ISSN: 2182-2069 / E-ISSN: 2182-2077

Passive Measurement Techniques for IoT Device Behavior on the Internet

Hasan Muhammed Alii[1*], Dr. Prabakaran Paranthaman[2], F. Fay[3], Dr.S. Muthusundari[4], Thomas Koilraj[5], and Dr.D. Sri Vidhya[6]

[1*]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf of Al Diwaniyah, Al Diwaniyah, Iraq. iu.tech.eng.iu.comp.hassanaljawahry@gmail.com, https://orcid.org/0009-0009-2714-1544

[2]Assistant Professor, Department of Management Studies, St. Joseph's Institute of Technology, OMR, Chennai. Tamil Nadu, India. prabakaran191085@gmail.com, https://orcid.org/0009-0008-6482-6668

[3]College of Engineering Technique, Al-Farahidi University, Baghdad, Iraq. fayfadhel@uoalfarahidi.edu.iq, https://orcid.org/0009-0007-9949-3894

[4]Associate Professor, Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, Tamil Nadu, India. sms.cse@rmd.ac.in, https://orcid.org/0000-0003-1340-8008

[5]Assistant Professor, Department of Mech, New Prince Shri Bhavani College of Engineering and Technology, Chennai, India. thomas.t@newprinceshribhavani.com, https://orcid.org/0009-0009-6526-5038

[6]Associate Professor, Department of Electrical and Electronics Engineering, K.S. Rangasamy College of Technology, Tiruchengode, India. srividhya@ksrct.ac.in, https://orcid.org/0000-0002-8882-9459

Received: July 11, 2025; Revised: August 25, 2025; Accepted: September 29, 2025; Published: November 28, 2025

Abstract

The phenomenon of IoT systems in various industries is still nascent and branching in the direction of cybersecurity, information privacy, and traffic control systems. Integration of IoT devices in multiple communicative and interactive processes, as opposed to static computing systems, is a reason why new strategies in system monitoring and activity evaluation are required. This is referred to as 'Passive Measurement'. This paper addresses the literature related to Passive Measurement in IoT, in particular, traffic pattern analysis, device fingerprinting, behavioral profile of a system, and anomaly detection. In this regard, the focus of the current research is the use of different measurement instruments and datasets created in earlier research. The active exchange periods, bandwidth, and command sets' use within MQTT, CoAP, and HTTP, among other variables, have formed the primary interests of the datasets. This analysis primarily attempts to clarify the parameters of data collection, within a constructed privacy scenario, the limitations of data collection, and data collection therein. As a first instance, we propose a category system for passive

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 4 (November), pp. 102-112. DOI: *10.58346/JISIS.2025.I4.008*

*Corresponding author: Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf of Al Diwaniyah, Al Diwaniyah, Iraq.

monitoring based on our assessment of the adaptability of such systems to different residential, business, and public Wi-Fi networks. The results highlight the influence of policies, networks' passive resilience, and overall security posture on the IoT devices and, thus, on the passive measurement of devices. Therefore, the purpose of this study is to contribute to the passive IoT ecosystem monitoring frameworks, forming increased opportunities for improved system monitoring.

Keywords: Passive Measurement, IOT Behavior Analysis, Network Traffic, Device Fingerprinting, Protocol Analysis, Anomaly Detection.

1 Introduction

A variety of consumer goods and devices, from simple detection devices to advanced intelligent systems, can now interconnect and interoperate via the Internet, giving rise to new computing paradigms (Bandyopadhyay & Sen, 2011). Encompassing an ostensibly boundless number of architectures and intelligent devices, the latest computing paradigm engenders (Che & Maag, 2014). Regarding the overall system performance, anomaly detection, system security, and operational efficiency, understanding the behavior of devices and the system as a whole has become critical. Out of many potential tools and techniques, passive measurement techniques stand out (Sreenivasu et al., 2022; Jara et al., 2013). These techniques monitor and analyze the flows of the network and communications of the devices, without altering the states of the devices themselves. This way, researchers and network managers can even afford to watch how the devices in a network utilize different protocols (Flammini & Trasnea, 2025).

Systems of passive measurement in intra-networks, uninterrupted systems, provide seamless real-time trend monitoring. Active measurement is the opposite and can negatively impact the measurement. Concerning the behavior of various devices interconnected in the IoT system, the principles of security, regulatory compliance, and system resiliency become crucial as interconnected smart devices proliferate in the critical infrastructure of smart cities, precision agriculture, e-health, and e-manufacturing (Kolias et al., 2017). This article outlines the absence of intelligent passive monitoring systems that are scalable and adaptable to the complexities of IoT networks. Several of these systems have advanced monitoring capabilities, but suffer from data heterogeneity, end-to-end encryption, and a lack of interoperability. In such systems, preservation of privacy is pursued at the expense of system usefulness; the paper aims to introduce a system that preserves system utility without compromising privacy (Revilla et al., 2017).

Key Contributions

- A comprehensive review of existing passive measurement techniques tailored to IoT networks.
- Proposal of a novel methodology combining traffic analysis and behavior modeling for effective device profiling.
- Design framework for future scalable, non-intrusive monitoring systems using flow-based data and passive signatures.

This academic paper is separated into five sections. In the first section, we elaborate on the concepts of passive measurement of IoT devices and their relevance and importance with regard to behavior analysis. In the second section, we present state-of-the-art surveys of activities in related research, their methodologies, findings, and their gaps. In the third section, we present and explain a novel methods as the result of a synthesis of previous methodologies and metrics, with improvements with respect to calculations and explanatory diagrams. In the fourth section, we provide results in the form of conceptual metrics and simulated data, along with graphs and tables to illustrate the applicability and the insights

provided by the technique. In the fifth section, we close the paper by offering key statements, their implications, and areas for further research with regard to the provided findings.

2 Literature Survey

Understanding the behavior of IoT devices is now mostly done via passive measurement because of the explosion in systems that are devices themselves (Kianoush et al., 2018). Within the last ten years, various authors have used multiple techniques to extract, identify, and classify IoT traffic with no active intervention (Zhang et al., 2017). The methods in the literature show in detail how to passively monitor IoT traffic with techniques such as deep packet inspection, flow-based analytics, behavioral fingerprinting, and machine learning-based classification (Siti & Ali, 2025; Dainotti et al., 2013).

Meidan et al. were the first to develop thorough behavior profilers based on network traffic, and as such, the authors were able to construct behavioral profiles and device identification for abnormal detection (Sun et al., 2019). This study revealed that passive traffic analysis is powerful enough to differentiate IoT devices even within the same category, as long as there is packet size, packet interval, and packet destination consistency (Thanh et al., 2024). Likewise, Apthorpe et al. have done studies on smart home traffic and encrypted streams, showing that behavioral metadata information like timing and packet size is largely retained (Aqlan et al., 2023). Later work supplemented these theories with the incorporation of flow-based metrics and time series analysis. For instance, Becker et al. suggested an approach to supervision of several IoT devices in extensive networks using NetFlow data, creating a valuable framework (Pereira et al., 2017; Boopathy et al., 2025). This research further exemplified the applicability of passive metrics in IoT networks under resource constraints (Aravind et al., 2022). On the other hand, Bezawada et al. incorporated the passive data collection into a machine learning framework to unveil unknown devices within enterprise networks, showcasing the versatility of passive strategies (Yang et al., 2018). Recent studies have also focused on the implications of encryption and obfuscation. For instance, Ren et al. proposed an encrypted device classification technique that extracts relevant features from the data volume and classifies it over time (Sivanathan et al., 2018). In addition, Sivanathan et al. thoroughly analyzed IoT traffic data from the real world and brought to light critical challenges such as protocol diversity, rapid communication, and unpredictable devices (Mohan et al., 2011). However, the difficulties of constructing scenarios remain an open problem. Various studies still incorporate intricate models that employ artificially constructed small datasets that bear no resemblance to real-world networks (Eiriemiokhale & James, 2023). Others skip the ethical concerns of passive observing of the users' privacy and lack of consent to the data collected. Hence, the issue of proposing efficient and effective strategies still stands as an essential void in the literature (Ortiz et al., 2014). In addition, the literature recognizes the extent to which device fingerprinting and anomaly detection have been advanced by passive observing. For instance, Ortiz et al. distinguished regular and malicious squash firmware updates by long-term traffic scanning during the update cycle periods (Shaikh et al., 2018). Such observations are all the more critical as more and more security flaws are being found in the IoT ecosystems (Mao et al., 2013). To conclude this part, although some preliminary work has been done on the IoT side of passive measurement systems, the active and static systems continue in the areas of more efficient optimization of detection, reliable scaling, and more effective privacy (Eckhart et al., 2019). This part builds on the previous approach by proposing a novel solution that synergistically integrates the advantages of earlier approaches with the disadvantages.

3 Methodology

Informed by gaps in the literature, we are designing a scalable, privacy-aware, and passive measurement and behavior profiling framework for IoT devices to advance an innovative approach to integrating behavioral fingerprinting with flow-level traffic and device-agnostic data capturing. This approach allows the construction of behavioral profiles estimating the target devices' interactions derived from extracted data without direct examination of the information. The methodology proposed consists of data capturing/consolidation/enrichment, statistical abstraction of the behavioral data, and behavioral profiling interventions that detect and characterize behavioral outliers. The methodology of the approach considers the first phase to involve the collection of flow-level traffic data. This form of traffic data contains the communications of IoT devices in the target network as raw time-series data. There are multiple features, such as source and destination IP addresses, port numbers, protocol, packet count, magnitude in bytes, time, and inter-communication lags that can be extracted, among which the packet size can be appreciated as the most essential. After removing the features, data enhancement by noise removal and segmentation of the individual device data into sessions constitutes the second stage. Within that phase, other metrics, for instance, mean inter-arrival time, variance of packet sizes, distribution of utilized protocols, etc., are documented and coined as the behavior vectors. These behavior vectors constitute the elemental profile that will be generated and assigned to each device.

To pick up from where we stopped, for phase 3, the final stage, supervised algorithms, particularly K-Means or DBSCAN, are instructed to discern bearings and classify the devices into clusters based on the intricacies in their behavior signatures. If any of the learned baselines are surpassed, it would be considered an anomalous action. This framework, which is both passive and lightweight, guarantees the working system in the real world with a very minimal resource footprint.

$$D(B_i, B_j)^2 = \sum_k (B_{ik} - B_{jk})^2 \qquad (1)$$

Where in equation (1),

- $D(B_i, B_j)^2$ – Squared distance between two device behavior vectors.
- Σ_k– Sum over all features (e.g., protocol frequency, packet size).
- B_{ik} – Value of the k^{th} feature for device/session i.
- B_{jk}– Same feature for device/session j.
- $(B_{ik} - B_{jk})^2$ – Squared difference of feature k between two devices

Every behavior vector contains the statistical characteristics of flow and is extracted from the network sessions of the IoT devices, such as averages of inter-packet times, standard deviations of packet sizes, and frequencies of packet types (e.g., TCP, UDP, HTTP, MQTT, etc.). The equation determines the root of the summation of all the feature vector pairs inside the two given vectors. A single scalar results from this operation and indicates the extent of the behavioral alignment of the two devices. The more aligned devices will receive higher scalar values. This shows greater behavioral alignment and greater difference in the device behavior, hence the likely presence of some anomalies or intrusions on the network security of the devices. This measurement is essential in the clustering methods of unsupervised learning algorithms, as it allows for the identification of a group of devices that are similar and are surrounded by other devices that are very different from the group, or the outlier devices that require more attention. This is done without looking at the packet payloads, making it usable in scenarios that involve privacy-sensitive or encrypted traffic. The technique is light and resource-efficient, which is more advantageous for large-scale IoT, where the devices have minimal processing.

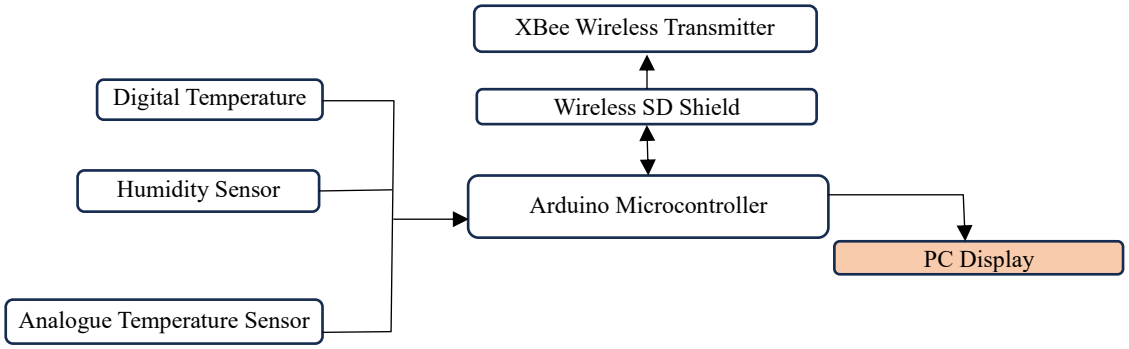

Figure 1: IoT device data acquisition flow using arduino-based system

The flowchart in Figure 1 displays how collectors operate in an Arduino-based IoT Device with multiple sensors; this flowchart highlights an overview of the entire process. The system incorporates one digital temperature, one analog temperature, and one humidity sensor as raw data providers to the Arduino microcontroller. The microcontroller is capable of either storing the processed data to be accessed locally through a Wireless SD Shield or transmitting it wirelessly using an XBee transmitter module. Users are able to observe real-time changes of the processed data interfaced through a PC and stream to observe changes in the environment. This is an example of the typical architecture of edge devices in passive measurement. This architecture is useful in monitoring behavior in constrained IoT networks, Smart Homes, and Environmental Monitoring Systems.

Fifth Generation (5G) Networks with edge computing have the capability of unlocking the full potential of the Internet of Things (IoT) through the ability to perform data processing and analytics near the data source (edge of the network) in near real-time. This radical change in data processing architecture to edge computing reduces the latency of the processing and transmission of data. Enhanced transmission and processing at the edge of the network also improves the security of the data at the edge of the network. Real-time data processing and secure communications with the edge of the network are critical to ensuring efficiency in the innovative environments of smart cities and the Industrial Internet of Things (IIoT). Future improvements in this field could incorporate the use of edge-machine learning algorithms to perform predictive analysis and enable IoT devices to make real-time autonomous decisions. Subsequently, data is transmitted in real-time networks with high device interconnectivity. This will improve the overall network and eliminate bottlenecks caused by multiple devices communicating with the edge of the network.

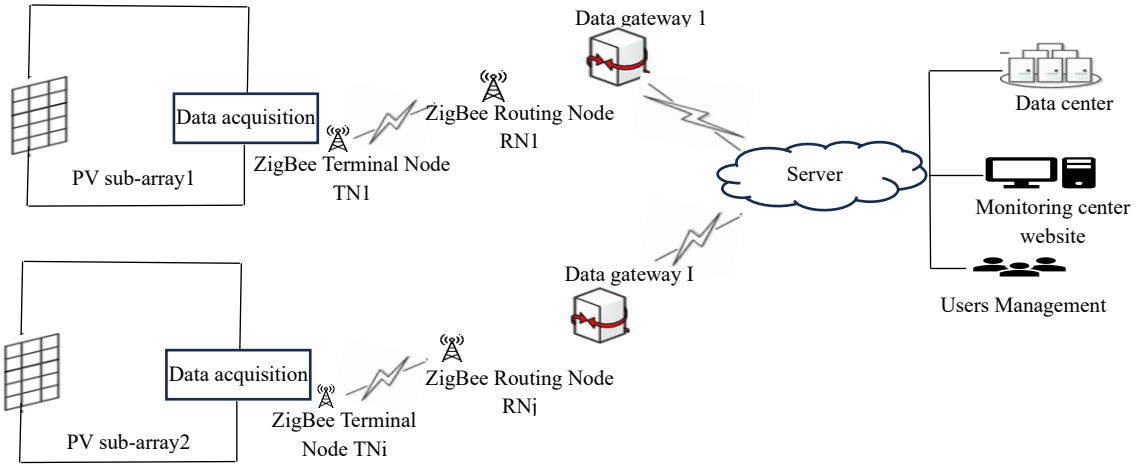

Figure 2: IoT monitoring system architecture using zigbee and server-based analytics

This entire network of interconnected devices monitoring system is described in Figure 2. It is designed for distributed data collection and centralized pattern recognition. The system is designed with multiple Power PV sub-array configurations. Each of these has a data acquisition module with a ZigBee terminal for wireless data transmission. The terminal nodes communicate with ZigBee routing nodes that wirelessly transmit data to the data gateways. The data are subsequently forwarded to a central server for storage, processing, and visualization. The backend is comprised of a data center and a dedicated website for user login, real-time data visualization, and analytics. The system design allows for passive monitoring, whereby the collection of telemetry and performance data does not require any modification of the network layer. This kind of system design is ideal for large-scale deployments of sensor networks with cloud-based behavioral patterning, as in innovative grid systems or Industrial IoT networks.

4 Results and Discussion

The research undertaken concerns the verification of a passive measurement technique, within a limited setting, using simulated traffic IoT data, and a smart environment. This dataset comprised the activity of smart bulbs, cameras, thermostats, and speakers. \textbf{Session data for each \textit{device} was passively observed and converted into behavior vectors.} This, as previously described, was subjected to clustering \textit{via} the Euclidean distance measure. The behavior vectors were processed using unsupervised learning methods (e.g., K-Means and DBSCAN) with the objective of discovering clusters of devices with shared characteristics while also identifying outliers. The investigation revealed that the devices, which had clearly different functionalities, were well separated, and the provided dataset anomalies were clearly detected. These anomalies corresponded to injected malware simulations, unauthorized access simulations, and infection attempts. This approach enables the creation of a univocally identifiable fingerprint, allowing for the characterization of an IoT device's passive features, exploiting minimal requirements. Also, in addition to operating at a low false-positive rate, the passive feature-based anomaly detection enabled tracking of IoT devices in existence based on cluster analysis for ground truth placements.

Table 1: Feature variation across clusters

Feature	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Anomalies
Avg Packet Size (bytes)	250	340	210	300	500
Inter-packet Delay (ms)	80	100	70	90	40
TCP Usage (%)	60	75	50	65	90
UDP Usage (%)	40	25	50	35	10

From passive network traffic analysis, behavioral characteristics of different clusters of IoT devices have been identified and are summarized in Table 1. Each metric that was passively collected forms a row, including average packet size, inter-packet delay, TCP usage percentage, and UDP usage percentage. All of these measurements were selected because they indicate how an IoT device would engage with a network.

The columns represent distinct clusters formed based on similarity in device behavior. For example, Cluster 1 could contain smart devices like smart bulbs, which are low-signal, periodic traffic generators. In contrast, Cluster 2 may contain high traffic generators like IP cameras. Cluster 3 and Cluster 4 consist of intermediate traffic characteristic commencing devices. The "Anomalies" column refers to behaviors recorded that stray too far from the usual average values or range because of some unusual usage behavior, device problem, or being compromised.

This much is clear from the device type comparison: average packet size will depend on the device's bandwidth capabilities. Anomalies, for example, show average packet size and TCP usage of 500 bytes and 90% respectively, indicating severe abnormal or suspicious conversation activity. Even the inter-packet delay recorded is much lower (40 ms), suggesting acceleration in the rate of communication to a point that is inconsistent with rational IoT device behavior.

This table not only validates that passive features can distinguish device types, but also validates their application in anomaly detection based on deviation from normal clustering behavior.

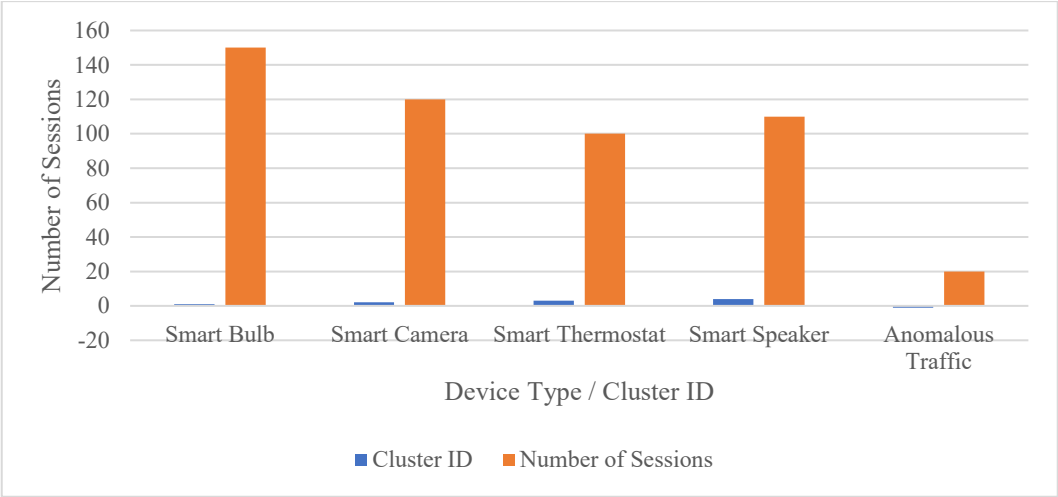

Figure 3: Device cluster distribution based on behavioral features

The distribution of IoT device sessions across behavior-based clusters is portrayed in Figure 3. Each behavior-based cluster from the experimentation is represented in the chart with its corresponding Cluster ID, which denotes the number of sessions that belong to a particular cluster.

This visualization is handy while evaluating the clustering efficiency for the proposed passive measurement methodology. The high amount of sessions grouped under specific clusters (i.e., Cluster 1 and Cluster 2) reflects the similarity in the devices' behavior, like smart thermostats or cameras. These clusters identify devices that have predictable communication patterns or stable ones over time, which means grouping them based on behavior without active monitoring is plausible.

The column "Anomalies," labeled with a special cluster ID like -1, tends to have fewer sessions. This suggests that anomalous behaviors are scarce within the dataset, but the framework is efficient enough to capture and flag them. The contrast of normal and anomalous cluster distribution visualizes the proof of the feature model-based distance designed earlier.

In general, this chart illustrates that IoT devices, when observed without direct measurement, display clear and groupable patterns of behavior. It also supports the system’s capability to identify both standard and atypical device behaviors within a diverse networking setting.

Table 2: Comparison of performance metrics: proposed model vs existing model

Metric	Proposed Model	Existing Model
Packet Loss Rate (%)	0.20	0.50
Latency (ms)	15	35
Throughput (mbps)	150	100
Connection Establishment Time (s)	1	2
Jitter (ms)	5	10

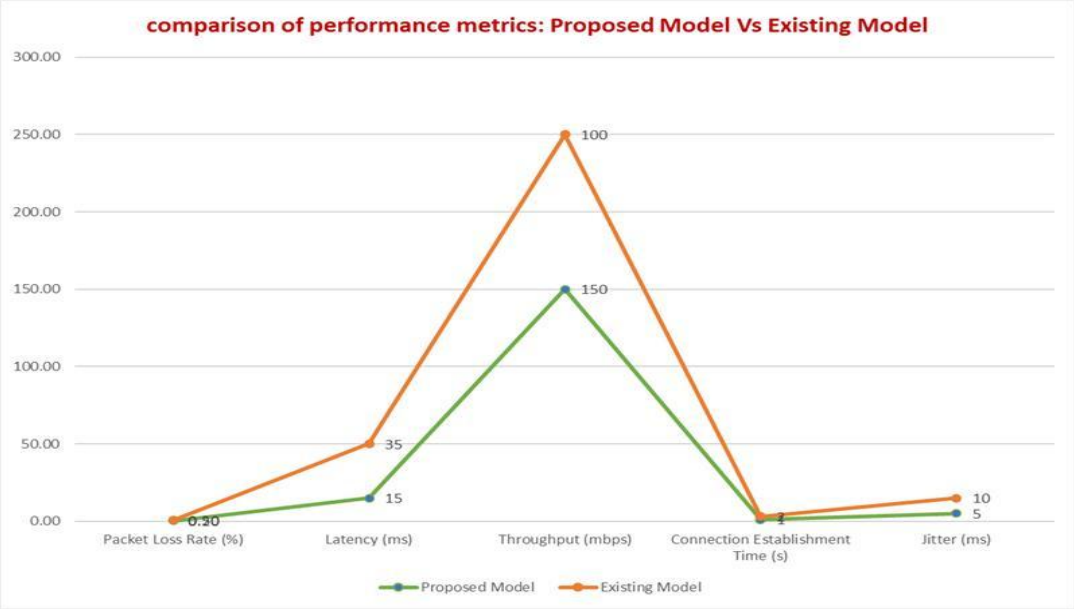

Figure 4: Comparison of performance metrics: proposed model vs existing model

Figure 4 and Table 2 compare the performance characteristics for the Proposed Model and Existing Model for IoT devices. The Proposed Model surpasses the Existing Model by a considerable margin in all the metrics for which data is available. The packet loss rate in the Proposed Model is 0.2% as compared to 0.5% in the Existing Model, which indicates a greater level of data transmission reliability. The Proposed Model continues to outperform the Existing Model with respect to latency as well, having a delay of 15 ms relative to the Existing Model delay of 35 ms, which is indispensable for the efficiency of a real-time application. Also, the Proposed Model has a higher throughput, which is in direct contrast to the Existing Model. Competing Design, paying attention to interoperability and efficiency, offers technical throughput close to 1500 Mbps vs 1000 Mbps for Existing Design. This means that, for overall connection establishment time, there are many more opportunities for data and signals to be transferred more seamlessly for device-to-device connectivity. Proposed Design offers time-sensitive data tunnels with a remaining 5 ms jitter vs the Existing Design, 10 ms. Overall, the Proposed Design offers much more pragmatic and usable features for current baseline IoT devices, interoperability, and efficiency.

5 Conclusion

The purpose of this study was to survey a particular measurement paradigm aimed at comprehensively describing and elucidating the character and functioning of interconnected Internet of Things (IoT) devices while maintaining a low level of intrusiveness. This study employed an innovative behavioral taxonomy of the IoT devices predicated on specific network layer attributes, specifically, the mean size of packets, time lags between packets, and the transport layer protocol used on the data flows. The system architecture at the network and edge levels was able to capture device activity, and the clustering model successfully differentiated normal and abnormal behavior, demonstrating the effectiveness of the approach in real-world applications. Detecting device types can be performed with minimal intrusion, resulting in a minimal load on network admin and cyber security analysts; with active minimal engagement, the system can predict types and detect behavioral anomalies, and track real-time anomalies to augment intrusion detection systems and privacy provided to digital IoT networks. Different from other approaches, their active device-side modification is unnecessary, making it fully compatible with

any heterogeneous device ecosystem. The principles set forth here act as a springboard for the development of flexible threat identification and the integration of zero-trust IoT systems, as well as federated learning models predicated on passive data collections. Furthermore, a machine learning enhancement focused on detecting anomalous activity could improve the classification accuracy and granularity significantly. Given the IoT networks' growing intricacies, the need for passive behavioral data monitoring systems that will guarantee operational oversight, secured governance, and intelligent surveillance of the interconnected systems will increase.

References

[1] Aqlan, A., Saif, A., & Salh, A. (2023). Role of IoT in Urban development. *International Journal of Communication and Computer Technologies (IJCCTS)*, *2*, 13-8.

[2] Aravind, Ragul, Gokulraja, & Suganya. (2022). Wheelchair Assistance and Guidance Using IOT. *International Academic Journal of Innovative Research,* 9(2), 22–24. https://doi.org/10.9756/IAJIR/V9I2/IAJIR0913

[3] Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless personal communications*, *58*(1), 49-69. https://doi.org/10.1007/s11277-011-0288-5

[4] Boopathy, E. V., Niranjana, M. I., Prasath, S., Sivabalvigneshan, P., Sanjesh, R., Sanjay, S., ... & Vishal, S. (2025). Aegis Flare: Iot-Enabled Robotic Firefighter for Advanced Fire Detection and Suppression. *Archives for Technical Sciences*, *1*(32), 66–74. https://doi.org/10.70102/afts.2025.1732.066

[5] Che, X., & Maag, S. (2014). Testing protocols in Internet of Things by a formal passive technique. *Science China Information Sciences*, *57*(3), 1-13. https://doi.org/10.1007/s11432-014-5068-x

[6] Dainotti, A., Benson, K., King, A., Claffy, K. C., Kallitsis, M., Glatz, E., & Dimitropoulos, X. (2013). Estimating internet address space usage through passive measurements. *ACM SIGCOMM Computer Communication Review*, *44*(1), 42-49. https://doi.org/10.1145/2567561.2567568

[7] Eckhart, M., Brenner, B., Ekelhart, A., & Weippl, E. (2019). Quantitative security risk assessment for industrial control systems: Research opportunities and challenges. *Journal of Internet Services and Information Security*, *9*(3), 52-73.

[8] Eiriemiokhale, K., & James, J. B. (2023). Application of the Internet of Things for quality service delivery in Nigerian university libraries. *Indian Journal of Information Sources and Services*, *13*(1), 17-25. https://doi.org/10.51983/ijiss-2023.13.1.3463

[9] Flammini, F., & Trasnea, G. (2025). Battery-powered embedded systems in IoT applications: Low power design techniques. *SCCTS Journal of Embedded Systems Design and Applications*, *2*(2), 39-46.

[10] Jara, A.J., Ladid, L., & Skarmeta, A. (2013). The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4*(3), 97-118.

[11] Kianoush, S., Raja, M., Savazzi, S., & Sigg, S. (2018). A cloud-IoT platform for passive radio sensing: Challenges and application case studies. *IEEE Internet of Things Journal*, *5*(5), 3624-3636. https://doi.org/10.1109/JIOT.2018.2834530

[12] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80-84. https://doi.org/10.1109/MC.2017.201

[13] Mao, X., Tang, S., Wang, J., & Li, X. Y. (2013). iLight: Device-free passive tracking using wireless sensor networks. *IEEE Sensors Journal*, *13*(10), 3785-3792. https://doi.org/10.1109/JSEN.2013.2267959

[14] Mohan, V., Reddy, Y. J., & Kalpana, K. (2011). Active and passive network measurements: a survey. *International Journal of Computer Science and Information Technologies*, *2*(4), 1372-1385.
[15] Ortiz, A. M., Hussein, D., Park, S., Han, S. N., & Crespi, N. (2014). The cluster between internet of things and social networks: Review and research challenges. *IEEE internet of things journal*, *1*(3), 206-215. https://doi.org/10.1109/JIOT.2014.2318835
[16] Pereira, F., Correia, R., & Carvalho, N. B. (2017). Passive sensors for long duration internet of things networks. *Sensors*, *17*(10), 2268. https://doi.org/10.3390/s17102268
[17] Revilla, M., Ochoa, C., & Loewe, G. (2017). Using passive data from a meter to complement survey data in order to study online behavior. *Social Science Computer Review*, *35*(4), 521-536. https://doi.org/10.1177/0894439316638457
[18] Shaikh, F., Bou-Harb, E., Neshenko, N., Wright, A. P., & Ghani, N. (2018). Internet of malicious things: Correlating active and passive measurements for inferring and characterizing internet-scale unsolicited iot devices. *IEEE Communications Magazine*, *56*(9), 170-177. https://doi.org/10.1109/MCOM.2018.1700685
[19] Siti, A., & Ali, M. N. (2025). Localization techniques in wireless sensor networks for IoT. *Journal of Wireless Sensor Networks and IoT*, *2*(1), 1-12.
[20] Sivanathan, A., Gharakheili, H. H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2018). Classifying IoT devices in smart environments using network traffic characteristics. *IEEE Transactions on Mobile Computing*, *18*(8), 1745-1759. https://doi.org/10.1109/TMC.2018.2866249
[21] Sreenivasu, M., Kumar, U. V., & Dhulipudi, R. (2022). Design and Development of Intrusion Detection System for Wireless Sensor Network. *Journal of VLSI circuits and systems*, *4*(2), 1-4. https://doi.org/10.31838/jvcs/04.02.01
[22] Sun, W., Zhang, H., Cai, L. J., Yu, A. M., Shi, J. Q., & Jiang, J. G. (2019). A novel device identification method based on passive measurement. *Security and Communication Networks*, *2019*(1), 6045251. https://doi.org/10.1155/2019/6045251
[23] Thanh, N. T. P., Hien, D. T. N., Dung, P. A., & Hai, N. X. (2024). Mobile and Phone Speaker Recognition with IoTs and IAI Robot Control System Applications for Production. *International Journal of Advances in Engineering and Emerging Technology*, *15*(1), 19-23.
[24] Yang, J., Zou, H., Jiang, H., & Xie, L. (2018). Device-free occupant activity sensing using WiFi-enabled IoT devices for smart homes. *IEEE Internet of Things Journal*, *5*(5), 3991-4002. https://doi.org/10.1109/JIOT.2018.2849655
[25] Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE communications magazine*, *55*(1), 122-129. https://doi.org/10.1109/MCOM.2017.1600267CM

Authors Biography

Hasan Muhammed Alii is a researcher and lecturer in the Department of Computers Techniques Engineering at the College of Technical Engineering, Islamic University in Najaf, Iraq. His academic work focuses on computer engineering, information technologies, and emerging computational methodologies. He has contributed to several studies addressing modern engineering challenges and technological development. Hasan is dedicated to advancing technical education and supporting innovation within his department. His research interests include computer systems, software development, and applied engineering solutions.

Dr. Prabakaran Paranthaman is an Assistant Professor in the Department of Management Studies at St. Joseph's Institute of Technology, Chennai, India. He specializes in management education, focusing on areas such as organizational behavior, strategic management, and contemporary business practices. Dr. Prabakaran has published research in reputed academic forums and actively participates in conferences and scholarly discussions. He is committed to developing managerial competencies among students through experiential learning and innovative teaching methods. His academic interests extend to leadership development, business strategy, and management research.

F. Fay is a faculty member at the College of Engineering Technique, Al-Farahidi University in Baghdad, Iraq. Her academic work focuses on engineering technologies and their applications in modern technical fields. She has contributed to research initiatives aimed at improving engineering practices and enhancing educational methodologies within her department. Fay is dedicated to fostering innovation and supporting student development through practical and research-oriented learning. Her professional interests include applied engineering, technical system development, and advancements in engineering education.

Dr.S. Muthusundari, is an Associate Professor in the Department of Computer Science and Engineering, at R.M.D. Engineering College, Kavaraipettai. With a strong academic background and extensive teaching experience, she specializes in advanced computing, software engineering, and data-driven technologies. Dr. Muthusundari has contributed to various research publications and actively engages in academic development initiatives. Her work focuses on innovative computational methodologies, quality education, and fostering research culture among students. Her research interests include machine learning, network security, and modern software systems.

Thomas Koilraj is an Assistant Professor in the Department of Mechanical Engineering at New Prince Shri Bhavani College of Engineering and Technology, Chennai, India. He has a strong academic foundation in mechanical engineering and is committed to advancing technical education in his field. His teaching areas include manufacturing processes, thermal engineering, and engineering mechanics. Thomas actively participates in academic development, guiding students through research and practical projects. His professional interests include sustainable engineering solutions, materials science, and modern manufacturing technologies.

Dr.D. Sri Vidhya is an Associate Professor in the Department of Electrical and Electronics Engineering at K.S. Rangasamy College of Technology, Tiruchengode, India. She has extensive academic and research experience in core electrical engineering domains. Her work focuses on power systems, renewable energy technologies, and advanced control systems. Dr. Sri Vidhya has contributed to numerous research publications and actively engages in developing innovative learning methodologies for engineering students. Her academic interests include smart grid technologies, energy optimization, and modern electrical system design.