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

Review of Spam Detection using AI Techniques for Smart Home Device Environment

Parikkshit Malviya[1], Arun Jhapate[2]

[1] Research Scholar, Department of CSE, SIRT College Bhopal

[2]Assistant Professor, Department of CSE, SIRT College Bhopal

Abstract— **This review explores the application of Artificial Intelligence (AI) techniques for predicting the academic success of college students, highlighting their growing role in higher education research and practice. AI-based models, including machine learning and deep learning approaches, have demonstrated significant potential in analyzing diverse academic, behavioral, demographic, and socio-economic factors that influence student performance. By leveraging large and complex datasets, these techniques enable early identification of at-risk students, support personalized learning strategies, and assist institutions in improving retention and overall outcomes. The paper synthesizes recent developments, discusses strengths and limitations of AI-driven prediction models, and outlines future directions for creating ethical, accurate, and student-centered solutions.**

Keywords*— *AI, Student, Academic, Success.

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has transformed modern living spaces into intelligent environments, where smart home devices such as voice assistants, connected cameras, smart refrigerators, thermostats, and security systems interact seamlessly to provide convenience, automation, and energy efficiency. While these devices significantly improve quality of life, they also introduce new avenues for cyber threats and malicious activities [1]. One of the major concerns in this context is the problem of spam, which extends beyond traditional email or messaging spam to include unsolicited commands, malicious network traffic, phishing attempts, and deceptive notifications targeted at smart home ecosystems. Spam detection in smart home device environments is therefore an emerging and critical research area, aiming to protect users from privacy breaches, financial loss, and device malfunction caused by unwanted or malicious communications[2].

Unlike conventional computing systems, smart home devices typically have limited computational power, memory, and battery capacity, which makes them more vulnerable to attacks and less capable of running complex security applications. Hackers and malicious actors exploit these limitations to inject spam traffic or commands, often disguising them as legitimate device communications[3]. For instance, a compromised IoT camera may receive spam instructions that manipulate its functionality, or a smart speaker may process unsolicited voice commands designed to steal sensitive information. Such attacks not only disrupt the operation of individual devices but also compromise the entire home network, as many devices share interconnected communication channels. Detecting spam in such resource-constrained and heterogeneous environments is therefore more challenging than in traditional systems[4].

The problem of spam in smart home environments is multifaceted. It can manifest as unsolicited advertisements, phishing content, denial-of-service traffic, or malware propagation disguised as normal device activity. The detection process requires distinguishing between legitimate commands (e.g., a user adjusting the thermostat) and malicious or irrelevant ones (e.g., unauthorized repeated commands to exhaust resources)[5]. Moreover, since smart home devices often rely on cloud services and wireless networks, spam traffic may enter through multiple gateways, making it essential to develop detection mechanisms that operate both locally on devices and across the broader network infrastructure. Failure to detect spam effectively can degrade system performance, cause device overload, compromise user trust, and even lead to physical security risks within the smart home[6].

Traditional spam detection methods, such as rule-based filters and keyword matching, are insufficient in this dynamic environment due to the evolving nature of spam and the diversity of device communication protocols. As a result, researchers are increasingly turning to advanced approaches such as machine learning, deep learning, and artificial intelligence-based models[7]. These techniques enable systems to analyze patterns in network traffic, user behavior, and device interactions to identify anomalies indicative of spam. For example, machine learning classifiers can be trained on labeled datasets to distinguish between normal and malicious commands, while deep learning architectures can capture complex temporal and spatial correlations in device communications. However, deploying these advanced models in real-world smart home devices requires lightweight designs that balance security accuracy with resource efficiency[8].

Another significant aspect of spam detection in smart home environments is the privacy and ethical consideration. Collecting and analyzing device communication data for spam detection purposes may expose sensitive information about user behavior, daily routines, or personal preferences. Therefore, privacy-preserving techniques, such as federated learning and edge-based detection mechanisms, are increasingly being explored[9]. These approaches allow models to learn from distributed data without transferring sensitive information to central servers, ensuring both security and privacy in smart homes. Additionally, the ethical design of spam detection mechanisms must prevent biases and avoid over-restriction of legitimate user activities, ensuring that the system remains transparent, reliable, and user-friendly[10].

The importance of robust spam detection in smart home device environments cannot be overstated. As the number of IoT-enabled devices continues to rise, the attack surface for spam-related threats expands proportionally, making users more vulnerable to cyber exploitation. Effective detection mechanisms will not only enhance the resilience of smart homes but also increase user confidence in adopting IoT technologies[11]. The future of this field lies in the integration of lightweight AI models, collaborative detection frameworks across devices, and adaptive security systems capable of evolving with emerging threats. By addressing these challenges, researchers and practitioners can build smarter, safer, and more trustworthy home environments that fully realize the promise of IoT technologies[12].

II. LITERATURE SURVEY

R. Agarwal et al., [1] proposed a novel spam detection approach using Natural Language Processing (NLP) with AMALS models, focusing on enhancing the accuracy of identifying spam content in digital communications. Their method leverages advanced NLP techniques to analyze text semantics and context rather than relying solely on traditional keyword-based filtering. The study showed significant improvements in precision and recall, demonstrating the ability to detect sophisticated spam messages that bypass older detection models. By integrating AMALS with NLP, the framework provided adaptive learning capabilities, enabling continuous performance improvement as spam patterns evolve. This contribution highlights the role of contextual language analysis in building resilient spam detection systems.

Y. Li et al., [2] investigated deep learning-enabled spam detection tailored for IoT-based smart environments, where devices generate heterogeneous data streams. Their framework employed convolutional and recurrent neural networks to capture temporal and structural patterns in IoT traffic for distinguishing spam from legitimate activity. The study addressed the resource limitations of IoT devices by optimizing model design for lightweight deployment without sacrificing accuracy. Results indicated that deep learning models significantly outperformed conventional machine learning methods in terms of detection rates and false-positive reduction. This work demonstrates the practical feasibility of deep learning for securing smart home and IoT ecosystems against spam-related threats.

A. Sharma et al., [3] focused on lightweight anomaly and spam detection for resource-constrained IoT devices, proposing an efficient detection mechanism suitable for environments with limited processing power and memory. Their approach combined statistical analysis with simplified machine learning models to ensure real-time spam identification without overwhelming the device resources. The study emphasized achieving a balance between model accuracy and computational cost, a critical factor in IoT security solutions. Experimental results showed that the proposed method could maintain high detection performance while consuming minimal energy and processing time. This work contributes to the growing demand for scalable and efficient security solutions in IoT-enabled smart homes.

S. Banerjee et al., [4] explored the use of federated learning for spam traffic detection in smart homes, aiming to address privacy concerns in centralized training approaches. Their system enabled multiple devices to collaboratively train detection models without sharing raw data, preserving user privacy while enhancing model generalization. The study showed that federated learning models achieved comparable accuracy to centralized systems while significantly reducing risks of data leakage. Moreover, the distributed learning approach improved adaptability to local device conditions and spam variations. This research highlights federated learning as a promising privacy-preserving strategy for spam detection in IoT environments.

P. Kumar et al., [5] developed a hybrid machine learning model for spam filtering in IoT networks, integrating both supervised and unsupervised techniques for improved accuracy. Their approach combined clustering methods with classification algorithms to handle the diverse and evolving nature of spam traffic in IoT ecosystems. The hybrid model demonstrated enhanced performance in detecting spam across multiple communication protocols, addressing the heterogeneity of IoT data sources. The study also emphasized the importance of adaptability, showing that the model could evolve with emerging spam strategies. This contribution underscores the effectiveness of hybrid approaches in strengthening IoT spam detection frameworks.

M. Alazab et al., [6] proposed a deep learning-based solution for detecting spam and phishing in IoT networks, addressing the growing risks of malicious traffic targeting connected devices. Their architecture utilized advanced neural networks to learn complex patterns in large-scale IoT data, achieving superior detection performance compared to traditional methods. The study emphasized the dual capability of the system in handling both spam and phishing threats, providing comprehensive protection for IoT environments. Experimental evaluations demonstrated high accuracy and robustness across diverse datasets, validating the effectiveness of deep learning in real-world scenarios. This work represents a significant step toward building intelligent and adaptive security systems for IoT-based smart homes.

H. Zhang et al., [7] presented an ensemble-based spam detection framework for cloud-assisted smart homes, combining multiple classifiers to improve accuracy and reliability. Their approach leveraged the scalability of cloud resources to handle large volumes of smart home data, ensuring real-time detection. By integrating decision trees, random forests, and boosting methods, the ensemble model reduced false positives compared to single classifiers. The results showed improved robustness against diverse spam traffic patterns, demonstrating the benefit of ensemble learning in complex IoT environments. This work highlighted how cloud integration can enhance the performance of spam detection models in smart homes.

J. Kim et al., [8] explored anomaly and spam traffic detection within home IoT networks, emphasizing lightweight methods suitable for device-level deployment. Their study combined traffic pattern analysis with machine learning algorithms to distinguish between normal and malicious/spam behaviors. The system was tested on real-world IoT device data, showing strong performance in detecting low-volume spam that often bypasses traditional filters. The researchers also highlighted challenges such as dynamic network conditions and limited device resources. This contribution underlined the importance of efficient and adaptable detection techniques for protecting IoT-enabled smart households.

R. A. Braga et al., [9] proposed a machine learning approach for spam filtering in IoT-based smart systems, targeting the unique traffic characteristics of connected devices. The model integrated supervised classification with feature engineering to capture device-specific patterns. Their framework achieved higher detection rates compared to baseline statistical methods, showing the effectiveness of machine learning for IoT spam control. Additionally, the study discussed scalability issues, proposing methods for reducing computational overhead. This work contributed to advancing machine learning applications in IoT environments where heterogeneity and dynamic spam strategies pose significant challenges.

A. K. Sahu et al., [10] developed a data mining-based spam detection system designed for heterogeneous IoT environments. Their method focused on extracting meaningful features from large, diverse datasets to train efficient classifiers capable of detecting spam across multiple device types. The research highlighted the challenges of integrating different communication protocols and data formats in IoT. Experimental analysis demonstrated that data mining techniques could handle these complexities, improving overall detection performance. This work emphasized the role of data-driven insights in creating adaptable spam detection solutions for diverse IoT ecosystems.

D. Choudhury et al., [11] introduced a rule-based spam filtering model specifically tailored for smart device communications. Their approach relied on predefined rules derived from traffic behavior and known spam signatures to classify malicious activity. While rule-based systems offer transparency and interpretability, the study acknowledged their limitations in adapting to evolving spam strategies. Nonetheless, the model performed effectively in controlled environments, providing a baseline for further integration with adaptive techniques. This research underscored the continued relevance of rule-based systems as part of hybrid spam detection architectures in IoT security.

C. D. Manning et al., [12] provided a comprehensive review of machine learning approaches for spam detection, highlighting advancements and challenges from a broader perspective. Their work discussed classification algorithms such as Naïve Bayes, Support Vector Machines, and neural networks, comparing their effectiveness across datasets. Importantly, they emphasized issues such as class imbalance, feature selection, and evolving spam tactics. The review also proposed future directions, including hybrid models and adaptive systems for emerging environments like IoT. This foundational study remains influential in guiding research on machine learning-based spam detection frameworks.

III. CHALLENGES

Spam detection in smart home device environments poses unique challenges compared to traditional computing and networking contexts. One of the foremost issues is the resource limitation of IoT devices, which typically have constrained processing power, memory, and battery life. Deploying complex machine learning or deep learning models on such devices is difficult without compromising system performance, leading to a trade-off between accuracy and efficiency.

Another significant challenge lies in the heterogeneity of IoT devices and communication protocols. Smart homes integrate a wide range of devices, from sensors and cameras to smart assistants, all communicating using diverse standards such as ZigBee, Z-Wave, Wi-Fi, and Bluetooth. This variety creates highly inconsistent data patterns, making it difficult to design universal spam detection models that generalize across all devices.

Data privacy and security concerns also complicate spam detection in smart homes. Collecting and centralizing device data for model training increases the risk of exposing sensitive user information. While privacy-preserving methods such as federated learning have been proposed, they introduce additional complexities like communication overhead and synchronization issues.

Another critical issue is the evolving nature of spam and malicious traffic. Attackers continuously adapt their strategies to bypass detection models, leading to concept drift in data. Static detection systems quickly become obsolete, highlighting the need for adaptive and continuously updating models. However, updating models in distributed smart home environments without disrupting functionality remains a technical hurdle.

The imbalance in spam versus normal traffic data further challenges the training of effective detection systems. Spam traffic typically forms a small fraction of overall IoT communication, leading to skewed datasets where standard machine learning models may favor the majority class. Addressing this imbalance requires specialized techniques such as oversampling, synthetic data generation, or cost-sensitive learning.

Interpretability and user trust present non-technical yet crucial challenges. Most advanced spam detection systems employ complex black-box models such as deep learning, which lack transparency. For smart home users, especially non-technical ones, understanding why a device blocks or flags certain communication is important for trust and adoption. Balancing detection accuracy with explainability is therefore a pressing concern.

IV. CONCLUSION

Spam detection in smart home device environments is an increasingly vital area of research, as the integration of IoT devices in everyday life exposes users to new forms of malicious and unsolicited traffic. While machine learning, deep learning, and hybrid approaches have shown promising results in enhancing detection accuracy, challenges such as device resource constraints, data heterogeneity, evolving spam strategies, privacy concerns, and the need for model interpretability continue to hinder widespread adoption. Addressing these issues requires the development of lightweight, adaptive, and privacy-preserving models that balance performance with efficiency and user trust. By advancing innovative detection frameworks and integrating them seamlessly into smart home ecosystems, future solutions can ensure a safer, more reliable, and user-friendly environment for connected households.

REFERENCES

1. R. Agarwal et al., "A Novel Approach for Spam Detection Using Natural Language Processing with AMALS Models," in IEEE Access, vol. 12, pp. 124298-124313, 2024, doi: 10.1109/ACCESS.2024.3391023.
2. Y. Li, K. Zhang, and M. Chen, “Deep learning-enabled spam detection in IoT-based smart environments,” *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 5123–5135, 2023.

3. A. Sharma and R. Kumar, "Lightweight anomaly and spam detection for resource-constrained IoT devices," in *Proc. 2022 IEEE Global Communications Conference (GLOBECOM)*, Rio de Janeiro, Brazil, 2022, pp. 1874–1879.
4. S. Banerjee, T. Nguyen, and H. Kim, "Federated learning for spam traffic detection in smart homes," *IEEE Access*, vol. 9, pp. 146928–146941, 2021.
5. P. Kumar and S. Singh, "Hybrid machine learning model for spam filtering in IoT networks," in *Proc. 2020 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2020, pp. 1–6.
6. M. Alazab, A. Lakshmanna, and P. Reddy, "Deep learning for spam and phishing detection in IoT networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6653–6662, 2019.
7. H. Zhang and L. Wang, "Spam detection in cloud-assisted smart homes using ensemble methods," *IEEE Access*, vol. 6, pp. 69650–69659, 2018.
8. J. Kim, Y. Park, and H. Choi, "Anomaly and spam traffic detection in home IoT networks," in *Proc. 2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, Hong Kong, 2017, pp. 1–8.
9. R. A. Braga, E. M. Horta, and J. R. Souza, "A machine learning approach for spam filtering in IoT-based smart systems," *IEEE Latin America Transactions*, vol. 14, no. 8, pp. 3900–3907, 2016.
10. A. K. Sahu and P. K. Singh, "Spam detection for heterogeneous IoT environments using data mining techniques," in *Proc. 2015 IEEE International Conference on Computer and Information Technology (CIT)*, Liverpool, UK, 2015, pp. 653–658.
11. D. Choudhury and S. Bhatnagar, "A rule-based spam filtering model for smart device communication," *IEEE Systems Journal*, vol. 8, no. 3, pp. 873–882, 2014.
12. C. D. Manning, R. Gupta, and A. J. Joshi, "Spam detection using machine learning approaches: A review and future directions," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 2046–2067, 2012.