Volume 12, No.9, September 2025

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

RESEARCH PAPER

Available online at http://www.jgrma.com

A SURVEY OF IOT COMMUNICATION PROTOCOLS FOR NETWORK TRAFFIC ANALYSIS IN CLOUD ENVIRONMENTS

Mr. Himanshu Barhaiya [1]

[1] Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Bhopal
himanshub@lnct.ac.in

Abstract: Intelligent and data-driven ecosystems have been created by the Internet of Things (IoT), which has revolutionized modern industries through the seamless connectivity of billions of devices and their integration with cloud computing environments. However, this convergence introduces significant challenges in network traffic analysis, scalability, resource optimization, and cybersecurity. This research study offers a thorough analysis of the protocols for Internet of Things communication and how they affect the behavior of traffic in cloud-integrated settings. Classifying protocols according to their power consumption, it examines the unique traffic patterns of popular protocols like HTTP, CoAP, and MQTT, and then divides them into LPWAN and short-range networks. To further improve performance and decrease latency, this study investigates traffic optimization methods, energy-aware tactics, and the integration of fog and edge computing. Machine learning (ML), deep learning (DL), and forensic methods have made great strides in improving security, monitoring traffic, and detecting anomalies, according to a comprehensive literature analysis. The results show that cybersecurity, energy efficiency, and scalability in IoT-cloud ecosystems are greatly enhanced when AI-driven traffic optimization is combined with lightweight communication protocols. Supporting safe, adaptable, and intelligent IoT-cloud infrastructures, this study also identifies important research gaps and suggests future possibilities, such as creating standardized datasets, real-time anomaly detection frameworks, and cross-protocol traffic optimization algorithms.

Keywords: Internet of Things (IoT), Communication Protocols, Cloud Environments, Network Traffic Analysis, Anomaly Detection

1. INTRODUCTION

In today's highly connected digital world, the interaction between devices, systems, and services has been revolutionized by the exponential growth of available technology. Out of all these innovations, the Internet of Things (IoT) has been a game-changer, allowing for the seamless connection of billions of smart devices in fields as diverse as smart cities, transportation, agriculture, healthcare, and industrial automation. By integrating sensors, embedded systems, and wireless communication technologies [1], IoT devices autonomously collect, process, and exchange vast volumes of data, enabling intelligent and data-driven decision-making. As these interconnected systems expand, communication protocols have become the foundation for ensuring seamless interaction and efficient data transmission across heterogeneous environments.

This technological revolution has increased in size a lot because of the combination of IoT and cloud computing, which has resulted in highly scalable and intelligent ecosystems. Cloud computing is able to store extensive amounts of sensor-generated data, provide extensive computing capabilities and real-time analytics that enable IoT environments to process extensive amounts of sensor-generated data effectively [2]. However, this constant stream of information between the IoT and the cloud servers creates serious concerns in the management of network traffic. Monitoring traffic behaviour, analysis and optimization is to deliver high system performance, low latency and reliability. At this point, the effectiveness of traffic analysis in cloud-integrated IoT environments directly depends on the selection and the deployment of proper communication protocols.

Regardless of the developments, IoT-Cloud ecosystems are increasingly becoming worried about the problem of security and data privacy. The nature of communication standards, alongside resource-limited IoT controlling devices and massive deployments, presents a number of vulnerabilities that can be exploited by hackers [3]. Inequality of security systems and lack of standardisation of updates, and the lack of sufficient authentication systems, continue to expose IoT architectures to cyber-attack. As a solution to these problems, effective and sensitive communication channels should be established in a position to facilitate both reliable data flow and adequate analysis of the network traffic to identify threats and avoid irregularities [4].

A number of communication protocols such as MQTT, CoAP, AMQP, HTTP/HTTPS, LoRaWAN and ZigBee are in the middle of facilitating the integration of IoT and Clouds [5][6]. Each protocol has its objectives and it balances between latency, scale, energy consumption and security. These differences create unique traffic streams, and it is necessary to know protocol-specific features to create an effective analytical framework.

Investigating the interplay of communication protocols and traffic behavior in cloud-based IoT environments [7], researchers and practitioners can tackle challenges related to performance [8], scalability, and security. This kind of knowledge is the foundation of the creation of robust, efficient and secure IoT- Cloud ecosystems that can serve the future generation of intelligent and autonomous applications.

1.1 Structured of the paper

The paper is structured in the following way, Section II presents IoT communication protocols and their applicability to cloud environments. Section III explores network traffic analysis in IoT systems, while Section IV examines protocol-specific traffic behaviors and optimization strategies. Section V reviews recent literature on IoT traffic, security, and anomaly detection techniques. Finally, Section VI presents the conclusion and outlines potential future research directions.

2. COMMUNICATION PROTOCOLS IN IOT SYSTEMS

Communication protocols are predefined rules and standards that enable seamless data exchange between devices in a network. In IoT systems, these protocols ensure reliable connectivity, data integrity, and interoperability among heterogeneous devices. Various Internet of Things (IoT) communication protocols can provide optimal security for data exchanged between IoT-connected devices [9][10]. Whereas protocols encrypt data passing, platforms make it combinable with other information to use it. The IoT platform plays a crucial role in delivering business value by linking IoT endpoints with applications and analytics. It serves as the core of an IoT solution [11], enabling the data collected from devices to be processed and effectively utilized by end-users.

2.1 Roles and Types of IoT Platforms

The IoT platforms are at the core of the IoT system, ensuring connectivity, processing, and integration of devices, as well as coordination of services. They offer the foundational requirements of tools and interfaces, whether open or closed source, that enable secure, scalable, and efficient communication between devices, users, and enterprise systems. The platforms also condone important operations such as device management, data analytics [10]and system interoperability to facilitate the development and application of IoT systems within organizations. There are two major types of IoT platforms, which are as follows:

2.1.1 Closed Source Platform

Closed-source IoT platforms are primarily developed by major IT companies as extensions of their existing cloud services and are typically offered in the form of SaaS or PaaS. For instance, Ericsson’s IoT Accelerator, based on the PaaS model, is designed for business partners by providing features such as connectivity, security, APIs, and user management [11]. It supports multiple protocols, including REST, AMQP, CoAP, and LWM2M, and seamlessly integrates with enterprise IT systems through service buses.

2.1.2 Open-Source Platform

Open-source IoT platforms are comparatively fewer in number than closed-source solutions, yet several notable options are available. For a more comprehensive evaluation, the analysis extended beyond official documentation and surveys to include source code review and local installation on a Linux-based environment. This approach enabled the assessment of additional aspects unique to open-source platforms, such as installation procedures and the quality of documentation [12]. Table 1 compares and contrasts open-source and closed-source software systems.

Table 1 Comparison of Closed-Source and Open-Source IoT Platforms

Aspect	Closed Source	Open Source
Ownership	Proprietary (e.g., Ericsson)	Community or organization-driven
Deployment	SaaS/PaaS	Self-hosted
Customization	Limited	Highly flexible
Protocol Support	REST, AMQP, CoAP, LWM2M	Varies, generally adaptable
Integration	Enterprise-ready via service buses	May require manual setup
Source Access	Not available	Fully accessible
Evaluation	Feature-based	Code review and real installation
Support	Vendor-backed	Community-based

2.2 IoT Communication Protocols

IoT communication protocols enable seamless data transmission between interconnected devices [13]. LPWANs and Short-Range Networks are the two primary classes of these protocols, as shown in Figure 1.

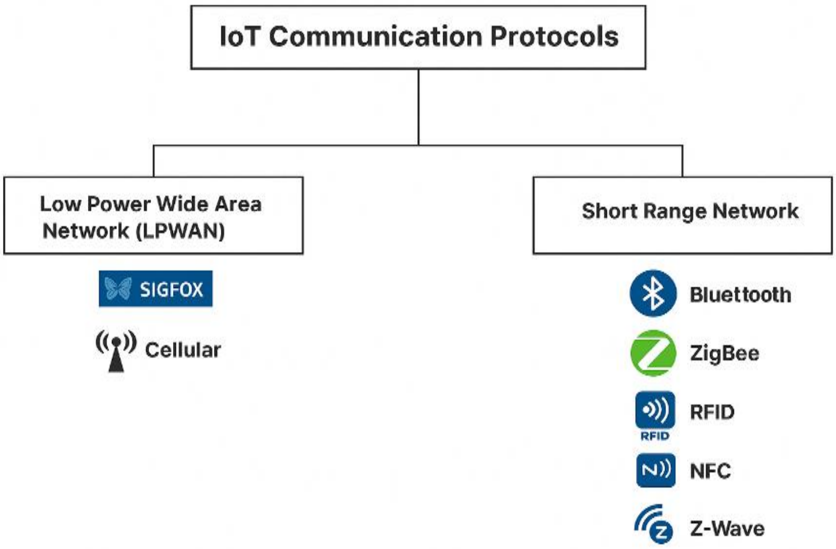
IoT Communication Protocols
Low Power Wide Area Network (LPWAN)
Short Range Network
SIGFOX
Cellular
Bluetooth
ZigBee
RFID
NFC
Z-Wave

Figure. 1: IoT communication protocols

2.3.1 Low Power Wide Area Network (LPWAN)

LPWAN is ideal for IoT settings because it offers a long-range communication solution with little bandwidth and power usage [14]. Some important technologies under LPWAN, along with their maturity levels and current challenges, are described as follows:

- **Sig Fox:** An energy-efficient communication protocol developed for sparse IoT uses, Sig Fox [15]. It is effectively utilized in scenarios such as remote monitoring, smart purchasing, and tracking smart devices.
- **Cellular:** Cellular networks also support IoT-based communication; however, traditional cellular technologies were originally designed for high-power devices [16]. Recent advancements have introduced optimized cellular LPWAN solutions that better meet the specific demands of IoT systems.

2.3.2 Short Range Network

Short-range networks play a crucial role in enabling efficient communication among smart devices while maintaining low power consumption [17]. Several widely used protocols fall under this category, as follows:

- 6LoWPAN: 6LoWPAN supports low-cost, low-power IPv6 communications over the IEEE 802.15.4 standard [18], making it ideal for low-data IoT applications.
- Bluetooth Low Energy: An energy-efficient short-range communication protocol, Bluetooth Low Energy (BLE) was launched as part of Bluetooth 4.0 [19] and has since been widely used in IoT devices.
- ZigBee: ZigBee is a reliable IoT protocol with a maximum range of up to 200 meters. It provides enhanced security features [20] and covers nearly twice the range of standard Bluetooth connectivity.
- Radio Frequency Identification: Radio-frequency identification (RFID) is an automatic identifying technology [21] that works well in Internet of Things (IoT) settings for tracking items, retrieving information, and managing data.
- Near-Field Communication: Near Field Communication (NFC) is an RFID-based, short-range wireless technology. It facilitates secure data exchange between two nearby devices within a few centimeters.
- Z-Wave: One popular wireless protocol for home automation systems is Z-Wave. It avoids signal interference by utilizing a dedicated radio frequency, ensuring stable and reliable connectivity.

3. NETWORK TRAFFIC ANALYSIS IN IOT

Network traffic is the flow of data packets within a network. This includes communication amongst the networked devices in the form of requests, responses, sensor information, multimedia information and control data. Network Traffic Analysis (NTA) is a key to understanding how systems behave in the Internet of Things (IoT) [22], resource management, and secure communication. As billions of heterogeneous devices produce huge data, traffic pattern monitoring and analysis identify traffic anomalies, regulate bandwidth, and ensure a dependable connection [23]. In contrast to traditional networks, IoT traffic is small, heterogeneous, and is frequently limited by a set of unproductive resources, which presents its own problems. Not only is effective NTA a performance improvement, but it also provides protection against threats, including denial-of-service assaults, data breaches, and unauthorized access, and is an essential element in the contemporary IoT setting.

3.1 Importance of traffic analysis in IoT systems

Network traffic analysis (NTA) is vital in the interpretation of the IoT device behavior, data safety and aids in digital forensics. Through this analysis, the researchers will be able to identify vulnerabilities, strange behaviors, and security threats by comparing communication among the IoT devices, the cloud systems, and the mobile applications connected with the security system. Table 2 illustrates the inter-relationship of devices in a smart home network with the details of the device categories, MAC address, and IP address, which may be useful in investigating the traffic patterns and possible security threats. NTA can also be used to give useful information on device activities in forensic contexts and assist in investigation of an incident [24].

- Network traffic can be one of the primary sources of post-event investigation evidence as it can be used to recreate the actions taken by both IoT devices and their users.
- The metadata associated with the packets (e.g., packet size, frequency of flows, destination addresses, data storage locations) can be of great forensic importance even in the case of encrypted communication.
- The universal nature of the IoT infrastructures in different jurisdictions may make gathering of evidence more difficult because international laws and privacy rules vary.
- The investigators have to reconcile the technical examination and legal requirements, which may have to work with national borders.
- The increasing complexity of IoT systems highlights the necessity of standard forensic models and harmonized laws that will serve as a strong tool in forensic network traffic analysis.

3.2 Traffic characteristics of different IoT protocols

IoT environments have a very diverse traffic behavior because various communication protocols are designed with different principles and operational needs [25]. It is possible to examine these features in three complementary perspectives:

- Server-level properties, which encompass the type of remote servers to which the IoT devices are connected, i.e. cloud platform, gateways or edge nodes.
- Flow-level properties, which characterize the traffic patterns, such as the duration of a session, the frequency of data transfer, throughput, and intervals of communication.
- Packet-level properties, which involve factors such as packet size distribution, transmission overhead, and protocol-specific encoding mechanisms.

Understanding these characteristics is crucial for optimizing resource allocation, enhancing quality of service (QoS), improving security, and developing effective traffic management strategies in IoT-cloud environments

Table 2 Connected Devices in Smart Home Network

Device	Alias Name	Category	MAC Address	IP Address
Logitech Circle-2	Cam1	IoT	44:73: D6:0C:36:AD	192.168.1.158
	Cam2		44:73: D6:09:BD:C9	192.168.1.186
Wyze Cam	Cam3		2C:AA:8E:95:F3:18	192.168.1.228
Eufy Indoor Cam	Cam4		8C:85:80:38:98:AF	192.168.1.182
Eufy Pan and Tilt	Cam5		8C:85:80:3A:12:B4	192.168.1.131
LittleElf Cam	Cam6		0C:8C:24:61:50:29	192.168.1.168
Epicka Smart Plug	Plug1		DC:4F:22:0E:C6:36	192.168.1.127
Amazon Smart Plug	Plug2		F8:54:B8:25:AA:C9	192.168.1.204
Smart Bulb	Bulb		84:0D:8E:7F:4B:B4	192.168.1.207
HP Envy Printer	Printer		94:57:A5:0C:5B:66	192.168.1.248
HP Elitebook	Laptop1	non-IoT	AC:FD:CE:01:7C:9B	192.168.1.105
HP ZBook	Laptop2		CC:2F:71:3B:0E:DE	192.168.1.247
Apple iPhone X	iPhone		34:08:BC:DE:E9:7E	192.168.1.203
Apple iPad	iPad		E8:8D:28:14:82:30	192.168.1.125
Samsung S20	Android		16:05:DD:78:5F:20	192.168.1.215

3.3 Network traffic monitoring and anomaly detection in IoT

IoT Network traffic monitoring consists of examining the information flowing among devices, gateways and cloud platforms to identify system performance, reliability and security. Traffic patterns are diverse as a result of the variety of IoT protocols: MQTT, CoAP, HTTP, TCP/IP, and so forth, which complicates monitoring. This is combined with cloud analytics and machine learning to automatically identify irregularities and enhance the performance of the network, using techniques like packet sniffing, flow analysis, deep packet inspection, and metadata-based strategies [26]. It is especially important to detect abnormal traffic patterns in areas like education and agriculture, where related devices produce vast amounts of data [27]. Improved methods of detecting anomalies can be used to avert malevolent behavior, protect data integrity, and ensure the reliability of applications based on the IoT.

4. PROTOCOL-SPECIFIC TRAFFIC BEHAVIOR IN CLOUD ENVIRONMENTS

The communication between IoT devices and cloud infrastructures presents major challenges as it can consist of heterogeneous communication protocols, various traffic patterns, and resource-constrained devices. Unlike conventional Internet traffic, IoT traffic is typically low-volume, intermittent, and protocol-specific, making modeling and monitoring complex. These variations affect network performance, QoS, energy efficiency, and security, increasing risks such as privacy breaches and DoS attacks (e.g., the Mirai botnet). To address these challenges, researchers analyze the protocol-specific behavior and develop traffic optimization strategies.

4.1 Case-wise Analysis of Popular Protocols

Essential to the efficacy of communication in IoT-cloud ecosystems is the criteria used in selecting the protocol, given that each protocol has its unique way of handling data exchanges, processing, and optimization in the context of heterogeneous devices and large-scale cloud structures. Such attributes of the traffic are explicitly linked to performance of such protocols, design principles and operational behavior of such protocols and more specifically MQTT, CoAP, and HTTP [28]. A detailed case-by-case discussion of these technologies shows the pros and cons of these technologies and their use in the different cloud-based IoT solutions.

4.1.1 Hyper Text Transport Protocol (HTTP)

HTTP is the basic client-server communication protocol of the Web, and HTTP/1.1 is the most prevalent version. It is request/response-based, wherein the client initiates a request and the server responds with a resource when the request is accepted. HTTP has also been increasingly used in the IoT, due to the proliferation of RESTful web services.

4.1.2 Constrained Application Protocol (CoAP)

CoAP is an IETF Constrained RESTful Environments (CoRE) lightweight protocol to suit constrained devices. It is similar to HTTP in that it utilizes the REST architecture and features the request/response paradigm, yet employs binary encodings of its headers, methods, and statuses to minimize overhead. UDP increases and again reduces the complexity, but at the sacrifice of reliability. In response, the IETF has proposed an extension of CoAP over TCP to address this issue, which is still under development.

4.1.3 Message Queue Telemetry Transport Protocol (MQTT)

The lightweight publish-subscribe communications protocol known as MQTT was developed for use with devices that have very limited resources. How to use MQTT is used over TCP, port 1883, which is reserved for establishing the Mosquitto broker. First designed by IBM and standardized by OASIS (v3.1), MQTT is an extremely popular IoT protocol, owing to its simplicity and small message header. It runs on top of TCP to achieve reliability, but it is energy-efficient compared to protocols such as HTTP and therefore very appropriate in constrained environments.

4.2 Traffic Optimization Strategies

As IoT deployments continue to expand at high rates, the amount of traffic created by billions of devices can flood cloud infrastructures unless this traffic is properly capped. Traffic control methods are thus imperative to address the effective utilization of network resources, minimize latency and scale within a given environment without undermining security and Quality of Service (QoS). The strategies can be applied at different levels of IoT communication, where their primary concern is to minimize overhead in data transfers, making the transmission process efficient, and intelligently controlling traffic patterns among devices, gateways, and the cloud.

4.2.1 Data Reduction Strategies

Data compression (DC), data prediction (DP), and data aggregation (DA) are the three main types of data reduction strategies [29]. These categories limit traffic directed to the destination node on different principles. DC converts and decompresses messages, DP approximates sensor values using predictive models at fewer transmissions, and DA compresses information (e.g., averages) rather than the values themselves, and thus conserves bandwidth and energy.

4.2.2 Edge and Fog Computing Integration

The edge and fog nodes located at the edges and close to the IoT devices allow the preprocessing and intelligent traffic control to be provided before data is sent to the cloud. This removes congestion of cloud networks, and is quicker to respond [30], and offers an ideal response in real-time. The system performance is optimized by such strategies as the distribution of loads in edge and cloud servers.

4.2.3 AI/ML-Based Traffic Management

Recent trends investigate machine learning in order to perform predictive traffic mapping, detect anomalies, and route customization [31]. The possibilities presented by AI-controllers in cloud-based IoT networks are the following: (1) flexibility in resource allocation, which enables the resource scheduling of transmissions to be dynamic and (2) the absence of congestion in traffic patterns.

4.2.4 Energy-Aware Optimization

IoT devices that are typically battery-powered are important with respect to energy efficiency. Data aggregation, duty cycling, lightweight protocols (such as MQTT-SN and CoAP), and edge computing can also be used to minimize transmissions. Scheduling with AI/ML further reduces energy consumption, allowing devices to last longer and be more sustainable.

5. LITERATURE REVIEW

This section provides a literature overview on anomaly detection, security, and IoT network traffic. It covers different approaches, such as ML, DL, and forensic techniques, and summarizes their methodology, main findings, limitations, and suggested areas for future research.

Takasaki, Korikawa and Hattori (2025) proposed a method determine the sample lengths, input to machine learning models, based on periodicity analysis of the converted evenly-spaced packet series. Compare the suggested strategy to the current one by evaluating its accuracy in a traffic classification task. The evaluation results show that the classification accuracy trained with the samples extracted from a part of input traffic is comparable to the accuracy trained with the samples extracted from all input traffic, whereas the accuracy of the existing method decreases as the number of days of input traffic decreases. When training with the samples extracted from all the input traffic, each traffic type is classified with 99% accuracy. The proposed method reduces the duration of traffic collection for maintaining the accuracy in the traffic classification [32].

Kapoor, Patidar and Arya (2025) The focus of the study on the network traffic patterns (data flow, packet characteristics and communication protocols) in order to identify anomalous behaviors that are likely to contain malicious activity. Forensic analysis techniques are applied to network logs to build up a picture of what attack scenarios might look like and where suspicious traffic is coming from. Statistical and machine learning methods are applied at an advanced level to classify traffic as normal or abnormal in order to improve detection accuracy. This method is a non-invasive, scalable means of real-time identification of IoT malware without exposing vulnerable IoT ecosystems to novel threats. [33].

Sharma and Babbar (2024) Anomaly detection in the context of the IoT plays a vital role in ensuring the safety and reliability of networks and connected devices. Frequently, it is not possible to detect complex and evolving threats with the help of the conventional rule-based approaches, which reasons why ML technologies are currently used. In this study, the approach to the study is to identify anomalies in IoT network traffic using machine learning, where the Army Cyber Institute Internet of Things (ACI-IoT) Network Traffic Dataset will be used. The dataset makes it easier to train, test, and assess anomaly detection algorithms by providing a thorough and accurate depiction of IoT network behaviours. Using supervised ML algorithms such as DT, RF, AdaBoost and XGBoost [34].

Santhosh Kumar, Selvi and Kannan (2023) This study conducts experiments on encrypted communication and measures the network's performance by comparing it to existing security metrics; it then uses these results to conduct a thorough analysis of the security of IoT networks using quality-of-service metrics in order to deploy intrusion detection systems. Lastly, to enhance communication security, suggest a novel IDS that makes use of a deep learning-based categorization method, specifically, fuzzy CNN. An increase in detection accuracy, improved efficiency in accurately detecting denial-of-service (DoS) assaults, and a decrease in false positive rates are the primary and most notable benefits of this system [35].

Perepelkin and Ivanchikova (2022) This study aims to investigate the use of neural networks as a solution to the problem of network traffic prediction in multiprovider cloud infrastructures. We do experimental research on traffic prediction for many sorts of applications and carefully evaluate the stages of tackling this challenge. In order to achieve the highest level of accuracy in estimating the amount of network traffic, the ideal parameters of the neural network design, error, and regularization functions were chosen [36].

Bajaj, Sharma and Singh (2021) The projected Internet of Things is rapidly expanding into more and more sectors of people's daily lives, including smart homes, smart farms, smart factories, and smart cities. The aforementioned domains make use of networked smart devices. Connected devices use wireless sensors to gather massive amounts of data, which is subsequently sent to the edge and cloud for processing over the network. More data is created by a rise in sensory devices, which in turn leads to an increase in wireless terminals [37].

Table 3 provides a summary of recent studies that compare and contrast IoT network traffic, security, and anomaly detection. The studies highlight their methods, main findings, difficulties, and suggested areas for further research.

Table 3: Comparative Analysis of Recent Studies on IoT Network Traffic, Security, and Anomaly Detection

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Takasaki, Korikawa and Hattori, (2025)	Traffic classification using periodicity analysis	Periodicity-based sample extraction for ML training	Comparable accuracy with reduced traffic samples; 99% accuracy on full dataset	Dependence on periodic traffic patterns; limited dataset scope	Extend to heterogeneous IoT traffic and evaluate scalability in real-time systems
Kapoor, Patidar and Arya, (2025)	IoT malware detection & network forensics	Forensic analysis of logs + ML classification	Non-intrusive, scalable solution; improved detection of malicious traffic	Handling encrypted traffic; evolving IoT malware patterns	Integrate deep learning with adaptive models for zero-day threats
Sharma and Babbar, (2024)	Anomaly detection in IoT networks	ML-based anomaly detection using ACI-IoT dataset (DT, RF, AdaBoost, XGBoost)	ML models achieve effective anomaly detection with labeled IoT dataset	Difficulty in detecting evolving/sophisticated attacks; dataset limitations	Incorporate unsupervised and deep learning models for adaptive anomaly detection

Santhosh Kumar, Selvi, and Kannan (2023)	IoT network security and IDS	Proposed a deep learning-based IDS using fuzzy CNN with QoS-based security metrics.	Improved detection accuracy, efficient DoS detection, and reduced false positives.	Evaluation limited to small-scale test scenarios; lacks real-time adaptability.	Extend IDS for large-scale heterogeneous IoT environments, improve real-time detection, and enhance scalability.
Perepelkin and Ivanchikova, (2022)	Network traffic prediction in multi-provider cloud	Neural networks with parameter optimization	High accuracy in traffic prediction; optimized architectures identified	Model generalization for diverse applications	Hybrid deep learning + time-series forecasting for dynamic workloads
Bajaj, Sharma and Singh, (2021)	IoT data growth and application domains	Survey on IoT data collection, wireless sensors & smart applications	Increasing data generation from sensory devices; growth in IoT domains	Data management and storage scalability	Edge computing and federated learning for efficient IoT data handling

6. CONCLUSION AND FUTURE WORK

The Internet of Things (IoT) has revolutionized various industries in the present digital age. It allows billions of smart devices to connect seamlessly and integrates them with cloud computing environments. This convergence has created intelligent, data-driven ecosystems, but it has also introduced complex challenges related to network traffic management, scalability, data privacy, and cybersecurity. The increased variety of IoT communication protocols and devices with constrained resources has rendered the effective analysis of traffic and safe data transfer a more pressing issue. This survey has offered a review of the entire IoT communication protocols and their impacts on network traffic analysis in cloud-integrated environments. It has discussed the use of the IoT platform, categorised protocols into both the long-range and short-range networks, and considered the protocol-specific traffic patterns of popular standards, including HTTP, CoAP and MQTT. Moreover, it surveyed the contemporary developments in traffic monitoring, anomaly detection, and security improvement through machine learning (ML), deep learning (DL) and forensic methods. The results indicate that lightweight protocols in combination with AI-based traffic optimization have resulted in a significant enhancement of performance, energy consumption and security, as well as provide support for real-time analytics and scalable IoT-cloud deployments.

Future work ought to be on standardized datasets, cross-protocol anomaly labels and real-time traffic optimization systems. Combining AI/ML-based methods with edge and fog computing will also be important in creating secure, adaptive and energy-efficient IoT-cloud architectures that can host next-generation intelligent applications and autonomous ecosystems.

REFERENCES

[1] M. Asano, T. Miyoshi, and T. Yamazaki, “Internet-of-Things Traffic Analysis and Device Identification Based on Two-Stage Clustering in Smart Home Environments,” *Futur. Internet*, 2024, doi: 10.3390/fi16010017.

[2] V. Shah, “Analyzing Traffic Behavior in IoT-Cloud Systems : A Review of Analytical Frameworks,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 9, no. 3, pp. 877–885, 2023, doi: 10.32628/IJSRCSEIT.

[3] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, “A survey on communication protocols and performance evaluations for Internet of Things,” *Digit. Commun. Networks*, 2022, doi: 10.1016/j.dcan.2022.03.013.

[4] N. K. Prajapati, “Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[5] J. Sidna, B. Amine, N. Abdallah, and H. El Alami, “Analysis and evaluation of communication Protocols for IoT Applications,” in *Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications*, 2020, pp. 1–6. doi: 10.1145/3419604.3419754.

[6] V. Seoane, C. Garcia-Rubio, F. Almenares, and C. Campo, “Performance evaluation of CoAP and MQTT with security support for IoT environments,” *Comput. Networks*, vol. 197, p. 108338, Oct. 2021, doi: 10.1016/j.comnet.2021.108338.

[7] S. A. Pahune, P. Matapurkar, S. Mathur, and H. Sinha, “Generative Adversarial Networks for Improving Detection of Network Intrusions in IoT Environments,” *2025 4th Int. Conf. Distrib. Comput. Electr. Circuits Electron.*, pp. 1–6, 2025, doi: 10.1109/ICDCECE65353.2025.

[8] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, “IoT: Communication protocols and security threats,” *Internet Things Cyber-Physical Syst.*, vol. 3, pp. 1–13, 2023, doi: 10.1016/j.iotcps.2022.12.003.

[9] R. Patel, “Optimizing Communication Protocols in Industrial IoT Edge Networks: A Review of State-of-the-Art Techniques,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 19, pp. 503–514, May 2023, doi: 10.48175/IJARSCT-11979B.

[10] M. Fahmideh and D. Zowghi, “An exploration of IoT platform development,” 2020. doi: 10.1016/j.is.2019.06.005.

[11] A. Al-Sakran, M. H. Qutqut, F. Almasalha, H. S. Hassanein, and M. Hijjawi, “An Overview of the Internet of Things Closed Source Operating Systems,” in *2018 14th International Wireless Communications and Mobile Computing Conference,*

IWCMC 2018, 2018. doi: 10.1109/IWCMC.2018.8450314.

[12] A. Martikkala, J. David, A. Lobov, M. Lanz, and I. F. Ituarte, "Trends for Low-Cost and Open-Source IoT Solutions Development for Industry 4.0," *Procedia Manuf.*, vol. 55, pp. 298–305, 2021, doi: 10.1016/j.promfg.2021.10.042.

[13] A.-S. Shadi, A. Mohammed, A. Kamal, and A. Mahmood, "Internet of Things (IoT) communication protocols: Review," in *2017 8th International Conference on Information Technology (ICIT)*, IEEE, May 2017, pp. 685–690. doi: 10.1109/ICITECH.2017.8079928.

[14] A. J. Onumanyi, A. M. Abu-Mahfouz, and G. P. Hancke, "Low Power Wide Area Network, Cognitive Radio and the Internet of Things: Potentials for Integration," *Sensors*, vol. 20, no. 23, Nov. 2020, doi: 10.3390/s20236837.

[15] A. A. F. Purnama and M. I. Nashiruddin, "Sigfox-based internet of things network planning for advanced metering infrastructure services in urban scenario," in *Proceedings - 2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology, IAICT 2020*, 2020. doi: 10.1109/IAICT50021.2020.9172022.

[16] J. Zakaria, J. Kundu, and H. Rza, "A Review paper on The Internet of Things (IoT) & Its Modern Application," *AIP Conf. Proc.*, vol. 2851, no. 1, pp. 4–9, 2023, doi: 10.1063/5.0178765.

[17] A. A. Bahashwan, M. Anbar, N. Abdullah, T. Al-Hadhrami, and S. M. Hanshi, "Review on Common IoT Communication Technologies for Both Long-Range Network (LPWAN) and Short-Range Network," in *Advances in Intelligent Systems and Computing*, 2020, pp. 341–353. doi: 10.1007/978-981-15-6048-4_30.

[18] G. K. Ee, C. K. Ng, N. K. Noordin, and B. M. Ali, "A Review of 6LoWPAN Routing Protocols," *Proc. Asia-Pacific Adv. Netw.*, 2010, doi: 10.7125/apan . 30.11.

[19] D. Rani and N. S. Gill, "Review of various IoT standards and communication protocols," *Int. J. Eng. Res. Technol.*, vol. 12, no. 4, 2019.

[20] A. Zohourian *et al.*, "IoT Zigbee device security: A comprehensive review," *Internet of Things*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100791.

[21] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings*, 2012. doi: 10.1109/CECNet.2012.6201508.

[22] J. H. Kalwar and S. Bhatti, "Deep Learning Approaches for Network Traffic Classification in the Internet of Things (IoT): A Survey," 2024, doi: https://doi.org/10.48550/arXiv.2402.00920.

[23] V. Shah, "Traffic Intelligence In Iot And Cloud Networks: Tools For Monitoring, Security, And Optimization," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 5, 2024, doi: 10.10206/IJRTSM.2025894735.

[24] T. Wu, F. Breitinger, and S. Niemann, "IoT network traffic analysis: Opportunities and challenges for forensic investigators?," *Forensic Sci. Int. Digit. Investig.*, vol. 38, Oct. 2021, doi: 10.1016/j.fsidi.2021.301123.

[25] M. Mainuddin, Z. Duan, and Y. Dong, "Network Traffic Characteristics of IoT Devices in Smart Homes," in *2021 International Conference on Computer Communications and Networks (ICCCN)*, IEEE, Jul. 2021, pp. 1–11. doi: 10.1109/ICCCN52240.2021.9522168.

[26] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, 2025.

[27] M. Yang and J. Zhang, "Data Anomaly Detection in the Internet of Things: A Review of Current Trends and Research Challenges," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 9, 2023, doi: 10.14569/IJACSA.2023.0140901.

[28] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–29, Nov. 2019, doi: 10.1145/3292674.

[29] D. Kreković, P. Krivić, I. Podnar Žarko, M. Kušek, and D. Le-Phuoc, "Reducing communication overhead in the IoT–edge–cloud continuum: A survey on protocols and data reduction strategies," *Internet of Things*, vol. 31, May 2025, doi: 10.1016/j.iot.2025.101553.

[30] C. Rajyalakshmi, K. R. Rao, and R. R. Ramisetty, "A review of fog and edge computing with big data analytics," in *Handbook of Big Data Analytics. Volume 1: Methodologies*, Institution of Engineering and Technology, 2021, pp. 297–316. doi: 10.1049/PBPC037F_ch8.

[31] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 10, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[32] C. Takasaki, T. Korikawa, and K. Hattori, "Sample Length Determination from Network Traffic based on Periodicity Analysis," in *2025 International Conference on Computing, Networking and Communications (ICNC)*, IEEE, Feb. 2025, pp. 7–11. doi: 10.1109/ICNC64010.2025.10994096.

[33] M. Kapoor, N. Patidar, and N. Arya, "Analyzing Network Traffic Features for IoT Malware Detection through Forensic Methods," in *2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT)*, IEEE, Mar. 2025, pp. 334–339. doi: 10.1109/CSNT64827.2025.10967726.

[34] A. Sharma and H. Babbar, "Analyzing Anomalies in IoT Networks using Machine Learning Solutions with ACI-IoT-2023 Network Traffic Dataset," in *2024 Asian Conference on Intelligent Technologies (ACOIT)*, IEEE, Sep. 2024, pp. 1–5. doi:

10.1109/ACOIT62457.2024.10939740.

[35] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, "A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things," *Comput. Intell. Neurosci.*, vol. 2023, no. 1, pp. 1–24, Jan. 2023, doi: 10.1155/2023/8981988.

[36] D. Perepelkin and M. Ivanchikova, "Problem of Network Traffic Prediction in Multiprovider Cloud Infrastructures Based on Neural Networks Methods," in *2022 11th Mediterranean Conference on Embedded Computing (MECO)*, IEEE, 2022, pp. 1–4. doi: 10.1109/MECO55406.2022.9797129.

[37] K. Bajaj, B. Sharma, and R. Singh, "Edge, Fog and Cloud-based Smart Communications for IoT Network-based Services &amp; Applications," in *2021 International Conference on Artificial Intelligence and Machine Vision (AIMV)*, IEEE, Sep. 2021, pp. 1–5. doi: 10.1109/AIMV53313.2021.9670975.