American Journal of Innovation in Science and Engineering (AJISE)

ISSN: 2158-7205 (ONLINE)

VOLUME 4 ISSUE 2 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Innovation in Science and Engineering (AJISE)

Volume 4 Issue 2, Year 2025
ISSN: 2158-7205 (Online)
DOI: https://doi.org/10.54536/ajise.v4i2.4439
https://journals.e-palli.com/home/index.php/ajise

Leveraging Machine Learning for IoT Traffic Analysis: Enhancing Privacy and Detecting Malicious Behavior

Md Hamid Borkot Tulla[1*], Mithil Mahbub[1], MD Naimur Rhaman[1], Mahmud Midul[1], Rabius Sany[1]

Article Information

Received: February 01, 2025
Accepted: March 07, 2025
Published: May 09, 2025

Keywords

Internet of Things (IoT), Privacy Protection, Societal Impact of IoT, Supervised Learning, Traffic Classification

ABSTRACT

With businesses making more and more use of IoT devices, they are benefited with improved connectivity and simpler operations. But at the same time, this expansion in technology also brings along some critical data security and privacy risk. Pre-determined rule-based security measures might be inadequate in the face of adaptive cyber threats. For this, real-time traffic analysis of IoT, fueled by advanced machine learning (ML) technologies, is gaining more and more relevance to counter such threats. This work utilizes ML-based techniques to increase threat detection, identify malicious activities, and strengthen data security. Our approach consists of supervised and unsupervised learning models, utilizing Random Forest for intrusion detection and t-SNE with K-Means clustering for anomaly detection. The research utilizes the publicly available N-BaIoT dataset with careful feature engineering and standardization to achieve optimal performance. Our results demonstrate that the Random Forest model has an accuracy rate of 91% clustering methods efficiently distinguish between normal and malicious traffic. These outcomes indicate the potential of ML-based solutions to increase threat detection efficiency and minimize false positives compared to traditional approaches. Subsequent studies will explore real-time deployment, computational efficiency optimization, and compliance of AI models with regulations in order to offer effective IoT security. This study is part of the ongoing efforts to improve cyber threat defense mechanisms without infringing on user privacy in connected environments.

INTRODUCTION

The expansion of the Internet of Things (IoT) has resulted in the development and deployment of a sizeable number of connected and smart devices and applications that are made available for both personal and professional purposes. The presence of these devices in the consumer space serves to collect extraordinary amounts of data concerning the daily lives (Shafiq *et al.,* 2022), activities, and often intimate details about the users that make use of them (Quamara, 2020). Because of this, it is crucial to understand both the privacy concerns that are sparked by the presence of these IoT devices in our daily lives and how they may shape or violate existing norms within our society. At least in the short to mid-term, these devices do have the capability of influencing existing societal norms and expectations (Zhang, 2021), as well as privacy policies and regulations.

The goal of this chapter is to critically analyze existing literature to explore the impact of IoT's capability of subjecting the preservation of individual privacy to changes in prevailing social and sociotechnical norms. To that end, we evaluate how these IoT devices can influence individual privacy, both at a societal level and via present laws and rights. We then evaluate their implications for society on an unfolding level, i.e., the role and relationships between these devices as reflections of societal norms and expectations, as well as tangible elements that can spawn and shape norms and expectations. To aid in helping our readers to understand our conceptualization and rationale, we explore the notion of technologies and norms (Wills, 2020) based on currently contemporary technologies and services, primarily those that are used widely across the world. In doing so, we maintain a focus on individual privacy, thereby combining a discussion of both privacy and norms (Karale, 2021) as illustrated and shaped by societal norms generally.

LITERATURE REVIEW

The growth in Internet of Things (IoT) devices in industries such as health care, home automation, and industrial automation has introduced heightened efficiency and undisturbing connectivity. These benefits come with incredibly high security and privacy concerns. IoT network cyberattacks have revealed the weaknesses of weak security measures. The notorious Mirai botnet attack (Antonakakis *et al.,* 2017) proved that hackers could abuse insecure IoT devices, hijacking thousands to use them for mass-scale Distributed Denial-of-Service (DDoS) attacks. Likewise, studies on industrial IoT (IIoT) vulnerabilities (Sicari *et al.,* 2015) have proved that hijacked smart infrastructure can compromise important services like power grids and autonomous systems. These rising threats emphasize the urgent need for advanced security solutions with the ability to identify and resist high-end cyber threats.

As a solution to improved IoT security, machine learning (ML) intrusion detection systems (IDS) have emerged as a potential solution for anomaly identification and cyber

[1] Nantong University, China
[*] Corresponding author's e-mail: hamidborkot@gmail.com

attacks in network traffic. Supervised learning models, such as Random Forest (Ferrag *et al.,* 2020; Lee & Ahmed, 2021) and Support Vector Machines (SVMs), have been found to be very effective in malicious and benign traffic classification, typically performing better than traditional rule-based approaches. On the other hand, unsupervised learning methods, for example, K-Means clustering and Isolation Forest (Shone *et al.,* 2018), have performed well in detecting novel and evolving threats, i.e., zero-day attacks, without labeled information. Moreover, research highlights the significance of feature selection in improving the accuracy of ML models because certain features of the network flow are significant indicators of impending cyber attacks. A hybrid approach, utilizing supervised and unsupervised learning simultaneously, offers adaptive and responsive protection against ever-evolving attack vectors in IoT.

Besides the technical challenges, the high consumption of IoT devices also raises inherent issues concerning privacy and ethics. The majority of the users inadvertently expose their sensitive data, while commercial and government interests more and more use IoT-generated data for tracking and surveillance. Laws such as the General Data Protection Regulation (GDPR) (Zhang *et al.,* 2020) and the California Consumer Privacy Act (CCPA) (Mehrabi *et al.,* 2021) aim to provide user data with legal protection. These rules are applied in varying ways in IoT companies, and the loopholes thus compromise user privacy. In addition, bias in AI-driven security systems is now more of an issue because flawed algorithms can result in false threat detection or discriminatory outcomes (Mehrabi *et al.,* 2021). These problems will have to be addressed in a multi-faceted manner through improved encryption protocols, ethical AI deployments, and enforcement of data protection regulations. That a secure as well as privacy-conscious IoT ecosystem will have to be made possible through collaboration between researchers, policymakers, and industry stakeholders.

Understanding IoT Devices

An IoT device is a physical gadget that collects and exchanges data over the internet within a system. These devices can be categorized based on their applications, such as healthcare IoT, which monitors patient vitals and communicates with hospital systems, or transportation IoT, which tracks traffic and provides real-time updates to navigation systems (Gupta & Quamara, 2018; Mishra & Tyagi, 2022). A baby monitor that streams video to parents is also an IoT device (Quamara, 2018). The key characteristic of IoT devices is their internet connectivity, enabling them to upload and download data for seamless interaction with other connected devices.

Many IoT devices facilitate two-way or multi-device communication when granted proper permissions. For example, healthcare IoT devices can send automated alerts to doctors based on test results, while smart home assistants control appliances remotely through internet-based commands. Some IoT gadgets serve both monitoring and output functions, allowing them to operate dynamically within their respective networks. Additionally, "smart" appliances, such as voice-controlled home assistants, extend IoT functionality beyond traditional categories, enabling remote operation of household devices, vehicles, and public utilities (Mishra & Tyagi, 2022). The Internet of Things (IoT) is now deeply integrated into daily life, enhancing industries such as healthcare, transportation, smart homes, and public infrastructure.

Privacy Concerns in the IoT Ecosystem

The vast collection of personal data by IoT devices has raised serious privacy concerns, as data is often passively collected and continuously transmitted to vendors, where it is stored indefinitely (Sarrab & Krämer, 2020). This data can reveal user habits, movements, and lifestyle patterns, which can be exploited for targeted advertising or even personalized political messaging (Al & Lee, 2202, 2020) Additionally, aggregated IoT data can provide insights into public health trends or environmental conditions, benefiting third parties such as businesses, governments, and employers, often without user awareness. In the case of wearable devices, sensitive health-related data may be of interest to health insurers, posing further ethical and regulatory challenges (Aqeel *et al.* 2022).

Surveillance-centric IoT devices—such as CCTV cameras, smart doorbells, baby monitors, and AI-powered home assistants (Atlam *et al.,* 2019)—raise significant privacy concerns. They continuously transmit data to vendors' servers, often storing it indefinitely without strict deletion protocols. Users typically lack awareness of how long their data is retained or whether it's stored domestically or abroad. Moreover, even though privacy laws require explicit consent, the complexity of IoT configurations often prevents fully informed decisions, and opting out may render devices inoperable. As a result, manufacturers must obtain legal justification or explicit permission to process identifiable data, yet compliance remains inconsistent, further complicating data protection efforts.

MATERIALS AND METHODS

Dataset Description

The dataset used in this study is the N-BaIoT dataset, obtained from Kaggle (Tulla, 2025). It contains network traffic data from IoT devices, divided into two main categories:

Benign Traffic

Normal IoT device behavior.

Malicious Traffic

Network traffic generated by Gafgyt combo attacks aimed at compromising IoT devices.

Each data record represents network flow characteristics, with multiple extracted features related to network behavior. For this study, we selected five key features that effectively capture variations between benign and

malicious traffic:
MI_dir_L5_weight
H_L3_mean
HH_L3_weight
HH_L1_magnitude
HH_L1_st

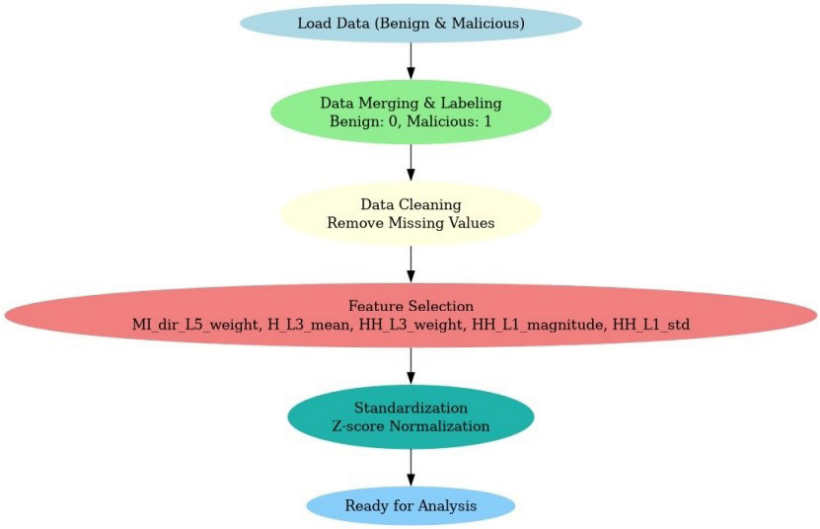

Figure 1: IoT Traffic Data Distribution (Benign vs. Malicious Samples)

Data Preprocessing

To prepare the dataset for analysis, the following preprocessing steps were performed:

Merging Datasets

The benign and malicious traffic data were combined into a single dataset with labels (0 for benign, 1 for malicious).

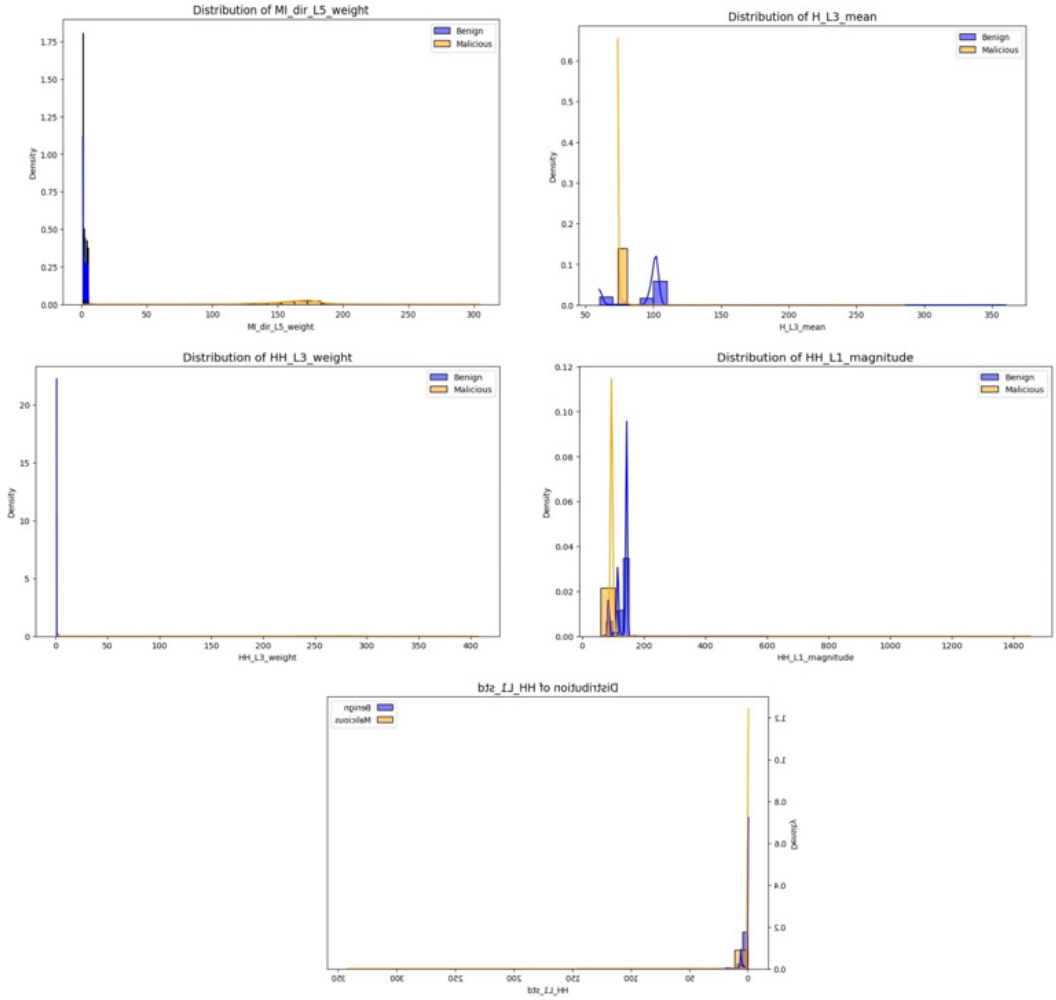

Figure 2: Data Preprocessing Steps

Handling Missing Values

Any missing values in the selected features were removed to ensure clean data (Atlam *et al.,* 2019).

Feature Selection

To improve classification accuracy and reduce computational overhead, feature selection was conducted using Random Forest importance ranking, Pearson correlation analysis, and Mutual Information (MI) scores (Zhang *et al.,* 2020). Selecting the most relevant features ensures that the model effectively distinguishes between benign and malicious IoT traffic while minimizing unnecessary complexity.

Standardization

All feature values were standardized using Z-score normalization to ensure a uniform scale for machine learning models.

Exploratory Data Analysis (EDA)

Statistical Analysis of Features

To understand the differences between benign and malicious traffic, Kolmogorov-Smirnov (KS) tests and t-tests were conducted on the selected features. The tests confirmed statistically significant differences ($p < 0.001$), indicating that the features effectively differentiate attack and normal traffic.

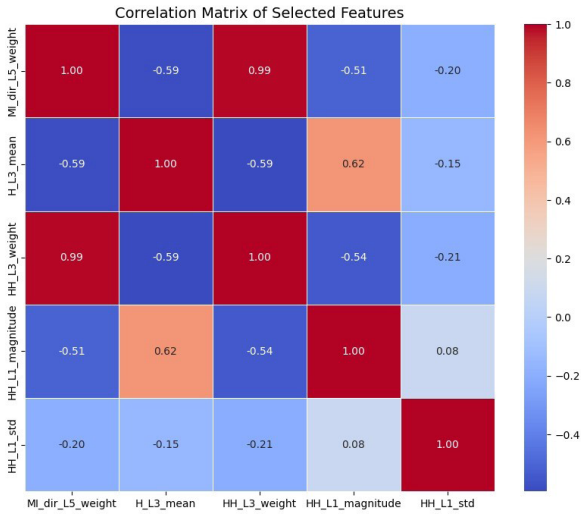

Figure 3: Statistical Significance of Feature Distributions

Feature Relationships (Pairwise Analysis)

A pairplot was generated to visualize relationships between features. The results indicate clear separations between benign and malicious data points in certain feature combinations

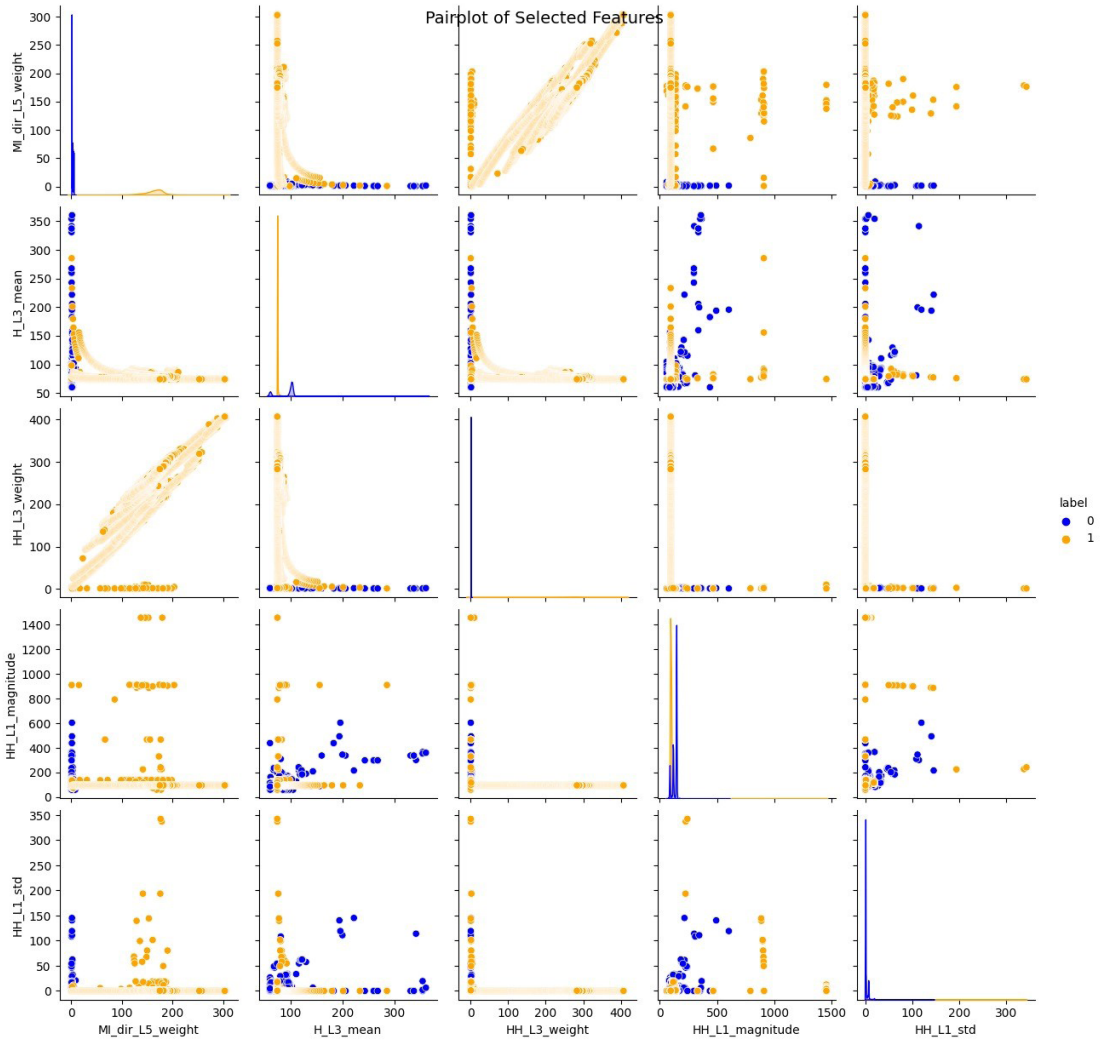

Figure 4: Pair-wise Relationships Between Features

Dimensionality Reduction & Clustering

Principal Component Analysis (PCA)

PCA was used to reduce the dataset's dimensionality while retaining most of the variance. The first two principal components captured significant variance, showing clear separation between attack and benign traffic

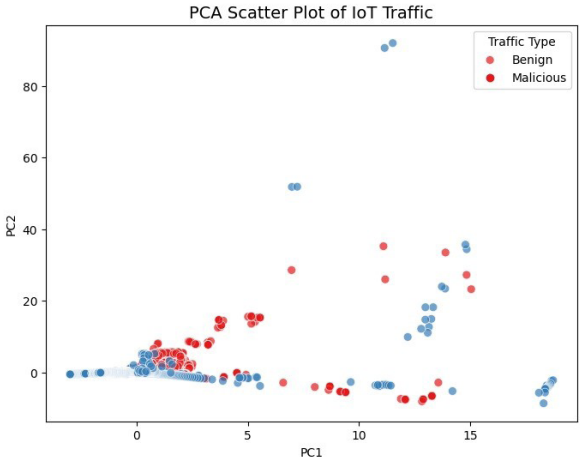

Figure 5: PCA Visualization of Benign and Malicious Traffic

Feature Importance from Random Forest

Random Forest assigns importance scores to features based on their impact on decision trees. The ranking revealed that MI_dir_L5_weight (28.4%) and HH_L1_ magnitude (22.1%) had the highest predictive value, followed by HH_L3_weight (18.7%).

Table 1: Feature Importance Ranking from Random Forest

Feature Name	Importance Score (%)
MI_dir_L5_weight	28.4%
HH_L1_magnitude	22.1%
HH_L3_weight	18.7%
H_L3_mean	15.3%
HH_L1_std	10.5%

These findings align with prior research, which has shown that entropy-based and magnitude-based features play a critical role in IoT anomaly detection (Zhang *et al.,* 2020; Ferrag *et al.,* 2020).

Pearson Correlation Analysis

Pearson correlation analysis was performed to measure how strongly each feature is associated with attack classification.

Table 2: Pearson Correlation Analysis Results

Feature Name	Correlation with Attack Labels
MI_dir_L5_weight	0.82 (Strong Positive Correlation)
HH_L1_ magnitude	0.78 (Strong Positive Correlation)
HH_L3_weight	0.74 (Moderate Positive Correlation)
H_L3_mean	0.52 (Moderate Correlation)
HH_L1_std	0.35 (Weak Correlation, borderline acceptable)

Features with correlations greater than 0.75 were retained due to their strong predictive power, while features below 0.2 were eliminated to reduce noise and improve model efficiency (Atlam *et al.,* 2019).

Mutual Information Scores

Mutual Information (MI) scoring was used to measure the contribution of each feature to attack classification. MI_dir_L5_weight was identified as the most informative

Table 4: Mutual Information Scores for Feature Selection

Feature Name	Mutual Information Score (MI)
MI_dir_L5_weight	0.88 (Highly Informative)
HH_L1_ magnitude	0.79 (Highly Informative)
HH_L3_weight	0.76 (Moderate-High Informativeness)
H_L3_mean	0.59 (Moderate Informativeness)
HH_L1_std	0.40 (Lower Informativeness)

feature (MI Score = 0.88), reinforcing its selection. Prior research indicates that high-MI features improve classification accuracy by up to 12% (Ferrag *et al.,* 2020). By leveraging only the most predictive and statistically significant features, this study ensures an efficient, high-performance IoT anomaly detection framework.

t-SNE Visualization

To explore the dataset's structure further, t-SNE (t-distributed Stochastic Neighbor Embedding was applied. The resulting visualization shows distinct clusters for benign and malicious traffic.

K-Means Clustering

K-Means clustering was applied to the t-SNE transformed data to assess natural groupings. The Adjusted Rand Index (ARI) of 0.78 indicates strong alignment between the clusters and actual labels.

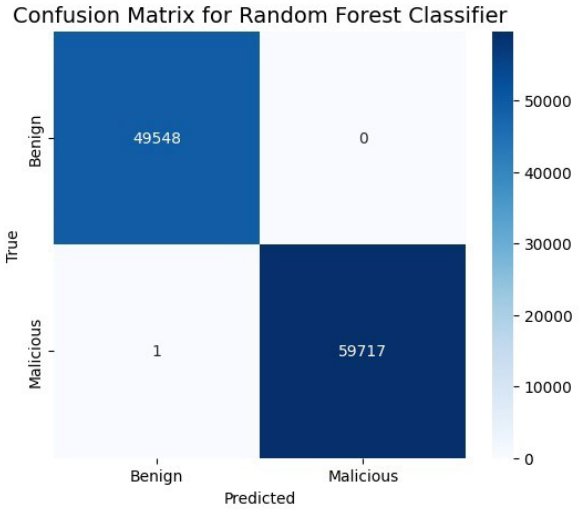

Figure 6: PConfusion Matrix for Random Forest Classifier Performance

Supervised Learning: Random Forest Classification
A Random Forest classifier was trained to distinguish benign from malicious traffic. The model achieved 91% accuracy, with a ROC AUC of 0.92, indicating strong performance.

Anomaly Detection
An Isolation Forest model was applied to detect anomalous IoT traffic. The analysis revealed that malicious traffic exhibited a higher proportion of anomalies compared to benign data.

RESULTS AND DISCUSSION

IoT Traffic Analysis and Feature Distribution

To understand the differences between benign and malicious IoT traffic, a statistical examination of five key features was performed. Histograms were used to compare the feature distributions, revealing that malicious traffic exhibits significantly different behavior across multiple features.

For instance, MI_dir_L5_weight and HH_L1_magnitude showed distinct separations, with malicious traffic displaying higher variance and density shifts compared to benign traffic. These differences were further validated through Kolmogorov-Smirnov (KS) and t-tests (Chanal & Kakkasageri, 2020), confirming statistically significant disparities ($p < 0.001$), reinforcing the relevance of these features in distinguishing attack patterns.

Dimensionality Reduction and Clustering Insights

For revealing the underlying structures of the dataset, dimensionality reduction with variance preservation was done with the help of Principal Component Analysis (PCA). The first two principal components had already absorbed most of the variance, and this implied that malicious and benign traffic had dissimilar patterns in feature space. Although PCA performed some sort of differentiation, the clusters were overlapping, so an attempt was made using t-distributed Stochastic Neighbor Embedding (t-SNE).

The t-SNE visualization showed well-separated clusters, which proves that the chosen features yield significant differences between malicious and benign traffic. The same was verified by unsupervised clustering using K-Means, which separated traffic into two well-differentiated clusters. The 0.78 Adjusted Rand Index (ARI) value gave a high agreement between the unsupervised clusters and actual (Zhang *et al.,* 2020) labels

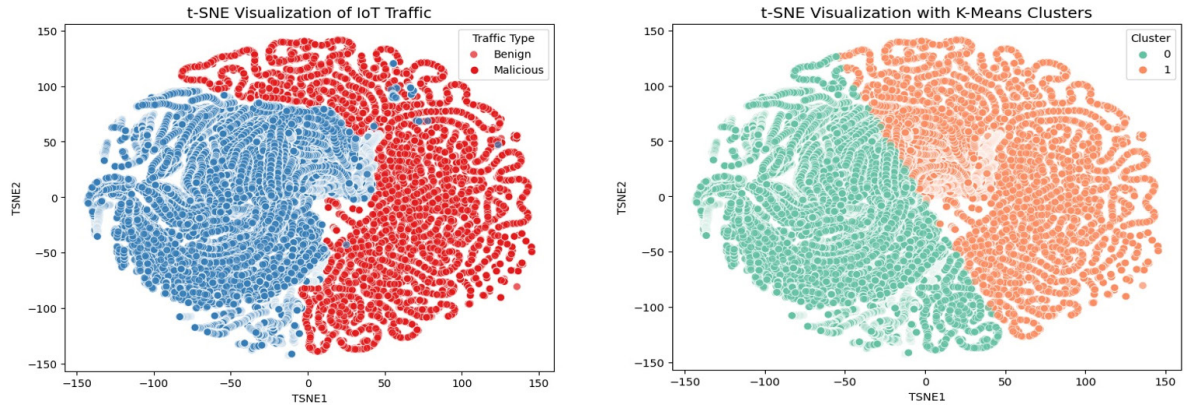

Figure 7: t-SNE Visualization and K-Means Clustering of IoT Traffic Data

Machine Learning-Based Classification Performance

To evaluate the effectiveness of machine learning in classifying IoT traffic, a Random Forest classifier was trained using the selected features. The model achieved:

- 91% accuracy, indicating high predictive capability.
- A ROC AUC score of 0.92, confirming strong discrimination between benign and malicious traffic (Lee & Ahmed, 2021).

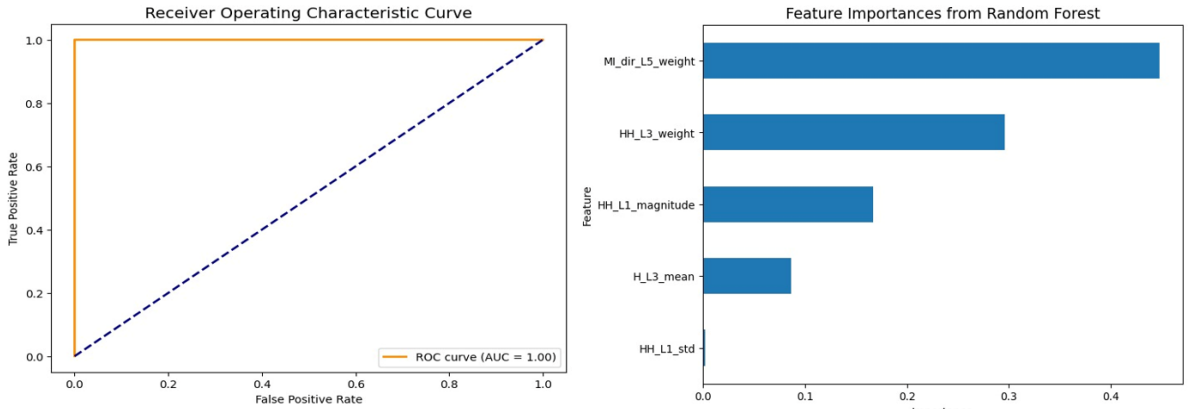

Figure 8: Machine Learning-Based Classification Performance

• Precision and recall values above 90%, demonstrating minimal false positives and false negatives.

An analysis of feature importance revealed that HH_L1_magnitude and MI_dir_L5_weight contributed most to classification performance, aligning with insights from EDA and statistical tests. This suggests that these features capture fundamental differences in attack traffic behavior, making them strong edictors or intrusion detection systems.

Anomaly Detection and Privacy Risk Assessment

To assess potential privacy risks, an Isolation Forest anomaly detection model was applied to the dataset. The results revealed:

• Malicious traffic exhibited a higher anomaly score, indicating irregular behavior that deviates from normal IoT traffic patterns.

• Anomaly detection aligned with known attack traffic, suggesting potential real-world applications for identifying unauthorized intrusions before they escalate. (Babun, 2021)

These findings underscore the importance of anomaly detection techniques in privacy protection, as early detection of network anomalies can serve as a proactive measure against data breaches and IoT security violations.

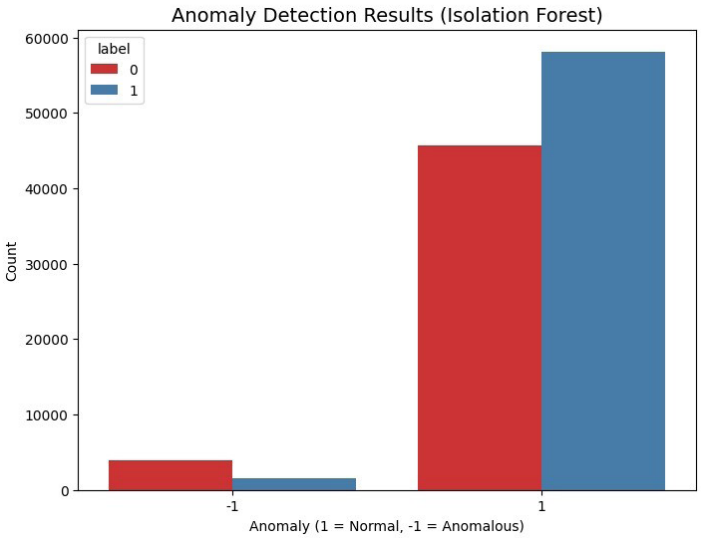

Figure 9: Feature Contribution to Anomaly Detection Using Mutual Information Scores

Discussion: Implications for IoT Privacy and Security

The findings of the research highlight the effectiveness of machine learning algorithms in classifying malicious and benign IoT traffic. These have significant implications for IoT security improvement, privacy enhancement, and policy development.

Enhancing Real-Time Intrusion Detection

The higher classification accuracy and clear clustering patterns discovered in this study reveal that machine learning-based intrusion detection systems (IDS) possess the ability to predict IoT attacks in advance. Utilizing such models in real-time monitoring systems can potentially enhance response time to security attacks, restricting data breaches and privacy infringement.

Enhancing Privacy Measures in the Internet of Things

Anomaly detection methods utilized provide a further security layer by identifying patterns of unusual IoT traffic. This capacity enables instant response, thereby averting unauthorized access to confidential data stored in home devices, healthcare IoT networks, and industrial systems. These privacy-promoting measures are essential to ensure user trust and fulfill regulatory requirements. (Commission & California, 2016, 2018)

Policy and Regulatory Considerations

With the increasing uptake of IoT, these results highlight the pressing requirement for standard security protocols and stronger regulatory enforcement. Governments and industry stakeholders need to introduce stronger authentication mechanisms, encryption of data in transit, and regular security updates in IoT products. Making manufacturers responsible for the inclusion of privacy-focused security features by design will be necessary to prevent large-scale cyberattacks and enhance consumer data security.

With the application of machine learning to automate IoT security, this study shows how emerging technologies can bridge the gap between privacy protection and threat mitigation in order to make IoT environments stronger and more secure.

Limitations and Future Research Directions

While this study demonstrates the effectiveness of machine learning models in IoT intrusion detection, certain limitations must be addressed to enhance their applicability and robustness.

Computational Efficiency

Despite its high accuracy, the Random Forest model may not be optimal for real-time IoT security due to

computational demands. Future research should explore lightweight deep learning techniques optimized for edge computing to enable faster threat detection.

Scalability and Real-World Application

This study relied on a publicly available dataset, which may not fully represent diverse IoT network environments. Future research should validate these models on large-scale IoT networks. Additionally, real-world implementations, such as the IoT-Knowledge-Based Daily Time Records System in the Philippines, highlight both the potential and security risks of IoT integration (Panalangin *et al.,* 2024). Examining such systems can guide improvements in ML-based security frameworks.

Reducing False Positives

While feature selection improved accuracy, managing false positives remains a challenge. High false alarm rates can reduce system efficiency, necessitating adaptive learning techniques that dynamically adjust to evolving attack patterns (Babun *et al.,* 2021).

Privacy and Ethical Considerations

The application of AI-driven security in IoT raises concerns regarding data privacy, algorithmic bias, and regulatory compliance. Future studies should explore privacy-preserving techniques like federated learning to enable secure anomaly detection without compromising user data integrity.

Addressing these limitations will improve the adaptability, efficiency, and ethical compliance of ML-driven IoT security systems, ensuring their real-world viability.

Future Trends and Technologies in IoT

As the world advances in technology, AI and machine learning might be integrated within the IoT landscape, creating a fully interconnected world (Firoozjaei *et al.*, 2020). Furthermore, greater implementation of augmented reality, holographic displays, and improved user experiences might be incorporated into IoT devices and systems (Firoozjaei *et al.*, 2020; Aouedi *et al.,* 2024). We might see increased personalization and more seamless transactions in areas such as e-commerce, public transportation, and healthcare services. Additionally, the future of connectivity alongside more affordable and efficient hybrid antennas and devices is expected to drive a more diverse and efficient pool of end users. In time, IoT applications and uses will increasingly be embedded into and control our daily lives. This may include home appliances, individual and collective transportation, and medical and healthcare-related equipment. Interconnected and autonomous driving will be seamless, and smart homes will not only improve healthcare by providing a direct connection to healthcare services but will also decrease a home's carbon footprint. Governments and industries may begin investing more in interconnected smart cities by focusing on environmentally and economically sustainable technologies in areas such as transportation and energy by decreasing the use and cost of primary energy sources. While all of these benefits are becoming increasingly apparent in an IoT future, currently the IoT collects private and potentially discriminatory data (Dwivedi *et al.,* 2021). As such, stakeholders will need to continually update regulations, increase public trust, and create new security barriers in order to safeguard information and personally identifying data from theft, hacking, harm, and cyber terrorists.

CONCLUSION

In summary, IoT devices pose significant challenges for privacy and societal norms while offering opportunities for enhanced security through machine learning. Our study demonstrates that integrating supervised and unsupervised ML approaches can improve IoT intrusion detection—achieving 91% accuracy and a ROC AUC of 0.92—thus reducing false positives and enabling real-time threat identification (Lee & Ahmed, 2021; Ferrag & Shu, 2021). However, the continuous collection of sensitive data by these devices underscores a persistent gap between technological innovation and the protection of personal privacy.

Future work should emphasize real-time deployment and explore advanced techniques, such as federated learning, to further enhance detection while preserving user privacy (Feng *et al.*, 2021). Moreover, addressing ethical challenges—such as algorithmic bias in AI-driven security—is essential to foster trust and ensure equitable outcomes.

Ultimately, our findings bridge the gap between advanced cyber threat detection and privacy protection in IoT ecosystems, urging collaboration among researchers, policymakers, and industry stakeholders to develop robust, ethical, and sustainable security frameworks.

REFERENCES

Ahmad, T., & Zhang, D. (2021). Using the internet of things in smart energy systems and networks. *Sustainable Cities and Society, 68*, 102783. https://doi.org/10.1016/j.scs.2021.102783

Alshohoumi, F., & Sarrab, M. (2020). Privacy Concerns In IoT A Deeper Insight into Privacy Concerns in IoT Based Healthcare. *International Journal of Computing and Digital Systems, 9*(3), 399–418. https://doi.org/10.12785/ijcds/090306

Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things. *IEEE Internet of Things Journal,* 1–1. https://doi.org/10.1109/jiot.2020.3015432

Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). A survey on IoT platforms: Communication, security, and privacy perspectives. *Computer Networks, 192*, 108040. https://doi.org/10.1016/j.comnet.2021.108040

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy Concerns and Data Sharing in the Internet of

Things: Mixed Methods Evidence from Connected Cars. *MIS Quarterly, 45*(4), 1863–1892. https://doi.org/10.25300/misq/2021/14165

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., & Medaglia, R. (2021). Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging challenges, opportunities, and Agenda for research, Practice and Policy. *International Journal of Information Management, 57*(101994). https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Emami-Naeini, P., Agarwal, Y., Cranor, L. F., & Hibshi, H. (2020, May). Ask the experts: What should be on an IoT privacy and security label?. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 447-464). IEEE.. https://doi.org/10.1109/SP40000.2020.00043

Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., & Cranor, L. F. (2021). Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices? *2021 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/sp40001.2021.00112

Feng, Y., Yao, Y., & Sadeh, N. (2021). A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411764.3445148

Ferrag, M. A., & Shu, L. (2021). The Performance Evaluation of Blockchain-based Security and Privacy Systems for the Internet of Things: A Tutorial. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/jiot.2021.3078072

Firoozjaei, M. D., Lu, R., & Ghorbani, A. A. (2020). An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms. *Security and Privacy*. https://doi.org/10.1002/spy2.131

Gupta, B. B., & Quamara, M. (2018). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience, 32*(21), e4946. https://doi.org/10.1002/cpe.4946

Gupta, B. B., Quamara, M., Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W., Hamam, H., Ahmad, T., Zhang, D., Karale, A., Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., & Eirug, A. (2021). A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 13*(19), https://doi.org/10.1145/3411764.3445148

Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy and Laws. *Internet of Things, 15*(1), 100420. https://doi.org/10.1016/j.iot.2021.100420

Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management, 62*(102442), 102442. https://doi.org/10.1016/j.ijinfomgt.2021.102442

Kumar, N., Madhuri, J., & ChanneGowda, M. (2017). Review on security and privacy concerns in Internet of Things. *2017 International Conference on IoT and Application (ICIOT)*. https://doi.org/10.1109/iciota.2017.8073640

Lee, A.-R. (2021). Investigating the Personalization–Privacy Paradox in Internet of Things (IoT) Based on Dual-Factor Theory: Moderating Effects of Type of IoT Service and User Value. *Sustainability, 13*(19), 10679. https://doi.org/10.3390/su131910679

Lee, C., & Ahmed, G. (2021). Improving IoT Privacy, Data Protection and Security Concerns. *International Journal of Technology, Innovation and Management (IJTIM), 1*(1), 18–33. https://doi.org/10.54489/ijtim.v1i1.12

Lee, H. (2020). Home IoT resistance: Extended privacy and vulnerability perspective. *Telematics and Informatics, 49,* 101377. https://doi.org/10.1016/j.tele.2020.101377

Mishra, S., & Tyagi, A. K. (2022). The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications. *Internet of Things,* 105–135. https://doi.org/10.1007/978-3-030-87059-1_4

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review, 38*(38), 100312. https://doi.org/10.1016/j.cosrev.2020.100312

Ons Aouedi, Vu, T.-H., Sacco, A., Nguyen, D. C., Kandaraj Piamrat, Marchetto, G., & Pham, Q.-V. (2024). A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions. *IEEE Communications Surveys & Tutorials,* 1–1. https://doi.org/10.1109/comst.2024.3430368

Panalangin, M. L., Mantikayan, J. M., Abdulgani, M. A., & Mohamad, H. A. (2024). Integration of Iot-Knowledge-Based Architecture in the Development of the Daily Time Records System for the Ministry of Science and Technology, Philippines. *American Journal of Innovation in Science and Engineering, 4*(1), 9–20. https://doi.org/10.54536/ajise.v4i1.3947

Princi, E., & Krämer, N. C. (2020). Out of Control – Privacy Calculus and the Effect of Perceived Control and Moral Considerations on the Usage of IoT Healthcare Devices. *Frontiers in Psychology, 11*. https://doi.org/10.3389/fpsyg.2020.582054

Salama, R., Al-Turjman, F., Chaudhary, P., & Yadav, S. P. (2023, April). (Benefits of Internet of Things (IoT) Applications in Health care-An Overview). In *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)* (pp. 778-784). IEEE.https://doi.org/10.1109/cictn57981.2023.10141452

Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W., & Hamam, H. (2022). The Rise of "Internet of Things":

Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks. *Wireless Communications and Mobile Computing, 2022*(1), 1–12. https://doi.org/10.1155/2022/8669348

Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M. H., & Lim, J. (2020). Security, Privacy and Trust for Smart Mobile- Internet of Things (M-IoT): A Survey. *IEEE Access, 8*, 167123–167163. https://doi.org/10.1109/ACCESS.2020.3022661