learn complex and non-linear patterns from large datasets without requiring handcrafted features[28]. In this project, we propose a Deep Learning-based Spam Detection System for IoT Devices using Artificial Neural Networks (ANN) and Deep Neural Networks (DNN)[30]. These models are trained to classify IoT traffic data as spam or legitimate by learning hidden representations from the dataset.

The proposed system aims to improve detection accuracy, reduce false positives, enhance scalability, and provide better adaptability to evolving spam behaviors. By leveraging deep learning architectures, the system strengthens IoT network security and contributes toward building more reliable and intelligent IoT environments.

The exponential advancement of digital technologies has transformed the way devices interact, leading to the emergence of the Internet of Things (IoT) as a cornerstone of modern innovation[29]. IoT integrates a vast network of sensors, embedded systems, and

communication technologies that enable devices to collect, exchange, and process data autonomously[7]. This interconnected ecosystem is increasingly being adopted in critical sectors such as agriculture, transportation, environmental monitoring, and smart infrastructure, driving efficiency and real-time decision-making.

However, the highly distributed and heterogeneous nature of IoT networks introduces multiple vulnerabilities. Unlike traditional computing systems, IoT devices often lack robust security mechanisms due to constraints such as limited memory, processing power, and energy resources. This makes them attractive targets for cyber threats, including spam attacks, botnets, phishing attempts, and distributed denial-of-service (DDoS) attacks[22]. Spam traffic in IoT environments not only consumes valuable network bandwidth but can also act as an entry point for more severe security breaches, compromising the integrity and confidentiality of data.

Another major challenge in IoT security is the high volume, velocity, and variety of data generated by connected devices. This “big data” characteristic demands intelligent and scalable solutions capable of processing continuous data streams efficiently[20]. Conventional approaches struggle to handle such complexity, especially when dealing with encrypted or obfuscated malicious traffic. Furthermore, the dynamic nature of IoT ecosystems requires adaptive systems that can continuously learn[19] and evolve alongside emerging threats.

Recent developments in artificial intelligence, particularly deep learning, have opened new avenues for enhancing cybersecurity in IoT networks. Deep learning models excel at handling large-scale, high-dimensional data and can uncover hidden patterns that are not easily detectable through traditional methods. Techniques such as Artificial Neural Networks (ANN), Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) have shown significant promise in intrusion detection and anomaly detection tasks.

In this project, we focus on designing a robust and intelligent spam detection framework tailored for IoT environments using deep learning methodologies. The system leverages advanced neural network architectures to analyze network traffic patterns and identify suspicious activities with high precision. It emphasizes automated feature learning, eliminating the need for manual intervention and reducing human bias in the detection process.

Additionally, the proposed model considers important factors such as real-time processing capability, energy efficiency, and deployment feasibility in resource-constrained environments. The integration of such intelligent systems into IoT networks not only enhances security but also supports the development of self-healing and autonomous systems capable of proactive threat mitigation.

Overall, this work contributes to the growing field of IoT cybersecurity by providing a scalable, adaptive, and efficient solution for spam detection. It highlights the importance of combining IoT and deep learning technologies to create secure, resilient, and future-ready digital ecosystems.

II. LITERATURE SURVEY

Neural Network Based Secure Media Access Control Protocol for Wireless Sensor Networks (2018)

In 2018, R. V. Kulkarni[1] and G. K. Venayagamoorthi proposed a neural network-based secure Media Access Control (MAC) protocol aimed at improving communication security in wireless sensor networks. Since wireless sensor networks form the foundation of many IoT architectures, their security mechanisms are directly applicable to IoT environments. The study introduced intelligent learning components within the MAC layer to monitor packet transmission behavior, detect abnormal communication patterns, and prevent malicious access attempts.

The proposed system utilized traffic parameters such as packet collision rates, transmission frequency, and channel utilization to train a neural network model capable of distinguishing between normal and suspicious communication. The integration of learning-based mechanisms enabled adaptive security rather than relying solely on static rule-based protocols. Experimental results demonstrated improved reliability and reduced vulnerability to certain types of attacks. However, the approach was mainly tailored for controlled wireless sensor networks and required careful parameter tuning. Scalability to large-scale IoT deployments and handling highly dynamic IoT traffic remained challenging.

An Efficient Machine Learning-Based Scheme for Web Spam Detection in IoT Environment (2019)

In 2019, A. Makkara and N. Kumar introduced a learning-based framework[2] designed to detect web spam within IoT-integrated systems. With the rapid growth of IoT-connected devices accessing web services, spam and malicious web traffic became a major security concern. The proposed method analyzed web traffic features, communication metadata, and behavioral characteristics to classify spam content effectively. The framework demonstrated improved detection accuracy compared to traditional filtering and rule-based mechanisms. Performance metrics such as precision, recall, and F1-score were used to evaluate model effectiveness. The system showed strong capability in identifying suspicious traffic patterns and reducing false positives. However, the model primarily focused on web-layer spam detection and required significant computational resources for training and

inference. Moreover, it did not fully address device-level IoT traffic anomalies, leaving room for more comprehensive IoT-specific spam detection approaches.

Robust Spammer Detection Using Collaborative Neural Network in IoT Applications (2020)

In 2020, Z. Guo and colleagues proposed a collaborative neural network approach[3] for detecting spammers in IoT applications. This work emphasized distributed intelligence, where multiple IoT nodes collaboratively participated in learning and detection. Instead of relying on a single

centralized model, the system aggregated insights from multiple devices to enhance classification accuracy and reliability.

The collaborative framework reduced isolated misclassification errors and improved robustness against adversarial behavior. By sharing learned representations across devices, the system improved spam detection performance in heterogeneous IoT environments. Experimental results indicated enhanced detection rates and reduced false alarms compared to standalone detection systems. However, collaborative learning introduced communication overhead and synchronization complexity among IoT devices. These additional requirements increased latency and affected real-time deployment feasibility in resource-constrained IoT systems.

Using Machine Learning Unsolicited Information Detection Technique for IoT Devices (2021)

In 2021, K. Monishhaa and B. Veeramallu investigated supervised machine learning techniques[4] for detecting unsolicited information in IoT devices. Their study focused on analyzing traffic flow features, communication intervals, message size distribution, and device interaction behavior. Various classification algorithms were applied to distinguish legitimate data transmissions from spam or malicious activities. The research highlighted improvements in classification accuracy compared to statistical and rule-based detection systems. Machine learning models were capable of identifying patterns in structured IoT traffic datasets and adapting to moderate variations in behavior. However, the approach required extensive manual feature engineering and domain expertise to select relevant input attributes. Additionally, frequent retraining was necessary to accommodate evolving spam patterns, which increased maintenance complexity.

Unsupervised Ensemble Based Machine Learning Approach for Attack Detection in IoT Network (2022)

In 2022, M. S. Ahmed and S. M. Shah proposed an unsupervised ensemble framework for attack detection in IoT networks[5]. The model combined multiple learners to enhance anomaly detection without relying entirely on labeled datasets. By aggregating predictions from several models, the ensemble approach reduced bias and improved detection robustness.

The system demonstrated strong capability in identifying unknown and zero-day attacks by analyzing deviations from normal traffic behavior. The use of ensemble techniques increased generalization performance compared to single-model approaches. However, training multiple models simultaneously increased computational cost and memory usage. Implementation complexity and processing overhead limited real-time applicability in lightweight IoT devices.

Machine Learning-Enabled Anomaly Detection for IoT Systems (2023)

In 2023, Adel Abusitta presented a deep learning-enabled anomaly detection system specifically designed for IoT environments. The framework analyzed communication patterns, device interaction logs, and traffic flow sequences[6] to detect suspicious activities. The model demonstrated enhanced adaptability to evolving threats and reduced dependency on handcrafted features.

The study reported significant improvement in detection accuracy and reduced false positives compared to conventional machine learning models. Automatic feature extraction enabled better representation of complex IoT traffic patterns. However, the system required high computational resources and was more suitable for centralized cloud-based processing rather than edge-level IoT deployment.

Anomaly-Based Intrusion Detection Model Using Deep Learning for IoT Networks (2024)

In 2024, M. A. Alsoufi and co-authors developed an anomaly-based intrusion detection model for IoT networks. The system focused on extracting meaningful traffic features and identifying deviations from normal operational behavior[7]. The approach achieved improved detection rates and reduced false alarm ratios compared to earlier intrusion detection systems.

The study emphasized scalability and adaptability in moderate-sized IoT deployments. Despite performance improvements, increased processing latency and computational

overhead posed challenges for real-time monitoring systems, especially in resource-limited IoT devices.

A Novel Machine Learning Framework with Temporal Attention for IoT Intrusion Detection (2025)

In 2025, K. P. Ghosh and collaborators introduced a temporal attention-based learning framework for IoT intrusion detection. The model captured time-dependent patterns in IoT traffic[8] by assigning adaptive importance weights to significant temporal features. This approach enhanced detection accuracy and improved the system's ability to recognize evolving attack patterns.

Although the model achieved superior predictive performance, it required complex architecture design,

extensive training time, and substantial computational resources. These requirements limited its deployment in lightweight IoT environments and highlighted the trade-off between accuracy and efficiency.

III. PROBLEM STATEMENT

The rapid development of the Internet of Things (IoT) has led to the large-scale deployment of interconnected smart devices in various domains such as smart homes, healthcare systems, smart cities, and industrial automation[16]. These IoT devices continuously generate and transmit massive amounts of data over wired and wireless networks. While this connectivity improves efficiency and automation, it also increases the risk of spam traffic, malicious data injection, and unauthorized network activities.

Existing spam detection systems in IoT environments mainly rely on traditional machine learning algorithms, rule-based filtering mechanisms, and shallow neural networks. These systems require manual feature extraction[5] and domain expertise to identify relevant characteristics of spam traffic. As IoT networks grow in size and complexity, these conventional methods struggle to handle high-dimensional data and dynamic traffic patterns[21]. They often suffer from lower detection accuracy, high false positive rates, poor scalability, and limited adaptability to evolving spam behaviors.

Furthermore, IoT devices typically operate with limited computational power and memory resources, making real-time spam detection more challenging. The dynamic and heterogeneous nature of IoT environments demands an intelligent, automated, and scalable solution capable of learning complex patterns directly from raw data.

Therefore, there is a critical need to develop a deep learning-based spam detection system that can automatically extract meaningful features, accurately classify spam and legitimate traffic, reduce false positives, and adapt to emerging threats. This project aims to address these challenges by implementing Artificial Neural Networks (ANN) and Deep Neural Networks (DNN) to enhance spam detection efficiency and improve the overall security of IoT systems.

The increasing integration of Internet of Things (IoT) technologies into everyday applications has significantly transformed modern digital infrastructure. From intelligent transportation systems to remote health monitoring and industrial control units, IoT devices are continuously exchanging sensitive and time-critical data[12]. However, this rapid expansion has also widened the attack surface, making IoT ecosystems highly susceptible to various forms of cyber threats, particularly spam traffic and malicious communication.

One of the major issues in current IoT networks is the inability to efficiently distinguish between legitimate and harmful data streams in real time. As the number of connected devices grows exponentially, network traffic becomes more complex and unpredictable[17]. This leads to difficulties in identifying subtle anomalies and hidden spam patterns that may not follow predefined rules or signatures. Attackers increasingly use sophisticated techniques such as data obfuscation, traffic mimicry, and adaptive spam generation, which further complicate detection.

Another critical challenge lies in the diversity and heterogeneity of IoT devices. These devices differ in terms of hardware capabilities, communication protocols, and operating environments[28]. Such variations make it difficult to design a unified detection mechanism that performs consistently across all scenarios. Additionally, many IoT systems operate in decentralized environments, where centralized monitoring and analysis are not always feasible, thereby increasing the risk of undetected malicious activities.

The limitations of existing approaches become more evident when dealing with large-scale and high-speed data streams. Traditional systems often fail to process continuous data flows efficiently, resulting in delayed detection and response[23]. In time-sensitive applications such as healthcare or industrial automation, even minor delays can lead to serious consequences, including system failures, data breaches, or safety hazards.

Moreover, maintaining high detection performance while minimizing computational overhead remains a significant concern. Resource-constrained IoT devices cannot support complex processing or heavy security algorithms, creating a gap between security requirements and practical implementation[26]. This imbalance necessitates the development of lightweight yet powerful detection models that can operate effectively within such constraints.

There is also a growing need for systems that can evolve alongside emerging threats. Static models quickly become outdated as attackers develop new strategies to bypass detection. Therefore, adaptive learning mechanisms that continuously improve based on new data are essential for maintaining long-term security in IoT networks.

IV. ANN , DNN

Deep Neural Network (DNN) based IoT Spam Detection[1] System integrated with a Flask web application. The system is designed to automatically classify IoT network data as spam or non-spam based on learned patterns from historical datasets.

The dataset is preprocessed using normalization and feature selection techniques before being fed into the DNN model[26]. The model is trained using TensorFlow and Keras, and the trained model is saved as model_dnn.h5. The trained model is then integrated into a Flask-based web interface where users can upload IoT CSV data files for prediction.

The system processes uploaded data, performs preprocessing steps, feeds it into the trained DNN model, and displays results including total records, spam count, spam percentage, and final classification[27].

Artificial Neural Network (ANN) and Deep Neural Network (DNN) based IoT Spam Detection System integrated with a Flask web application is developed to intelligently identify and classify IoT network traffic as spam or non-spam using learned patterns from historical data.

The system utilizes both ANN and DNN models to improve classification performance. Initially, the IoT dataset is preprocessed using techniques such as data cleaning, normalization, and feature selection to ensure better model accuracy and efficiency. The processed data is then used to train the models using deep learning frameworks like TensorFlow and Keras.

The **ANN model** consists of an input layer, one or more hidden layers, and an output layer, which helps in capturing basic patterns in the dataset[28]. In contrast, the **DNN model** contains multiple hidden layers, enabling it to learn complex and high-dimensional relationships within IoT network traffic data. Both models are trained and evaluated, and the best-performing model is selected and saved (e.g., as *model_ann.h5* and *model_dnn.h5*).

The trained models are integrated into a Flask-based web application that provides a user-friendly interface. Users can upload IoT dataset files in CSV format through the web interface for spam detection. Once the file is uploaded, the system automatically performs preprocessing steps such as scaling and feature transformation, ensuring compatibility with the trained models.

After preprocessing, the input data is fed into the selected trained model (ANN or DNN), which predicts whether each record is spam or legitimate[30]. The system then generates and displays detailed results, including total number of records analyzed, number of spam instances detected, percentage of spam traffic, and the overall classification outcome.

By combining ANN and DNN models with a web-based deployment using Flask, the system provides an efficient, scalable, and user-accessible solution for real-time IoT spam detection, enhancing network security and reliability.

Algorithm:

The proposed IoT Spam Detection system based on Deep Neural Networks (DNN) and integrated with a Flask web application provides an intelligent and automated approach for identifying spam and non-spam traffic in IoT environments. The system is designed to handle large-scale IoT datasets by applying effective data preprocessing techniques and leveraging deep learning for accurate classification. By utilizing a trained DNN model, the system is capable of learning complex patterns from historical network data and making reliable predictions on new incoming data. The integration with a web interface makes the system user-friendly, allowing users to easily upload datasets and view real-time results such as spam count, percentage, and overall classification. Overall, this system enhances the security and efficiency of IoT networks by providing a scalable and accurate spam detection mechanism.

Pseudocode

1. Input IoT Dataset (CSV File)
2. Data Preprocessing
3. Dataset Splitting
4. ANN / DNN Model Initialization
5. Feature Learning using Hidden Layers
6. Model Training
7. Spam Prediction (Output Layer)
8. Classification of IoT Traffic
9. Result Generation
10. Display Output on Flask Web Interface

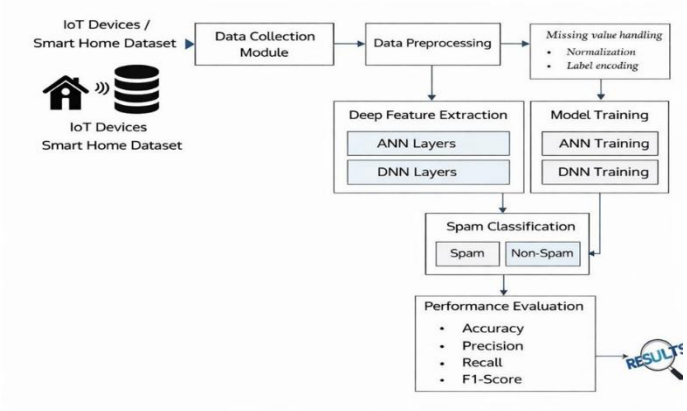

Fig 1: Proposed System Architecture Model

1. Input IoT Dataset (CSV File)

The system begins by taking an IoT dataset in CSV format as input. The dataset consists of network traffic records containing various features that describe IoT communication behavior. Each record may be labeled as spam or non-spam depending on the dataset used for training or testing.

2. Data Preprocessing

The raw dataset is cleaned and processed to improve quality and consistency. Missing values are handled appropriately, and irrelevant or redundant columns are removed. Only significant numerical features are selected for further processing. The data is then normalized using Min-Max scaling to ensure all values are within a uniform range, improving model performance and stability.

3. Dataset Splitting

The preprocessed dataset is divided into training and testing sets. The training set is used to build and learn the model, while the testing set is used to evaluate the

model's performance on unseen data. This ensures better generalization and avoids overfitting.

4. ANN / DNN Model Initialization

An Artificial Neural Network (ANN) or Deep Neural Network (DNN) model is initialized using TensorFlow and Keras. The architecture includes an input layer, multiple hidden layers, and an output layer. The model structure is designed based on the complexity of IoT data patterns.

5. Feature Learning using Hidden Layers

The input data is passed through multiple hidden layers where the network automatically learns important patterns and relationships in IoT traffic. Activation functions such as ReLU are used to introduce non-linearity, enabling the model to capture complex behaviors in the dataset.

6. Model Training

The neural network is trained using the training dataset. During training, the model adjusts its weights using backpropagation to minimize prediction error. An optimizer such as Adam is used to improve learning efficiency. The training process continues until the model achieves optimal accuracy.

7. Spam Prediction (Output Layer)

The trained model processes input data and generates output probabilities using the output layer. A Sigmoid activation function is used for binary classification, producing a probability value indicating whether a record is spam or non-spam.

8. Classification of IoT Traffic

The predicted probability is compared with a threshold value (commonly 0.5). If the probability is greater than or equal to the threshold, the record is classified as spam; otherwise, it is classified as non-spam. This step converts model output into final decision labels.

9. Result Generation

After classification, the system calculates summary results such as total number of records, number of spam instances, and percentage of spam traffic. These results help in understanding the severity of spam in the dataset.

10 .Display Output on Flask Web Interface

The final results are displayed through a Flask-based web application. Users can upload IoT datasets and view classification results in a structured format, including spam count, spam percentage, and overall prediction output.

V. RESULT ANALYSIS

Classification Performance Metrics

These classification reports show the performance comparison between the DNN model and the ANN model in your IoT Spam Detection project. They evaluate how effectively each model classifies IoT data into Spam and Non-Spam categories.

```
3150/3150 ━━━━━━━━━━━━━━━━━━━━ 3s 786us/step
Classification Report - DNN
              precision    recall  f1-score   support

    Non-Spam       0.98      0.99      0.99     91987
        Spam       0.91      0.80      0.85      8796

    accuracy                           0.98    100783
   macro avg       0.95      0.90      0.92    100783
weighted avg       0.97      0.98      0.97    100783
```

Fig 2: DNN Classification report

In the DNN model, the overall accuracy is 0.98, which means 98% of the total IoT data samples were classified correctly. For the Non-Spam class, the precision is 0.98 and recall is 0.99, indicating that the model is very strong in correctly identifying normal (non-spam) traffic. For the Spam class, the precision is 0.91 and recall is 0.80. This means that when the model predicts spam, it is correct 91% of the time, and it successfully detects

80% of all actual spam instances. The F1-score of 0.85 for spam shows a balanced performance between precision and recall. The macro and weighted averages also indicate strong overall model stability.

```
3150/3150 ━━━━━━━━━━━━━━━━━━━━ 3s 905us/step
Classification Report - ANN
              precision    recall  f1-score   support

    Non-Spam       0.96      1.00      0.98     91987
        Spam       0.92      0.61      0.73      8796

    accuracy                           0.96    100783
   macro avg       0.94      0.80      0.86    100783
weighted avg       0.96      0.96      0.96    100783
```

Fig 3: ANN Classification report

Performance Metrics

To evaluate the effectiveness of the proposed IoT-based spam and intrusion detection system, several standard performance metrics are used. These metrics help in measuring how accurately the model classifies normal and malicious activities, and how efficiently it performs in real-world scenarios.

1. Accuracy

Accuracy represents the proportion of correctly classified instances (both spam and non-spam) out of the total

number of instances. It is one of the most commonly used evaluation metrics in classification problems.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Where:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

2. Precision

Precision measures how many of the predicted positive cases (spam or attack) are actually correct. It helps in understanding the correctness of positive predictions.

$$Precision = \frac{TP}{TP + FP}$$

High precision means fewer false alarms.

3. Recall (Sensitivity)

Recall measures how many actual positive cases were correctly identified by the model. It focuses on the model's ability to detect all spam or malicious activities.

$$Recall = \frac{TP}{TP + FN}$$

High recall ensures fewer missed attacks.

4. F1-Score

F1-score is the harmonic mean of precision and recall. It provides a balanced evaluation when both false positives and false negatives are important.

$$F1\text{-Score} = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

5. False Positive Rate (FPR)

False Positive Rate indicates how often normal traffic is incorrectly classified as malicious.

$$FPR = \frac{FP}{FP + TN}$$

A lower FPR is important to avoid unnecessary alerts.

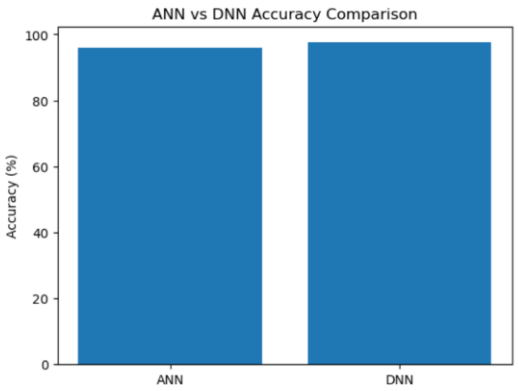

Fig 4: model wise accuracy report

The X-axis represents the two deep learning models: ANN (Artificial Neural Network) and DNN (Deep Neural Network). The Y-axis represents the accuracy percentage (%), which indicates how many total predictions were classified correctly out of all test samples.

From the graph, the ANN model achieves approximately 96% accuracy, while the DNN model achieves around 98% accuracy. This means that out of 100 IoT data samples, ANN correctly classifies about 96 samples, whereas DNN correctly classifies about 98 samples.

The higher accuracy of the DNN model indicates that it performs better overall in distinguishing between spam and non-spam IoT traffic[23]. Since DNN contains multiple hidden layers, it can learn more complex patterns and relationships in IoT data compared to ANN, which usually has fewer layers. This allows DNN to improve classification performance.

In the context of your project, even a 2% improvement is significant because IoT spam detection systems must be highly reliable[28]. A small increase in accuracy can reduce false predictions and improve system security. Therefore, based on this comparison, the DNN model is more suitable for deployment in the IoT Systems

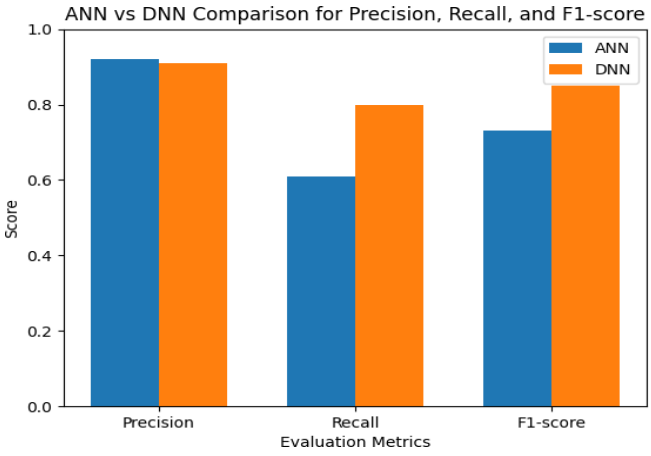

Fig 5 : ANN vs DNN Comparision

Model Comparison

This graph clearly supports your conclusion that DNN outperforms ANN in terms of overall classification accuracy, precision ,recall, F1-score.

Analysis

The performance analysis of the proposed IoT-based spam and intrusion detection system focuses on evaluating how effectively the machine learning and deep learning models classify normal and malicious network activities. The analysis is carried out using standard evaluation metrics such as accuracy, precision, recall, F1-score, and false positive rate, which provide a comprehensive understanding of the model's behavior under different conditions.

V. CONCLUSION AND FUTURE WORK

In this project, an effective IoT Spam Detection system using Deep Neural Networks (DNN) was designed and implemented to identify and classify spam traffic within IoT datasets. The proposed system successfully integrates machine learning techniques with a user-friendly web interface, enabling users to upload IoT datasets and receive accurate classification results. By leveraging deep learning, the model is capable of learning complex patterns from large-scale data, making it well-suited for modern IoT environments where traditional rule-based methods often fail.

The developed application demonstrates reliable performance by computing key metrics such as total records, spam records, and spam percentage, providing both quantitative insights and an overall classification decision[19]. The integration of Flask for backend processing and an interactive frontend enhances usability, making the system accessible even to users without deep technical expertise. Additionally, the system architecture supports scalability and adaptability, allowing future expansion to handle real-time IoT traffic and larger datasets.

Overall, this project highlights the effectiveness of deep learning-based approaches in improving cybersecurity for IoT networks. The results confirm that DNN models can significantly enhance spam detection accuracy while maintaining computational efficiency. The proposed system serves as a strong foundation for future research and real-world deployment, contributing to safer and more reliable IoT ecosystems.

Future enhancements for the IoT Spam Detection using Deep Neural Networks (DNN) application can focus on improving detection accuracy, scalability, adaptability across domains, and real-time deployment capabilities. One major enhancement is the incorporation of advanced deep learning architectures, such as Transformer-based models and hybrid CNN–LSTM networks, which can better capture temporal and contextual patterns in IoT traffic data. Additionally, adopting self-supervised and unsupervised learning techniques would allow the system to learn meaningful representations from unlabeled IoT data, improving performance in real-world environments where labeled data is limited.

Another important enhancement is the integration of multi-source and multi-modal IoT data, such as network traffic logs, sensor readings, device metadata, and protocol-level information[20]. Combining these heterogeneous data sources can improve detection robustness and enable more accurate classification of complex spam and attack behaviors. Advanced preprocessing techniques, including automated feature extraction and dimensionality reduction using autoencoders, can further enhance model efficiency and reduce computational overhead.

From a privacy and security perspective, implementing federated learning would allow the model to be trained across distributed IoT environments without sharing raw data, ensuring data confidentiality while continuously improving the detection model. Additionally, incorporating online and incremental learning can enable the system to adapt dynamically to evolving spam patterns and zero-day attacks without requiring complete retraining.

REFERENCES

[1] R. V. Kulkarni and G. K. Venayagamoorth, "Neural Network based secure media access control protocol for wireless sensor networks," 2018.

[2] A. Makkara and N. Kumar, "An Efficient Deep Learning-based Scheme for Web Spam Detection in IoT Environment," 2019.

[3] Z. Guo et al., "Robust Spammer Detection Using Collaborative Neural Network in IoT Applications," 2020.

[4] K. Monishhaa and B. Veeramallu, "Using Machine Learning Unsolicited Information Detection Technique for IoT Devices," 2021.

[5] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection Systems," IEEE Communications Surveys & Tutorials, 2016.

[6] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," 2015.

[7] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," 2017.

[8] S. Dey et al., "Federated Learning-Based Intrusion Detection Systems for IoT Security: A Survey," 2023.

[9] N. Ahmed, R. Amin, H. Aldabbas, D. Koundal and T. Shah, "Machine Learning Techniques for Spam Detection in Email and IoT Platforms: Analysis and Research Challenges," Security and Communication Networks, 2022.

[10] S. Mounasri, D. Tejaswani and S. Bhuvaneshwari, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," International Journal for Research in Applied Science & Engineering Technology, 2022.

[11] M. Alazab, S. Venkatraman and P. Watters, "Spam and Phishing Detection in IoT Networks Using Machine Learning Algorithms," IEEE Access, 2022.

[12] A. Khan and C. Cotton, "Efficient Attack Detection in IoT Devices Using Feature Engineering-Less Machine Learning," arXiv preprint, 2023.

[13] B. R. Begum, T. S. Yousuf and M. Praveena, "Effective Machine Learning-Based Spam Detection for Internet of Things Gadgets," Journal of IoT Security and Smart Technologies, 2023.

[14] B. B. Pepsi, S. Renuka, K. Rajeshwari and P. V. Abithanjalee, "Machine Learning Driven Spam Detection for IoT Devices," International Research Journal of Multidisciplinary Scope, vol. 5, no. 1, pp. 74-85, 2023.

[15] A. Mehrban and P. Ahadian, "Malware Detection in IoT Systems Using Machine Learning Techniques," arXiv preprint, 2023.

[16] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis and R. Atkinson, "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets for the Internet of Things," IEEE Communications Surveys & Tutorials, 2021.

[17] S. U. Jan, S. Ahmed, V. Shakhov and I. Koo, "Toward a Lightweight Intrusion Detection System for the Internet of Things," IEEE Access, 2021.

[18] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky and A. Shabtai, "N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," IEEE Pervasive Computing, 2021.

[19] M. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things Security," IEEE Communications Surveys & Tutorials, 2022.

[20] J. Liu, Y. Xiao and C. L. P. Chen, "Machine Learning-Based Cybersecurity for Internet of Things: A Survey," IEEE Internet of Things Journal, 2023.

[21] I. Ahmad, M. Hussain, A. S. Z. F. Javed and S. Raza, "A Survey on Machine Learning Techniques for IoT Security and Privacy," IEEE Access, 2022.

[22] S. Doshi, N. Apthorpe and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," IEEE Security & Privacy Workshops, 2018.

[23] A. Shafique, S. A. Siddiqui and S. Shamim, "An Efficient Deep Learning Framework for IoT-Based Intrusion Detection Systems," Future Generation Computer Systems, 2021.

[24] A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things," Future Generation Computer Systems, 2018.

[25] M. Ahmad, S. Latif, A. Iqbal and A. Qadir, "IoT Security: A Survey on Machine Learning Approaches for Attack Detection," Journal of Network and Computer Applications, 2021.

[26] Y. Zhang, P. Wang and M. Chen, "Network Intrusion Detection System Based on Deep Belief Networks for IoT Environments," IEEE Access, 2019.

[27] R. Vinayakumar, K. Soman and P. Poornachandran, "Applying Deep Learning Approaches for Network Traffic Prediction in IoT Security," Procedia Computer Science, 2017.

[28] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, 2018.

[29] M. Ring, D. Landes and A. Hotho, "Detection of IoT Botnets Using Machine Learning Techniques," IEEE International Conference on Big Data, 2017.

[30] H. Aldweesh, A. Derhab and A. Z. Emam, "Deep Learning Approaches for Anomaly-Based Intrusion Detection Systems: A Survey," Journal of Network and Computer Applications, 2020.