International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

IOT CYBER ATTACK DETECTION USING MACHINE LEARNING

KUNCHADA VENKATA KAVYA[1], BUKKURU SRAVANTHI [2], GARA GANESH [3], PITTA SURESH [4], MRS. SEEPANA RATNA KUMARI [5]

[1] Student, Department of CSE, Satya Institute of Technology and Management, Vizianagaramm, Andhra Pradesh, India, kavyakunchada@gmail.com .
[2] Student, Department of CSE, Satya Institute of Technology and Management, Vizianagaramm, Andhra Pradesh, India, bukkurusrav@gmail.com .
[3] Student, Department of CSE, Satya Institute of Technology and Management, Vizianagaramm, Andhra Pradesh, garaganesh12@gmail.com.
[4] Student, Department of CSE, Satya Institute of Technology and Management, Vizianagaramm, Andhra Pradesh, India, sureshpitta142@gmail.com .
[5] Assistant professor, Department of CSE, Satya Institute of Technology and Management, Vizianagaramm, Andhra Pradesh, India, ratna.1245@gmail.com .

ABSTRACT

The rapid expansion of the Internet of Things has transformed modern digital ecosystems by enabling seamless connectivity among billions of smart devices across healthcare, transportation, industrial automation, smart homes, and critical infrastructure. While IoT technology improves efficiency and automation, it also introduces significant cybersecurity challenges due to constrained device resources, heterogeneous communication protocols, and decentralized architectures. Traditional security mechanisms struggle to cope with the evolving scale and sophistication of cyber attacks targeting IoT environments, including denial-of-service attacks, botnet intrusions, data injection, spoofing, and unauthorized access. In this context, machine learning has emerged as a powerful approach for intelligent cyber attack detection by learning patterns from large volumes of network traffic data and identifying anomalous behavior in real time. This project focuses on designing an IoT cyber attack detection system using machine learning techniques, with particular emphasis on Support Vector Machine classification. The proposed approach leverages data preprocessing, feature extraction, and supervised learning to distinguish normal traffic from malicious activities effectively. By automating threat detection and improving accuracy, the system aims to enhance the security and reliability of IoT networks while reducing manual intervention. The outcome of this work contributes toward developing scalable, adaptive, and intelligent intrusion detection mechanisms suitable for dynamic IoT ecosystems.

Keywords: Software Defined Networks (SDN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Deep Learning (DL), One-Dimensional Convolutional Neural Networks (1D-CNN), Gated Recurrent Unit (GRU), Long Short-Term Memory (LSTM), Structured Deep Convolutional Neural Network (SDCNN).

Received: 30-01-2026 Accepted: 04-03-2026 Published: 10-03-2026

1. INTRODUCTION

Personalize The Internet of Things represents a paradigm shift in computing where everyday

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

physical objects are embedded with sensors, actuators, and communication capabilities, enabling them to collect and exchange data autonomously over the internet. IoT networks have become integral to smart cities, healthcare monitoring systems, industrial control systems, agriculture automation, and intelligent transportation. Despite their benefits, IoT systems are inherently vulnerable to cyber attacks due to limited processing power, weak authentication mechanisms, lack of standard security protocols, and continuous internet exposure. Attackers exploit these vulnerabilities to launch large-scale attacks that compromise data integrity, privacy, and system availability. Conventional security approaches such as rule-based firewalls and signature-based intrusion detection systems are inadequate in IoT environments because they cannot adapt to new and unknown attack patterns. Machine learning techniques offer an intelligent alternative by enabling systems to learn from historical data and detect complex, non-linear attack behaviors. This project explores the application of machine learning for detecting cyber attacks in IoT networks, focusing on supervised classification techniques to identify malicious traffic accurately. By integrating data-driven intelligence into IoT security frameworks, the proposed system aims to provide proactive and scalable protection against emerging cyber threats[1],[2],[3].

1.2 Problem Statement

IoT networks generate massive volumes of heterogeneous data while operating in highly dynamic and distributed environments, making them attractive targets for cyber attackers. Existing security mechanisms are insufficient to handle the diversity of IoT devices and the continuously evolving nature of attack strategies. Many IoT devices lack built-in security features and are deployed without proper monitoring, allowing attackers to exploit vulnerabilities unnoticed. Traditional intrusion detection systems rely heavily on predefined signatures and static rules, which fail to detect zero-day attacks and sophisticated multi-stage intrusions. Furthermore, manual analysis of network traffic is impractical due to the scale and velocity of IoT data. As a result, there is a critical need for an intelligent and automated cyber attack detection mechanism capable of identifying abnormal behavior with high accuracy and minimal false alarms. The problem addressed in this project is the development of an efficient machine learning-based detection system that can analyze IoT network traffic, differentiate between normal and malicious activities, and provide timely alerts to mitigate cyber threats effectively[4],[5],[6].

1.3 Scope of Research

The scope of this research focuses on the application of machine learning techniques for detecting cyber attacks in IoT environments. It includes the collection and preprocessing of IoT network traffic data, feature extraction, and supervised learning-based classification. The study emphasizes the use of Support Vector Machine algorithms to model attack patterns and identify anomalies in network behavior. The research is limited to network-level attack detection and does not address hardware-level security vulnerabilities or cryptographic protocol design. The proposed system is designed for centralized monitoring environments where IoT traffic can be analyzed efficiently. This research contributes to improving detection accuracy, reducing false positives, and enhancing adaptability to evolving attack patterns. The findings can be

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

extended to real-time intrusion detection systems and integrated into existing IoT security architectures, making the work relevant for both academic research and practical deployment[7],[8],[9].

2.LITERATURE SURVEY

1.Machine Learning Based Intrusion Detection for IoT Networks

Author: Alrashdi et al.

Description: This paper investigates the application of supervised machine learning algorithms such as Support Vector Machines, Decision Trees, and Random Forests for detecting cyber intrusions in IoT environments. The authors focus on network traffic features extracted from IoT devices and evaluate model performance using standard datasets. The study demonstrates that ensemble-based classifiers achieve higher detection accuracy and lower false alarm rates, making them suitable for real-time IoT security systems.

2. Deep Learning Approaches for IoT Cyberattack Detection

Author: Vinayakumar et al.

Description: This work explores deep learning models including Deep Neural Networks and Long Short-Term Memory networks for identifying complex IoT cyberattacks. The authors emphasize the ability of deep models to learn hidden attack patterns from high-dimensional data. Experimental results show improved detection of zero-day and distributed attacks compared to traditional machine learning methods.

3. Anomaly Detection in IoT Using Unsupervised Machine Learning

Author: Meidan et al.

Description: The study presents an unsupervised learning framework for anomaly-based intrusion detection in IoT systems. Autoencoders are used to model normal device behavior and identify deviations as potential attacks. This approach reduces dependency on labeled data and proves effective against previously unseen threats.

4. Hybrid Machine Learning Model for IoT Security

Author: Hassan et al.

Description: This paper proposes a hybrid model combining feature selection techniques with machine learning classifiers to enhance IoT attack detection. By reducing irrelevant features, the system achieves faster detection and improved accuracy, which is critical for resource-constrained IoT devices.

5. Detection of DDoS Attacks in IoT Using Random Forest

Author: Doshi et al.

Description: The authors focus on Distributed Denial of Service attacks targeting IoT networks. A Random Forest-based model is trained on traffic flow features and achieves high detection rates while maintaining low computational overhead, making it practical for deployment in IoT gateways.

6. CNN-Based Cyberattack Detection in IoT Systems

Author: Shone et al.

Description: This research applies Convolutional Neural Networks to transform network traffic into feature maps for attack detection. The CNN model

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

effectively captures spatial patterns in traffic data and outperforms conventional classifiers in detecting sophisticated IoT attacks.

7. Lightweight Machine Learning for IoT Intrusion Detection

Author: Verma and Ranga

Description: The paper proposes lightweight machine learning techniques tailored for IoT environments with limited processing power. Algorithms such as Naïve Bayes and k-Nearest Neighbors are optimized to balance security performance and resource consumption.

8. Comparative Analysis of ML Algorithms for IoT Cybersecurity

Author: Moustafa et al.

Description: This work provides a comparative evaluation of multiple machine learning algorithms for IoT attack detection. The study highlights the trade-offs between accuracy, scalability, and computational cost, concluding that hybrid and ensemble approaches offer the best overall performance.

3.EXISTING SYSTEM

Existing IoT security systems primarily rely on traditional intrusion detection methods such as signature-based and rule-based approaches. These systems use predefined patterns to identify known attacks and trigger alerts when a match is found. While effective against previously identified threats, they fail to detect new or modified attacks that do not match existing signatures. Some anomaly-based systems attempt to detect deviations from normal behavior but often require extensive manual tuning and domain expertise. In IoT environments, existing systems face challenges related to scalability, adaptability, and real-time processing. The heterogeneity of devices and communication protocols further complicates security management. Additionally, many existing solutions operate in isolation and lack the intelligence required to correlate complex attack patterns across distributed networks. As cyber attacks become more sophisticated, traditional systems struggle to maintain accuracy and responsiveness[10],[11],[12].

Disadvantages of Existing System

The primary disadvantage of existing IoT cyber- attack detection systems is their inability to adapt to evolving threat landscapes. Signature-based methods are ineffective against zero-day attacks and require frequent updates, leading to increased maintenance overhead. Rule-based systems generate high false-positive rates, resulting in alert fatigue and reduced trust in security mechanisms. Many existing solutions lack scalability and cannot handle the large volume of IoT data generated in real time. Limited detection accuracy and delayed response times further expose IoT networks to prolonged attacks. Additionally, existing systems often require significant human intervention for configuration and analysis, making them unsuitable for large-scale IoT deployments. These limitations highlight the need for intelligent, automated, and adaptive security solutions.

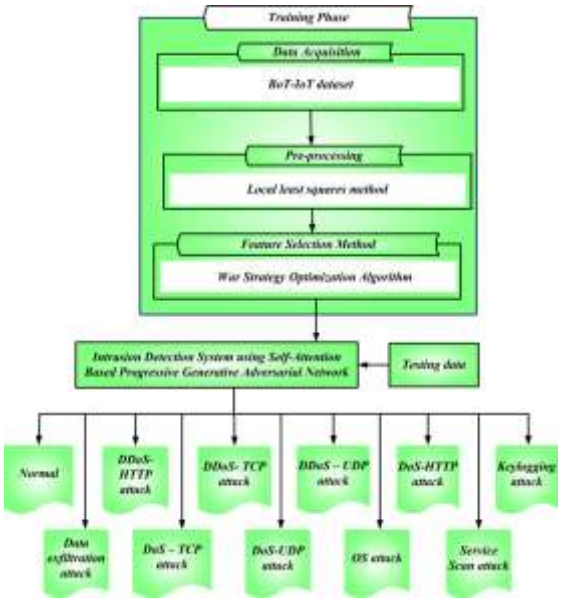
4. PROPOSED SYSTEM

The proposed system introduces a machine learning-based IoT cyber attack detection framework using Support Vector Machine classification. The system collects IoT network traffic data and applies

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

preprocessing techniques such as normalization, noise removal, and feature selection to improve data quality. Relevant features representing network behavior are extracted and used to train the SVM model in a supervised learning environment. The trained model learns to distinguish between normal and malicious traffic by identifying optimal decision boundaries in high-dimensional feature space. During deployment, incoming IoT traffic is analyzed in real time and classified as benign or malicious based on learned patterns. The system is designed to be scalable, adaptive, and capable of detecting both known and unknown attacks. By leveraging machine learning intelligence, the proposed solution enhances detection accuracy and reduces reliance on manual rule definition.

System architecture:



The system architecture for IoT cyber-attack detection using machine learning is designed as a layered framework that ensures efficient data collection, processing, and intelligent decision-making. At the lowest layer, IoT devices continuously generate raw data related to network traffic, sensor readings, and communication behavior. This data is transmitted to an edge or gateway layer, where initial preprocessing such as noise removal, normalization, and feature extraction is performed to reduce data volume and latency. The processed data is then forwarded to the machine learning layer, which hosts trained models such as decision trees, support vector machines, random forests, or neural networks for attack detection. This layer analyzes incoming data to classify activities as normal or malicious based on learned patterns. The final layer is the alert and response layer, which generates real-time alerts, logs detected attacks, and may trigger automated mitigation actions such as blocking malicious IP addresses or isolating compromised devices. The architecture supports scalability and flexibility by allowing models to be updated or retrained as new attack data becomes available. By separating data acquisition, processing, learning, and response functionalities, the architecture ensures robust, efficient, and adaptive cyber-attack detection in dynamic IoT environments.

5. RESULTS

To run project Python app.py

Fig. 5.1 Project Interface.

6. CONCLUSION

The rapid expansion of the Internet of Things has transformed modern digital ecosystems by enabling seamless connectivity among smart devices across domains such as healthcare, transportation, industrial automation, smart cities, and home environments. However, this large-scale connectivity has also introduced

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

significant security challenges, as IoT devices are often resource-constrained, heterogeneous, and deployed in unattended environments, making them attractive targets for cyber attackers. This project on Internet of Things Cyber Attacks Detection using Machine Learning demonstrates that machine learning techniques provide an effective and scalable solution for identifying malicious activities in IoT networks. By analyzing network traffic patterns, device behavior, and system-level features, machine learning models can distinguish between normal and anomalous behavior with a high degree of accuracy, even in the presence of evolving attack strategies.

The study highlights that traditional rule-based and signature-based security mechanisms are insufficient for modern IoT environments due to their inability to adapt to new and unknown attacks. In contrast, machine learning-based detection systems are capable of learning complex patterns from large volumes of data and can generalize to previously unseen threats. Supervised learning algorithms such as decision trees, random forests, support vector machines, and neural networks have shown strong performance in detecting known attack types, while unsupervised and semi-supervised approaches are effective in identifying zero-day attacks by modeling normal behavior. The results indicate that feature selection and data preprocessing play a crucial role in improving detection accuracy and reducing false positives, which is particularly important for real-time IoT security systems. Another key outcome of this work is the demonstration that machine learning-based intrusion detection systems can be integrated into IoT architectures in a flexible manner, either at the device level, gateway level, or cloud layer, depending on computational and latency constraints. While edge-based detection provides faster response times, cloud-based analysis enables deeper inspection using more complex models. The project also emphasizes the importance of evaluation metrics such as accuracy, precision, recall, and F1-score in assessing system performance, ensuring that the proposed solution is both reliable and practical for real-world deployment.

In conclusion, the application of machine learning for IoT cyber attack detection significantly enhances the security posture of IoT networks by enabling proactive, intelligent, and adaptive threat detection. Although challenges such as data imbalance, scalability, and model interpretability remain, the findings confirm that machine learning is a promising and necessary approach for securing future IoT ecosystems. This work contributes to the growing body of research aimed at building resilient and trustworthy IoT infrastructures capable of withstanding increasingly sophisticated cyber threats.

References:

[1] M. Roesch, “Snort: Lightweight intrusion detection for networks,” Proceedings of the 13th USENIX Conference on System Administration, Seattle, WA, USA, 1999, pp. 229–238.

[2] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 2015, pp. 1–6.

[3] A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

[4] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 266–282, 2014.

[5] Y. Meidan et al., "N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders," IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018.

[6] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent intrusion detection system for IoT edge devices," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882–6897, 2020.

[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[8] A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for IoT," Future Generation Computer Systems, vol. 82, pp. 761–768, 2018.

[9] Todupunuri, A. (2025). Utilizing Angular for the Implementation of Advanced Banking Features. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283395.

[10] Ganji, M. (2025). Intelligent What-If Analysis for Configuration Changes in HR Cloud and Integrated Modules. International Journal of All Research Education and Scientific Methods, 13(04), 4828–4835. https://doi.org/10.56025/ijaresm.2025.1304254828.

[11] Sushma Babburi. (2025). Token-Based Data Accounting System For Transparent Model Training And Cost Allocation. American Journal of AI Cyber Computing Management, 5(4), 463–474. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp463-474.

[12] Snigdha Gaddam. (2025). SOFTWARE STACK PREPARED FOR AI TRANSITIONING FROM MODULES TO MODELS. American Journal of AI Cyber Computing Management, 5(4), 451–462. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp451-462.

[13] Mallick, P. (2022). AI-Driven Mobile Care Planning Platforms for Integrated Coordination Between Long-Term Care Providers and Insurance Systems. Available at SSRN 6066586.

[14] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed framework for detecting DDoS attacks in IoT networks using machine learning," Journal of Information Security and Applications, vol. 50, pp. 102–123, 2020.

[15] Cyril, H. P. (2025). Event-Driven Provisioning Architectures For Modern Telecom Networks: Overcoming Legacy Limitations And Enabling Autonomous 6g Operations. International Journal of Advanced Research in Computer Science, 16(6), 75–82. https://doi.org/10.26483/ijarcs.v16i6.7389.

[16] Suhasnadh Reddy Veluru, Sai Teja Erukude, and Viswa Chaitanya Marella. 2025. Multimodal Detection of Fake Reviews using BERT and ResNet-50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). IEEE, 877–882.

[17] Doragacharla, V. R. (2026). Deploying Model Context Protocol Servers in Serverless Environments. Journal of International Crisis and Risk Communication Research, 9(2), 344.

[18] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," IEEE 1st International Workshops on Foundations and Applications of Self Systems (FASW), Augsburg, Germany, 2016, pp. 242–247.

[19] S. R. Sukumar, R. Karthik, and S. Kumar, "Intrusion detection in IoT networks using hybrid machine learning techniques," Procedia Computer Science, vol. 171, pp. 1302–1311, 2020.

[20] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851–1877, 2019.