A Cybersecurity Framework for Optimizing Broadband QoS in IoT Systems Using Machine Learning

Dusengumuremyi Olivier
ZCAS University
Lusaka, Zambia
dusengumuremyio@gmail.com

Christopher Chembe
NIPA
Lusaka, Zambia

Aaron Zimba
ZCAS University
Lusaka, Zambia
Aaron.zimba@zcasu.edu.zm

Abstract: ***The integration of Internet of Things (IoT) technologies in healthcare, particularly in Intensive Care Units (ICUs), holds transformative potential for patient monitoring and clinical decision-making. However, performance is often limited by high network latency and cybersecurity vulnerabilities, which are especially critical in time-sensitive applications such as remote monitoring and telemedicine. Achieving both ultra-low latency and strong data confidentiality in resource-constrained ICU environments remains a major challenge, as traditional methods fall short of meeting these dual requirements. This paper proposes a machine learning (ML)-driven cybersecurity framework that optimizes broadband Quality of Service (QoS) while ensuring robust data security in ICU-based IoT networks. The framework integrates supervised and unsupervised learning models for dynamic, context-aware adaptation to network conditions and emerging threats. Key features include intelligent traffic prioritization, secure communication protocols, and adaptive bandwidth allocation. Expected outcomes are reduced latency, improved confidentiality, and enhanced reliability of ICU systems. Beyond technical contributions, the framework promotes trust in digital healthcare and advances interdisciplinary research across ML, network optimization, and medical cybersecurity.***

Keywords: Internet of Things; Intensive Care Units; Machine Learning; Cybersecurity; Quality of Service; Data Confidentiality

I. INTRODUCTION

Modern life is greatly impacted by Internet of Things (IoT) applications, particularly in intelligent healthcare. Applications' seamless operation and user experience depend on dependable Quality of Service (QoS). However, as IoT systems become more networked, they become more vulnerable to cybersecurity attacks, necessitating the implementation of robust security frameworks. To retain security while still providing the necessary performance, it is difficult to strike a compromise between stringent QoS criteria and robust security measures that IoT applications demand. According to some recent research, a system that combines random forest for traffic categorization with reinforcement learning for adaptive routing can improve network security and performance in IoT-enabled wireless sensor networks [1]. [2]developed a machine learning security framework that uses Software Defined Networking (SDN) and Network Function Virtualization (NFV) to accurately identify anomalies in Internet of Things devices**.**[3] achieved a maximum throughput of 94% by developing a dynamic-progressive deep reinforcement learning technique to enhance IoT QoS. [4] With a 99.9% accuracy rate in identifying cyberattacks, this study's machine learning (ML)-based security model for Internet of Things (IoT) devices outperforms previous models. Network security and performance management have historically been handled independently, which is inappropriate for contemporary Internet of Medical Things (IoMT) applications. The study outlines a suggested architecture and assesses potential future paths while investigating the creation of integrated, intelligent frameworks that use machine learning (ML) to achieve a thorough balance between security and quality of service (QoS).

One promising strategy to address contemporary challenges is machine learning (ML), which enhances network security and efficiency through adaptive and intelligent traffic handling. Unlike static approaches, ML-driven models adjust to evolving threat landscapes and traffic patterns, providing context-aware solutions suited for dynamic intensive care unit (ICU) environments. This study proposes a novel ML-driven cybersecurity framework to optimize broadband quality of service (QoS) and ensure data confidentiality in healthcare IoT systems. By integrating supervised and unsupervised learning models, the framework implements secure communication protocols, intelligent traffic

 ISBN: 978-9982-95-500-3

prioritization, and adaptive decision-making. The proposed strategy aims to mitigate patient risks, enhance the reliability of ICU operations, and bolster confidence in digital healthcare technology by reconciling network performance with security.

In ICU IoT networks, this work offers a hybrid machine learning-driven approach that simultaneously optimizes latency and data confidentiality. It combines secure communication protocols with sophisticated resource management to allow for context-aware, adaptive operation. Through transdisciplinary breakthroughs in machine learning, network optimization, and medical cybersecurity, the framework offers a useful basis for smart healthcare systems.

II. RELATED WORK

IoT integration in healthcare has garnered a lot of research interest, with studies concentrating on data confidentiality, cybersecurity, and Quality of Service (QoS) optimization. This section outlines the research gap this work attempts to fill and examines previous techniques taken in relation to these subjects.

IoT and Broadband QoS in Healthcare

A higher quality of life and quicker access to medical services are provided by the healthcare industry's combination of IoT and cloud computing [5]. Nevertheless, the need for real-time processing and large data quantities make it difficult to guarantee Quality of Service (QoS) [5] [6]. In healthcare, narrowband IoT (NBIoT) offers a cost-effective way for integrating wireless sensor networks, especially for patient monitoring and emergency scenarios. [7]. For healthcare systems to function effectively, QoS metrics like latency, throughput, and availability are essential[6]. To mitigate QoS issues, fog computing can be used to cut down on processing and transmission delays related to cloud-based analysis of data gathered by IoT devices [8]. This strategy can enhance reaction times and the general quality of healthcare services when paired with advanced computing and machine learning [6] [8]. For healthcare IoT systems to send patient data with the least amount of latency, especially in intensive care units, dependable broadband connections are essential. Previous studies have investigated edge computing, congestion control techniques, and bandwidth allocation algorithms to lower latency in medical IoT networks. These methods increase the speed at which data is transmitted, but they frequently ignore security needs, making systems susceptible to intrusions.

Cybersecurity Challenges in Healthcare IoT

To balance security and speed in IoT networks, the Transport Layer Security (TLS) and Message Queuing Telemetry Transport (MQTT) protocols are crucial. Even if these actions result in higher latency and lower throughput during peak loads, they can nevertheless have a significant impact on service quality. Combining the MQTT protocol with TLS can reduce security overhead and data delay; performance can be decreased by 62% for encryption and authentication combined and by 53% for the maximum authentication period[9] [10] [11] [12]. For IoT communications to remain secure and operate well, these studies emphasize the necessity of optimized strategies that dynamically modify security measures based on threat assessments and operational demands.

Healthcare IoT devices are frequently targeted by hackers due to the extremely sensitive nature of the data they handle [13] developed a machine learning-based intrusion detection system (IDS) that can recognise fraudulent traffic using the UNSW-NB15 dataset.[14] proposed elliptic curve cryptography (ECC), a low-power encryption method for protecting portable devices. These techniques improve network security, but they frequently ignore QoS problems. In circumstances requiring life-critical healthcare, high-security systems may lead to increased processing overhead and latency. Because medical information is important, hackers often target IoT-enabled institutions. Access control, encryption, and intrusion detection systems (IDS) have all been widely utilized to safeguard patient data [3]. However, many traditional cybersecurity methods increase computer costs, which exacerbates delay issues in critical care unit operations. Trade-offs between security and performance are still a common limitation.

 ISBN: 978-9982-95-500-3

C. *Machine Learning for QoS and Security*

In the healthcare industry, machine learning (ML) has become a potent instrument that provides answers for a range of uses, such as cybersecurity, diagnosis, and treatment [15]. Machine learning (ML) approaches in cybersecurity can help shield healthcare networks from ransomware assaults; Random Forest is especially useful for early prediction[16]. By predicting illnesses and finding trends in medical data, machine learning algorithms are helping to create effective decision support systems for healthcare applications [17]. Additionally, the technology is being used in sectors like neuroimaging, genetics, radiography, and electronic medical records[18]. Even while machine learning has the potential to completely transform healthcare, there are still obstacles to overcome, such as privacy and ethical issues and the requirement for thorough testing and validation of ML models[15, 18]. Recently, there has been study on the use of machine learning to improve network performance and security. Unknown threats have been successfully identified by unsupervised methods like clustering and autoencoders, while anomaly detection and traffic classification have been accomplished by supervised models like decision trees and random forests. ML has the potential to improve healthcare delivery and security overall, but more study and development are required. Additionally, machine learning is being implemented in IoT environments, which calls for careful consideration of data protection and performance. In order to optimize bandwidth distribution and reduce congestion in IoT networks, other works make use of reinforcement learning. Despite these developments, there are still few frameworks that combine cybersecurity measures designed for ICU-based IoT systems with ML-driven QoS optimization.

Table 1: Comparison of Related Works on QoS, Security, and ML in Healthcare IoT

Author(s)	Focus Area	ML Used	QoS Metrics	Security Mechanisms	Healthcar e Focus	Key Limitations
Mosenia & Jha (2017)	IoT Security in Healthcare	No	No	Authentication, Data Privacy	Yes	No QoS optimization; high computational overhead
Chen et al. (2021)	QoS using Reinforcement Learning	Yes (RL)	Latency, Bandwidth	No	Partial	Ignores confidentiality and security threats
Alsheikh et al. (2021)	ML for IoT Security	Yes (Supervised)	No	Anomaly Detection, Classification	No	Not healthcare-specific; lacks QoS integration
Zhang et al. (2019)	Lightweight Security for IoT Devices	No	No	ECC, Key Management	Yes	No adaptive QoS or ML-based threat detection
Choudhury et al. (2020)	Deep Learning for Data Confidentiality	Yes (Deep Learning)	No	Privacy Leakage Detection	No	Requires high resources; no QoS performance analysis
Roman et al. (2018)	IoT Security Architecture	No	No	Secure Architecture, Compliance (	Yes	No dynamic ML; static security model

ISBN: 978-9982-95-500-3

				HIPAA)		

Table2: Comparative Analysis of Current Solutions for QoS and Cybersecurity in Healthcare IoT

Focus Area	**Methods / Techniques**	**Key Contributions**	**Limitations**
QoS in Healthcare IoT	Bandwidth allocation, edge computing	Reduced latency and improved data flow in IoT networks	Limited focus on security and data confidentiality
ICU Broadband Optimization	Congestion control mechanisms	Enhanced reliability of patient monitoring systems	Overheads under high data load; no adaptive security
Cybersecurity in IoT	Encryption, access control, IDS	Strong data protection in healthcare IoT	Increased computational cost; worsens latency
Privacy-Preserving IoT	Lightweight encryption protocols	Improved confidentiality with reduced computation	Partial focus on latency; not scalable for ICU
ML for Anomaly Detection	Decision trees, random forests	Accurate detection of known threats	Weak performance against evolving/unknown threats
ML for Intrusion Detection	Clustering, autoencoders	Effective against unknown cyberattacks	Lacks QoS optimization and resource awareness
ML for QoS Optimization	Reinforcement learning, dynamic allocation	Adaptive traffic handling, reduced congestion	Does not integrate confidentiality and security

Adaptive security, data confidentiality, and machine learning-based traffic management must all be included into a new framework in order to handle the particular trade-offs between security and latency in critical care IoT.

D. *Research Gaps in ML-Driven Cybersecurity for Critical Care IoT*

Three major shortcomings are identified in the literature: ML-driven solutions are not sufficiently adapted for resource-constrained intensive care unit contexts; QoS optimization and cybersecurity are not fully integrated; and latency and confidentiality trade-offs are not evaluated in real-world healthcare scenarios. To improve data handling in critical care, a holistic strategy is required to integrate data confidentiality, adaptive security, and ML-based traffic management.

Table3: Research gap identified

Primary Research Gap	Core Problem/Limitation in Current Solutions	Key References
Inadequate Real-Time Adaptability	Solutions frequently lack real-time adaptability for dynamic QoS/confidentiality needs and rely on single, heavy security mechanisms,	[19] , [20], [21]

 ISBN: 978-9982-95-500-3

	leading to high computational overheads and missed security/traceability integration.	
Independent Security and QoS Optimization	Security and QoS are treated separately; security measures (e.g., protocols with TLS) severely degrade network performance (latency, throughput). There is a lack of co-optimization strategies.	[10] , [11], [22] [23, 24], [25, 26]
Incomplete Healthcare-Specific QoS Integration	Systems fail to integrate crucial healthcare-specific QoS measures like latency adequately. The potential of AI/Edge Computing for optimizing these critical metrics is currently under-leveraged and not systematically evaluated.	[27], [28]
Inefficient Models for Constrained Devices	Existing ML models are often too heavy and resource-intensive for resource-constrained ICU IoT devices, demanding novel lightweight, intelligent models to ensure both high security and energy efficiency.	[29], [30], [31], [32], [31, 33]

The current Internet of Things (IoT) environment in intensive care units (ICUs) poses a number of significant issues, chief among them being the absence of integrated Quality of Service (QoS) and strong security measures. Additionally, the systems show little flexibility in response to these environments' intrinsic resource constraints. Moreover, comprehensive evaluations of the trade-offs between secrecy and latency, a critical balance for real-time applications are scarce. A thorough investigation that effectively combines the three crucial features of low latency, high quality of service, and lightweight cybersecurity is thus now lacking in the field of remote patient monitoring. Last but not least, although machine learning is widely used in the healthcare industry for anomaly detection, its integration with intelligent routing or bandwidth optimization is less prevalent, offering a substantial lost chance to increase efficiency.

In order to overcome existing constraints, the proposed study intends to create an Integrated QoS and Security Framework utilizing a Machine Learning (ML)-based approach. This would optimize throughput, latency, and jitter while also guaranteeing confidentiality and anomaly detection in network systems. Hybrid supervised and unsupervised Machine Learning (ML) and adaptive security mechanisms are used to optimize both security and Quality of Service (QoS) in Intensive Care Unit (ICU) Internet of Things (IoT) networks. The aim is to maximize confidentiality and minimize latency, which will be verified in actual ICU scenarios.

III. PROPOSED FRAMEWORK

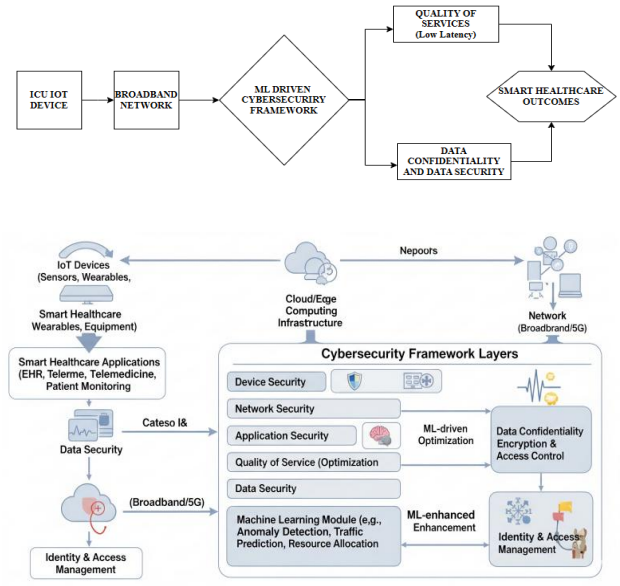
In order to address the twin problems of high latency and cybersecurity vulnerabilities in healthcare IoT systems, namely in critical care units (ICUs), we have proposed a machine learning-driven cybersecurity framework. To guarantee strong data secrecy and broadband QoS optimization, the system combines dynamic security measures, adaptive bandwidth allocation, and intelligent traffic management.

A. *Framework Overview*

The proposed system is designed as a layered architecture that unifies network optimization and

 ISBN: 978-9982-95-500-3

cybersecurity. At its core, the framework employs a hybrid machine learning approach that combines supervised models (for traffic classification and prioritization) with unsupervised models (for anomaly and intrusion detection). This dual strategy ensures context-aware decision-making while maintaining adaptability to evolving threats and network conditions.



Figures 1: Proposed Framework Architecture

Table 4: Combined QoS and Confidentiality Optimization: A Comparison of Conventional and ML-Driven IoT Security

Traditional Methods	**Proposed ML-Driven Framework**
Static bandwidth allocation, priority scheduling	Adaptive bandwidth allocation using ML
Strong encryption protocols but high latency	Lightweight and adaptive encryption integrated with ML
Rule-based IDS (reactive, rigid)	Real-time anomaly detection (ML-based, proactive)
Optimizes either QoS or Security, not both	Joint optimization: Low Latency and Confidentiality
Not adaptive to ICU traffic surges or new attacks	Context-aware, self-learning, dynamic response

IV. METHODOLOGY

In order to improve research results and effect, hybrid research approaches integrate many techniques and disciplines. The design science will develop the framework for this study, while the experimental quantitative will assess the metrics, including data security (data confidentiality) metrics and quality of service metrics, respectively. In the discipline of information systems research, design science research (DSR) has gained popularity within the last ten years. Hevner et al. (2004) introduced seven principles for effective DSR in their seminal work. These principles were examined from a process perspective and proposed changes to improve their applicability [34]. [35] developed and refined a six-step DSR process that includes problem identification, solution objectives, design and development, demonstration, assessment, and communication. Offering a structured framework for conducting and presenting DSR in information systems is the aim of this methodology.

Research Design and Approach

The study uses a hybrid approach, combining several approaches to produce better results. Design Science Research (DSR), which focuses on the development of a new, efficient framework, is the main foundation of this design. The goal is to specifically design, build, and assess a cybersecurity framework powered by machine learning with the goal of improving broadband Quality of Service (QoS) and data confidentiality in Internet of Things (IoT) systems. The development and iterative improvement of the framework adhere to Design Science principles, producing a tangible artifact.

Evaluation and Data

The study uses an experimental quantitative technique to thoroughly assess the framework. This entails evaluating the created item against important

 ISBN: 978-9982-95-500-3

metrics by testing it on pertinent datasets. In order to ensure relevance to crucial IoT applications, the datasets used include simulated ICU traffic in addition to well-known medical and critical care data repositories like PhysioNet and MIMIC-III. To evaluate various aspects of the cybersecurity and QoS processes, the evaluation uses a variety of Machine Learning (ML) Models, including Random Forest (RF), Support Vector Machine (SVM), Reinforcement Learning (RL) employing Q-learning, and Autoencoders.

The evaluation demonstrates that the proposed framework balances **ultra-low latency** and **strong data confidentiality** while maintaining resource efficiency. This dual optimization addresses critical needs in ICU-based IoT environments, where both speed and security are vital for patient safety.

Key Performance Metrics

A wide range of measures that are essential for network security and performance will be used to evaluate the effectiveness of the developed framework and its machine learning models. Latency, jitter, and throughput are some of the quantitative metrics used to assess the improvement in broadband quality of service. Metrics like detection accuracy (for identifying threats) and resource efficiency (for sustainable deployment on IoT devices) are used to assess the security component and efficacy of the ML-driven defense mechanisms. The resultant cybersecurity solution is guaranteed to be both innovative and empirically successful because to this integrated methodological framework, which combines DSR for design with experimental quantitative methodologies for validation.

VI. CONCLUSION

In order to improve patient outcomes, foster trust, and stimulate interdisciplinary research to increase system responsiveness and scalability, it is imperative that IoT healthcare delivery struck a balance between data security, which safeguards sensitive patient information, and Quality of Service (QoS), which guarantees quick, dependable access to critical data in critical settings like the intensive care unit.

A structured comparison of a few research on broadband QoS optimization, cybersecurity, and machine learning in healthcare IoT systems is presented in this subsection in order to summarize the results from the body of existing literature. In their respective fields, these research provide significant contributions. Some concentrate on protecting sensitive health data, others on guaranteeing dependable network performance, and some use machine learning approaches for dynamic adaptation. A closer look, however, shows that the majority of works address these issues separately and frequently fail to integrate security enforcement procedures with QoS needs. Improved speed may erode data protection, while increased security may jeopardize timeliness in latency-sensitive healthcare scenarios like telemedicine or remote patient monitoring.

ACKNOWLEDGMENT

Sincere thanks are extended by the authors to ZCAS University and the organizers of the 7th International Conference in Information and Communication Technologies for their support of this study. We also recognize the assistance of mentors and colleagues who helped shape this work by offering insightful advice.

REFERENCES

[1] Abubakar Wakili et al, "Machine Learning for QoS and Security Enhancement of RPL in IoT-Enabled Wireless Sensors," *Sensors International,* 2024.

[2] Bagaa et al, "A Machine Learning Security Framework for Iot Systems," *IEEE Access,* 2020.

[3] Salman et al., "Enhancing quality of service in IoT through deep learning techniques," *Periodicals of Engineering and Natural Sciences,* 2023.

[4] Hosam El_S. et al, "Using machine learning algorithms to enhance IoT system security," *Scientific Reports,* 2024.

[5] Houriyeh Khodkari, S. Ghazi-Maghrebi, A. Asosheh, M. Hosseinzadeh, "Smart Healthcare and Quality of Service

Challenges," *International Symposium on Telecommunications,* pp. 253-257, 2018.

[6] Younas, Muhammad Irfan, et al., " "Toward QoS monitoring in IoT edge devices driven healthcare," *"Sensors ,* no. 8885, pp. 23-21, 2023.

[7] Routray, Sudhir K. and Sharath Anand., "Narrowband IoT for healthcare," in *International Conference on Information Communication and Embedded Systems (ICICES)* , Kundalahalli Bangalore, 2017.

[8] Dankan Gowda V, Avinash Sharma, B. K. Rao, R. Shankar, P. Sarma, Abhay Chaturvedi, Naziya Hussain, "Industrial quality healthcare services using Internet of Things and fog computing approach," *Measurement: Sensors,* vol. 24, 2022.

[9] Christopher Uzoma Asonze, Olumide Samuel Ogungbemi, Favour Amarachi Ezeugwa, Anthony Obulor Olisa, Oluwaseun Ibrahim Akinola, O. O. Olaniyi, "Evaluating the Trade-offs between Wireless Security and Performance in IoT Networks: A Case Study of Web Applications in AI-Driven Home Appliances," *Journal of Engineering Research and Reports,* pp. 411-432, 2024.

[10] Z. Fadlullah, A. Benslimane, "Joint Provisioning of QoS and Security in IoD Networks: Classical Optimization Meets AI," *IEEE Internet of Things Magazine,* pp. 40-46, 2021.

[11] A. R. Alkhafajee, A. M. A. Al-muqarm, A. H. Alwan, Zaid Rajih Mohammed, "Security and Performance Analysis of MQTT Protocol with TLS in IoT Networks," *4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA),* pp. 206-211, 2021.

[12] Sultan Alharby, N. Harris, A. Weddell, J. Reeve, "The Security Trade-Offs in Resource Constrained Nodes for IoT Application," 2018.

[13] A. Abdulghani, M. Hammoudeh, and H. Abu-Amara, , "Intelligent Intrusion Detection for IoT-Based eHealth Systems," *EEE Access,* vol. 9, p. 145218–145230, 2021.

[14] A. Kassem, R. Awad, and F. Alotaibi, "Lightweight ECC Encryption for Wearable Healthcare Devices," *IEEE Sensors Journal,* vol. 23, no. 1, p. 134–145, 2023.

[15] Devi P. Bharathi, P. Ravindra, Kumar R. Kiran, "Machine learning solutions for the healthcare industry: A review," *i-manager's Journal on Artificial Intelligence & Machine Learning,* vol. 1, no. 1, pp. 41-47, 2023.

[16] Aadil Khan, Ishu Sharm, "Machine Learning-Based Methodology for Preventing Ransomware Attacks on Healthcare Sector," in *2023 International Conference on Research Methodologies in Knowledge Management, Artifi*, Chennai, India, 2023.

[17] K. Shailaja, B. Seetharamulu, M. Jabbar, "Machine Learning in Healthcare: A Review," in *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 2018.

[18] Hafsa Habehh, S. Gohel, "Machine Learning in Healthcare," *Current Genomics,* vol. 22, no. 4, pp. 291-300, 2021.

[19] Ijaz Ahmad, H. Shahid, Ijaz Ahmad, J. Islam, Kazi Nymul Haque, E. Harjula, "Adaptive Lightweight Security for Performance Efficiency in Critical Healthcare Monitoring," *International Symposium on Medical Information and Communication Technology,* pp. 78-83, 2024.

[20] Aamir Hussain, Tariq Ali, Faisal Althobiani, U. Draz, Muhammad Irfan, S. Yasin, Saher Shafiq, Zanab Safdar, A. Głowacz, Grzegorz Nowakowski, Muhammad Salman Khan, Samar M. Alqhtani, "Security Framework for IoT Based Real-Time Health Applications," *Electronics,* 2021.

[21] ajdini, Johana, Ursina Hajdini and Klejdi Cankja. H, "Putting the pieces together: towards an integrative framework for healthcare performance," *" Journal of health organization and management ahead-of-print ahead-of-print ,* 2024.

[22] Zakaria Laaroussi, Oscar Novo, "A Performance Analysis of the Security Communication in CoAP and MQTT," *Consumer Communications and Networking ConferenceLaaroussi, Zakaria and Oscar Novo. "A Performance Analysis of the Security Communication IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) ,* pp. 1-6, 2021.

[23] Sheikh, Anjum, Sunil Kumar and Asha Ambhaikar. , "A Secure Trust-Based Routing Framework for Improving the QoS of Internet of Things Based Networks," *4th International Conference on Computing and Communications Technologies (ICCCT) ,* pp. 149-154, 2021.

[24] Shital Pawar, Meghana P. Lokhande, Sandip Thite, J. A. P, R. Samant, Rohini Jadhav, Jadhav D B, "Security and QoS (Quality of Service) Related Current Challenges in IoT," *International Journal of Electronics and Communication Engineering,* vol. 10, no. 4, pp. 9-20, 2023.

[25] Bhatnagar, Manisha and Dolly Thankachan, "Identifying the Effects of Security Measures on QoS Variations for IoT Network: An Application Perspective," *Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) ,* pp. 290-299, 2021.

[26] Shital Pawar, Meghana P. Lokhande, Sandip Thite, J. A. P, R. Samant, Rohini Jadhav, Jadhav D B, "Security and QoS (Quality of Service) Related Current Challenges in IoT," *International Journal of Electronics and Communication Engineering,* vol. 10, no. 4, pp. 9-20, 2023.

[27] M. Younas, Muhammad Jawed Iqbal, Abdul Aziz, Ali Hassan Sodhro, "Toward QoS Monitoring in IoT Edge Devices Driven Healthcare—A Systematic Literature Review," *Italian National Conference on Sensors,* 2023.

[28] Sarina Aminizadeh, Arash Heidari, Mahshid Dehghan, Shiva Toumaj, Mahsa Rezaei, Nima Jafari Navimipour, Fabio Stroppa, Mehmet Unal, "Opportunities and challenges of artificial intelligence and distributed systems to improve the quality of healthcare service," *Artif. Intell. Medicine,* 2024.

[29] Soumyalatha Naveen, Manjunath R. Kounte, Mohammed Riyaz Ahmed, "LOW LATENCY DEEP LEARNING INFERENCE MODEL FOR DISTRIBUTED INTELLIGENT IOT EDGE CLUSTERS," *IEEE Access,* pp. 1-1, 2021.

[30] "A Study on Edge Computing through Machine Learning for IoT Devices," *International Conference on Forensics, Analytics, Big Data, Security (FABS),* pp. 1-6, 2021.

[31] Amgbara, Sofiritari Ibikoroma, Chukwuebuka Akwiwu-Uzoma and Ola David., " Exploring lightweight machine learning models for personal internet of things (IOT) device security," *World Journal of Advanced Research and Reviews ,* 2024.

[32] Joshi, Rajeev, Raaga Sai Somesula and Srinivas Katkoori., "Empowering Resource-Constrained IoT Edge Devices," *A Hybrid Approach for Edge Data Analysis." IFIP Internet of Things ,* 2023.

[33] Chatterjee, Baibhab, Shreyas Sen, Ningyuan Cao and Arijit Raychowdhury., " Context-Aware Intelligence in Resource-Constrained IoT Nodes: Opportunities and Challenges," *IEEE Design & Test ,* vol. 36, pp. 7-40., 2019 .

[34] Hannes Göbel, Stefan Cronholm, "Design science research in action - experiences from a process perspective," 2012.

[35] K. Peffers, T. Tuunanen, Charles E. Gengler, M. Rossi, Wendy Hui, V. Virtanen, J. Bragge, "Design Science Research Process: A Model for Producing and Presenting Information Systems Research," *arXiv.org,* 2007, 2020.

 ISBN: 978-9982-95-500-3