International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 9, September 2025)

AI-based Technique for Prediction-Model of Spam-detection in IoT Device: A Review

[1]Rajni Soni, [2]Akhilesh A. Waoo*
[1,2]Department of CSE, AKS University, Satna, MP, India
*akhileshwaoo@gmail.com

Abstract— **This review presents an overview of AI-based techniques for the prediction and detection of spam in IoT devices, highlighting recent advancements and methodologies in the field. With the rapid growth of IoT networks, devices are increasingly vulnerable to unsolicited messages and malicious spam, which can compromise system performance, security, and user privacy. Artificial Intelligence (AI) approaches, including machine learning and deep learning models, have shown significant potential in accurately identifying and filtering spam by analyzing patterns in device communication, network traffic, and user behavior. This review discusses various AI algorithms, their effectiveness, challenges in implementation, and comparative performance in IoT environments. The study emphasizes the importance of adaptive and scalable AI solutions capable of handling the heterogeneous and dynamic nature of IoT networks. Overall, the review provides insights into the current state of AI-driven spam detection, identifies gaps in existing research, and suggests future directions for enhancing the reliability and security of IoT devices through intelligent predictive models.**

Keywords*— *Smart home, Spam, IOT, Security, AI.

I. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most transformative technologies in recent years, connecting a vast array of devices—including sensors, smart appliances, wearable gadgets, and industrial machinery—through networked infrastructures [1]. This connectivity enables seamless data exchange, automation, and intelligent decision-making across various domains such as healthcare, smart cities, industrial automation, and home automation. However, the rapid expansion of IoT networks also introduces significant security and privacy challenges, as these devices often operate with minimal computational resources and limited security mechanisms. One of the most prevalent threats in IoT environments is spam, which can manifest as unsolicited messages, phishing attempts, malware, or malicious command injections targeted at devices and users. Spam not only affects the performance and reliability of IoT systems but can also compromise sensitive data and lead to network congestion, ultimately reducing the efficiency of connected devices [2].

Traditional approaches to spam detection, such as rule-based filtering or signature-based methods, are often insufficient in IoT contexts due to the dynamic, heterogeneous, and resource-constrained nature of these networks. Rule-based systems require constant updates and cannot easily adapt to new spam patterns, while signature-based techniques are limited to known attack vectors and fail to detect novel or evolving threats[3]. These limitations have motivated the development of prediction models that leverage advanced computational techniques to detect spam proactively. Prediction models use historical and real-time data from IoT devices to identify patterns and anomalies indicative of spam activity. By analyzing features such as network traffic, device behavior, message content, and temporal patterns, these models can classify incoming messages or events as legitimate or malicious, enabling timely intervention and prevention[4].

In recent years, Artificial Intelligence (AI)-based techniques have emerged as a powerful solution for spam detection in IoT devices. Machine learning algorithms—

including Support Vector Machines (SVM), Decision Trees, Random Forests, and K-Nearest Neighbors (KNN)—have been employed to create predictive models capable of learning from historical data and adapting to changing spam behaviors [5]. More advanced deep learning approaches, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, can automatically extract complex features from IoT traffic and message content, achieving higher detection accuracy even in large-scale and high-dimensional datasets. AI-based prediction models can also incorporate ensemble learning and hybrid methods to further improve detection performance, reduce false positives, and enhance system robustness [6].

The implementation of prediction models in IoT devices, however, is not without challenges. Resource constraints—such as limited processing power, memory, and energy—pose restrictions on the complexity of AI models that can be deployed on edge devices[7]. Additionally, IoT networks are highly heterogeneous, involving diverse communication protocols, device types, and operating environments, which complicates the development of universally applicable detection models. Data privacy is another critical concern, as prediction models often require access to sensitive device and user data to function effectively[8]. Addressing these challenges requires designing lightweight, adaptive, and distributed AI models capable of operating efficiently at the edge, while ensuring secure data handling and maintaining detection accuracy.

The significance of effective spam detection in IoT environments extends beyond security. By preventing unsolicited messages and malicious activity, prediction models help maintain the operational efficiency, reliability, and longevity of IoT systems. They also enhance user trust in connected devices, which is critical for widespread adoption and integration of IoT technology in everyday life[9]. As IoT networks continue to grow in scale and complexity, the development of intelligent, adaptive, and high-performance spam detection models becomes increasingly important to safeguard device ecosystems and ensure uninterrupted service delivery[10].

The prediction-model approach for spam detection in IoT devices represents a crucial area of research that combines AI, data analytics, and cybersecurity. By leveraging machine learning and deep learning techniques, these models offer proactive and adaptive solutions capable of addressing evolving spam threats in dynamic IoT environments. The ongoing research focuses on optimizing model accuracy, efficiency, and scalability while overcoming resource and privacy challenges, making AI-based spam detection a cornerstone for the secure and reliable functioning of modern IoT systems.

II. LITERATURE SURVEY

T. Perumal et al. [1] proposed an IoT-centric framework for multiactivity recognition in smart home environments. The system leverages IoT sensors to monitor and interpret various resident activities. Data collected from devices is processed to identify patterns and context-aware behaviors. Machine learning algorithms were applied to enhance accuracy in activity recognition. The study emphasizes real-time monitoring and automation for smart homes. Results demonstrated improved reliability and adaptability of IoT systems in residential settings.

Ashwini A. Waoo et al. [2] Artificial Intelligence (AI) involves computer science in agriculture and resulted in an agricultural revolution. This type of technology has played a major role in the security of crop yield from various factors like climate changes, growth of population, issues in employment, and the security of food. The main concern of this chapter is to compile the various applications of Artificial intelligence in agriculture as irrigation, weeding, spraying with sensors, and other means embedded in robots and drones.

A. Makkar et al. [3] present a fuzzy-based approach to strengthen cyber defense in next-generation IoT networks. The methodology uses fuzzy logic to handle uncertainties in IoT device behavior and communication. Security threats are detected by evaluating anomalies in real-time data streams. The approach aims to improve network resilience while minimizing false positives. Simulation results indicate robust performance in diverse IoT scenarios. The study highlights the importance of adaptive security mechanisms for complex IoT environments.

Brijesh K. Soni et al. [4] exploring technology and science, in the same scenarios, we are also trying to explore a popular technology named “Deep-Learning”, which is a giant technology in the software industry around the world. Here in this chapter, we start with the basic concept of deep learning including the framework and library frequently used to develop such types of applications. Further, in the middle part various deep learning models were discussed with a practical approach using the MNIST dataset. These models are used for solving various complex problems in the domain of computer vision and natural language processing.

Al-Thelaya et al. [5] focused on spam detection in social networks using graph-based feature analysis. The model examines sequences of user interactions to identify suspicious messaging patterns. Machine learning techniques are applied to classify normal versus spam activity. The study highlights the effectiveness of structural and temporal features in detection. Results indicate high accuracy and low false-positive rates. The methodology can be adapted for IoT communication networks for proactive spam prevention.

S. Nigam et al. [6] AI-powered bots are designed to assist workers with disabilities in various work environments. It explores adaptive interfaces and supportive features that enable these bots to meet the diverse needs of individuals facing visual, auditory, motor, and cognitive challenges. By synthesizing existing research, this review emphasizes the possibility of AI to explore workplace inclusivity, assesses the effectiveness of different assistive technologies, and identifies critical gaps in current studies. Furthermore, the paper highlights emerging trends in AI-driven accessibility tools and provides recommendations for future research and development initiatives.

Zhang et al. [7] investigated evasion attacks using Wasserstein Generative Adversarial Networks (WGANs). The study focused on generating adversarial examples to bypass machine learning-based security systems. WGANs were used to craft realistic perturbations in network data. The proposed method highlights vulnerabilities in AI-driven IoT security frameworks. Experiments demonstrated the potential for evasion even in robust detection systems. This research underscores the need for resilient AI models against adversarial threats in IoT networks.

A. Makkar et al. [8] proposed a cognitive IoT-based scheme for web spam detection using AI techniques. The approach leverages machine learning to analyze traffic patterns and identify malicious content. The model emphasizes adaptability to dynamic IoT environments. Performance evaluation showed high detection accuracy and reduced false positives. The study highlights the role of cognitive computing in securing IoT systems. It provides insights into integrating AI for proactive spam management.

A. K. Singh et al. [9] introduced a fuzzy C-means algorithm for filtering spam messages and emails. The model clusters messages based on similarity and relevance to detect spam. Fuzzy logic allows the handling of ambiguous or partially matching data. Experiments confirmed improved detection efficiency compared to traditional methods. The approach is suitable for IoT applications where real-time message filtering is required. This research emphasizes the importance of intelligent clustering for spam mitigation.

A. A. Waoo et al., [10] Wireless sensor networks are one of the attractive and emerging research domains, with tremendous applications in various aspects like health care monitoring, area monitoring, environmental/ earth real time sensing and monitoring of industries, etc. A WSN are capable of sensing and detecting different minute changes in events by means miniature sensor nodes dispersed over that network area. Each sensor node has the sensor for detection, controller, storage memory, A/D converter, battery and transceiver. Sensing, processing and communication are three main operation of a sensor node.

T. Qiu et al. [11] proposed SIGMM, a machine learning algorithm for identifying spammers in industrial mobile cloud computing environments. The model analyzes behavioral patterns and communication features of users. It emphasizes real-time detection and high accuracy in industrial IoT setups. Experimental results demonstrated effective spammer identification and low false positive rates. The approach combines data-driven learning with domain-specific optimization. It contributes to secure and reliable cloud-based IoT communications.

G. Kumar and V. Rishiwal et al. [12] performed a statistical analysis of Twitter data using a language model with Kullback-Leibler Divergence (KLD). The study focused on detecting anomalous patterns and spam content on social media. KLD was applied to measure differences between expected and observed message distributions. The method supports real-time monitoring of large-scale IoT social interactions. Results indicated effective spam detection and improved data filtering. This research highlights the importance of statistical modeling in securing IoT-enabled communication platforms.

III. CHALLENGES

Challenges in AI-Based Spam Detection for IoT Devices

Despite significant advancements in AI-driven spam detection for IoT devices, several challenges remain that impact the effectiveness, scalability, and practicality of these solutions.

1. Resource Constraints: IoT devices often have limited computational power, memory, and energy capacity. Deploying complex AI or deep learning models directly on these devices can be impractical, necessitating lightweight or edge-computing solutions.

2. Heterogeneity of IoT Networks: IoT ecosystems comprise a wide variety of devices, protocols, and communication standards. Designing a universal spam detection model that can operate effectively across diverse device types and network configurations is challenging.

3. Dynamic and Evolving Threats: Spam and malicious activities continuously evolve, making static detection approaches ineffective. AI models must adapt to new patterns and unknown attack vectors in real time, which requires continuous learning and model updating.

4. Data Privacy and Security: AI models rely on data from IoT devices for training and prediction. Collecting and analyzing sensitive user data raises privacy concerns, and ensuring secure data handling while maintaining detection accuracy is a significant challenge.

5. High False Positives and Negatives: Achieving an optimal balance between precision and recall is difficult. Excessive false positives can block legitimate messages or actions, while false negatives may allow spam or attacks to pass undetected.

6. Scalability and Real-Time Processing: Large-scale IoT deployments generate massive data streams, demanding models that can process data in real time without introducing latency. Maintaining high performance at scale remains a technical challenge.

7. Integration with Existing Infrastructure: AI-based spam detection systems must integrate seamlessly with existing IoT networks, communication protocols, and cybersecurity frameworks. Compatibility and interoperability issues can complicate deployment.

8. Explainability and Trust: Many AI models, especially deep learning-based ones, operate as black boxes, making it hard for users and administrators to understand or trust their decisions. Ensuring model transparency and interpretability is critical for adoption.

Addressing these challenges requires a combination of lightweight AI models, adaptive learning strategies, secure data handling, and scalable architectures that can operate efficiently in dynamic IoT environments.

IV. CONCLUSION

AI-based spam detection in IoT devices has emerged as a crucial solution to secure increasingly connected and dynamic networks. The reviewed studies demonstrate that machine learning, deep learning, and hybrid approaches can effectively identify spam, malicious messages, and anomalous behaviors, significantly improving detection accuracy and system reliability. However, challenges such as resource constraints, heterogeneous device environments, evolving threats, privacy concerns, and the need for real-time processing remain critical barriers. Despite these limitations, AI-driven prediction models provide adaptive, scalable, and intelligent mechanisms that enhance the resilience of IoT ecosystems. Overall, integrating AI-based spam detection into IoT networks ensures robust security, protects sensitive data, and supports the efficient operation of connected devices, paving the way for safer and more reliable IoT infrastructures.

REFERENCES

1. T. Perumal, E. Ramanujam, S. Suman, A. Sharma, and H. Singhal, "Internet of Things Centric-Based Multiactivity Recognition in Smart Home Environment," in IEEE Internet of Things Journal, vol. 10, no. 2, pp. 1724-1732, 15 Jan.15, 2023, doi: 10.1109/JIOT.2022.3209970.
2. Ashwini A. Waoo; Jyoti Pandey; Akhilesh A. Waoo, "Artificial Intelligence in Agricultural Engineering," in Innovative Engineering with AI Applications , Wiley, 2023, pp.83-99, doi: 10.1002/9781119792161.ch5.
3. A. Makkar, U. Ghosh, P. K. Sharma, and A. Javed, "A Fuzzy-based approach to Enhance Cyber Defence Security for Next-generation IoT," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3053326.
4. Brijesh K. Soni; Akhilesh A. Waoo, "Deep Learning," in Innovative Engineering with AI Applications , Wiley, 2023, pp.41-64, doi: 10.1002/9781119792161.ch3.
5. K. A. Al-Thelaya, T. S. Al-Nethary and E. Y. Ramadan, "Social Networks Spam Detection Using Graph-Based Features Analysis and Sequence of Interactions Between Users," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 206-211, doi: 10.1109/ICIoT48696.2020.9089509.
6. S. Nigam and A. A. Waoo, "Advance Collaborative AI-Driven Bots Using RPA to Enhance Workplace Inclusivity for Employees with Disabilities in India," *2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT)*, Bhopal, India, 2025, pp. 610-617, doi: 10.1109/CSNT64827.2025.10968725.
7. J. Zhang, Q. Yan and M. Wang, "Evasion Attacks Based on Wasserstein Generative Adversarial Network," 2019 Computing, Communications and IoT Applications (ComComAp), 2019, pp. 454-459, doi: 10.1109/ComComAp46287.2019.9018647.
8. A. Makkar, N. Kumar and M. Guizani, "The Power of AI in IoT: Cognitive IoT-based Scheme for Web Spam Detection," 2019 IEEE Symposium Series on Computational Intelligence (SSCI), 2019, pp. 3132-3138, doi: 10.1109/SSCI44817.2019.9002885.
9. A. K. Singh, S. Bhushan and S. Vij, "Filtering spam messages and mails using fuzzy C means algorithm," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1-5, doi: 10.1109/IoT-SIU.2019.8777483.
10. A. A. Waoo and S. Sharma, "Analysis of Energy Efficient Coverage and Prolonging Lifetime by Comparing Homogenous and Heterogeneous Wireless Sensor Networks," 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), Bhopal, India, 2018, pp. 1-4, doi: 10.1109/ICACAT.2018.8933686.
11. T. Qiu, H. Wang, K. Li, H. Ning, A. K. Sangaiah, and B. Chen, "SIGMM: A Novel Machine Learning Algorithm for Spammer Identification in Industrial Mobile Cloud Computing," in IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2349-2359, April 2019, doi: 10.1109/TII.2018.2799907.
12. G. Kumar and V. Rishiwal, "Statistical Analysis of Twitter Data Using Language Model With KLD," 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1-6, doi: 10.1109/IoT-SIU.2018.8519938.