RESEARCHERID
THOMSON REUTERS
[Vaidehi, 9(5), May 2024]
ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"TRAFFIC INTELLIGENCE IN IOT AND CLOUD NETWORKS: TOOLS FOR MONITORING, SECURITY, AND OPTIMIZATION"

Vaidehi Shah
Independent Researcher
shahvaidehi4795@gmail.com

ABSTRACT

The Internet of Things (IoT) and Cloud Computing are the upcoming industry trends that will bring about transformative changes in all sectors. The integration of these two technologies is gaining traction as a potent combination for the collection, processing, visualization, and utilisation of data. This paper explores the evolving landscape of traffic intelligence in IoT-cloud environments by focusing on real-time monitoring, anomaly detection, and network optimization. It highlights the role of Software Defined Networking (SDN) in enhancing traffic visibility and control through centralized management and programmable policies. Key security strategies such as encryption, segmentation, and runtime threat detection are discussed to safeguard communication between devices and the cloud. The study also reviews various traffic monitoring tools, comparing their capabilities and use cases. Furthermore, the paper outlines optimization techniques that help address issues such as network congestion, last-mile connectivity, and scalability. A detailed literature review is conducted, summarizing recent research contributions that leverage AI, fog computing, and federated learning to improve traffic management and security. Despite significant advancements, challenges remain in achieving real-time adaptability, interoperability, and holistic protection. This study provides insights into designing intelligent, secure, and resilient IoT-cloud networks capable of supporting the dynamic demands of future smart environments.

Key Words: Traffic Intelligence, Internet of Things (IoT), Cloud Computing, Software Defined Networking (SDN), Network Traffic Monitoring, Machine Learning.

I. INTRODUCTION

In the era of digital transformation, cloud computing and the IoT have emerged as foundational technologies powering modern applications, smart cities, and enterprise systems. Their combined capabilities, offering scalable computing resources, flexible service models, real-time data processing, and ubiquitous connectivity, have led to their widespread adoption across various industries. Security threats and performance problems are becoming more prevalent in more complicated IoT and cloud systems. Their open, dynamic nature makes traffic monitoring and data protection challenging, and traditional tools are often insufficient [1]. Conventional approaches like firewalls and rule-based IDS often rely on static rules and predefined thresholds, which are ineffective against dynamic and high-dimensional traffic patterns typical in cloud environments. Rule-based systems are unable to swiftly adjust to the evolving landscape of network assaults, which range from Distributed Denial of Service (DDoS) to covert malware infiltrations, leading to a high rate of false positives and missed threats [2]. This limitation creates critical blind spots in traffic intelligence and leaves systems exposed to unforeseen and complex cyberattacks [3].

The emergence of SDN as a potential solution to these restrictions is encouraging. SDN is ideal for ever-changing cloud and IoT environments because it decouples the control and data planes, which allows for centralized

management, network programmability, and flexible policy enforcement [4][5]. SDN's real-time visibility into network behavior enables quicker detection of anomalies and facilitates efficient resource allocation. However, despite its laboratory success, the scalability and performance of SDN-based traffic monitoring systems in large-scale deployments still require further research and validation [6]. Parallel to architectural advancements like SDN, AI, especially ML and DL, has revolutionized traffic monitoring and anomaly detection in network security.

Despite these advancements, practical challenges remain. Issues such as real-time performance, scalability, model generalization to new and unseen attack types, and integration with existing infrastructure continue to hinder full-scale implementation. Therefore, while AI-driven and SDN-enabled frameworks offer powerful tools for enhancing traffic intelligence, a comprehensive approach that combines monitoring, security, and optimization across all layers of IoT-cloud systems is still evolving. This paper's objective is to investigate the present state of Traffic Intelligence in IoT and cloud networks by examining the methods, technologies, and tools used for monitoring traffic in real-time, detecting anomalies, and optimizing networks. By reviewing advance systems and identifying critical research gaps, this study provides insights into building secure, efficient, and intelligent infrastructures capable of withstanding the demands of modern digital ecosystems.

A. Structure of Paper

The paper is organized as follows: An overview of cloud network designs and the integration of IoT is given in Section II. Section III discusses SDN-based traffic monitoring frameworks and tools; Section IV outlines key security strategies for IoT-cloud environments; Section V presents optimization techniques for effective traffic management; and Section VI offers a comprehensive literature review, research gaps in traffic-intelligent IoT-cloud networks. Section VII present the conclusion with future research.

II. OVERVIEW OF IOT AND CLOUD NETWORK ARCHITECTURES

IoT and Cloud Computing are the most sought-after trends in the technology world. IoT refers to the objects or things that are interconnected over the Internet, and the connected things are able to exchange data among them. The IoT is made possible by embedded sensors and the technology that allows them to interact with one other without human activity. The scalability, cost-effectiveness, and flexibility of cloud computing are enhanced by the fact that users have on-demand access to various computing resources such as networks, storage, and applications. Its popularity is driven by automation, massive storage, and service flexibility. When integrated with IoT, it forms a Cloud IoT platform depicted in Figure 1, enabling seamless connectivity, data processing, and efficient service delivery across devices. To date, there are major Cloud IoT platforms in the market that provide a seemingly less seamless interface between IoT and Cloud services.

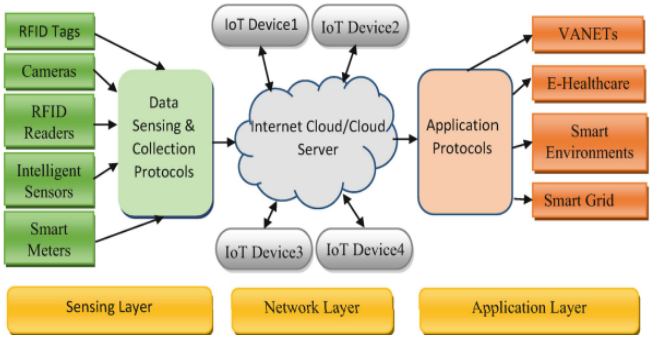

Fig.1. Cloud-Based Smart IoT Architecture [7]

A. Architecture of IoT Networks

The protocol stack for the IoT is like an expansion of the TCP/IP protocol architecture. Within this continuation, many levels and aspects of the IoT architectural stack were presented. The IoT has seen more design changes due to rising demand and applications. A three-layer model was used in early IoT scenarios, with cloud computing at the top and sensors and actuators at the base. Service-oriented architecture (SOA) proved to be the next viable strategy for implementing IoT. The foundation of SOA is a component-based paradigm that may be constructed to link different services via protocols and interfaces. Recent research indicates that Cisco's seven-layer architecture is the most

ISSN : 2455-9679
SJIF Impact Factor : 6.008

workable and appropriate solution for the IoT. The early Cisco research, as seen in Figure 2, provides a detailed explanation of the 7-layer method as well as possible applications.

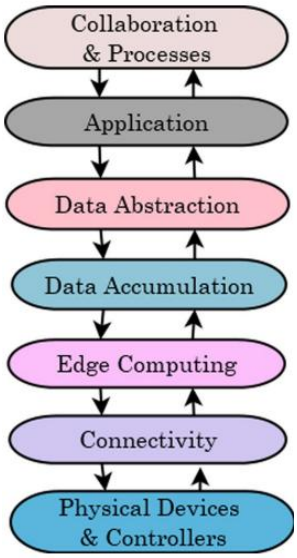

Fig.2. IoT 7-Layer Architecture [8]

The IoT architecture comprises several interconnected layers that work together to enable intelligent, responsive systems. At the foundation lies the Physical Devices and Controllers Layer, which includes sensors and actuators the "things" of the IoT, responsible for direct interaction with the physical environment [9]. This layer relies on Edge Intelligence to ensure distributed processing, autonomy, and low-latency responses. The Connectivity layer sits above this, facilitating the smooth transfer of data by connecting edge devices to cloud systems via a variety of communication protocols. Prior to transmission to the cloud, data undergoes low-latency processing and routing at the Edge Computing layer. Next, the Data Accumulation layer stores and normalizes large volumes of data, which the Data Abstraction layer then organizes into structured formats. The Application Layer enables core IoT functions like monitoring and analytics, while the Collaboration layer connects business systems and users, turning insights into economic and societal value.

B. Integration of IoT with Cloud Computing

There is no functional difference between the cloud and the IoT from an application perspective. Viewed from one perspective, the cloud's almost infinite possibilities might be advantageous to the IoT. The ability of the cloud to provide a strong solution for managing and combining the advantages of the IoT, as well as apps that test out devices or the data that produce, is among its most important features. On the other hand, the IoT may help the cloud by enabling it to grow its capacity to manage real-time applications in a redundant, dispersed, and dynamic way, as well as for the provision of first-hand services in a broad range of living situations [10][11]. The Cloud acts as a generally attractive layer between the applications and the objects. It may cover the important topics and tasks required to complete the last-mentioned. In a multi-cloud setting, for example, this architecture will influence future application developments, which in turn will introduce new difficulties that must be closely monitored (see Figure 3).

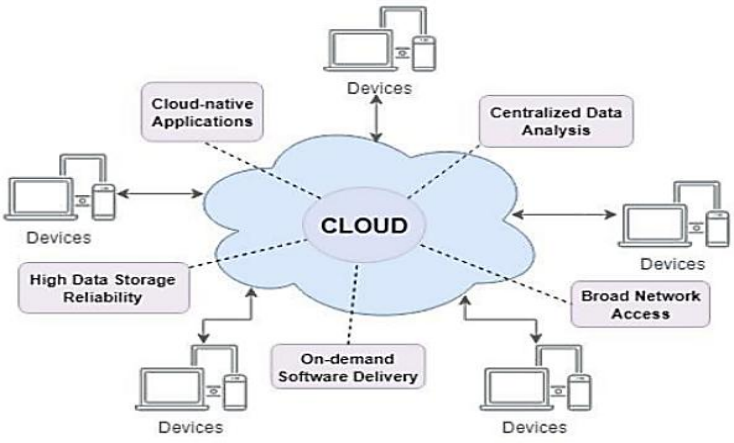

Fig.3. Integrated Cloud-based IoT System

These difficulties stem from data collection, processing, and transmission. The components of the "Internet of Things" include collecting, obtaining access to, planning, envisioning, recording, and participating in a tremendous amount of data. The most practical and cost-effective way to handle data sent by the IoT is via cloud computing. With cloud computing, data may be stored on-demand at the point of confinement with no effort and almost constant access. The IoT in the cloud provides a foundation for efficient and intelligent use of data, applications, and physical infrastructure [12]. As Table I illustrates, despite their differences, cloud computing and the Internet of Things have almost complementary qualities. This complementarity is the main justification for the integration that several academics have suggested [13].

TABLE I. COMPARISON OF THE IOT WITH CLOUD COMPUTING

Items	IoT	Cloud Computing
Characteristics	IoT is pervasive (things are everywhere). These are real world objects.	Cloud is ubiquitous (resources are available from everywhere). These are virtual resources
Processing capabilities	Limited computational capabilities.	Virtually unlimited computational capabilities.
Storage capabilities	Limited storage or no storage capabilities.	Unlimited storage capabilities.
Connectivity	It uses the Internet as a point of convergence.	It uses the Internet for service delivery.
Big data	It is a source of big data.	It is a means by which to manage big data.

III. TRAFFIC MONITORING IN IOT-CLOUD ENVIROMENTS

Monitoring system to detect traffic anomalies (such as the characteristics of DDoS attacks) and start automatic response. SDN reimagines network administration by decoupling the data plane from the control plane. Figure 4 describes their SDN-based cloud monitoring framework. This separation enables programmable operation through centralized control, which contrasts sharply with the traditional distributed architecture. A standardized API connects these layers and defines the division of roles. For example, the control layer is responsible for global traffic decisions, while the data layer only performs rule-based forwarding. This architecture provides two operational advantages: unified network supervision and automatic resource coordination. Practitioners utilize these features to achieve cost-effective customization and dynamic security policies, including real-time threat mitigation. SDN controller coordinates traffic management, collects real-time data from physical switches through southbound interface, and coordinates with security applications through the northbound interface to realize dynamic policy adjustment.

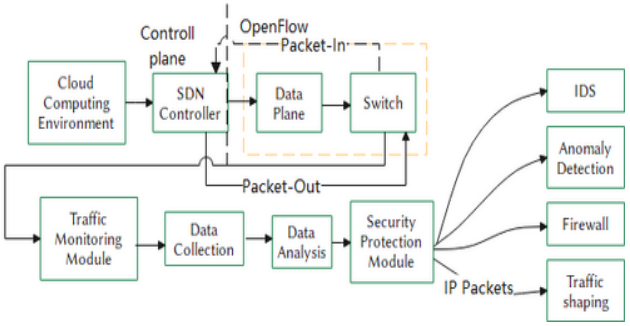

Fig.4. Network traffic monitoring based on cloud computing [14]

In SDN architecture, as shown in Figure 4, the controller collects switch traffic data at fixed time intervals. It is helpful to evaluate the network health and estimate the bandwidth by analyzing the traffic pattern within the time window. Deep Packet Inspection (DPI) scans packet contents to detect threats such as DDoS attacks. Real-time tracking of traffic sources and protocols can enhance threat detection. Administrators monitor the network using visualization tools, which highlight congestion hotspots in the topology diagram. However, DPI brings challenges: enhanced detection results in higher processing delays. Optimizations such as signature caching and distributed rule processing help balance these tradeoffs.

A. Tools and Technologies for Traffic Monitoring

Network monitoring tools together with the advantages and downsides of each tool. Today, it can find a plethora of technologies designed to gather and monitor network data. Wireshark, TcpDump, NfDump, PcapWT, Xplico, NetworkMinor, NetIntercept, Snort, PyFlag, Iris, and Bro are just a few tools in this category. The various network monitoring tools are shown in Figure 5, which will be referenced later on.

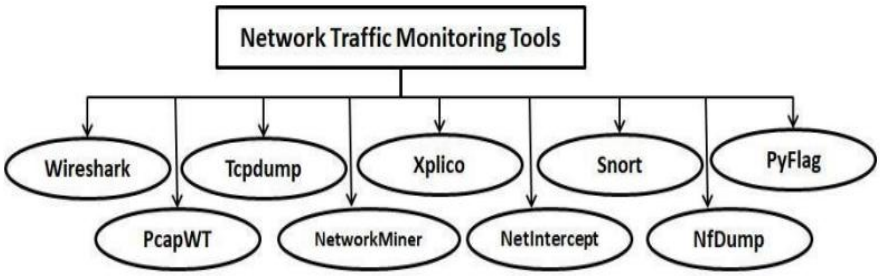

Fig.5. Network Traffic Monitoring Tools [15]

- **Wireshark:** The most popular network traffic analyzer is this one. It may be used to capture network traffic in real time using the libpcap (packet capture) format. It works with a variety of operating systems, such as Windows and Linux versions. By doing this, network activity is captured as packets and stored in a packet buffer for subsequent review and analysis.
- **TcpDump:** The TCP Dump utility has its roots in the 1990s and the work of the Lawrence Berkeley National Laboratory. Typical command line packet sniffer and analyzer functionality. All of the network's incoming and outgoing packets are examined and the results are given. Its primary use is in manner of operation that is intended to be promiscuous [16].
- **Xplico:** It collects network traffic and transforms it into a form that manipulators may utilize, making it a type of sniffer tool. The primary use of this utility is to extract audio sessions from streams. Xplico comes pre-installed with the Linux Kali distribution, making it ideal for penetration testing.
- **PyFlag:** The Australian Department of Defence was the original source of PyFlag, which was distributed under the GPL in 2007. Web page reconstruction, email analysis, and other fields make use of its implementation approaches [17].
- **NfDump:** This tool assists in gathering packet data as it travels through the network's nodes, including IP addresses. This utility is a synonym for tcpdump and gives the user access to a command line interface. The output of this tool is shown on the command line interface.
- **PcapWT:** The ability to handle enormous data sets is one of the tool's benefits. According to a recent case study, it outperforms tcpdump by a factor of one hundred [18]. In contrast to more conventional methods, it can quickly investigate large arrays of packet data utilizing a wavelet tree data structure.
- **NetworkMiner:** The first version of NetworkMiner was released in 2007. Packet sniffing and incident response are made easier using this tool for network forensic investigation. Extracting audio from VoIP conversations, identifying geoIP addresses, mapping, and ports are just a few of its many uses.
- **NetIntercept:** NetIntercept was first established in 2007. This network monitoring and analysis utility is installed at the network interface. In order to be prepared for deployment, it is packaged with hardware. This program offers thorough packet analysis and inspection at a respectable pace.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

IV. SECURITY IN TRAFFIC-INTELLIGENT IOT-CLOUD NETWORKS

Protecting the network that connects IoT devices is the main objective of IoT network security. This entails protecting lines of communication among devices and the network as well as between devices [19]. Firewalls, intrusion detection systems, and encryption are important precautions. While using cloud technology and linked devices offers numerous benefits, there are risks involved. To avoid traps and dead ends, the labyrinth must be carefully navigated. Likewise, IoT cloud security necessitates attentiveness to successfully address a range of issues and difficulties. Examine the six manageable IoT cloud security tactics shown in Figure 6.

Fig.6. Strategies for Managing IoT Cloud Security

A. Track and Manage Your Devices

Maintain an up-to-date inventory of all IoT devices, their configurations, and statuses. Mapping device connectivity helps identify potential vulnerabilities and ensures better visibility into your IoT ecosystem. Apply firmware updates and security patches regularly to close known security gaps.

B. Use Up-to-Date Encryption Protocols

Secure your sensitive information by encrypting it while it is in transit and at rest using a robust standard like AES. Ensure encryption keys are strong, unique, and rotated regularly to maintain robust protection against unauthorized access.

C. Conduct Regular Penetration Testing

Perform simulated attacks to identify and fix vulnerabilities in IoT devices, networks, and applications. These tests should be conducted periodically and after major infrastructure changes to ensure continuous security readiness.

D. Segment Your Network

Enhance security by isolating IoT devices from critical systems using network segmentation. Use firewalls and strict access controls between segments to contain breaches and limit their impact.

E. Invest in Observability

Implement scalable observability tools that provide real-time monitoring, alerts, and analytics across the IoT infrastructure. Early detection of anomalies helps mitigate threats before it escalate.

F. Deploy Runtime Security Measures

Use behavior analytics and real-time monitoring to detect unusual activities during device operation. Ensure secure communication with control servers for rapid threat response and mitigation.

V. OPTIMIZATION TECHNIQUES FOR TRAFFIC MANAGEMENT

Network optimization is a continuous set of changes and adaptations that are updated and improved as an organization gains a better knowledge of its network and user needs rather than a single strategy or plan. The ability to foresee demands and requirements as the organization grows is crucial for effective network optimization [20]. There are several different methods for optimizing networks. Some things, like ensuring your software and hardware are up to date, are easier. More technical methods exist, such as improving your company's network configuration or obtaining useful insights via the use of network monitoring tools. A few things that could influence optimization of a network are these:

ISSN : 2455-9679
SJIF Impact Factor : 6.008

- **Network size:** The quantity of users, apps, endpoints, and network devices on your network may significantly affect network data flows and bandwidth use.
- **Geographical Distance:** The speed-of-light issue is very much a reality for networks that cover huge geographical distances.
- **Last and middle-mile problems:** The ability to anticipate and mitigate issues in the last and middle miles between endpoints is essential for network engineers in the age of remote work, VPNs, and cloud computing. The last mile refers to the first or final leg of a data transmission from an Internet service provider to its final destination. Infrastructure that spans the distance between the first and final miles, often owned by many ISPs, is referred to as the middle mile.
- **Wired and wireless connectivity issues:** The performance of a network may be affected by the physical medium that transmits data over it. Connection issues caused by frayed or loose wires may be a major hassle to resolve. Similarly, basic Wi-Fi repeaters may cause network congestion and unreliable Wi-Fi can affect performance.algorithms.

VI. LITERATURE REVIEW

This section summarizes several methods to traffic monitoring, focusing on the technologies that have been utilized to solve certain concerns.

Musa et al. (2023) suggested a framework that could greatly benefit smart city transport by assisting with traffic prediction, forecasting, decongestion, minimizing lost time for road users, providing alternative routes, and making urban transport activities easier for city dwellers. By bolstering public transport and low-carbon emission zones, the proposed integrated framework may potentially benefit smart city pollution issues. Sustainable traffic management and a smaller carbon impact are two goals that smart cities can work towards with these technologies [21].

Rai et al. (2023) recommend an IoT-based Intelligent Traffic Signal System (ITSS) that uses programmable microcontrollers and inductive loops to detect traffic intensity in real-time. For efficient and timely vehicle movement, the centralized control unit's communication mechanisms establish the traffic signal timing and synchronize with real-time traffic density. The light post's timing is adjusted in real-time based on traffic congestion, which improves vehicle flow and reduces traveler wait. The offered solution outperforms fixed systems thanks to its autonomous on-demand traffic signaling system [22].

Monica et al. (2023) contemporary advancements such as GPS, which provide up-to-the-minute traffic information and emergency vehicle monitoring, AI and DL that can predict traffic solutions, data processing in the cloud, and the IoT that collects data in real-time and offers possible answers. Topics covered in this article include traffic control using AI, the Internet of Things, and GPS. It suggests an improved system for managing traffic signals that prioritizes emergency cars, cuts down on commute time, and monitors vehicles [23].

Abunadi et al. (2022) puts forth a system architecture for managing network traffic that integrates smart farming with fog computing. To begin, the suggested architecture effectively prevents the wasteful use of transmission bandwidth by monitoring redundant information. The second step in creating a reliable network of agricultural sensors is to use fog nodes to address security issues and increase reliability by preventing malicious transmission. The suggested approach outperformed previous similar efforts in terms of energy efficiency, security, and network connection, as shown by numerous simulation-based trials [24].

Nguyen et al. (2021) provide a method for monitoring traffic that is based on federated DDQN as a way to make the edge nodes' learning performance much better. Results from rigorous simulations show that the DeepMonitor can completely avoid the flow-table overflow problem at the edge nodes. When compared to an existing solution, FlowStat, DeepMonitor improves upon it by increasing the average number of match-fields in a flow rule by over 37% for needs with medium and diverse granularity levels and by over 41.9% for needs with high granularity levels. As a conclusion, an intrusion detection system's DDoS attack detection performance may be improved by as much as 22.83% when compared to FlowStat when DeepMonitor is used [25].

Guo and Yuan (2021) evaluate traffic optimization targets with techniques for routing computation (such as greedy and top-k-shortest pathways, or KSP) and optimization of routes (such as genetic, simulated annealing, and particle swarm optimization). Three optimization algorithms, network congestion management and prevention algorithms, resource

preemption algorithms, and balancing of all network traffic algorithms, are also proposed for the operator's network. Then, for each of the three operator network optimization goals listed above, it provides optimization strategies. Lastly, in order to confirm that the control mechanism and algorithms are successful, large-scale tests are conducted. Findings from the experiments show that operator networks may achieve smarter network management and traffic optimization with the use of SDN and AI [26].

Several recent studies have explored diverse approaches to intelligent traffic monitoring, leveraging technologies such as IoT, AI, SDN, fog computing, and DL to address congestion, optimize signals, and prioritize emergency vehicles. While these contributions have shown promising results, as summarized in Table II, key limitations remain. Most solutions are domain-specific and lack integration across heterogeneous systems, which is essential for managing complex urban traffic scenarios. Moreover, challenges related to data privacy, scalability, and real-time adaptability are often underexplored. These research gaps underscore the need for a comprehensive, interoperable, and secure traffic management framework that enables real-time decision-making under dynamic urban conditions.

TABLE II. SUMMARY OF RECENT RESEARCH ON TRAFFIC MONITORING APPROACHES IN IOT AND CLOUD

Author	Proposed Approach/Framework	Technologies Used	Key Contributions	Future Work
Musa et al. (2023)	Integrated framework for smart cities' transportation and traffic decongestion	AI, Traffic Prediction, Smart City Tools	Reduces congestion, promotes public transport, supports low-carbon zones, and enhances urban mobility.	Integration with smart infrastructure and real-time environmental data.
Rai et al. (2023)	IoT-based Intelligent Traffic Signal System (ITSS) with emergency vehicle prioritization	IoT, Infrared Sensors, Inductive Loops, Microcontroller	Enables real-time signal control, reduces delay, and ensures emergency vehicle priority.	Scaling to larger cities and inclusion of pedestrian and bicycle traffic modules.
Monica et al. (2023)	AI-driven traffic signal management system with real-time tracking and congestion reduction	GPS, AI, Deep Learning, IoT, Cloud Computing	Offers predictive traffic solutions, vehicle tracking, and congestion mitigation using multiple integrated technologies.	Improve algorithmic complexity, scalability, and privacy-preserving data models.
Abunadi et al. (2022)	Fog computing framework for smart farming and traffic-related network control	Fog Computing, Secure Communication Protocols	Enhances bandwidth usage, prevents malicious traffic, and improves energy efficiency in distributed networks.	Extend fog-based monitoring to other smart infrastructure such as traffic cameras and sensors.
Nguyen et al. (2021)	Federated DDQN-based DeepMonitor for edge-based traffic intelligence and DDoS detection	Federated Learning, Deep Reinforcement Learning, Edge Computing	Prevents flow-table overflow, improves rule matching efficiency, and enhances DDoS detection by up to 22.83%.	Apply DeepMonitor in multi-tenant edge networks with complex real-world traffic flows.
Guo and Yuan (2021)	AI and SDN-based traffic control with optimization modules and intelligent routing	SDN, AI, Genetic Algorithms, PSO, Simulated Annealing	Enables intelligent network control, load balancing, and routing using advanced optimization methods.	Develop real-time adaptive optimization models for dynamic traffic and user demand patterns.

VII. CONCLUSION

The integration of IoT and cloud computing offers transformative potential for real-time traffic monitoring, intelligent decision-making, and scalable network management. Through the adoption of SDN, AI, and advanced security mechanisms, significant progress has been made in addressing challenges related to network visibility, anomaly

detection, and performance optimization. However, critical gaps remain, particularly in ensuring real-time adaptability, cross-platform interoperability, and robust protection against evolving cyber threats. Future research should focus on developing unified frameworks that combine AI-driven analytics, federated learning, and decentralized architectures such as edge and fog computing to enhance responsiveness and reduce latency. Additionally, integrating privacy-preserving techniques and context-aware policies will be essential for building secure, intelligent, and resilient IoT-cloud ecosystems capable of sustaining the demands of rapidly evolving digital infrastructures.

REFERENCES

[1] M. Gaglianese, S. Forti, F. Paganelli, and A. Brogi, "Assessing and enhancing a Cloud-IoT monitoring service over federated testbeds," *Futur. Gener. Comput. Syst.*, vol. 147, pp. 77–92, Oct. 2023, doi: 10.1016/j.future.2023.04.026.

[2] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 6, 2023.

[3] M. Hammoudeh *et al.*, "Network Traffic Analysis for Threat Detection in the Internet of Things," *IEEE Internet Things Mag.*, 2021, doi: 10.1109/iotm.0001.2000015.

[4] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," *IEEE Internet Things J.*, 2020, doi: 10.1109/JIOT.2020.2997651.

[5] S. S. S. Neeli, "Critical Cybersecurity Strategies for Database Protection against Cyber Attacks," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, 2023.

[6] R. Patel, "Advancements in Renewable Energy Utilization for Sustainable Cloud Data Centers : A Survey of Emerging Approaches," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 5, pp. 447–454, 2023.

[7] A. Antim and L. La Blunda, "An Extensive Review on Interfaces between IoT and Cloud Computing," 2021.

[8] M. Mansour *et al.*, "Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions," *Energies*, vol. 16, no. 8, Apr. 2023, doi: 10.3390/en16083465.

[9] J. Guth *et al.*, "A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences Institute of Architecture of Application Systems A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences," *Internet Everything Algorithms, Methodol. Technol. Perspect.*, 2018.

[10] H. R. Abdulqadir *et al.*, "A Study of Moving from Cloud Computing to Fog Computing," *Qubahan Acad. J.*, 2021, doi: 10.48161/qaj.v1n2a49.

[11] A. Goyal, "Enhancing Engineering Project Efficiency through Cross-Functional Collaboration and IoT Integration," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 396–402, 2021.

[12] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog Computing and the Internet of Things: A Review," *Big Data Cogn. Comput.*, vol. 2, no. 2, p. 10, Apr. 2018, doi: 10.3390/bdcc2020010.

[13] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," *Futur. Gener. Comput. Syst.*, 2016, doi: 10.1016/j.future.2015.09.021.

[14] X. Yin, X. Chen, L. Chen, G. Shao, H. Li, and S. Tao, "Research of Security as a Service for VMs in IaaS Platform," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2837039.

[15] P. Kaur and N. Misra, "A Methodical Review on Network traffic monitoring and Analysis tools," *JAC A J. Compos. Theory*, vol. 12, no. 9, pp. 1964–1968, 2019.

[16] F. Fuentes and D. Kar, "Ethereal vs. Tcpdump: a comparative study on packet sniffing tools for educational purpose," *J. Comput. Sci. Coll.*, 2005.

[17] A. Byrski, W. Stryjewski, and B. Czechowicz, "Adaptation of PyFlag to Efficient Analysis of Seized Computer Data Storage," *J. Digit. Forensics, Secur. Law*, 2010, doi: 10.15394/jdfsl.2010.1071.

[18] Y.-H. Kim, R. Konow, D. Dujovne, T. Turletti, W. Dabbous, and G. Navarro, "PcapWT: An efficient packet extraction tool for large volume network traces," *Comput. Networks*, vol. 79, pp. 91–102, Mar. 2015, doi: 10.1016/j.comnet.2014.12.007.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

[19] S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based IoT Networks," *J. Crit. Rev.*, vol. 6, no. 7, 2019, doi: 10.53555/jcr.v6:i7.13156.

[20] R. Patel, "Artificial Intelligence-Powered Optimization of Industrial IoT Networks Using Python-Based Machine Learning," *J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 138–148, 2023, doi: 10.56472/25832646/JETA-V3I8P116.

[21] A. A. Musa, S. I. Malami, F. Alanazi, W. Ounaies, M. Alshammari, and S. I. Haruna, "Sustainable Traffic Management for Smart Cities Using Internet-of-Things-Oriented Intelligent Transportation Systems (ITS): Challenges and Recommendations," *Sustain.*, 2023, doi: 10.3390/su15139859.

[22] S. C. Rai, S. P. Nayak, B. Acharya, V. C. Gerogiannis, A. Kanavos, and T. Panagiotakopoulos, "ITSS: An Intelligent Traffic Signaling System Based on an IoT Infrastructure," *Electronics*, vol. 12, no. 5, Feb. 2023, doi: 10.3390/electronics12051177.

[23] M. C *et al.*, "Intelligent Traffic Monitoring, Prioritizing and Controlling Model based on GPS," in *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, IEEE, Mar. 2023, pp. 297–299. doi: 10.1109/ICIDCA56705.2023.10100296.

[24] I. Abunadi, A. Rehman, K. Haseeb, L. Parra, and J. Lloret, "Traffic-Aware Secured Cooperative Framework for IoT-Based Smart Monitoring in Precision Agriculture," *Sensors*, vol. 22, no. 17, Sep. 2022, doi: 10.3390/s22176676.

[25] T. G. Nguyen, T. V. Phan, D. T. Hoang, T. N. Nguyen, and C. So-In, "Federated Deep Reinforcement Learning for Traffic Monitoring in SDN-Based IoT Networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 4, pp. 1048–1065, Dec. 2021, doi: 10.1109/TCCN.2021.3102971.

[26] A. Guo and C. Yuan, "Network Intelligent Control and Traffic Optimization Based on SDN and Artificial Intelligence," *Electronics*, vol. 10, no. 6, Mar. 2021, doi: 10.3390/electronics10060700.