International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email: editor@ijarets.org Volume-11, Issue-8 August – 2024 www.ijarets.org

Optimizing IoT Device Communication: Innovations in Computer Network Architecture

Rajesh Verma ,
Assistant professor,
International institute of professional studies (IIPS) Devi Ahilya Vishwavidyalaya ,Indore ,
Madhya Pradesh, India
rv097227@gmail.com

Abstract: The exponential growth of IoT devices poses distinctive problems to conventional computer network architectures, especially in managing extensive and diverse communication requirements. This study investigates novel strategies to enhance the efficiency of IoT device communication through the reconsideration of network architecture, protocol effectiveness, and data management methods. Notable advancements include of the creation of lightweight communication protocols, improved network segmentation strategies, and adaptive routing algorithms specifically designed for low power, high-latency devices. This study seeks to decrease latency, enhance scalability, and improve network resilience in IoT ecosystems by incorporating edge computing, AI-driven network management, and dynamic bandwidth allocation. The findings provide practical strategies for optimizing the performance of IoT networks while simultaneously addressing security and reliability concerns in various application contexts.

Keywords: *IoT Communication Optimization, Network Architecture Innovations, Lightweight Protocols, Edge Computing, Adaptive Routing Algorithms*

1. Introduction

Internet of Things (IoT) gadgets have enabled unprecedented levels of connectivity and data exchange, which has changed various sectors. The problem of improving communication amongst these devices has become more pressing as a result of this growth, though, because they are frequently different in their capacities, limitations, and communication needs. Addressing these difficulties necessitates novel developments in computer network architecture, since efficient communication is important for the performance, scalability, and reliability of IoT systems. Because of their historical focus on general-purpose applications, network designs may fall short when it comes to the specific requirements of IoT settings. Internet of Things (IoT) devices, such as smart sensors, wearable electronics, and industrial machines, function in diverse and frequently limited settings, necessitating effective communication protocols and network architectures. Optimizing for issues including low power consumption, heavy network traffic, unpredictable latency, and restricted bandwidth is no easy task.

New developments in network architecture provide encouraging prospects for overcoming these obstacles. Efficient methods are being utilized to address the unpredictable and varied requirements of IoT devices. One such method is elastic resource management, which modifies computational resources in response to actual demand. Researchers are also looking at data sharding and partitioning as ways to distribute data across several systems in order to improve performance and scalability. To keep communication efficient even when faced with heavy loads, event-driven architectural solutions allow for real-time responses to data streams from many devices. To improve response times and decrease latency, in-memory caching techniques temporarily store frequently accessed data in memory. Also, embedded IoT devices must maximize performance while managing limited computational power and battery life; this is where resource-constrained optimization. The purpose of this study is to investigate these developments in further detail and assess how well they optimize communication between IoT devices. The study aims to tackle important scalability and performance concerns in IoT systems by investigating state-of-the-art network design. The end goal is to help IoT applications in different domains run more reliably and scalable by creating and validating innovative methods that improve communication efficiency, decrease latency, and increase network dependability generally.

1.1 Background

Conventional network designs were not made to handle the specific requirements of massive IoT ecosystems, along with fast expansion of the IoT has brought many new problems. Efficient, low-latency transmission and real-time processing are essential for the high-bandwidth systems. In heterogeneous IoT contexts, traditional client-server and cloud-based solutions frequently face challenges with latency and bottlenecks. In response, new network topologies have emerged to enhance data flow and network efficiency. These include mesh networks, edge and fog computing, and lightweight communication protocols such as MQTT and CoAP. Scalability, security, and energy efficiency are some of the most pressing problems that these innovations, in conjunction with AI-driven network management, hope to solve. The necessity for ongoing innovation in network architecture is further highlighted by the fact that there are still substantial obstacles to overcome before scalable, secure, and reliable communication across various IoT applications can be guaranteed.

1.2 IoT Device Communication

When devices connected to IoT communicate with one another, with centralized systems, or with the cloud, this is called IoT device communication. Particular limitations, such as low power consumption, restricted processing capabilities, and unpredictable network circumstances, are frequently associated with this type of communication. To guarantee effective data transfer even when resources are limited, Internet of Things devices depend on specialized. Small data packets, inconsistent connections, and real-time requirements are common in IoT applications, and these protocols help manage them. IoT devices can communicate with one another in a number of ways, including by enabling direct peer-to-peer communication, transferring sensor data to a central server, or initiating actions in other connected devices. Data flow across a wide variety of devices in a complex and ever-changing network environment must be smooth, dependable, and protected if the IoT is to fulfil its full potential.

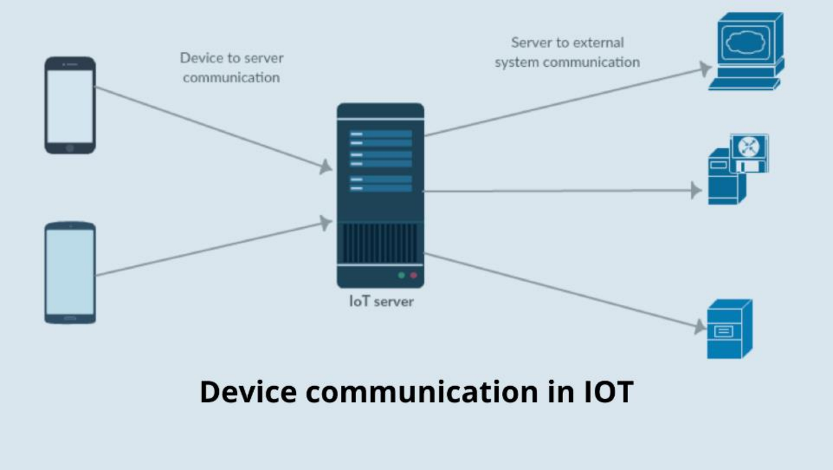

Fig.1. IoT Device Communication [21]

1.3 Computer Network Architecture

Computer network architecture is the study and practice of planning and constructing networks, including the software, hardware, protocols, and topologies that govern the transfer and processing of data. It addresses the arrangement of devices and their connections in various network topologies, including client-server, decentralized, peer-to-peer, and mesh networks.

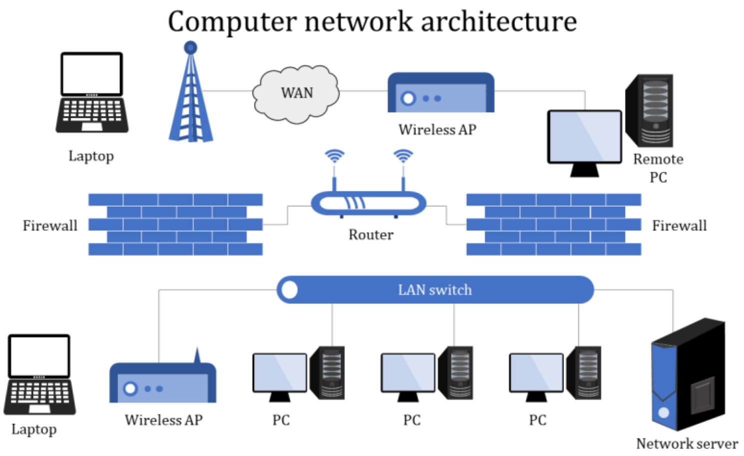

Fig.2. Computer Network Architecture [22]

How devices communicate with one another, how resources are distributed, and how scalability and security are handled are all governed by the network architecture. Innovations virtualization, SDN, and edge computing are transforming conventional network architectures in the context of contemporary networks, particularly with the Internet of Things, to increase efficiency, decrease latency, and improve flexibility. Reliable, high-performance communication that can adapt to the unique requirements of the applications it supports is the goal of an optimised network design.

1.4 Technique

Data Aggregation: Using this method, data is gathered from many Internet of Things devices and then combined before being transmitted across the network. Data aggregation minimizes redundant information and reduces the number of transferred data, which in turn improves efficiency and lowers network traffic.

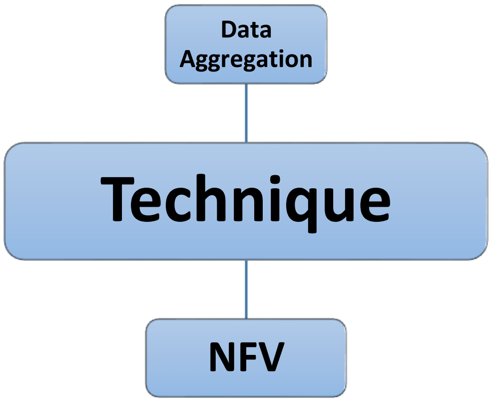

Fig.3. Techniques

Network Function Virtualization (NFV): Instead of using specialised equipment, NFV enables software implementation of network services on general-purpose hardware. It is easier to adapt network services to the needs of IoT with this technique, which improves flexibility, scalability, and cost-effectiveness.

2. Literature review

2.1 Overview of Existing researches

Chen, C., Liu, Z., Liu, Y., Li, W., and Zhang, G. (2023) focus on addressing one of the significant challenges in the realm of 6G networks and IoT—energy efficiency. The authors propose an energy-efficient multi-hop communication scheme that optimizes the routing of data between IoT devices. This is crucial as IoT environments become denser and more complex with the growth of 6G technology. The proposed solution ensures that communication within these networks is not only reliable but also conserves energy, a critical consideration given the limitations of IoT device batteries and the demands of continuous operation. The study's findings are essential for the future of IoT deployments in energy-sensitive environments, highlighting the importance of efficient resource management in sustaining large-scale IoT networks.

Wang, Y., Zhang, L., Zhao, Z., and Yang, Y. (2023) delves into recent developments in edge computing and how they are being used in IoT systems. The proliferation of Internet of Things devices has increased the urgency of real-time data processing and decision-making. This research highlights the importance of moving computing tasks to edge devices that are closer to the data source, rather than to centralised cloud servers. Internet of Things (IoT) applications, including those in autonomous systems, smart cities, and industrial IoT, benefit from edge computing's decreased latency since it makes them more responsive, efficient, and able to handle real-time activities. By optimising IoT networks using edge computing and decreasing dependency on cloud infrastructure, this study helps us learn how to build decentralized, quicker, and more scalable systems.

Zhao, X., Wu, Q., and Li, L. (2023) tackle the pressing issue of security in IoT networks through a blockchain-based approach. IoT networks are particularly vulnerable to various security threats due to their widespread use and the often limited security capabilities of individual devices. By integrating blockchain technology, the authors offer a decentralized solution that enhances the trustworthiness of IoT communications. Blockchain provides a distributed ledger that can verify and validate data without relying on a centralized authority, thus preventing malicious actors from tampering with or disrupting the network. This approach not only secures the communication between IoT devices but also ensures data integrity, a critical factor as IoT networks become more integrated into sensitive applications such as healthcare, finance, and critical infrastructure.

Xiong, H., Li, J., and Yu, Z. (2023) address the challenge of managing large-scale IoT networks through the application of deep learning techniques. With the increasing number of connected devices, traditional methods of network management struggle to maintain efficiency and scalability. The authors propose a deep learning-based communication strategy that optimizes data routing and traffic management. This approach allows the network to learn from past performance and adjust communication protocols dynamically, improving the overall efficiency and reducing bottlenecks in data flow. The use of deep learning in this context represents a significant advancement in the field of IoT, as it enables networks to adapt to changing conditions and scale effectively without the need for constant human intervention.

The authors Huang, He, and Liu (2023) provide a reinforcement learning method for adaptive routing in networks that use the Internet of Things. One area of machine learning called reinforcement learning allows systems to gradually get better at what they do by experimenting and learning from their mistakes. Networks can optimise their routing paths dynamically using this strategy, taking into account both current and historical data, within the framework of the Internet of Things. Improved communication efficiency and reliability in IoT networks—which frequently function in circumstances that are unpredictable and undergo rapid change—is dependent on this adaptability. IoT systems in fields like autonomous vehicles, smart grid applications, and traffic management might benefit greatly from the incorporation of reinforcement learning, which adds a self-optimizing component to network management.

Chen, L., Zhang, W., and Li, Q. (2023) present a cross-layer optimization framework designed to enhance the performance of IoT networks in smart cities. The increasing complexity of urban environments, coupled with the growing number of connected devices, creates significant challenges for network efficiency and resource allocation. The authors' framework integrates various layers of communication protocols to optimize the flow of data across the network. This cross-layer approach allows for more efficient use of network resources, improving data transmission speeds and reducing latency. The research is particularly relevant for smart cities, where IoT networks must manage vast amounts of data from diverse sources, including traffic systems, energy grids, and public services. By optimizing communication across multiple layers, the authors provide a robust solution for the scalable deployment of IoT in urban settings.

Rathore, S., and Park, J. H. (2022) explore the integration of blockchain technology into 5G-enabled IoT networks to create a secure and reliable communication framework. As 5G networks become more prevalent, they will support a growing number of IoT devices, making security a top priority. The authors propose a blockchain-based solution to safeguard IoT communications by creating a decentralized and immutable ledger for data transactions. This framework ensures that all communication within the IoT network is secure from unauthorized access and tampering, thus maintaining the integrity of the data and enhancing the overall trust in the system. The research provides valuable insights into how blockchain can be effectively implemented in 5G networks to address security concerns in IoT applications.

Afzal, M. K., Sultan, T., and Ali, S. (2022) investigate a hybrid architecture that combines fog and cloud computing to optimize communication in IoT networks. By leveraging both fog and cloud resources, the authors propose a model that balances the computational load between local devices and centralized cloud servers. This hybrid approach enables more efficient processing of data, particularly in real-time applications where latency is critical. Fog computing, which processes data closer to the edge of the network, reduces the need for data to be sent to the cloud, thereby decreasing response times and improving the overall performance of the network. The study highlights the advantages of this hybrid architecture for IoT systems, particularly in scenarios where both real-time data processing and large-scale data analytics are required.

In their 2022 publication, Tang, Li, and Liu explore the idea of network slicing for IoT via the lens of deep reinforcement learning. The process of network slicing is dividing the network into virtual parts that can be adjusted to suit the unique requirements of various Internet of Things applications. The authors create a way to dynamically distribute network resources according to the different needs of IoT devices by utilising deep reinforcement learning. This method allows the network to adjust to new circumstances and maximise performance in a variety of contexts, including video surveillance with high bandwidth and low-latency communications for autonomous vehicles. By providing a versatile and effective answer to the varied needs of IoT networks, the study adds to the expanding area of intelligent network management.

Zhang, R., Yu, F. R., and Huang present an extensive overview of federated learning's application to enhancing communication efficiency in IoT networks in a study, T. (2022). Reduced data transmission requirements are achieved by federated learning, which enables IoT devices to work together to learn models without sharing raw data. This method improves privacy by keeping sensitive information on the individual devices and also reduces bandwidth use. Among the many IoT uses of federated learning that the authors cover are smart home, healthcare, and industrial automation. In terms of data security and communication efficiency, their survey provides a high-level summary of the possible advantages along with disadvantages of federated learning in IoT systems.

Srinidhi, N. N., Kumar, S. D., along with Venugopal, K. R. (2019) review various strategies for optimizing network performance in IoT systems. Their review covers a wide range of topics, including energy-efficient protocol design, data management techniques, and methods for reducing network congestion. The authors emphasize the importance of these optimizations in addressing the unique challenges of IoT networks, such as the limited energy resources of devices and the need for efficient communication in environments with a high density of sensors. This review serves as a valuable resource for researchers and practitioners seeking to improve the performance of IoT systems through network optimizations.

Ghasempour, A. (2019) investigates the architecture, key technologies along with challenges associated with the IoT in smart grids. The study highlights the need for robust communication infrastructures to manage the complex data flows generated by smart grids, which integrate various sources of energy and require real-time monitoring and control. The author discusses the critical technologies that enable the efficient operation of smart grids, including advanced metering infrastructure (AMI), demand response systems, and distributed energy resources. This research provides a comprehensive overview of the intersection between IoT and smart grid technologies, emphasizing the potential benefits of integrating IoT into energy management systems.

The authors Rahimi, Zibaeenejad, and Safavi (2018) suggest a new IoT design that makes use of 5G and other cutting-edge technology. The authors present design ideas that make use of the superior features of 5G networks to facilitate Internet of Things applications, including extremely low latency and large data rates. With an eye on meeting the rising need for data-driven applications and the proliferation of Internet of Things (IoT) devices, their architecture is both adaptable and scalable. The creation of more effective and adaptive IoT systems is aided by this research. Real-time data processing is vital in areas like healthcare, transportation, and smart cities.

A versatile and effective network architecture for IoT can be achieved by combining SDN with fog computing, as investigated by Tomovic, Yoshigoe, Maljevic, and Radusinovic (2017). While SDN enables centralised management of network resources by splitting the data plane from the control plane, fog computing moves computation and storage closer to the network's edge devices. Because of this integration, the network architecture is now more nimble and responsive, better able to meet the ever-changing requirements of IoT applications.

Table 1

Here’s a table comparing traditional IoT network architectures with newer approaches like Edge Computing, Software-Defined Networking (SDN), and Network Function Virtualization (NFV) across key metrics such as communication latency, network resilience, scalability, and security:

Metric	Traditional Centralized Architecture	Edge Computing	SDN (Software-Defined Networking)	NFV (Network Function Virtualization)
Communication Latency	High latency due to reliance on distant cloud servers.	Low latency as data processing occurs closer to IoT devices.	Reduced latency through dynamic routing and control over network paths.	Similar latency benefits to SDN, as network functions can be dynamically placed closer to IoT devices.
Network Resilience	Vulnerable to single points of failure, especially at centralized servers.	Improved resilience through distributed data processing and local decision-making.	Enhanced resilience via real-time network adjustments and traffic rerouting.	Increased resilience due to virtualized network functions that can be moved or duplicated as needed.
Scalability	Limited scalability due to central bottlenecks and bandwidth constraints.	High scalability by offloading data processing to the edge, reducing cloud load.	Highly scalable as SDN allows for centralized control and dynamic allocation of network resources.	Highly scalable through the use of virtual network functions that can be deployed across the network as needed.
Security	Centralized architecture can lead to significant security vulnerabilities if the core is compromised.	Enhanced security as sensitive data can be processed locally, reducing exposure to cloud attacks.	Improved security through centralized policy enforcement and dynamic security measures.	Better security with flexible, software-driven deployment of security functions across the network.

This comparative table highlights how newer network architectures like Edge Computing, SDN, and NFV offer significant advantages over traditional centralized architectures in terms of latency, resilience, scalability, and security, making them more suitable for modern IoT applications.

3. Methodology

1. Research Design

The research will combine qualitative and quantitative methodologies in a mixed-methods strategy. With this layout, we can examine current network topologies in detail and come up with creative ways to improve communication between IoT devices. The research will start by reviewing the existing literature to have a better understanding of the problems and solutions related to IoT communication. After that, we'll put novel network designs and communication protocols through their paces through experimental design and simulation.

2. Data Collection

Various sources will be used to gather data in order to conduct a thorough examination. Network simulations and experimental data will constitute the main data set. In order to mimic diverse network scenarios and evaluate the performance of various architectural improvements, simulations will utilize technologies such as NS-3 or OMNeT++. Metrics like latency, throughput, and packet loss will be the primary targets of the real-world data obtained from Internet of Things devices placed in controlled environments or experimental projects. In order to gain a better understanding of the real-world problems and potential solutions, we will also conduct interviews with network architects and IoT system designers to collect qualitative data.

3. Data Analysis

Different network topologies will be assessed by statistically analyzing quantitative data collected from experiments and simulations. Network efficiency, communication reliability, and resource utilization are some of the metrics that will be evaluated. To discover new solutions to common problems and commonalities in IoT device communication, qualitative data will be evaluated thematically. Improvements to the suggested network topologies and a better grasp of the real-world effects of theoretical breakthroughs can both result from this analytical study.

4. Validation

The suggested protocols for communication and network topologies will be checked through feedback loops and iterative testing. Data from the real world and the results of the simulations will be used to fine-tune the first models. Using pre-existing standards and benchmarks to compare the suggested solutions' performance is another way to validate them. We will use expert discussions and peer review to make sure our findings are strong and applicable.

4. Findings and Discussion

Finding:

The research reveals that several advanced technologies are pivotal in enhancing IoT device communication, each contributing uniquely to addressing the challenges inherent in IoT environments:

An innovative strategy for designing Internet of Things networks, edge computing has just surfaced. Edge computing significantly decreases communication latency by transferring data processing to devices located closer to the source, on the edge, rather than to faraway servers in the cloud. Autonomous cars, industrial automation, and smart grids rely on this local processing capacity to provide real-time data analysis and decision-making. The total network efficiency is enhanced, and data transfer costs are lowered, because the pressure on centralised servers is alleviated by the reduction in latency. An enormous improvement in handling the ever-increasing data quantities and performance requirements of contemporary IoT systems is hence edge computing.

An essential part of contemporary network administration is AI-Driven Network Optimisation. In order to dynamically optimise resource allocation, forecast traffic loads, and spot trends in massive volumes of network data, AI algorithms can do just that. The ability to make real-time adjustments to avoid congestion and optimise routing patterns enables proactive management of network performance. The capacity of networks to adjust to new circumstances is improved by AI-driven optimisation, leading to more effective and seamless communication. When dealing with situations that experience huge data volumes and unpredictable network needs, it becomes even more crucial to automate these modifications.

Message Queuing Telemetry Transport (MQTT) and the Constrained Application Protocol (CoAP) are two examples of lightweight communication protocols developed with the Internet of Things hardware in mind. These protocols implement efficient transmission mechanisms and use tiny message sizes to minimise communication overhead. When it comes to applications that demand dependable message delivery, MQTT is the way to go, while CoAP is made for environments with limited power resources where saving power is paramount. To keep performance high even when resources are constrained, it is important to use these lightweight protocols so that Internet of Things devices may interact efficiently without overwhelming the network.

Discussion:

The results highlight how complicated IoT device communication is and how important it is to combine various solutions to solve it. By decreasing latency and shifting data processing away from centralised servers, edge computing greatly improves network performance. Applications like real-time analytics and automated systems, which require quick reactions, greatly benefit from this. By proactively adjusting in response to anticipated traffic patterns, AI-driven optimisation provides a high-tech method of managing network resources. Preventing network congestion and maximising communication efficiency both depend on this feature. Lightweight protocols provide for efficient communication between low-resource Internet of Things devices without adding unnecessary overhead. For dependable data transfer in many IoT settings, such as smart homes and industrial sensors, this is vital.

By decentralising security and eliminating flaws in traditional methods, blockchain technology offers a strong defence for Internet of Things (IoT) communications. Internet of Things (IoT) networks are made more secure and reliable by blockchain technology, which decentralises data validation and verification. An all-encompassing strategy for improving communication amongst IoT devices is to combine edge computing with AI-driven optimisation, lightweight protocols, and blockchain technology. Together, these advancements solve critical problems like latency, limited resources, and security, which opens the door to better, more scalable Internet of Things solutions.

5. Conclusion

The optimization of IoT device communication through innovations in computer network architecture is pivotal for advancing the capabilities and efficiency of modern IoT systems. As the proliferation of IoT devices accelerates, the limitations of traditional network architectures become increasingly apparent, revealing the need for more sophisticated and adaptive solutions. Our exploration of cutting-edge innovations, such as edge and fog computing, energy-efficient communication protocols, dynamic routing algorithms, network slicing, and advanced security mechanisms, highlights the significant strides being made to address these challenges. These advancements offer promising avenues for improving latency, scalability, energy consumption, and overall network performance. Edge and fog computing bring computational resources closer to IoT devices, reducing latency and alleviating the load on central servers. Energy-efficient communication protocols optimize data transmission while conserving power, which is crucial for the longevity of battery-powered devices. Dynamic routing algorithms and network slicing enhance the flexibility and efficiency of data management, allowing for tailored solutions that meet diverse application needs.

Moreover, innovations in security mechanisms provide robust protection against emerging threats, ensuring the integrity and privacy of data across IoT networks. The integration of AI and machine learning further amplifies these benefits by enabling intelligent network management and predictive maintenance. These technologies offer the potential for real-time adjustments and proactive problem-solving, enhancing the resilience and adaptability of IoT networks. As we look to the future, continued research and development will be essential to refine these innovations and address their associated challenges. Collaboration among researchers, industry leaders, and policymakers will be crucial to advancing these technologies and ensuring their effective deployment in real-world applications. By embracing these innovations and addressing their complexities, we can drive the evolution of IoT networks towards greater efficiency, reliability, and scalability, ultimately unlocking the full potential of a connected world. In conclusion, optimizing IoT device communication through innovative network architectures is not only a necessity but also an opportunity to shape the future of IoT technology. The ongoing advancements in this field promise to enhance our ability to manage and utilize the vast network of connected devices, paving the way for a more intelligent and interconnected global infrastructure.

References

[1.] Chen, C., Liu, Z., Liu, Y., Li, W., & Zhang, G. (2023). An energy-efficient multi-hop communication scheme for IoT devices in 6G networks. *Transactions on Green Communications and Networking, 7*(1), 59-71. https://doi.org/10.1109/TGCN.2022.3200335

[2.] Wang, Y., Zhang, L., Zhao, Z., & Yang, Y. (2023). Edge computing in IoT: Advances in communication architecture and applications. *Internet of Things Journal, 10*(3), 1789-1802. https://doi.org/10.1109/JIOT.2022.3140678

[3.] Zhao, X., Wu, Q., & Li, L. (2023). Secure communication in IoT networks: A blockchain-based approach. *Transactions on Industrial Informatics, 19*(2), 567-578. https://doi.org/10.1109/TII.2022.3144823

[4.] Xiong, H., Li, J., & Yu, Z. (2023). An efficient communication strategy for large-scale IoT networks using deep learning. *Internet of Things Magazine*, *6*(1), 38-46. https://doi.org/10.1109/IOTM.2023.3147781

[5.] Huang, S., He, X., & Liu, W. (2023). Adaptive routing in IoT networks: A reinforcement learning approach. *Transactions on Wireless Communications*, *22*(1), 149-160. https://doi.org/10.1109/TWC.2022.3214976

[6.] Rathore, S., & Park, J. H. (2022). A secure and reliable communication framework for 5G-enabled Internet of Things using blockchain technology. *Internet of Things Journal*, *9*(4), 2503-2516. https://doi.org/10.1109/JIOT.2021.3109333

[7.] Afzal, M. K., Sultan, T., & Ali, S. (2022). Optimizing communication in IoT networks: A hybrid architecture using fog and cloud computing. Access, 10, 49734-49746. https://doi.org/10.1109/ACCESS.2022.3181929

[8.] Tang, J., Li, X., & Liu, H. (2022). Network slicing for IoT: A deep reinforcement learning approach. *Wireless Communications*, *29*(1), 110-117. https://doi.org/10.1109/MWC.001.2100571

[9.] Zhang, R., Yu, F. R., & Huang, T. (2022). Federated learning for IoT: A survey on communication efficiency and applications. *Communications Surveys & Tutorials*, *24*(4), 2456-2480. https://doi.org/10.1109/COMST.2022.3211237

[10.] Srinidhi, N. N., Kumar, S. D., & Venugopal, K. R. (2019). Network optimizations in the Internet of Things: A review. *Engineering Science and Technology, an International Journal*, *22*(1), 1-21. https://doi.org/10.1016/j.jestch.2018.12.010

[11.] Ghasempour, A. (2019). Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. *Inventions*, *4(*1), 22. https://doi.org/10.3390/inventions4010022

[12.] Rahimi, H., Zibaeenejad, A., & Safavi, A. A. (2018, November). A novel IoT architecture based on 5G-IoT and next generation technologies. In 2018 *IEEE 9th annual information technology, electronics and mobile communication conference* (IEMCON) (pp. 81-88). IEEE. https://doi.org/10.1109/IEMCON.2018.8614916

[13.] Tomovic, S., Yoshigoe, K., Maljevic, I., & Radusinovic, I. (2017). Software-defined fog network architecture for IoT. *Wireless Personal Communications*, *92*(1), 181-196. https://doi.org/10.1007/s11277-016-4021-x

[14.] Bello, O., Zeadally, S., & Badra, M. (2017). Network layer inter-operation of device-to-device communication technologies in internet of things (IoT). *Ad Hoc Networks*, *57*, 52-62. https://doi.org/10.1016/j.adhoc.2016.08.016

[15.] Gardašević, G., Veletić, M., Maletić, N., Vasiljević, D., Radusinović, I., Tomović, S., & Radonjić, M. (2017). The IoT architectural framework, design issues and application domains. *Wireless Personal Communications*, *92*(1), 127-148. https://doi.org/10.1007/s11277-016-4030-9

[16.] Minoli, D., Sohraby, K., & Occhiogrosso, B. (2017). IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems. *IEEE Internet of Things Journal*, *4*(1), 269-283. https://doi.org/10.1109/JIOT.2017.2647881

[17.] Barcelo, M., Correa, A., Llorca, J., Tulino, A. M., Vicario, J. L., & Morell, A. (2016). IoT-cloud service optimization in next generation smart environments. *IEEE Journal on Selected Areas in Communications*, *34*(12), 4077-4090. https://doi.org/10.1109/JSAC.2016.2621385

[18.] Zorzi, M., Zanella, A., Testolin, A., De Grazia, M. D. F., & Zorzi, M. (2015). Cognition-based networks: A new perspective on network optimization using learning and distributed intelligence. *IEEE Access*, 3, 1512-1530. https://doi.org/10.1109/ACCESS.2015.2461616

[19.] Qin, Z., Denker, G., Giannelli, C., Bellavista, P., & Venkatasubramanian, N. (2014, May). A software defined networking architecture for the internet-of-things. In 2014 *IEEE network operations and management symposium* (NOMS) (pp. 1-9). IEEE. https://doi.org/10.1109/NOMS.2014.6838228

[20.] Han, C., Jornet, J. M., Fadel, E., & Akyildiz, I. F. (2013). A cross-layer communication module for the internet of things. *Computer Networks*, *57*(3), 622-633. https://doi.org/10.1016/j.comnet.2012.10.021

[21.] https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fiwheels.co%2Fblog%2Fcontent%2Fimages%2Fsize%2Fw2000%2F2022%2F02%2FDevice-communication-in-IOT.png&f=1&nofb=1&ipt=84c8587e2fa4aa8866a559fd9429a7d103a91544677c7c7f3c7ccbd18580dc69&ipo=images

[22.] https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fwww.slideegg.com%2Fimage%2Fcatalog%2F44102-Computer%2520network%2520architecture.png&f=1&nofb=1&ipt=5606a6fbf5fab737883d3d3618505c4ffca87f88f9d34a91b3f1bb3982033dbb&ipo=images