International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

Analyzing Traffic Behavior in IoT-Cloud Systems : A Review of Analytical Frameworks

Vaidehi Shah

Independent Researcher

ARTICLEINFO

Article History:

Accepted: 11 June 2023

Published: 25 June 2023

Publication Issue

Volume 9, Issue 3

May-June-2023

Page Number

877-885

ABSTRACT

The tasks of the network administrator will be to monitor the numerous applications running on the network and perform a deep analysis of the network traffic. This encompasses tasks such as anomaly detection, network surveillance, and system optimization to derive meaningful information about network traffic. The article explores IoT-cloud designs in detail, examining their performance against network traffic and identifying critical security objectives. It looks at different traffic analysis methods, packet, flow statistics, and behavior modeling and looks at key security threats sarcastically, Distributed Denial of Service (DDoS), phishing, and SQL injection attacks. The paper further describes the most important security objectives that are needed to defend IoT-cloud environments, including confidentiality, integrity, and availability and reviews various cyber threats, like DDoS, man-in-the-middle, phishing, as well as SQL injection threat. Based on a literature review, this paper examines modern tools and techniques to implement traffic monitoring and anomaly detection, outlining their advantages and drawbacks in the existing solutions. By methodologically reviewing recent developments, the article will help researchers and practitioners to innovate more secure and smarter systems to conduct IoT-cloud traffic analysis.

Keywords : IoT-data, Cloud, IoT-Cloud Systems, Traffic Behavior Analysis, Network Traffic Modeling, Cyber–Physical Systems.

Introduction

The explosive growth of the IoT has accelerated the transformation of classical cyberphysical systems to interconnected and intricate ecosystems that have billions of connected devices. The different applications of these systems are as varied as intelligent transportation to smart homes and cities, as well as healthcare and industrial automation. This exponential boom is also compounded by the embarking of cloud computing, resulting to IoT-Cloud systems offering scalability, data storage, in real-time analytics, and remote devices management. These systems provide greater flexibility and performance, and support facile connectivity and smart decision-making at scale [1][2].

Copyright © 2023 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

Combining IoT and cloud infrastructures with these advantages come with new challenges, specifically in terms of developing and managing the diverse traffic characteristics which are particular to the IoT network. In contrast to normal Internet traffic, IoT traffic is highly heterogeneous, low-volume and infrequent transmissions, varied communication protocols and unpredictable data flows [3]. Furthermore, there is the issue of myriads of the resource-constrained devices that tend to be used in dynamic and erratic settings, making the efforts of modeling and monitoring the traffic quite complicated. These complexities do not only influence network performance and quality of services, but also increase vulnerabilities to data privacy, security vulnerabilities, and denial-of-service (DoS) vulnerability like the cases of the Mirai botnet.

The issue has spurred the development of a series of works to study the analytical frameworks to model, simulate and analyze IoT-Cloud traffic behavior. These frameworks are designed to profile traffic trends, identify anomalies, evaluate the entropy-based behavioral signature and improve situational awareness based on machine learning and statistics. Traffic generators (e.g., IoTT Gen) have been implemented to achieve realistic traffic conditions to test experiments to enhance the comprehension of the network enactment under possible situations. The proposed review paper is a systematized survey of the state-of-the-art analytical models that aim at the analysis of traffic behavior in IoT-Cloud systems. It emphasizes procedures utilized, their strengths and weaknesses, as well as gaps in the research. This synthesis of current developments is expected to offer a reference base to future researchers and practitioners interested in creating strong, safe, and optimal traffic analysis solutions that can respond to the dynamic needs of an IoT-Cloud environment.

Structure of Paper

This paper is structured into various sections: Section II describes the IoT-based cloud architecture and outlines essential security goals. Section III discusses analytical frameworks for traffic behavior. Section IV explores the landscape of Cloud-IoT threats and integration challenges. Section V presents a literature review of recent studies, highlighting existing research gaps and future directions. Section VI present the conclusion with future direction.

Cloud Architecture Based on IoT

Many components are implanted to create an intelligent network of linked objects, including RFID, gateways, sensor technology, and other smart technologies. A basic IoT cloud architecture is shown in Figure 1. Data is collected in the perception layer from several sources, including Internet of Things (IoT) devices and sensors worn by humans. The network layer is where gateways to the internet get their data. The edge computing layer is responsible for cleaning and preparing data. In addition, the cloud platform was used to do data analytics and predictions utilizing a variety of ML algorithms. The primary objective of the IoT is to improve and simplify human life, either by assisting people in making better decisions or by reducing stress, repetitive tasks, and interpersonal interactions via IoT computer technology, the proponent of the IoT.

Figure 1. IoT Cloud Architecture [4]

These days, smart network IoT applications are in high demand across all industries. industries including smart cities, retail, healthcare, education, and agriculture, among many more. In order to reduce transportation expenses and increase pricing prediction based on historical data analytics, IoT is used in agriculture for crop harvesting. The IoT is often used in energy conservation to notify the end user of the need to save power. There is a wide variety of research going on, including several models for the IoT in healthcare and various methodologies for the prediction of various diseases. The IoT and cloud computing have many

applications in healthcare, one of which is real-time patient health monitoring. This type of monitoring makes use of sensor technology, sends raw data to the cloud for analysis, and also alerts doctors and careers to potential problems at an early stage. The analysis and prediction processes make use of various data mining and ML methods.

Security Goals in Cloud-IoT Environments: A Comprehensive Overview

The interconnection of devices and the massive amounts of sensitive data they produce and handle make security a top priority in Cloud-IoT settings. As internet of things (IoT) devices and cloud computing become increasingly pervasive in its daily lives and critical infrastructure, protecting the privacy, authenticity, and accessibility of data and services has grown into an enormous undertaking. This thorough review aims to investigate the main security goals, challenges, and strategies that are essential for safeguarding Cloud-IoT settings in a constantly evolving digital ecosystem. Security goals in a cloud system are shown in Figure 2. The security objectives must be established in information, programs, and hardware maintained on the cloud so that data stored in the programs and applications retain their confidentiality, availability, and integrity.

Figure 2. Security objective in cloud environment

Businesses can employ these objectives to further shape their security objectives and inform the implementation of the right security measures. Environment security objectives are important to guarantee data and service availability, confidentiality and integrity hosted in the cloud provider. These objectives assist organisations in setting a framework of security implementation and articulating their security objectives. Security goals and policies should be reviewed and updated frequently to ensure strong cloud security posture and reaction to constantly changing threats.

- **Confidentiality:** Data confidentiality encompasses the routines of denying unauthorized persons the ability to access sensitive data. Only authorized individuals will have access to or be able to divulge the information.
- **Identification and Recognition:** Identification is a one-of-a-kind method of giving people or devices characteristics that set them apart from one another. Validation of the asserted identity is associated with recognition. A user can be identified by comparing their password entered with their stored password [5].
- **Privacy:** Security measures are put in place to protect individual data privacy. It also guarantees the responsible handling of data. Information about personnel must be protected [6].
- **Authentication:** The process of authentication measures includes verifying people's identities and guarding against unwanted access. The user must provide their account and password in order to participate.
- **Availability:** The term "availability" describes how easy it is for an authorized user to access and use data when needed. Protecting data availability against threats like denial-of-service attacks, outages, and other interruptions is an important part of sustaining availability.
- **Integrity:** Integrity guarantees that information is accurate, consistent, and unchangeable for the course of its existence. Additionally, it guarantees the reliability of the information.

Analytical Frameworks for Traffic Behavior

Network behaviour analysis involves collecting and analyzing data from corporate networks in order to spot any suspicious conduct or unusual action by entities. The modern tools for analyzing network behaviour gather NetFlow data in order to establish a baseline for

typical network activities. Network behaviour analysis documents and draws attention to the unusual occurrence for security operators when a network object exhibits behaviour that deviates from the norm. Businesses use network behaviour analysis to automatically identify threats that security teams find difficult to identify. Utilizing state-of-the-art machine learning (ML) methods, solutions for network behaviour analysis are able to accurately distinguish between different kinds of network applications, with accuracy levels often exceeding 90%. Analyzing network behaviour helps strengthen network security by monitoring traffic patterns and drawing attention to suspicious activities. This is a change from the way network security operations have always been conducted, which involves using tried-and-true methods like signature recognition, packet inspection, and blocking harmful websites to protect networks. The alternative is network behaviour analysis, which uses machine learning to discover patterns in data collected from many sources on a network's operation. Any abrupt change in these trends can be a sign of malicious behaviour.

Overview of Network Traffic Analysis

Network security issues have become relevant as more people use the Internet and it has continued to increase. The issue of network security has been one of the determinants of the national security, social and economic development. In a complex network environment, timely detection and response to various network security threats is a huge challenge. As a crucial tool for keeping networks secure, network traffic analysis and anomaly detection methods may monitor and analyze network traffic in real-time to discover suspicious activity and safety incidents. Network traffic is the amount of data sent over a network in some period of time, commonly expressed as the number of packets or bytes. There are primarily three approaches to network traffic analysis:

1) Packet Analysis

The information in the key fields of the data packets in the network (e.g. source/destination IP, port number, protocol type, etc.) is obtained by capturing and parsing of the data packets to enable a fine-grained analysis of the network traffic [7]. Commonly used packet analysis tools include Wireshark, Tcpdump, etc. It is especially useful in identifying specific types of attacks like malware transmission, unauthorized access attempts, or policy violations through techniques like Deep Packet Inspection (DPI). However, its effectiveness can be limited in modern networks where data is increasingly encrypted, making payload analysis difficult.

2) Flow Statistics Analysis

By measuring and analyzing the statistical characteristics of network traffic (such as flow rate, number of connections, packet size distribution, etc.), the overall patterns and change trends of traffic are characterized. Commonly used statistical indicators include mean, variance, probability distribution, etc. Packets that share characteristics (such as a 5-tuple: source IP, destination IP, source port, destination port, protocol) and travel in a single direction are called network flows.

3) Flow Behavior Analysis

By modeling and analyzing the behavioral characteristics of network traffic (such as communication frequency, duration, interaction patterns, etc.), the behavioral patterns and anomalous events behind the traffic are mined [8]. Common behavior analysis methods include association rule mining, sequence pattern mining, etc. It aims to understand how network entities, such as IoT devices, applications, or users, behave under normal and abnormal conditions by studying characteristics like traffic bursts, inter-arrival times, flow durations, and entropy of traffic features. This method is particularly effective in dynamic and heterogeneous environments like IoT-cloud systems, where devices generate diverse and often unpredictable traffic patterns. Flow behavior analysis is increasingly used for IoT device identification, anomaly detection, and threat prediction, enabling more intelligent and adaptive network security and management strategies.

Landscape of Cloud-IoT Threats

The convergence of the IoT with cloud computing has raised security issues. There are a lot of risks and

weaknesses introduced by combining these two technologies, which might affect the availability, confidentiality, and integrity of data and services. This investigation delves into the complex nature of Cloud-IoT security problems, examining the intricacies, possible impacts, and crucial requirement of strong security methods to guard against developing risks in linked systems. The many kinds of cloud-based assaults are shown in Figure 3. Customers and cloud service providers alike are vulnerable to these types of attacks. In the context of cloud computing, an attacker is someone who seeks to do malicious acts by taking advantage of security holes in cloud infrastructure, platforms, or services.

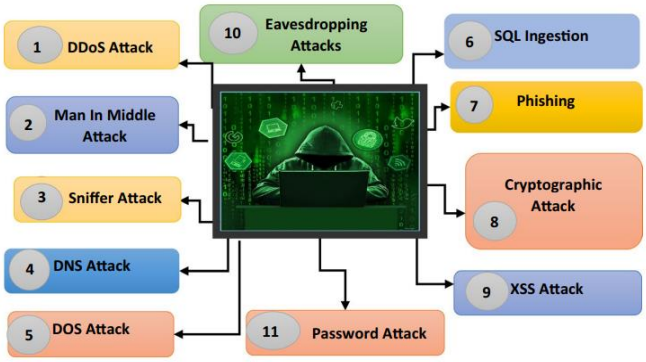

Figure 3. Threats in cloud computing environment

Attackers find cloud systems very appealing because they often store large amounts of data and provide computing resources that may be utilized for a variety of objectives, such launching cyberattacks, stealing private information, or creating disruptions. Attackers target cloud infrastructures for a variety of reasons, such as resource exploitation, data theft, or service disruption. Attackers use a variety of strategies and techniques to compromise cloud systems. There are many other types of attacks that may occur, including as eavesdropping, malware, insider threats, SQL injection, phishing, distributed denial-of-service (DDoS) assaults, and more [9][10].

- **DDOS Attack:** The goal of a distributed denial-of-service attack is to overload a network with traffic in order to interrupt normal network operations [11]. A denial-of-service attack is an attempt to block users from reaching the network.
- **Man-in-Middle Attack:** A man-in-the-middle attack often entails the hacker altering the dialogue between the target and the attacker. An attacker may change the discussion or eavesdrop on important information in a man-in-the-middle attack. Threats from MitM attacks may compromise the security and integrity of sensitive data.
- **Sniffer Attack:** This kind of attack involves an unauthorized individual intercepting and controlling network communication. The objective is to record and analyze the data as it travels throughout the network.
- **DNS Attack:** Domain name system assaults target the mechanism that translates human-readable names into IP addresses. Threats to the availability, integrity, and confidentiality of the DNS system from assaults might disrupt internet services.
- **DOS Attack:** The goal of a DoS attack is to disrupt a service by overwhelming the resources of the target, usually via the use of a hacked computer or device.
- **SQL Ingestion:** SQL Ingestion is the activity in which an attacker can poison the parameters of a web application with malicious source code. Attackers mostly target SQL databases in an effort to modify them. An attacker may execute the SQL statement in this sort of attack by taking advantage of poor input.

Phishing Attack: In phishing, the attackers employ miscellaneous strategies to disclose confidential information, including credit card numbers, username, passwords, and personal details. Phishing attacks can imitate reputable companies, banks, or websites in order to lure the victims to commit an action that can compromise their safety.

- **Cryptographic Attacks:** Privacy, authenticity, and data integrity are three areas where cryptography plays an essential role. A security hole in the current system is exploited by the assailant. Cryptographic systems are no longer secure due to attacker compromise.

- **XSS Attacks:** Cross-site scripting (XSS) is a significant attack that happens when a script or other susceptible code is inserted into a user's web page. By executing the scripting code in the user's browser, the attacker hopes to get private information about the victim.
- **Eavesdropping Attacks:** A kind of assault known as eavesdropping occurs when an unauthorized individual attempts to listen in on or smell a discussion between two individuals in order to steal information. The attacker even alters the data in this kind of assault.
- **Password Change Request Interception Attack:** An attacker is trying to sneak up on genuine users by stealing their password changes. This is how a browser-server interaction can be intercepted.

Issues and Challenges in Integration of IoT with Cloud

Traffic Behavior in the IoT-Cloud ecosystems is a growing and multidimensional challenge as such systems grow in scale and complexity. Unlike traditional network systems, IoT-Cloud architectures operate in highly dynamic environments where data is generated at the edge by heterogeneous devices and transmitted to remote cloud servers for processing and storage [12]. This creates a multifaceted traffic landscape characterized by variability, unpredictability, and resource constraints. The diversity of gadgets is one of the main obstacles. The computing power, energy capacities, data generating rates, and communication protocols of IoT devices might range greatly. The issues and challenges in integrating IoT with the cloud are measured based on different parameters like quality of service, security, network performance, reliability, heterogeneity and energy efficiency.

- **Quality of service (QoS):** QoS is a major challenge for wired and wireless networks which handle different network traffic. Issues in network traffic, resource management, data and device security affect the overall quality of service. Thus, best approaches should be followed to enhance QoS.
- **Security:** The security issues in the IoT-cloud integrated model are high due to the data transmission medium. IoT devices utilize insecure wireless medium to transfer data to the cloud. from the cloud it has been transferred to user application. The insecure wireless medium is vulnerable to attacks. So, security procedures should be incorporated for enhanced data security.
- **Network performance:** Network performance will get reduced when IoT and cloud computing are integrated due to their basic characteristics. Due to increased storage and computation guidelines, balancing network performance and improving QoS becomes more difficult.
- **Reliability:** A reliability concern arises when IoT is integrated with cloud services. For example, in smart transportation, the communication and network are unreliable due to vehicle movement. This leads to issues in reliability in terms of data center visualization.
- **Heterogeneity:** The IoT network includes multiple devices which have different memory, bandwidth, and energy consumption requirements. Additionally, these devices require different communication and implementation procedures, which introduces more heterogeneity challenges in secure communication.
- **Energy Efficiency:** There is constant data transmission from IoT devices to the cloud, which records all activity in real-time. This will increase the energy consumption in IoT devices. Thus, data transmission and processing in an IoT-cloud environment remains an open issue.

Literature Review

Recent years have seen a plethora of surveys and review papers devoted to the topic of IOT-cloud network traffic analysis, with academics tackling a wide range of problems and offering a variety of solutions.

Konopa, Fesl and Janecek (2022) draws attention to the use of image processing methods to the study of network traffic, especially when conducting automated and efficient analyses. The authors highlight the current difficulties in finding appropriate picture representations for certain contexts and settings, and

they talk about how deep neural networks and artificial intelligence might be used to analyze network traffic images [13]

Papadogiannaki and Ioannidis (2021) concentrates on the problems caused by the growing usage of encryption for network communication. The paper summarizes the current research on methods for decrypting encrypted network data and highlights the limitations of conventional deep packet inspection tools. Future research paths in encrypted traffic analysis and processing are outlined, and the scientific community acknowledges ongoing attempts to address these constraints [14].

Nguyen-An et al. (2021) used a new tool for generating traffic for the IoT called IoTT Gen to conduct comprehensive measurement studies. This application can simulate situations which involve numerous devices and network conditions by creating traffic amongst a number of devices. They explored the traffic characteristics of IoT by computing the value of entropy of the traffic parameters and analyzing visually the traffic in terms of behaviour shape graphs. It provides a new method of traffic entropy-based device detection by computing the entropy values of traffic characteristics. The strategy applies ML in classifying the data. The proposed method can identify devices at an accuracy of 94% and is stable against unanticipated network behaviour due to the spread of chaotic traffic anomalies [15].

Deri and Sartiano (2020) addresses the results to traffic analysis of both private and public networks, and describes how experimental monitoring actions were included in a free and open-source toolbox to analyze traffic and probe beyond the packets. It were able to successfully characterize and fingerprint encrypted traffic produced by household IoT and non-IoT devices by combining the suggested metrics with deep packet inspection, as proven by the validation procedure [16].

Hafeez et al. (2020) evaluated IoT-Keeper using a substantial data set of typical IoT devices gathered in a real-world testbed. The approach proposed by us reached a high score of accuracy (≈0.98) and low false that was low (≈0.02) on this dataset. Moreover, their testing shows that IoT-Keeper would be able to detect and prevent numerous network malware without any complicated hardware or special attack signature [17].

Kim and Hong (2019) suggests a method for autonomous network traffic control that considers edge technology recycling. In the case of a civil complaint, this intelligent internet live monitoring solution will promptly show field photographs, noise, vibration, and gas measurements online and preserve them effectively to avoid on-site images. The IoT, data collecting, analytics capabilities, and gateways to send processed information to cloud servers are all part of the intelligent IoT edge computing technology that is proposed here. It used smart construction monitoring to illustrate a representative service [18].

Despite growing research in IoT-cloud network traffic analysis, several critical gaps remain, as highlighted in Table I. Existing studies focus on specific areas such as image-based traffic representation, entropy modeling, or encrypted traffic inspection, but these approaches often lack scalability and adaptability across heterogeneous and dynamic IoT environments. Traditional deep packet inspection techniques are increasingly ineffective due to widespread traffic encryption, and alternative methods are still limited in real-world applicability. Machine learning models proposed so far struggle to remain robust against evolving traffic behaviors and adversarial threats, especially in resource-constrained edge settings. Moreover, few frameworks integrate lightweight, explainable AI with edge computing for real-time, encrypted traffic analysis and intelligent decision-making. This underscores the need for unified, scalable, and interpretable solutions capable of handling encrypted, diverse, and dynamic IoT-cloud traffic efficiently.

TABLE I. SUMMARY OF KEY LITERATURE ON NETWORK TRAFFIC ANALYSIS IN IOT-CLOUD ENVIRONMENTS

Author	Focus Area	Techniques/Tools Used	Challenges	Solution	Future Work
Konopa, Fesl, and Janecek (2022)	Image-based network traffic analysis	Image representations, AI, Deep Neural Networks	Difficulty in selecting suitable image representations for specific environments	Applied AI/DNNs to network traffic images to enhance automated traffic analysis	Explore optimized and adaptive image encoding techniques for real-time deployment in diverse IoT-cloud environments.
Papadogiannaki and Ioannidis (2021)	Encrypted network traffic analysis	Literature review on deep packet inspection and encrypted traffic	Traditional deep packet inspection (DPI) fails with encrypted traffic	Explored alternative approaches to DPI; reviewed advances in encrypted traffic analytics	Develop privacy-preserving traffic analysis methods and AI-based models capable of learning from limited decrypted data.
Nguyen-An et al. (2021)	IoT device traffic behavior and classification	IoTT Gen traffic generator, entropy analysis, machine learning	Unpredictable behavior and difficulty in classifying traffic from diverse IoT devices	Used entropy-based analysis and ML classification to identify traffic patterns	Integrate real-time entropy computation for live classification and extend the tool to handle mobile/edge devices.
Deri and Sartiano (2020)	Encrypted traffic characterization in home networks	DPI toolkit, custom monitoring metrics	Difficulty in identifying traffic behavior of encrypted packets from IoT and non-IoT devices	Combined DPI with new metrics for accurate traffic fingerprinting	Enhance toolkit capabilities for cloud-native deployments and test on larger, real-world encrypted traffic datasets.
Hafeez et al. (2020)	Detection of malicious activity in IoT networks	IoT-Keeper, real-world dataset, lightweight ML methods	Detecting attacks without signatures, high false positives in traditional systems	Developed lightweight anomaly detection model with low resource usage	Expand to multi-layered IoT infrastructures and include adaptive learning to detect evolving attack patterns.
Kim and Hong (2019)	Edge-based IoT traffic monitoring and control	Intelligent IoT edge computing system, real-time environmental data display	Need for efficient data monitoring and quick response in smart environments	Proposed architecture using edge computing, gateways, and cloud integration	Investigate integration of 5G/6G networks and blockchain for secure, scalable IoT edge-cloud coordination.

Conclusion

The preservation of the integrity and security of computer networks is essential in the current era of ubiquitous digital connectivity. This review paper presents a comprehensive examination of the Real-Time Network Traffic Monitoring and Anomaly Detection System, emphasizing its user-friendly interface and robust historical analytical capabilities. This paper provides a comprehensive examination of IoT-cloud environments, beginning with an architectural overview and an outline of fundamental security objectives, including confidentiality, integrity, availability, and privacy. Analytical frameworks for traffic behavior analysis were discussed, highlighting packet-level inspection, flow statistics, and behavioral modeling. A taxonomy of major security threats, including DDoS, phishing, SQL injection, and encrypted traffic vulnerabilities, was presented. Additionally, a structured literature review identified various tools and techniques, along with their limitations in terms of scalability and adaptability. Despite significant progress, existing solutions remain limited in their ability to analyze encrypted and evolving traffic patterns, especially in resource-constrained edge settings. Future research should focus on developing lightweight, explainable AI algorithms capable of real-time encrypted traffic analysis. Integrating entropy-based behavioral modeling with edge computing and privacy-preserving machine learning techniques will be crucial for enhancing threat detection and situational awareness. Further improvement of future IoT-cloud ecosystems' security, scalability, and resilience may be achieved by using new technologies like 5G/6G connectivity, federated learning, and blockchain.

References

1. A. Subahi and G. Theodorakopoulos, “Detecting IoT User Behavior and Sensitive Information in Encrypted IoT-App Traffic,” Sensors, vol. 19, no. 21, Nov. 2019, doi: 10.3390/s19214777.
2. S. Garg, “Next-Gen Smart City Operations with AIOps & IoT: A Comprehensive look at Optimizing Urban Infrastructure,” J. Adv. Dev. Res., vol. 12, no. 1, pp. 1–9, 2021, doi: https://doi.org/10.5281/zenodo.15364012.
3. A. Sivanathan et al., “Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics,” IEEE Trans. Mob. Comput., vol.

18, no. 8, pp. 1745–1759, Aug. 2019, doi: 10.1109/TMC.2018.2866249.

4. C. Patil and A. Chaware, "Integration of Internet of Things, Cloud Computing: Review," IOP Conf. Ser. Mater. Sci. Eng., vol. 1022, no. 1, pp. 1–9, Jan. 2021, doi: 10.1088/1757-899X/1022/1/012099.
5. E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of IoT security," Comput. Sci. Rev., vol. 44, May 2022, doi: 10.1016/j.cosrev.2022.100467.
6. Y. Sharma, H. Gupta, and S. K. Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing," in 2019 Amity International Conference on Artificial Intelligence (AICAI), IEEE, Feb. 2019, pp. 898–902. doi: 10.1109/AICAI.2019.8701398.
7. M. F. Umer, M. Sher, and Y. Bi, "Flow-based intrusion detection: Techniques and challenges," Comput. Secur., vol. 70, pp. 238–254, Sep. 2017, doi: 10.1016/j.cose.2017.05.009.
8. J. Wang and I. C. Paschalidis, "Botnet Detection Based on Anomaly and Community Detection," IEEE Trans. Control Netw. Syst., vol. 4, no. 2, pp. 392–404, Jun. 2017, doi: 10.1109/TCNS.2016.2532804.
9. Y. Tian, M. M. Kaleemullah, M. A. Rodhaan, B. Song, A. Al-Dhelaan, and T. Ma, "A privacy preserving location service for cloud-of-things system," J. Parallel Distrib. Comput., vol. 123, pp. 215–222, Jan. 2019, doi: 10.1016/j.jpdc.2018.09.005.
10. A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," Telecommun. Syst., vol. 76, no. 1, pp. 139–154, Jan. 2021, doi: 10.1007/s11235-020-00733-2.
11. S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based IoT Networks," J. Crit. Rev., vol. 6, no. 07, pp. 1028–1033, 2019, doi: 10.53555/jcr.v6.
12. K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/IJARSCT-6268B.
13. M. Konopa, J. Fesl, and J. Janecek, "Promising new Techniques for Computer Network Traffic Classification: A Survey," in 2020 10th International Conference on Advanced Computer Information Technologies (ACIT), IEEE, Sep. 2020, pp. 418–421. doi: 10.1109/ACIT49673.2020.9208995.
14. E. Papadogiannaki and S. Ioannidis, "A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures," ACM Comput. Surv., vol. 54, no. 6, pp. 1–35, Jul. 2022, doi: 10.1145/3457904.
15. H. Nguyen-An, T. Silverston, T. Yamazaki, and T. Miyoshi, "IoT Traffic: Modeling and Measurement Experiments," IoT, vol. 2, no. 1, pp. 140–162, Feb. 2021, doi: 10.3390/iot2010008.
16. L. Deri and D. Sartiano, "Monitoring IoT Encrypted Traffic with Deep Packet Inspection and Statistical Analysis," in 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, Dec. 2020, pp. 1–6. doi: 10.23919/ICITST51030.2020.9351330.
17. I. Hafeez, M. Antikainen, A. Y. Ding, and S. Tarkoma, "IoT-KEEPER: Detecting Malicious IoT Network Activity Using Online Traffic Analysis at the Edge," IEEE Trans. Netw. Serv. Manag., vol. 17, no. 1, pp. 45–59, Mar. 2020, doi: 10.1109/TNSM.2020.2966951.
18. K. Kim and Y. G. Hong, "Autonomous network traffic control system based on intelligent edge computing," in 2019 21st International Conference on Advanced Communication Technology (ICACT), IEEE, Feb. 2019, pp. 164–167. doi: 10.23919/ICACT.2019.8701939.