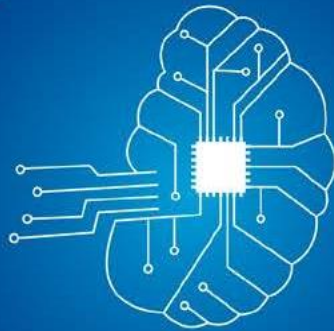**NEAR EAST UNIVERSITY**

JOURNAL FOR ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS

Volume: 4 Issue:1

www.neu.edu.tr

JOURNAL OF ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS
International, Refereed Journal

Address and Contact
Yakın Doğu Üniversitesi İnovasyon ve Bilişim Teknolojileri Merkezi
International Research Center for AI and IoT
Yakın Doğu Bulvarı, PK: 99138Lefkoşa / KKTC Mersin 10 –TÜRKİYE
Tel:+90 (392) 223 64 64/+90 (392) 680 20 00Faks:+90 (392) 223 64 61
http://dergi.neu.edu.tr/ https://iot.neu.edu.tr/

Publication Contact

Prof. Dr. Fadi AL-TURJMAN

Publication Board

Prof. Dr. Fadi Al-Turjman

CONTENTS

Intelligent Medical Applications Blockchain-Powered 6G Networks

Ramiz Salama[1*], Fadi Al-Turjman[2, 3]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT,
Near East University Nicosia, Mersin 10, Turkey

[2]Artificial Intelligence, Software, and Information Systems Engineering Departments, AI and Robotics Institute,
Near East University, Nicosia, Mersin10, Turkey

[4]Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin10, Turkey
*Corresponding author Email: ramiz.salama@neu.edu.tr

Abstract

The demand for intelligent, effective, and secure medical applications has increased due to the quick development of healthcare technologies. In order to provide complicated medical services, 6G networks promise ultra-high-speed communication, minimal latency, and huge interconnectedness. 6G networks can offer a strong and secure framework for intelligent medical applications when combined with blockchain technology, guaranteeing data accessibility, privacy, and integrity. By facilitating decentralized, transparent, and impenetrable medical data management, blockchain improves data security. By enabling smooth real-time data exchange between medical devices, patients, and healthcare professionals, this integration can provide more precise diagnosis, effective treatment, and individualized healthcare solutions. With a focus on important use cases including telemedicine, remote patient monitoring, and AI-based diagnostics, this paper examines how blockchain-powered 6G networks have the potential to transform healthcare by offering intelligent, scalable, and secure medical services..

Keywords: 6G networks, blockchain technology, and smart healthcare

1. Introduction

This article examines how blockchain technology can be incorporated into healthcare systems, emphasizing how it can be enhanced when paired with 6G networks.
Blockchain is a secure, decentralized ledger technology that improves healthcare efficiency, privacy, and data integrity. It functions over a network of computers, or nodes, in which a cryptographic hash connects each transaction. A highly safe and transparent system is produced as a result of this decentralization, which does away with the need for a central authority to supervise transactions. Because of its revolutionary potential, blockchain makes it possible to securely store and exchange patient records, treatment histories, and other private medical data, which lowers expenses and boosts productivity [1–3]. The influence of the technology is further increased by smart contracts, which automatically activate predetermined conditions.
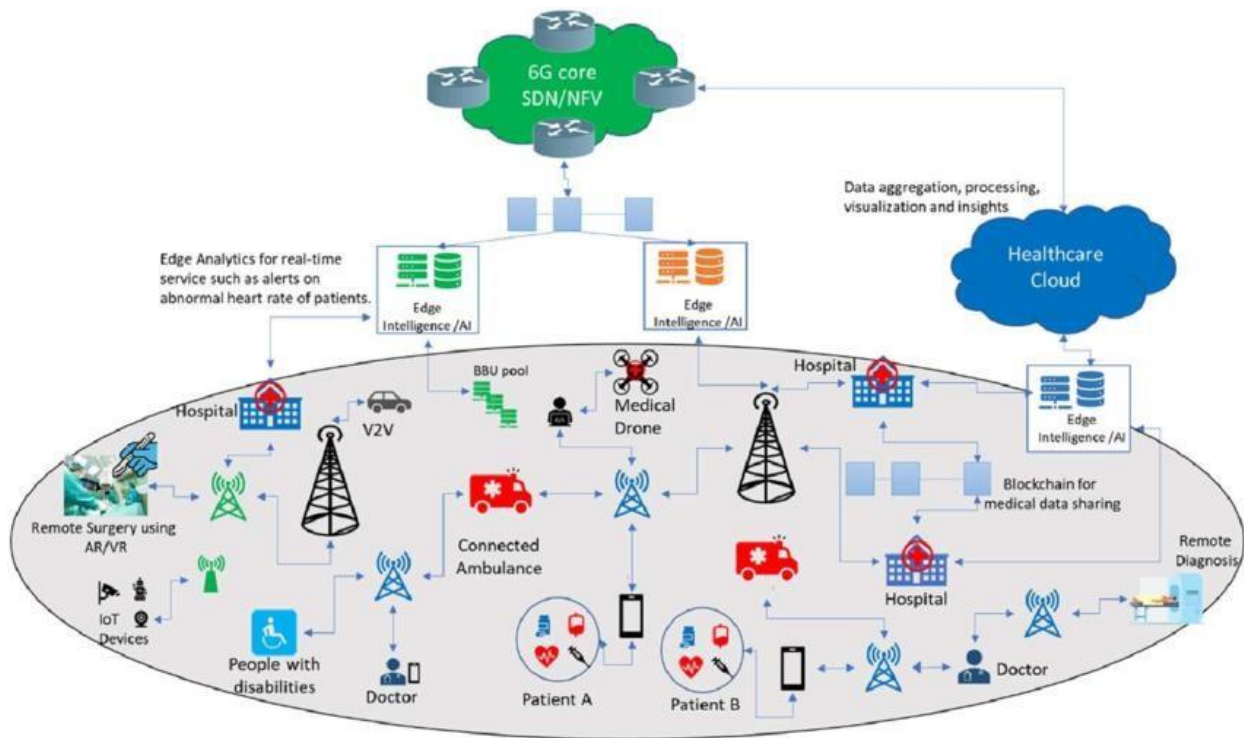
Figure 1. 6G Enabled-IoT for future Smart healthcare.

1.1. Using Blockchain Technology in Medical Practice

The essay explores the ways in which blockchain technology might be used in healthcare to address persistent issues including data security, transparency, and interoperability. The investigation of its possibilities prepares the ground for the discussion of 6G networks that follows. Blockchain integration in healthcare signifies a revolutionary change in the way the sector handles, preserves, and disseminates private medical data. The various facets of how blockchain smoothly becomes an essential part of the healthcare ecosystem are explored in this section. The safe and compatible transfer of patient data across different organizations, including clinics, hospitals, and insurance companies, is one of the biggest problems in the healthcare industry. Blockchain solves this by providing a distributed, decentralized ledger that guarantees the accuracy and unchangeability of medical records. There is only one source of truth for all parties involved because every network participant has an identical copy of the ledger [4,5].

1.2. Strengthening Security via Dispersion
The decentralization of blockchain ensures safe data distribution throughout the network by removing a central point of vulnerability. In addition to improving security, this gives people more authority over their health information, protecting privacy and adhering to HIPAA rules.

1.3. Streamlined Interaction
Blockchain overcomes interoperability issues by offering a standardized, secure framework for data sharing, enabling automated transactions between healthcare systems.

1.4. Audible and Clear
By safely recording transactions, lowering errors, fraud, and illegal access, and encouraging a more dependable and accountable environment, blockchain improves the trust in the healthcare system.

1.5 Supply chain management and medication traceability
Blockchain improves pharmaceutical and medical device traceability across the supply chain, guaranteeing authenticity and enabling quick action in the event of an emergency or recall.

1.6 Empowerment of Research and Development
Blockchain technology in healthcare provides safe, private data exchange, speeding up medical research and maybe resulting in treatment breakthroughs. It has an impact on supply chain logistics and creates a cooperative setting for research and development, opening the door to an ecosystem that is safer, more effective, and more patient-friendly.

1.7 6G Communications' Significance
By providing revolutionary features that work in tandem with blockchain, 6G networks expand the potential of blockchain in the healthcare space and open the door for intelligent healthcare applications as well as the next wave of wireless communication technology.

1.8 Enhanced Data Transfer Rates
Large datasets may be sent almost instantly thanks to 6G networks' notable data transmission speeds, which outperform 5G. This makes real-time access to patient data for diagnosis and decision-making possible, which is essential in blockchain applications and healthcare.

1.9 Exceptionally Low Latency
Ultra-low latency provided by 6G networks minimizes delays in medical applications. For snap judgments, like remote surgery, this lowers latency. It improves smart contract responsiveness when combined with blockchain, increasing the effectiveness of automated procedures.

1.10 Wide-ranging Networking of Devices
6G networks facilitate smooth healthcare connectivity by supporting large numbers of linked devices. Blockchain securely handles the data produced by these devices, allowing smart contracts to interact with health data in real time for record updates and treatments.

1.11. Network Slicing Customization
By customizing network segments to suit specific requirements, 6G's network slicing technology improves performance and dependability through blockchain-enabled systems, optimizing healthcare applications.

1.12 Strengthened Security Protocols
In a fast changing healthcare scene, 6G networks, which combine blockchain and cryptographic techniques, offer sophisticated security features for protecting healthcare data and improving cybersecurity.

1.13. Supporting Immersion Technology
6G networks are essential for improving data transfer speeds, lowering latency, and guaranteeing strong security while enabling immersive technologies like AR and VR in healthcare. Additionally, they facilitate widespread device connectivity, opening the door to a future in which healthcare is more intelligent, responsive, secure, and accessible, improving the state of healthcare as a whole.

2. Intelligent Medical Applications Driven by Blockchain

2.1 Overview and Title
In order to transform patient care, data management, and operational efficiency in the healthcare industry, this section examines blockchain-enabled smart healthcare applications [6].

2.1 Patient-Centered Health Records
Blockchain ensures privacy, empowers patients, and improves data security and trust by transforming traditional healthcare records into a decentralized, patient-centric system.

2.2 Traceability of Pharmaceutical Supply Chains
By permitting end-to-end traceability, guaranteeing medicine validity, lowering fraud risk, and expediting prompt recalls or crises, blockchain tackles the problems of counterfeit medications and transparency in pharmaceutical supply chains [7].

2.3 Automation of Insurance Claims Processing
By automating the processing of health insurance claims, blockchain technology lowers administrative costs, fraud, delays, and errors while increasing efficiency and transparency.

2.4. Drug Development and Clinical Trials
Blockchain ensures openness and integrity while improving data management in clinical trials and drug development. Data collection and participant recruiting are two examples of tasks that smart contracts automate.

2.5 Credentialing and Medical Licensing
Blockchain makes it easier to verify the credentials of healthcare professionals, lowering the risk of fraud and speeding up onboarding. By storing and confirming medical credentials in a decentralized manner, blockchain benefits patients and providers alike.

2.6 Combining Real-Time Monitoring with IoT
Blockchain integration with IoT devices enables remote monitoring, chronic illness management, and early intervention in critical cases, allowing for real-time patient health monitoring.

2.7 Health Data Research and Analytics
Blockchain speeds up research projects and may result in new treatments, medications, and healthcare advances by enabling the safe, private exchange of health data for scientific purposes.

2.8 Managing Identity and Access
Blockchain improves security and compliance in the healthcare industry by offering a decentralized identity management solution. It makes it possible for smart contracts to regulate

who has access to particular data, improving productivity and patient empowerment. Clinical trials, medication development, and medical records are all being transformed by blockchain-enabled smart healthcare systems.

2.9. Smart healthcare buzzwords and 6G networks
Finding and utilizing pertinent keywords is essential to maximizing search engine exposure for 6G networks and smart healthcare in order to guarantee the article's relevancy and accessibility.

2.10. Overview of Intelligent Medical Applications Driven by Blockchain
The main features of blockchain-enabled smart healthcare applications are briefly summarized in this abstract in order to set the stage for further in-depth discussion in the parts that follow.

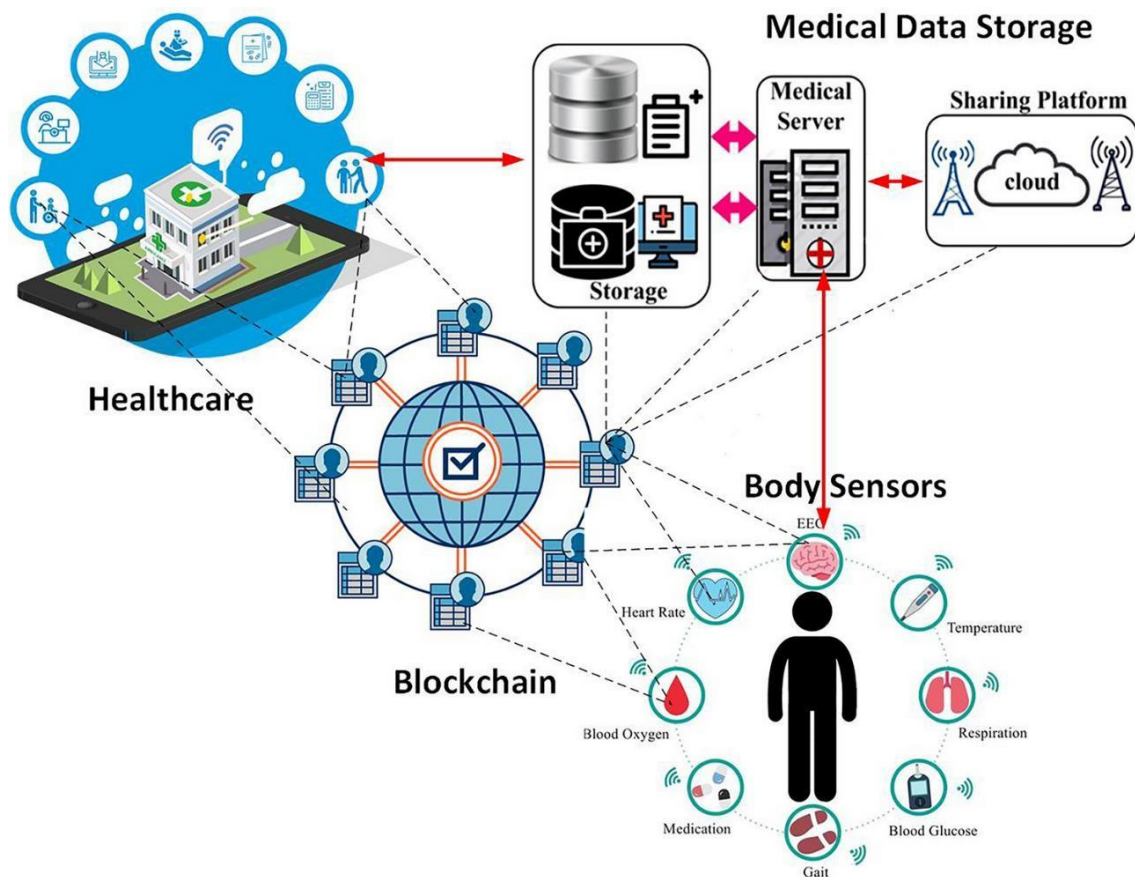**Figure 2.** Blockchain in internet of medical things.

3. Previous Domain Experience

3.1 Overview of Recent Studies
This paper examines how blockchain has developed in the healthcare industry and how it integrates with 6G networks, offering a thorough assessment of the state of blockchain-enabled smart healthcare applications at this ever-changing nexus of technology and healthcare [8].

3.2. The Evolution of Blockchain in the Medical Domain
Significant milestones have been reached in the blockchain's path in healthcare, with early research concentrating on patient privacy, security, and data interoperability. Practical applications have surfaced over time, demonstrating blockchain's feasibility in clinical trials, supply chain management, and electronic health records.

3.3 The advancement of 6G network technology
Rapid advancements in 6G networks are improving healthcare capacities. The effects of faster data rates, reduced latency, and device connection have all been studied in relation to 5G networks. Recent research emphasizes the special capabilities of 6G, such as network slicing for specialized services, ultra-reliable low-latency communication for surgical operations, and holographic communication for telemedicine.

3.4. Issues and Solutions
The literature focuses on issues including scalability, energy efficiency, and regulatory compliance that arise with blockchain-enabled smart healthcare applications in 6G networks. In addition to initiatives to create industry standards and legal frameworks, creative ideas include hybrid blockchain designs, consensus mechanism optimizations, and AI integration.

3.5. Inter-disciplinary Cooperation
In order to create and execute smart healthcare applications, cross-disciplinary collaborations in blockchain and 6G networks are being used more and more to bridge expertise from other sectors.

3.6. Adoption and Acceptance Trends
In order to address user perspectives, data security, privacy, and usability concerns, prior research has examined the acceptance and adoption patterns of blockchain-enabled healthcare solutions among practitioners, patients, and stakeholders.

3.7. Potential Research Paths
In addition to integrating cutting-edge technologies like edge computing and artificial intelligence, researchers are investigating blockchain-enabled smart healthcare applications in 6G networks, creating decentralized identification solutions, and creating innovative consensus methods. Researchers are guided by this retrospective analysis to tackle obstacles, adopt cooperative strategies, and include blockchain and 6G in healthcare.

4. 6G Networks with Blockchain-Powered Intelligent Medical Applications

4.1. Analyzing Applications of Blockchain
This section explores the complexities of blockchain technology and emphasizes how it might improve data security in applications related to healthcare [9].

4.2 Implementing Intelligent Healthcare Solutions
The deployment of smart healthcare solutions is covered in the article, along with information on their features, advantages, and possible drawbacks in certain applications.

4.3. Including 6G Network Features

This article provides a forward-looking view of the potential of both technologies by examining the combination of blockchain technology with 6G networks in smart healthcare applications [41] [42].

Figure 3. Role of blockchain for 6G networks

5. Findings and Conversation

5.1 The Positive Impact of Blockchain on Healthcare

The talk highlights how blockchain can improve healthcare by protecting patient privacy, data integrity, and safe exchange of medical information [10].

5.2. Better 6G Network Features

The advantages of 6G networks, such as quicker data transfer, lower latency, and improved connectivity, are examined in this section along with their potential applications in the healthcare industry.

5.3. Real-World Examples of Intelligent Healthcare Applications

Using real-world examples, the article illustrates how blockchain technology and 6G are revolutionizing healthcare delivery.

5.4. Support for Research and Development

By offering a safe, private platform for data sharing, blockchain improves healthcare research. This speeds up medical research, resulting in ground-breaking findings and creative cures. The impact of blockchain technology is felt in many healthcare ecosystems, giving people authority over their medical records. The benefits of blockchain will increase as 6G networks develop [11–13].

5.5. Supply Chain Management Done Right

By documenting each stage from production to distribution, blockchain technology improves pharmaceutical supply chain transparency and traceability, lowering the number of fake medications and increasing recall effectiveness [14].

5.6. Documents That Are Unchangeable and Untouchable
The immutability property of blockchain guarantees data integrity, promoting accuracy and trust in healthcare decision-making. It enhances patient histories, treatment plans, and clinical trial data while preventing manipulation and guaranteeing tamper-resistant health records [15-20].

6. Examples of Smart Healthcare Applications in Real Life Blockchain-Powered 6G Networks

Blockchain-powered smart healthcare apps in 6G networks offer a vision of the future of healthcare where efficiency, privacy, and data security are greatly enhanced. Blockchain can improve healthcare in 6G environments, as demonstrated by pilot projects and developing concepts, even though full-scale 6G networks are still being developed. Here are a few pilot projects and real-world examples that support this idea:

1. The European Union's My Health My Data (MHMD) initiative
• Overview: One of the first blockchain-based initiatives to allow for the safe and confidential exchange of medical data throughout Europe is MHMD. In order to allow patients to share medical information with researchers, healthcare organizations, and pharmaceutical businesses while still keeping ownership over their data, the project intends to create a decentralized, secure infrastructure.
• Relevance of 6G: Blockchain-enabled platforms like MHMD can further enhance the safe sharing of medical data, since 6G offers ultra-low latency and high-speed connectivity. In a 6G ecosystem, such systems can be more secure and responsive with AI-powered health diagnostics, real-time data interchange, and sophisticated telemedicine [43].

2. Blockchain-Based Health Data Platform MediBloc
• Overview: MediBloc is a blockchain-based healthcare data platform that gives people authority over their medical records. It offers a transparent, safe, and decentralized way to store, retrieve, and distribute medical records among various healthcare providers.
6G Relevance: MediBloc may gain from faster and more interoperable communication between healthcare systems in a 6G network. By offering precise, real-time data to help with diagnosis and individualized treatment suggestions, blockchain technology can enhance AI-driven healthcare services and stop unwanted access to private medical records [44] [45].

3. Robomed Network: AI and Blockchain for Telemedicine • Synopsis: Robomed offers telemedicine services that link patients with medical professionals by using blockchain technology and artificial intelligence. Blockchain guarantees the safe transmission of real-time data and the patient's medical history during telemedicine consultations.
Why 6G Relevance: Robomed's performance may be improved by 6G's low-latency capabilities, which might make telemedicine services almost instantaneous. Furthermore, blockchain guarantees the security and immutability of patient data, which is essential in the massive 6G network where more devices will be linked to the healthcare ecosystem.

4. Medicalchain: Blockchain for Health Record Exchange
• Synopsis: Medicalchain uses blockchain technology to safely store and handle medical records. With consent, patients, physicians, and other healthcare professionals can access data, guaranteeing privacy and control.
• 6G Relevance: Medicalchain's blockchain architecture will support safe data sharing and access management as the number of linked devices increases rapidly in a 6G world. The healthcare system might enable real-time patient condition monitoring using IoT devices with quicker data speeds and lower latency, while blockchain maintains data integrity.

5. Chronicled: Blockchain for Drug Supply Chain [21-25]
• Synopsis: Chronicled tracks the authenticity and provenance of medications in the supply chain using blockchain technology. It seeks to guarantee openness throughout the pharmaceutical supply chain and fight counterfeit medications.
• 6G Relevance: Blockchain-enabled supply chain management systems, such as Chronicled, may offer real-time tracking and identification of medications and medical supplies in a smart healthcare system driven by 6G. Due to faster and more effective connectivity between devices and systems, blockchain in 6G would allow for improved oversight and faster reaction times in stopping the distribution of fake medications.

6. Patientory: Blockchain-Powered Health Information Exchange
• Synopsis: Patientory is a blockchain-powered healthcare platform that facilitates the safe and effective exchange of health information between patients, insurers, and healthcare providers.
• 6G Relevance: Platforms such as Patientory may profit from the smooth and safe transfer of medical data among a vast network of interconnected devices in the context of 6G. While 6G allows for faster and more scalable health information sharing, blockchain guarantees the security of sensitive health data. Advanced applications like real-time tailored treatments and AI-driven healthcare analytics may be supported by this combo.

7. Principal Advantages of Blockchain in Healthcare Powered by 6G [26-30]:
• Improved Security and Privacy: Because 6G networks will be extensively interconnected, hackers will find it more difficult to alter healthcare data due to blockchain's decentralized structure.
• Real-Time Data Sharing: Blockchain will be able to provide real-time secure data sharing for applications such as remote surgery, real-time diagnostics, and AI-driven medical services thanks to 6G's high speed and low latency.
• *Decentralized Control:*
Since blockchain removes the need for a central authority to maintain or keep medical records, patients have more control over their data.
• Interoperability: Blockchain can facilitate interoperability between various healthcare providers, facilitating the safe and secure sharing of patient data. These illustrations show how blockchain is starting to change healthcare, and as 6G becomes available, these systems' potential will only grow.

7. The potential applications of smart healthcare Blockchain-Powered 6G Networks

Future possibilities for smart healthcare applications are enormous when paired with blockchain technology and 6G networks. A more secure, effective, and individualized healthcare experience will be made possible by the combination of these technologies, which has the potential to revolutionize the healthcare sector [31-40]. Future scopes include the following:

1. Improved Privacy and Security of Data
Blockchain can offer decentralized, tamper-proof data storage, guaranteeing patient data confidentiality and integrity.
6G networks will improve real-time data transmission with ultra-low latency, guaranteeing safe and quick data transfers between hospitals, patients, and healthcare devices. This combination will lower the risk of data breaches, ensure compliance with privacy laws (like the GDPR), and shield sensitive health information from cyberattacks.

2. Telemedicine, or real-time remote healthcare
• Real-time telemedicine services, which allow doctors to diagnose and treat patients remotely with little delay, will be made possible by 6G's high-speed and low-latency networks.
• By providing encrypted consultation records and health data histories, blockchain will guarantee safe and reliable communication between patients and healthcare practitioners, potentially greatly enhancing access to healthcare in rural and isolated locations.

3. Personalized and Precision Medicine
6G Networks will allow the rapid exchange of vast amounts of patient data (e.g., genomic data, health records, wearable data), facilitating the development of personalized medicine tailored to each patient's unique characteristics.
Blockchain can ensure that only authorized personnel access this sensitive data, giving patients more control over who can view and utilize their health information.
Drug traceability and validation on a blockchain can further ensure that medications administered are genuine and tailored to the patient's specific needs.

4. Interoperability and Data Sharing
6G can improve interoperability by connecting various healthcare systems and devices (IoT-based devices, wearables, medical records) in real time.
Blockchain technology can handle decentralized data between various healthcare players, including hospitals, insurance providers, and pharmaceutical companies, guaranteeing safe and transparent data exchange.
•This might result in the development of an international healthcare data network that allows for the secure cross-border exchange of patient data.

5. Predictive healthcare and AI-powered diagnostics
• AI-powered diagnostic tools can evaluate medical data in real-time with 6G's high-speed connectivity, resulting in quicker and more precise diagnoses.
• Blockchain ensures transparency and confidence in the decision-making process by validating and verifying the AI algorithms.
• Preventive care could be revolutionized by predictive healthcare models that use patient data to forecast illnesses before symptoms manifest.

6. Dispersed Health Markets
• Patients can take charge of their health data and possibly make money by sharing it with researchers or pharmaceutical corporations through blockchain-enabled decentralized health platforms.
• Users will be able to swiftly access or sell their anonymized health data without the need for middlemen thanks to 6G's smooth interaction on these platforms.
• This paradigm may also promote a patient-centered healthcare economy in which people own the value of their data.

7. Automated Healthcare Operations and Smart Hospitals
• 6G will give smart hospitals smooth connectivity, allowing real-time coordination across several systems like wearable technology, robotic surgery tools, AI-powered diagnostic equipment, and electronic health records (EHR).
• Blockchain will provide effective, safe, and auditable procedures by streamlining hospital operations, automating claims processing, managing employee credentials, and promoting transparency in the purchase of medical supplies.

8. Clinical studies and Research:
6G integration will enable quicker, more extensive data collection for medical research and clinical studies.
• By protecting patient identities and guaranteeing the immutability of trial results, blockchain can promote more moral and open research procedures.
• Because researchers can now quickly and securely access and analyze enormous datasets, this could hasten the discovery of new medications and therapies.

9. IoT Integration and Medical Device Security 6G will allow for incredibly quick communication between different Internet of Medical Things (IoMT) devices, increasing their efficiency in patient monitoring and care.
• By guarding against hacks and guaranteeing that device data is reliable, blockchain will guarantee the security and integrity of the data these devices gather and send.
• For wearable health monitoring, implanted devices, and other linked medical equipment, this will be especially crucial.

10. Disease tracking and global health monitoring
• By facilitating real-time monitoring of infectious illnesses, pandemics, and worldwide health trends, 6G can assist global health activities.
• Blockchain can assist organize international responses to health emergencies by enabling safe, transparent, and impenetrable data sharing between nations and health groups. This would be very helpful in reducing misinformation, maintaining data integrity, and managing pandemics in the future. By improving data security, encouraging real-time care, enabling tailored medicine, and promoting international health collaboration, the incorporation of blockchain technology into 6G networks will completely transform smart healthcare applications. When combined, these technologies will lay the groundwork for a future healthcare system that is more patient-centered, data-driven, and efficient.

6. Conclusion

To sum up, this essay has looked at how 6G networks and blockchain technology might transform healthcare applications. Blockchain guarantees data security, transparency, and interoperability, while 6G networks provide speed and connectivity never before possible. Together, they pave the way for innovative, perceptive healthcare solutions. The combination of 6G networks and blockchain technology presents a paradigm shift in the healthcare industry. This research has emphasized their collaborative potential, with a focus on the advantages for data security, connection, and overall healthcare efficiency. A day when intelligent healthcare solutions are not only a possibility but a reality will arrive if we embrace these developments as we navigate the ever evolving technology landscape.

References

1. Ahad, A., Jiangbina, Z., Tahir, M., Shayea, I., Sheikh, M. A., & Rasheed, F. (2024). 6G and Intelligent Healthcare: Taxonomy, technologies, open issues and future research directions. Internet of Things, 101068.
2. Sakthi, U., Alasmari, A., Girija, S. P., Senthil, P., Qamar, S., & Hariharasitaraman, S. (2024). Smart Healthcare Based Cyber Physical System Modeling by Block Chain with Cloud 6G Network and Machine Learning Techniques. Wireless Personal Communications, 1-25.
3. Alghamedy, F. H., El-Haggar, N., Alsumayt, A., Alfawaer, Z., Alshammari, M., Amouri, L., ... & Albassam, S. (2024). Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G. IEEE Access.
4. Kumar, N., & Ali, R. (2024). A smart contract-based robotic surgery authentication system for healthcare using 6G-Tactile Internet. Computer Networks, 238, 110133.
5. BOONSONG, W., Kumar, T. D., Archana, M. A., Umapathy, K., Omkumar, S., & Boovarahan, N. C. A. (2024). A Review on Blockchain Technology based Secure Intelligent Wearable Devices for 6G Systems. Przeglad Elektrotechniczny, (6).
6. Mohanaprakash, T. A., Kumar, D., Naveen, P., & Karuppiah, S. (2024). Cloud-Enabled Blockchain and IoT-Based Assisted Living System in 6G Networks: Enhancing Quality of Life and Privacy.
7. Kumar, N., & Ali, R. (2024). A smart contract-based 6G-enabled authentication scheme for securing Internet of Nano Medical Things network. Ad Hoc Networks, 163, 103606.
8. Dabas, D., Mehra, P. S., Chawla, D., Sharma, J., & Jamshed, A. (2024). 26G Internet for Intelligent of Things. Network Optimization in Intelligent Internet of Things Applications: Principles and Challenges, 19.
9. Chataut, R., Nankya, M., & Akl, R. (2024). 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. Sensors, 24(6), 1888.
10. Santhiyakumari, N. (2024). Blockchain-Powered Secure Communication Protocol for the Internet of Medical Things (IoMT). Journal of Information Technology and Digital World, 6(2), 167-178.
11. Kumar, A., & Chatterjee, K. (2024). Securing internet of medical devices using energy efficient blockchain for healthcare 4.0. Cluster Computing, 1-16.
12. Hasan, K. M. B., Sajid, M., Lapina, M. A., Shahid, M., & Kotecha, K. (2024). Blockchain technology meets 6 G wireless networks: A systematic survey. Alexandria Engineering Journal, 92, 199-220.

13. Sabuncu, Ö., & Bilgehan, B. (2024). Revolutionizing healthcare 5.0: Blockchain-driven optimization of drone-to-everything communication using 5G network for enhanced medical services. Technology in Society, 77, 102552.

14. Santhiyakumari, N. (2024). Blockchain-Powered Secure Communication Protocol for the Internet of Medical Things (IoMT). Journal of Information Technology and Digital World, 6(2), 167-178.

15. Chataut, R., Nankya, M., & Akl, R. (2024). 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. Sensors, 24(6), 1888.

16. Aziz, K., Dua, S., & Gupta, P. An Explainable and Comprehensive Federated Deep Learning in Practical Applications: Real World Benefits and Systematic Analysis Across Diverse Domains. In Federated Deep Learning for Healthcare (pp. 109-130). CRC Press.

17. Solunke, H., & Bhaladhare, P. (2024, March). Blockchain Approaches for Privacy Preservation: A Review. In 2024 1st International Conference on Cognitive, Green and Ubiquitous Computing (IC-CGU) (pp. 1-6). IEEE.

18. Al-Khatib, A., Ehsanfar, S., Moessner, K., & Timinger, H. (2024). Resources Reservation Schemes for Time-Sensitive Networked Vehicular Applications with a View on ISAC. IEEE Access.

19. CheSuh, L. N., Fernández-Diaz, R. Á., Alija-Perez, J. M., Benavides-Cuellar, C., & Alaiz-Moreton, H. (2024). Improve quality of service for the Internet of Things using blockchain & machine learning algorithms. Internet of Things, 26, 101123.

20. Salama, R., & Al-Turjman, F. (2024). Distributed mobile cloud computing services and blockchain technology. In Computational Intelligence and Blockchain in Complex Systems (pp. 205-214). Morgan Kaufmann.

21. Huan, N. T. Y., & Zukarnain, Z. A. (2024). A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications. IEEE Access.

22. Priyanka, N., Sethi, S., Sahai, A., Srivastava, A., Sambathkumar, M., & Boopathi, S. (2024). Reality for Human Experience in AI in the Digital Economy. In Multidisciplinary Applications of Extended Reality for Human Experience (pp. 374-400). IGI Global.

23. Mahesh, R., Anilkumar, K. B., Shwetha, S. N., Kumar, D. K., Santhosh, B. J., & Patil, H. (2024). IoT and Blockchain-Based Smart Grid Energy Management: Innovations and Applications. In Applying Internet of Things and Blockchain in Smart Cities: Industry and Healthcare Perspectives (pp. 99-130). IGI Global.

24. Putra, M. A. P., Karna, N., Alief, R. N., Zainudin, A., Kim, D. S., Lee, J. M., & Sampedro, G. A. (2024). PureFed: An Efficient Collaborative and Trustworthy Federated Learning Framework Based on Blockchain Network. IEEE Access.

25. Putra, M. A. P., Karna, N., Alief, R. N., Zainudin, A., Kim, D. S., Lee, J. M., & Sampedro, G. A. (2024). PureFed: An Efficient Collaborative and Trustworthy Federated Learning Framework Based on Blockchain Network. IEEE Access.

26. Javed, S., Hassan, A., Ahmad, R., Ahmed, W., Ahmed, R., Saadat, A., & Guizani, M. (2024). State-of-the-art and future research challenges in uav swarms. IEEE Internet of Things Journal.

27. Karydas, D., & Leligou, H. C. (2024). Federated Learning: Attacks and Defenses, Rewards, Energy Efficiency: Past, Present and Future. WSEAS Transactions on Computers, 23, 106-135.

28. Karydas, D., & Leligou, H. C. (2024). Federated Learning: Attacks and Defenses, Rewards, Energy Efficiency: Past, Present and Future. WSEAS Transactions on Computers, 23, 106- 135.

29. Le, H. D., Truong, V. T., Hoang, D. N., Nguyen, T. V., & Le, L. B. (2024, April). MetaCrowd: Blockchain-Empowered Metaverse via Decentralized Machine Learning Crowdsourcing. In 2024 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

30. Shen, M., Tan, Z., Niyato, D., Liu, Y., Kang, J., Xiong, Z., ... & Shen, X. (2024). Artificial Intelligence for Web 3.0: A Comprehensive Survey. ACM Computing Surveys, 56(10), 1-39.

31. Salama, R., & Al-Turjman, F. (2025). An overview of advanced networking technologies and the global value chain. Smart Global Value Chain, 79-90.

32. Salama, R., & Al-Turjman, F. (2024). A study of health-care data security in smart cities and the global value chain using AI and blockchain. In Smart Global Value Chain (pp. 165-172). CRC Press.

33. Jiang, T., Luo, H., Yang, K., Sun, G., Yu, H., & Huang, Q. (2024). Blockchain for Energy Market: A Comprehensive Survey. arXiv preprint arXiv:2403.20045.

34. Yu, M., Zhang, H., Ma, J., Duan, X., Kang, S., & Li, J. (2024). Cold Chain Logistics Supervision of Agricultural Products Supported Using Internet of Things Technology. IEEE Internet of Things Journal.

35. Guler, E. (2024). CITE-PSO: Cross-ISP Traffic Engineering Enhanced by Particle Swarm Optimization in Blockchain Enabled SDONs. IEEE Access, 12, 27611-27632.

36. Gerrits, L. (2024). IoT communications with blockchain and multi-chain: a case study in the automotive industry (Doctoral dissertation, Université Côte d'Azur).

37. Salama, R., & Al-Turjman, F. (2024). An Examination of the Cybersecurity Issue with Distributed Energy. The Smart IoT Blueprint: Engineering a Connected Future: Guiding Principles and Practical Strategies for Seamless Integration, 51.

38. Ahsan, M. S., & Pathan, A. S. K. (2024). The State-of-the-Art Access Control Models in IoT: A Survey on the Requirements, Scale, and Future Challenges. Scale, and Future Challenges.

39. Cheng, J., Yang, Y., Zou, X., & Zuo, Y. (2024). 5G in manufacturing: a literature review and future research. The International Journal of Advanced Manufacturing Technology, 131(11), 5637-5659.

40. Bo, P., Tu, W., Tu, X., Qu, F., & Wang, F. Y. (2024). Dual RIS-aided parallel intelligence surface for IoAMVSs: A co-design approach for 3C problems. IEEE Transactions on Intelligent Vehicles.

41. Gupta, M., Kumar, R., Larhgotra, A., & Ved, C. (2023). Emergence of Big Data and Blockchain Technology in Smart City. In *Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities* (pp. 83-101). CRC Press.

42. Juneja, A., Kumar, R., & Gupta, M. (2022, July). Smart Healthcare Ecosystems backed by IoT and Connected Biomedical Technologies. In *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 230-235). IEEE.

43. Gupta, M., Ahmed, S., Kumar, R., & Altrjman, C. (Eds.). (2023). *Computational Intelligence in Healthcare: Applications, Challenges, and Management*. CRC Press.

44. Kaur, G., Gupta, M., & Kumar, R. (2021). IoT based smart healthcare monitoring system: A systematic review. *Annals of the Romanian Society for Cell Biology*, 3721-3728.

45. Juneja, A., Kumar, R., & Gupta, M. (2022, July). Smart Healthcare Ecosystems backed by IoT and Connected Biomedical Technologies. In *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 230-235). IEEE.

Evaluating the Impact of Nursing Interventions in Postoperative Settings

Efe Precious Onakpojeruo[1,2] [0000-0001-8582-409X], Berna Uzun[1,3] [0000-0002-5438-8608]

[1] Operational Research Center in Healthcare, Department of Biomedical Engineering, Near East University, Nicosia 99138, Mersin 10, Turkey.,
[2] Department of Biomedical Engineering, Near East University, Nicosia 99138, Mersin 10, Turkey
[3] Department of Mathematics, Near East University, Nicosia 99138, Mersin 10, Turkey
efeprecious.onakpojeruo@neu.edu.tr, berna.uzun@neu.edu.tr

Abstract: Background: Postoperative critical care for cardiac surgical patients refers to the specialized care provided to patients in the intensive care unit (ICU) after they have undergone heart surgery. This care is designed for nurses to monitor and support the patient's recovery and may include a variety of interventions and treatments. **Objectives**: This systematic review aimed to identify the roles of nurses in postoperative critical care for cardiac surgical patients, considering factors that impact the length of stay in ICU, recovery time, the risks of cardiac surgery based on the types of heart surgery, and understanding the link between patients and the management of medical resources. **Methods**: To identify relevant studies, we utilized electronic databases such as PubMed, SCOPUS, Web of Science, and Springer. The search strategy involved using free-text terms related to the title and objectives of the study to retrieve articles from databases. We restricted our search to include only research published in journals subjected to peer review between June 2015 and December 2022. This time frame best reflects the evolution of treatment options, known risk factors, and technological advances in the medical field. Our initial search of four databases yielded 60,3080 papers. We then chose the most relevant papers by title and abstract. We accepted 20 papers, this collection includes case-control studies, randomized controlled trials studies, meta-analyses, and review studies. **Results and conclusion**: We observed that the postoperative roles of nurses in critical care for cardiac surgery patients contribute to minimizing the risk factors of cardiac surgery, mitigating the potential effects of cardiac surgery, adequate management of patients and resources in the hospital, and immensely contributing to the length of stay of patients in the ICU.

Keywords: cardiac surgery, postoperative critical care, length of stay, roles of nurses, intensive care unit

1. Introduction
What do we already know about this topic?
Post-heart surgery, patients receive specialized care in the ICU, managed by a team including nurses, doctors, and therapists for close recovery monitoring.
How does your research contribute to the field?
This systematic review identifies nurses' roles, postoperative activities, ICU stay factors, surgery types, and patient-resource links, contributing to a holistic understanding of postoperative care.
What are your research's implications towards theory, practice, or policy?
The study's insights highlight nurses' pivotal role in postoperative care, risk reduction, efficient resource management, and ICU stay.

2. Background

Critical care in cardiac surgery refers to the specialized care provided to patients who have undergone heart surgery and require close monitoring and support in the intensive care unit (ICU) [1]. These patients may have a variety of conditions that require close monitoring, such as heart attacks, heart failure, coronary artery disease, and other cardiac problems. In the ICU, patients will be monitored closely by nurses [2].

Postoperative nursing care for cardiac surgical patients typically involves close monitoring and management of the patient's vital signs, oxygenation, and fluid balance [3]. It may also involve managing pain, administering medications, and providing wound care. In the critical care setting, postoperative nursing care for cardiac surgical patients may involve providing mechanical ventilation, hemodynamic monitoring, and monitoring for complications such as infection or bleeding. The nursing care plan will be tailored to the individual patient's needs and may involve working closely with other healthcare professionals, such as physicians, respiratory therapists, and physical therapists [1], [2], [3].

Table 1: Some specific tasks that may be included in postoperative nursing care for cardiac surgical patients in the critical care setting include:

S/N	Specific Tasks	Definition
1.	Monitoring vital signs and oxygenation levels [4]	This may involve continuous monitoring of the patient's heart rate, blood pressure, respiratory rate, and oxygen saturation levels.
2.	Managing pain [5]	This may involve administering pain medication as prescribed and using non-pharmacological methods, such as positioning and relaxation techniques, to manage pain.
3.	Providing wound care [6]	This may involve cleaning and dressing the surgical wound and monitoring for signs of infection.
4.	Administering medications [7]	This may involve administering medications as prescribed, such as antibiotics to prevent infection or medications to manage heart rhythm.
5.	Providing mechanical ventilation [8]	This may involve using a ventilator to assist with breathing and monitoring the patient's response to ventilation.
6.	Hemodynamic monitoring [9]	This may involve using specialized equipment to monitor the patient's blood pressure, cardiac output, and other hemodynamic parameters.
7.	Monitoring for early identification and prevention of postoperative complications [9]	This may involve regularly checking for signs of infection, bleeding, or other complications and taking appropriate action if any are detected
8.	Nutrition [10]	Patients may receive nutrition through an IV or feeding tube to help support their recovery.
9.	Physical therapy [11]	Patients may receive physical therapy to help them regain strength and mobility after surgery.

The type of postoperative care a patient needs and the length of time a patient spends in the ICU after cardiac surgery can vary widely depending on the surgery type, the surgery's complexity,

and the patient's overall health condition [12]. In some cases, patients may only spend a few days in the ICU, while others may require a longer stay. The goal of postoperative nursing critical care is to provide the necessary support and monitoring to allow the patient to recover and eventually be transferred to a regular hospital room [3].

Despite the plethora of studies identifying the roles of nurses in postoperative critical care for cardiac surgery patients, there has been no review combining the conclusions reached with regard to the different types of cardiac surgery and factors that can impact the length of stay in ICU, the risks imposed on cardiac surgical patients, the length of time it takes for patients to recover from cardiac surgery, or how this information can be put to use in patient care or in the management of resources. This study aims to address this knowledge gap by reviewing the relevant literature and suggesting directions for future investigation.

3. Objectives

The goal of this review was to identify the roles of nurses in postoperative critical care for cardiac surgical patients, as well as to gain an understanding of the various postoperative activities with respect to factors that impact the length of stay in ICU, recovery time, risks factors of cardiac surgery based on the types of heart surgery and gaining an understanding of the link between patients and the management of medical resources.

Questions

Our rationale for conducting this systematic review was based on the following;

1) What are the roles of nurses in postoperative critical care for cardiac surgical patients?
2) What factors contribute to a patient's length of stay in the ICU?
3) Do any of the selected studies investigate whether or not there is an application that could help improve the understanding of the connection between patients and the administration of medical resources?

4. Methods
Search strategy

The search strategy involved the use of free-text terms related to the title of the study. We also utilized the snowballing search method which involved the use of references from identified studies to find additional relevant studies with the objective of identifying additional studies that may not be captured through traditional free-text search methods by following citation trails. To enhance transparency and completeness of reporting, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses Statement (PRISMA) was used to conduct the flow diagram of inclusion and exclusion criteria as seen in Figure 1.

The following free-text terms were used to conduct electronic searches of PubMed, Web of Science (WOS), SCOPUS, and Springer: Roles of nurses in postoperative critical care in cardiac surgery patients, Postoperative activities of cardiac surgery Factors impacting length of stay in ICU, Types of cardiac surgery, and Risk factors of cardiac surgery. The searched terms and results are summarized in Table 2. The bibliographies of the included studies were combed for additional articles not uncovered by the electronic search.

Table 2: Searched terms used in databases

S/N	Keywords	Searched terms	Databases	Searched results
1.			PUBMED	48

	Roles of nurses	Roles of nurses in postoperative critical care in cardiac surgery patients	SPRINGER	7693
			SCOPUS	24
			WOS	6
2.	Postoperative activities	Postoperative activities of cardiac surgery	PUBMED	8482
			SPRINGER	38852
			SCOPUS	2509
			WOS	1370
3.	Length of stay	Factors impacting length of stay in ICU	PUBMED	1621
			SPRINGER	19043
			SCOPUS	21
			WOS	1176
4.	Cardiac surgery	Types of Cardiac Surgery	PUBMED	12771
			SPRINGER	186619
			SCOPUS	15381
			WOS	22351
5.	Risks factors	Risk factors of cardiac surgery	PUBMED	72309
			SPRINGER	156348
			SCOPUS	30931
			WOS	28226

5. Study criteria

The following criteria were used by a panel of three reviewers who are nurses and one anesthesiologist (AA, BB, and ME) to determine which abstracts to include and which to exclude.

Selection criteria

The articles were screened based on duplication, title, abstract, and full text of the publications using the specified selection and exclusion criteria:

1) Reported reviews or meta-analyses that included the roles of nurses in postoperative critical care for patients of all age groups who underwent any of the 7 types of cardiac surgeries namely, coronary artery bypass surgery, heart valve surgery, heart transplant, cardiac catheterization, pacemaker or defibrillator implantation, cardiac ablation, heart surgery for congenital heart defects only.
2) Reported studies published between June 2015 to December 2022 in the English language
3) Reported studies published in peer-reviewed journals from June 2015 to December 2022. We limited our search to this time frame because it best reflects the evolution of treatment options, known risk factors, and technological advances in the medical field [13], [14], [15]. These elements have probably evolved over time. There is a possibility that the recent improvements in perioperative and postoperative care have also contributed to this shift [13], [14], [15]. For this reason, we selected a time frame of 7 years and
4) Included studies whose primary objective was to assess the factors that influence the length of time patients spend in the ICU after cardiac surgery.

Exclusion criteria

Studies were excluded if they;

1. Are not published in English language

2. Had no reference to the roles of nurses in postoperative critical care for patients who underwent any of the 7 types of cardiac surgeries namely, coronary artery bypass surgery, heart valve surgery, heart transplant, cardiac catheterization, pacemaker or defibrillator implantation, cardiac ablation, and heart surgery for congenital heart defects.
3. Studies that only look at preoperative or intraoperative variables without considering postoperative variables such as recovery time or ICU length of stay.
4. Duplicate publications or those previously listed in another search database, and publications without the full text

Following the meticulous application of the eligibility and exclusion criteria, the literature screening yielded a final count of 20 research papers

6. Data extraction and quality assessment

We utilized four electronic databases such as PubMed, SCOPUS, Web of Science, and Springer. The search strategy involved the use of free-text terms related to the title of the study. We used a standardized data collection form to gather information from case-control studies, randomized controlled trial studies, meta-analyses, and review studies. Information related to the studies' designs, postoperative nursing activities, patient samples, surgical procedures, ICU stays, recovery times, resource management, and major risk factors like bleeding, infections, anesthetic reactions, stroke, tissue injury, and mortality. 20 papers were eventually accepted after meeting our criteria as seen in Figure 1.
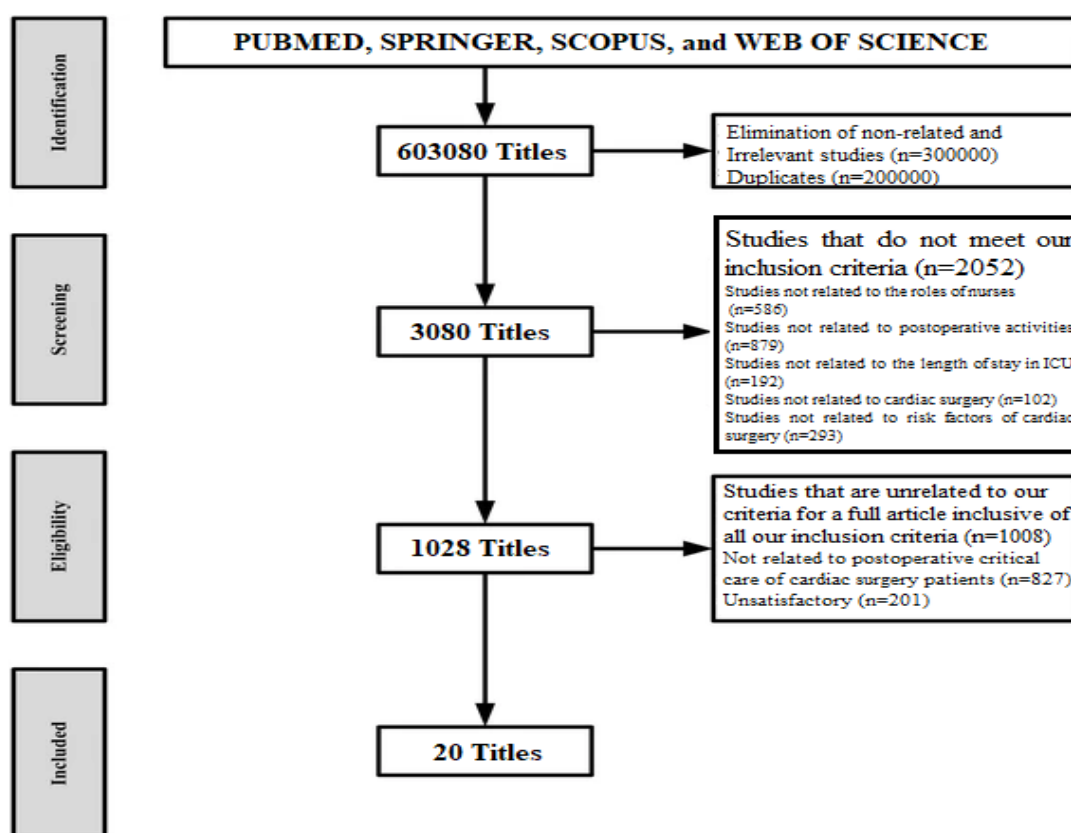

Identification

PUBMED, SPRINGER, SCOPUS, and WEB OF SCIENCE

603080 Titles → Elimination of non-related and Irrelevant studies (n=300000) Duplicates (n=200000)

Screening

3080 Titles → Studies that do not meet our inclusion criteria (n=2052)
Studies not related to the roles of nurses (n=586)
Studies not related to postoperative activities (n=879)
Studies not related to the length of stay in ICU (n=192)
Studies not related to cardiac surgery (n=102)
Studies not related to risk factors of cardiac surgery (n=293)

Eligibility

1028 Titles → Studies that are unrelated to our criteria for a full article inclusive of all our inclusion criteria (n=1008)
Not related to postoperative critical care of cardiac surgery patients (n=827)
Unsatisfactory (n=201)

Included

20 Titles

Fig. 1 Search process flow for articles included in the review

We looked for suggestions for managing resources, either individually or in conjunction with patients. In the context of this discussion, we refer to management intervention as any strategy with the goals of improving patient scheduling, reducing the length of time patients spend in the ICU, lowering patient risks, and improving patient flow or resource allocation.

Quality assessment

The paper quality was evaluated by checking that our researchers had accessed relevant material through the Near East University library's online catalog. We went through the articles on the library's website and made sure they met the following standards:

Selection

1. If the samples used in the studies are truly indicative of the population of patients who have undergone cardiac surgery
2. Justified by our inclusion criteria
3. Satisfactory information relating to our inclusion criteria
4. Case-by-case evaluation
5. Double-blind data recording and
6. Correlation self-report

The Near East University library is well-regarded for its extensive collection of scholarly resources, including prominent databases for research purposes. The decision to utilize the Near East University Library's online catalog for quality assessment was based on the rich array of academic materials accessible through this platform. To ensure the comprehensiveness and reliability of our quality assessment, we cross-referenced the resources available through the Near East University library with other reputable databases such as the Willey online library. This triangulation of sources aimed to enhance the robustness of our data collection and analysis.

7. Findings from reviewed studies

The initial search of the four databases we looked at yielded a total of 60,3080 papers. After that, we used the papers' titles and abstracts to determine which were most pertinent. 20 papers were eventually accepted after meeting our criteria. The papers included in this collection are case- control studies, randomized controlled trial studies, meta-analyses, and review studies. Some of the studies have specifically focused on the roles that nurses play in postoperative critical care for cardiac surgery patients, postoperative activities of cardiac surgery, factors that impact the length of stay in the intensive care unit, different types of cardiac surgery, risk factors for cardiac surgery, and studies that improve the understanding of the connection between patients and the administration of medical resources. Reviewed papers that met inclusion criteria have been summarized in Table 3.

Table 3: Studies Summary

S/N	Reference	Year	Number of patients included	Cardiac surgery type	Observed postoperative risk factors of	Observed factors impacting length of stay in ICU	Postoperative roles of nurses after cardiac surgery	The average stay in ICU	Findings

No.	Ref	Year	Number	Procedure	cardiac surgery				
1.	[16]	2022	347626	Coronary artery bypass	age	NA	Monitoring of patients	NA	The result of the survey reported a decrease in the observed mortality rate for all procedures, a reduced workload, and adjusted lifestyles due to advanced postoperative activities
2.	[17]	2022	250	Heart valve surgery	Acute kidney injury,	Acute kidney injury,	Monitoring of vital signs	5 days	Cardiac biomarkers predicted the outcome of cardiac surgery
3.	[18]	2022	3611	Heart transplantation	hemodialysis,	Stroke, pacemaker insertion, hemodialysis,	Coordinating care with other healthcare professionals	NA	There will be an increase in adult heart transplantation in the United States
4.	[19]	2021	31277	Surgical aortic valve replacement	Bleeding	Bleeding, stroke, cardiopulmonary bypass times	Coordinating care with other healthcare professionals	NA	Results from the survey showed that surgical aortic valve replacement has low levels of complicatio

									ns and low mortality risk considering both the preoperative and postoperative activities
5	[20]	2022	NA	Valve surgery	sternal wound infection	Sternal wound infection	Assisting with mobility, monitoring vital signs, coordinating care with other healthcare professionals	NA	A clear difference between the preoperative and postoperative quality of life was reported in elderly people who underwent valve surgery
6.	[21]	2022	NA	Coronary artery bypass graft surgery	sternal wound infection	sternal wound infection	Assisting with mobility, monitoring vital signs, coordinating care with other healthcare professionals	NA	The findings of this study reported an improvement in health-related quality of life after coronary artery bypass surgery.
7.	[22]	2022	313	Cardiac surgery	delirium	delirium	Coordinating care with other healthcare re		The results indicated that postoperative delirium is a major risk factor

						professionals		that can contribute to a decrease in the quality of life, and functional/cognitive abilities in patients after 3 years of cardiac surgery.
8.	[23]	2022	616	Heart valve surgery	Cardiac arrest	Cardiac arrest, pacemaker implantation	Monitoring of vital signs		Reported cardiac arrest as a risk factor for heart valve surgery
9.	[24]	2022	61	Cardiac surgery	VAP infections	VAP infections, acute kidney injury, nasal feeding	Coordinating care with other healthcare professionals	28	Ventilator-associated pneumonia (VAP) is a risk factor for cardiac surgery patients
10	[25]	2020	946	cardiac surgery	VAP infections, congested heart failure, preoperative glucose levels, blood transfusion, hypertension	VAP infections,	Coordinating care with other healthcare professionals	30	VAP is associated with cardiac surgery

1 1	[26]	20 19	2215	Coronary artery bypass	Increase d glucose	Increased glucose,	Monitori ng of vital signs	NA	Increased glucose is associated with coronary artery bypass
1 2	[27]	20 22	564	Infra inguinal revascular ization	Preopera tive hemoglo bin, Surgery stress, blood transfusi on	blood transfusio n, anemia, surgical stress	Coordin ating care with other healthca re professi onals	30	Blood transfusion, anemia, and other comorbiditi es and surgery stress as some of the complicatio ns resulting prolong stay in ICU after cardiac surgery.
1 3	[28]	20 18	NA	Cardiac surgery	Acute kidney injury	Acute kidney injury	Coordin ating care with other healthca re professi onals	NA	Acute kidney injury as a complicatio n impacting the length of stay in the ICU after cardiac surgery
1 4	[29]	20 16	NA	Cardiac surgery	age, atrial fibrillati on, cardiac arrhythm ia, low ejection fraction	obstructiv e pulmonar y disease, heart failure, renal dysfunctio n, severe pain	Monitori ng of vital signs	NA	Advanced age, atrial fibrillation, cardiac arrhythmia, obstructive pulmonary disease, heart failure, low ejection fraction, renal dysfunction,

									non-elective surgery status, and severe pain are common factors that impact the length of stay in the ICU
15	[30]	2022	196	Cardiac surgery	venous catheters infection	venous catheters infection	Providing wound care, Educating the patient and their family	10	Early postoperative interventions of nurses in the ICU reduces complications and length of stay in the ICU
16	[31]	2022	NA	Invasive surgeries	anxiety, depression, sleep disturbance	Delirium, depression	Educating the patient and their family	NA	Psychological issues such as anxiety, depression, delirium, sleep disturbance, etc. can be alleviated by the postoperative roles of nurses.
17	[32]	2022	NA	Surgery	Reintervention	post-operative complications	Educating the patient and their family, Coordinating care with other	NA	Nurses' involvement and experience in AI-based medical technology is a method of delivering

							healthcare professionals		advanced care to patients
18	[33]	2022	356	Implantable cardioverter defibrillator	Inappropriate shocks, induced ventricular arrhythmias	NA	Monitoring of vital signs	NA	Safety in extravascular implantable cardioverter defibrillator.
19	[34]	2020	149	Heart transplantation	bacterial infection	bacterial infection	Providing wound care, Coordinating care with other healthcare professionals	NA	Multidrug-resistant organisms is a burden to patients who underwent heart transplant.
20	[35]	2022	NA	Thoracic aortic surgery	Reoperation	post-operative complications	Close monitoring	NA	strategies for improving quality of life of patients who will undergo thoracic aortic surgery

We have classified the study into 4 categories in this present section. The categories encompass the way this review is sectioned to answer the questions, considering the types of cardiac surgery, the risk factors of cardiac surgery, the factors impacting length of stay in ICU, postoperative activities of cardiac surgery, and the role of nurses in postoperative critical care in cardiac surgery patients.

Nurses' approaches to cardiac surgery types

Cardiac surgery is a type of surgery that is performed on the heart or the blood vessels surrounding the heart. It is typically performed by a team of surgeons, cardiologists, and anesthesiologists [36]. There are several types of cardiac surgery, including:

1. Coronary artery bypass surgery: This surgery involves bypassing a blocked coronary artery using a blood vessel taken from another part of the body, such as the leg or chest. The blood vessel is used to create a new route for blood to flow to the heart [16].
2. Heart valve surgery: This surgery involves repairing or replacing a damaged heart valve. Heart valves can become damaged due to conditions such as heart disease, infection, or injury [17].
3. Heart transplant: This type of surgery involves replacing a damaged or diseased heart with a healthy heart from a donor [18].
4. Cardiac catheterization: This procedure involves inserting a thin tube (catheter) into a blood vessel and threading it through the body to the heart. It is used to diagnose and treat certain heart conditions [18].
5. Pacemaker or defibrillator implantation: This surgery involves implanting a device that helps regulate the heart's rhythm. A pacemaker is used to treat slow heart rhythms, while a defibrillator is used to treat fast, irregular rhythms [33].
6. Cardiac ablation: This procedure involves destroying or removing heart tissue causing abnormal electrical signals. It is used to treat certain types of arrhythmias (irregular heart rhythms) [37].
7. Heart surgery for congenital heart defects: This surgery is used to repair or correct heart defects that a person is born with. These defects can include heart structure or function problems [38].

The majority of the studies reported decreased risk factors following the roles of nurses in managing postoperative cardiac situations. A study by [16] targeted coronary artery bypass surgery. The outcomes of surgical operations after the postoperative activities of involved hospital management in the UK over the period of 15 years dating from 2002 to 2016 were reported in this study. The study used validated data acquired from the National Institute for Cardiovascular Outcomes Research. The data collected totaled 347626 coronary surgical procedures. The average age considered was 66 years. Their workload, risk factors, emergency health cases, other co- morbidities, and mortality cases after the surgery within these 15 years were considered. The result of the survey reported a decrease in the observed mortality rate for all procedures, a reduced workload, and adjusted lifestyles. The study reported an improved quality of care over the 15 years and also a consistent decline in overall cases of related coronary artery bypass in the UK.

Similarly, [19] reported outcomes of people who underwent surgical aortic valve replacement between April 2013 and March 2018 in the UK, and compared with transcatheter aortic valve implantation. About 31277 patients were included in the study. Their demographics, preoperative and postoperative risk factors, mortality rate, and operative data were all included as criteria for the review. Results from the survey showed that surgical aortic valve replacement has low levels of complications and low mortality risk considering both the preoperative and postoperative activities, even though factors like poor functioning of ventricles, emergency operations, higher Euro SCORE, and cardiopulmonary bypass times affected the outcomes. We further observed similar reports from other reviewed studies, [20], [21], [35], [39], [40], [41] as a result of the advanced postoperative activities of nurses and other hospital managing departments.

Postoperative risk factors of cardiac surgery
We observed several potential risk factors that can affect the outcome of cardiac surgery in our systematic review. These include:

1. Age: Older patients may be more at risk for complications due to their age and potentially underlying health conditions.
2. Pre-existing medical conditions: Patients with certain medical conditions such as diabetes, kidney disease, or lung disease may be at higher risk for complications after surgery.
3. Procedure type: Some types of cardiac surgery, such as valve replacements or coronary artery bypass grafts, may be more complex and have a higher risk of complications.
4. Surgical technique: The skill and experience of the surgical team can also play a role in the risk of complications.
5. Blood loss and transfusion: Blood loss during surgery can increase the risk of complications, as can the need for a blood transfusion.
6. Infection: Infection is a common complication after any surgery, and it can be particularly dangerous in the case of cardiac surgery due to the risk of infection spreading to the heart or other vital organs.
7. Heart attack: There is a risk of a heart attack occurring during or after surgery, which can be life-threatening.
8. Stroke: Stroke is a rare but serious complication of cardiac surgery that can result in significant disability or death.

It's important to discuss these and any other potential risk factors with patients and/or patient relations before any surgery to understand the potential risks and benefits of the procedure.

An independent risk factor called delirium has been reported to contribute to poor quality of life after postoperative activities of cardiac surgery. The study [22] evaluated the influence delirium possesses on the functional and cognitive abilities of patients within 3 to 4 years who underwent cardiac surgery. About 313 patients were included in the study ages 18 years and above. The following factors were considered for their evaluation; (concentration, development of memory problems, confusion, sleep disorders, emotional disorders, nightmares, and mobility. The results indicated that postoperative delirium is a major risk factor that can contribute to a decrease in the quality of life, and functional/cognitive abilities in patients after 3 years of cardiac surgery. Similarly, a study by [23], reported cardiac arrest as a risk factor for 14 patients amongst 616 patients that were included in the study. The study reported 4 death cases as the endpoint for some patients with such risk attacks, and 10 patients were given permanent pacemaker implantation. 5 out of the 10 patients were further reported dead due to prolonged MODs. Two other studies by [24], [25], reported ventilator-associated pneumonia (VAP) as a risk factor for cardiac surgery. For [24] 61 cases were included in the study of which 34 cases were VAP-infected. While for [25] 57 patients were identified to be VAP infected out of 946 patients. Similarly, [26], [34], [42] are studies reviewed and observed to be associated with postoperative risk factors after cardiac surgery.

Factors impacting length of stay in ICU after cardiac surgery

There are several factors that can impact the length of stay in the intensive care unit (ICU) after surgery or other medical procedures. These include:

1. Type of procedure: Some procedures, such as major surgery or organ transplantation, may require a longer stay in the ICU due to the complexity of the procedure and the need for close monitoring and support.
2. Patient's age and overall health: Older patients or those with underlying health conditions may require a longer stay in the ICU due to their increased risk of complications.

3. Complications: The presence of complications, such as infection or organ failure, can extend the length of stay in the ICU.
4. Recovery progress: The rate of recovery can also impact the length of stay in the ICU. Patients who are recovering quickly may be able to be transferred to a less intensive level of care more quickly, while those who are not recovering as quickly may need to remain in the ICU longer.
5. Availability of a hospital bed: In some cases, the length of stay in the ICU may be extended due to a lack of availability of a hospital bed in a less intensive care unit or on a regular hospital floor.
6. Insurance coverage: In some cases, the length of stay in the ICU may be limited by insurance coverage or other financial considerations.

It's important to discuss the expected length of stay in the ICU with your healthcare team to understand the factors that may impact it and to have a general idea of what to expect. Some of the factors impacting the length of stay in the ICU have been reported in a study by [27]. The study reported blood transfusion, anemia, and other comorbidities and surgery stress as some of the complications resulting prolong stay in ICU after cardiac surgeries specifically for infra inguinal revascularization. Similarly, a retrospective study by [28] and [43], reported acute kidney injury as a complication of postoperative risk factors impacting the length of stay in the ICU after cardiac surgery. In addition, a well-detailed systematic review reported other factors that may influence the length of stay in the ICU after cardiac surgery. The study [29] reported the following factors (advanced age, atrial fibrillation, cardiac arrhythmia, obstructive pulmonary disease, heart failure, low ejection fraction, renal dysfunction, non-elective surgery status, and even severe pain [44]) as some common factors that impact the length of stay in the ICU.

Postoperative roles of nurses after cardiac surgery

Performing cardiac surgery is not only difficult, but it also takes a significant amount of time and can be quite traumatic for the patient. The early intervention of nurses' postoperative activities is necessary to manage and mitigate the resulting risks of cardiac surgery. There are several key roles that nurses play in the postoperative care of patients who have undergone cardiac surgery. These roles include:

1. Monitoring vital signs: Nurses will closely monitor the patient's vital signs, including blood pressure, heart rate, and oxygen levels, to ensure that the patient is stable and recovering well.
2. Providing pain management: Nurses will administer pain medication as needed and help the patient manage any pain or discomfort they may be experiencing.
3. Assisting with mobility: Nurses will help the patient get out of bed and move around as soon as possible after surgery, as this can help prevent complications such as pneumonia or blood clots.
4. Providing wound care: Nurses will change dressings and monitor the patient's incision for any signs of infection or other complications.
5. Educating the patient and their family: Nurses will provide information and instruction to the patient and their family about what to expect during the recovery process and how to care for the patient at home.
6. Coordinating care with other healthcare professionals: Nurses will work closely with the patient's surgeon and other members of the healthcare team to ensure that the patient's care is coordinated and that all of their needs are being met.

A study by [30] reported that the early postoperative interventions of nurses in the ICU reduced the complications of cardiac surgery, especially infection-related risks and length of stay in the ICU. Another study by [31] focused on the psychological issues such as anxiety, depression, delirium, sleep disturbance, etc. that patients experience and how the roles of nurses help in alleviating its effects and reducing the length of stay in the ICU. Similarly, nurses' involvement and experience in AI-based medical technology as a method of delivering advanced care to patients were reported in a study by [32]. Another study by [45] reported the importance of nurses' educational needs in managing postoperative activities after cardiac surgery. Also [46] reported the involvement of nurses in monitoring ECG for the early detection of atrial fibrillation.

8. Discussion of findings
1. Cardiac Surgery and Types
Coronary Artery Bypass Surgery: The review highlighted a substantial decrease in observed mortality rates and improved quality of care over 15 years in the UK for patients undergoing coronary artery bypass surgery [6]. The study, encompassing 347,626 procedures, emphasized the positive impact of advanced postoperative activities and a consistent decline in overall cases.

Surgical Aortic Valve Replacement: A similar trend was observed in patients undergoing surgical aortic valve replacement, where outcomes indicated low complication levels and mortality risk [12]. Despite influencing factors like poor ventricular functioning and longer cardiopulmonary bypass times, these findings underscore the success of surgical interventions.

2. Postoperative Risk Factors of Cardiac Surgery
Delirium as a Risk Factor: Delirium emerged as a significant risk factor affecting the quality of life and functional/cognitive abilities of patients post-cardiac surgery [19]. The study emphasizes the importance of addressing postoperative delirium to enhance long-term patient outcomes.

Cardiac Arrest and Ventilator-Associated Pneumonia: Cardiac arrest and ventilator-associated pneumonia were identified as notable risk factors for heart valve surgery and cardiac surgery, respectively [20, 21, 22]. These findings stress the need for targeted interventions and preventive measures to mitigate these risks in postoperative cardiac care.

3. Factors Impacting Length of Stay in ICU After Cardiac Surgery
Complications Leading to Prolonged ICU Stay: Several factors were identified as contributors to prolonged ICU stays after cardiac surgery, including blood transfusion, anemia, comorbidities, and surgery-related stress [26, 27, 28]. Understanding and addressing these complications are crucial for optimizing postoperative care and resource management.

Multifactorial Influences: The comprehensive systematic review reported various factors influencing ICU length of stay, such as advanced age, atrial fibrillation, cardiac arrhythmia, and pain [29]. This multifaceted approach underscores the need for tailored strategies to address diverse patient needs.

4. Postoperative Roles of Nurses After Cardiac Surgery
Comprehensive Nursing Interventions: The review highlighted the pivotal role of nurses in postoperative cardiac care, encompassing monitoring vital signs, pain management, mobility assistance, wound care, patient and family education, and coordination with other healthcare professionals [31, 32, 33, 34, 35]. The collective impact of these interventions is crucial for minimizing complications and optimizing patient outcomes.

AI-Based Medical Technology: Nurses' involvement in AI-based medical technology emerged as a modern and effective approach to delivering advanced care, showcasing the integration of technological advancements in patient management [33].

Educational Needs of Nurses: Recognizing the importance of nurses' educational needs in managing postoperative activities after cardiac surgery, the review emphasizes the ongoing development of nursing skills and knowledge to meet evolving healthcare demands [34].

Early Detection through Monitoring: Nurses' involvement in monitoring electrocardiograms (ECGs) for the early detection of atrial fibrillation demonstrates the multifaceted role of nurses in not only postoperative care but also in the early identification of complications [35].

5.Implications for Theory-Policy and Practice

The findings from this systematic review have significant implications for theory, policy, and practice in cardiac surgery care [47]. The positive trends observed in mortality rates and complication levels suggest the efficacy of advanced postoperative activities, emphasizing the need for continued investment in healthcare resources and training.

Theory

These findings contribute to theoretical frameworks by highlighting the importance of tailoring interventions to specific cardiac surgery types and risk factors. The multifactorial nature of complications underscores the need for a comprehensive theoretical approach to postoperative care [47].

Policy

Policy implications include the need for standardized protocols addressing postoperative complications, as well as the integration of AI-based technologies in nursing practice. These policies should emphasize ongoing education for nurses to keep pace with evolving medical technologies.

Practice

In practice, healthcare professionals should prioritize early interventions, patient education, and collaborative care to minimize postoperative risks. The success observed in certain procedures emphasizes the importance of disseminating best practices across healthcare settings [48].

Limitations

Only studies originally published in English were considered for review. This means that potential studies that met the inclusion criteria but were written in a different language were not considered. Additionally, we did not explicitly include systematic reviews and meta-analysis studies published until the year 2015. Our focus was primarily on primary studies conducted between 2015 to 2022. Although we followed a methodological approach in selecting databases, data extraction, and quality assessment in the interest of transparency and completeness of reporting, expert opinion was not consulted in database development and data extraction. Furthermore, longitudinal follow-up studies were not included in this review. Longitudinal follow- up studies could provide valuable insights into the dynamics of postoperative care and recovery over time. Future reviews could explore the inclusion of such studies to enhance the understanding of long-term outcomes and variations in patient care practices [49][50].

9. Conclusion

Based on our systematic review, we can say that the postoperative roles of nurses in critical care for cardiac surgery patients help reduce surgical risks, lessen postoperative complications,

ensure efficient use of hospital resources, and significantly shorten patients' lengths of stay in the intensive care unit. The process of identifying the risk factors of cardiac surgery and the various risk factors for prolonged length of stay should not be treated in isolation from the intended use of the information gathered. That is to say, it is important to specify why identifying risk factors is useful. This will make it easier to incorporate influential factors into the decision-making process when allocating resources. More investigation is required to establish a causal relationship between variations in hospital resource utilization and management approaches that aim to maximize patient flow. The postoperative roles of nurses in the critical care of patients undergoing cardiac surgery also need further study. It is recommended that registered nurses take on postoperative responsibilities in critical care for cardiac surgery patients because nurses make a significant contribution to the overall health of patients who undergo cardiac surgery.

References

[1] R. S. Stephens and G. J. R. Whitman, "Postoperative critical care of the adult cardiac surgical patient. Part I: Routine postoperative care," *Crit Care Med*, vol. 43, no. 7, pp. 1477–1497, Jul. 2015, doi: 10.1097/CCM.0000000000001059.

[2] A. Aneman *et al.*, "Advances in critical care management of patients undergoing cardiac surgery," *Intensive Care Med*, vol. 44, pp. 799–810, 2018, doi: 10.1007/s00134-018-5182-0.

[3] J. Mehl and K. Hatton, "Postoperative Critical Care for Cardiac Surgical Patients," *Anesth Analg*, vol. 120, no. 6, p. 1426, Jun. 2015, doi: 10.1213/ANE.0000000000000590.

[4] C. Areia *et al.*, "Experiences of current vital signs monitoring practices and views of wearable monitoring: A qualitative study in patients and nurses," *J Adv Nurs*, vol. 78, no. 3, pp. 810–822, Mar. 2022, doi: 10.1111/JAN.15055.

[5] Z. Kia, M. Allahbakhshian, M. Ilkhani, M. Nasiri, and A. Allahbakhshian, "Nurses' use of non-pharmacological pain management methods in intensive care units: A descriptive cross-sectional study," *Complement Ther Med*, vol. 58, p. 102705, May 2021, doi: 10.1016/J.CTIM.2021.102705.

[6] S. Gairhe, "Nurse's roles in wound care and infection control : Surgical wound care in elderly," 2022, Accessed: Feb. 12, 2024. [Online]. Available: http://www.theseus.fi/handle/10024/781192

[7] M. Vaismoradi, S. Tella, P. A. Logan, J. Khakurel, and F. Vizcaya-Moreno, "Nurses' Adherence to Patient Safety Principles: A Systematic Review," *International Journal of Environmental Research and Public Health 2020, Vol. 17, Page 2028*, vol. 17, no. 6, p. 2028, Mar. 2020, doi: 10.3390/IJERPH17062028.

[8] H. ; Zaiton *et al.*, "Process from Mechanical Ventilation for Patients Post-Cardiothoracic Surgery: A Qualitative Study," *Univers J Public Health*, vol. 10, no. 4, pp. 393–401, 2022, doi: 10.13189/ujph.2022.100412.

[9] A. Bouchlarhem, Z. Bazid, N. Ismaili, and N. El Ouafi, "Cardiac intensive care unit: where we are in 2023," *Front Cardiovasc Med*, vol. 10, 2023, doi: 10.3389/FCVM.2023.1201414.

[10] G. Van Den Berg, H. Vermeulen, T. Conroy, H. Van Noort, M. De Van Der Schueren, and G. Huisman-de Waal, "Factors influencing the delivery of nutritional care by nurses for hospitalised

medical patients with malnutrition; a qualitative study," *J Clin Nurs*, vol. 32, no. 15–16, pp. 5147–5159, Aug. 2023, doi: 10.1111/JOCN.16614.

[11] G. García-Pérez-de-Sevilla and B. Sánchez-Pinto Pinto, "Effectiveness of physical exercise and neuromuscular electrical stimulation interventions for preventing and treating intensive care unit-acquired weakness: A systematic review of randomized controlled trials," *Intensive Crit Care Nurs*, vol. 74, p. 103333, Feb. 2023, doi: 10.1016/J.ICCN.2022.103333.

[12] "Postoperative care after cardiac surgery - UpToDate." Accessed: Dec. 22, 2022. [Online]. Available: https://www.uptodate.com/contents/postoperative-care-after-cardiac-surgery

[13] M. K. Wakefield, D. R. Williams, S. Le Menestrel, and J. L. Flaubert, Eds., "The Future of Nursing 2020-2030," Aug. 2021, doi: 10.17226/25982.

[14] C. Teresa-Morales, M. Rodríguez-Pérez, M. Araujo-Hernández, and C. Feria-Ramírez, "Current Stereotypes Associated with Nursing and Nursing Professionals: An Integrative Review," *Int J Environ Res Public Health*, vol. 19, no. 13, Jul. 2022, doi: 10.3390/IJERPH19137640.

[15] S. B. Junaid *et al.*, "Recent Advancements in Emerging Technologies for Healthcare Management Systems: A Survey," *Healthcare*, vol. 10, no. 10, Oct. 2022, doi: 10.3390/HEALTHCARE10101940.

[16] S. K. Ohri *et al.*, "Coronary artery bypass surgery in the UK, trends in activity and outcomes from a 15-year complete national series," *European Journal of Cardio-Thoracic Surgery*, vol. 61, no. 2, pp. 449–456, Jan. 2022, doi: 10.1093/EJCTS/EZAB391.

[17] A. Wozolek *et al.*, "Cardiac Biomarkers and Prediction of Early Outcome After Heart Valve Surgery: A Prospective Observational Study," *J Cardiothorac Vasc Anesth*, vol. 36, no. 3, pp. 862–869, Mar. 2022, doi: 10.1053/J.JVCA.2021.06.028.

[18] S. Madan, O. Saeed, S. J. Forest, D. J. Goldstein, U. P. Jorde, and S. R. Patel, "Feasibility and Potential Impact of Heart Transplantation From Adult Donors After Circulatory Death," *J Am Coll Cardiol*, vol. 79, no. 2, pp. 148–162, Jan. 2022, doi: 10.1016/J.JACC.2021.10.042.

[19] M. Jahangiri *et al.*, "Surgical aortic valve replacement in the era of transcatheter aortic valve implantation: a review of the UK national database," *BMJ Open*, vol. 11, p. 46491, 2021, doi: 10.1136/bmjopen-2020-046491.

[20] Y. S. Abdullahi, S. Chaubey, R. Casula, and T. Athanasiou, "The Impact of Valve Surgery on the Health-Related Quality of Life of Elderly Patients: Systematic Review," *Patient Reported Outcomes and Quality of Life in Cardiovascular Interventions*, pp. 185–209, 2022, doi: 10.1007/978-3-031-09815-4_10.

[21] Y. S. Abdullahi, S. Chaubey, R. Casula, and T. Athanasiou, "What Factors Predict an Improved Quality of Life Outcome Following Coronary Artery Bypass Graft Surgery? A Systematic Review," *Patient Reported Outcomes and Quality of Life in Cardiovascular Interventions*, pp. 17–48, 2022, doi: 10.1007/978-3-031-09815-4_3.

[22] O. de la Varga-Martínez, R. Gutiérrez-Bustillo, M. F. Muñoz-Moreno, R. López-Herrero, E. Gómez-Sánchez, and E. Tamayo, "Postoperative delirium: An independent risk factor for poorer quality of life with long-term cognitive and functional decline after cardiac surgery," *J Clin Anesth*, vol. 85, p. 111030, May 2023, doi: 10.1016/J.JCLINANE.2022.111030.

[23] P. Duchnowski, "Risk Factors of Sudden Cardiac Arrest during the Postoperative Period in Patient Undergoing Heart Valve Surgery," *Journal of Clinical Medicine 2022, Vol. 11, Page 7098*, vol. 11, no. 23, p. 7098, Nov. 2022, doi: 10.3390/JCM11237098.

[24] M. Wang *et al.*, "Risk factors for ventilator-associated pneumonia due to multi-drug resistant organisms after cardiac surgery in adults," *BMC Cardiovasc Disord*, vol. 22, no. 1, pp. 1–8, Dec. 2022, doi: 10.1186/S12872-022-02890-5/TABLES/5.

[25] N. Hassoun-Kheir *et al.*, "Risk factors for ventilator-associated pneumonia following cardiac surgery," *Journal of Hospital Infection*, vol. 105, no. 3, pp. 546–551, Jul. 2020, doi: 10.1016/J.JHIN.2020.04.009.

[26] K. C. Clement *et al.*, "Increased Glucose Variability Is Associated With Major Adverse Events After Coronary Artery Bypass," *Ann Thorac Surg*, vol. 108, no. 5, pp. 1307–1313, Nov. 2019, doi: 10.1016/J.ATHORACSUR.2019.06.046.

[27] Z. A. Matthay *et al.*, "Association of Intraoperative and Perioperative Transfusions with Postoperative Cardiovascular Events and Mortality After Infrainguinal Revascularization," *Ann Vasc Surg*, Jan. 2022, doi: 10.1016/J.AVSG.2022.07.004.

[28] J. Xu et al., "Acute Kidney Injury in Cardiac Surgery," Contrib Nephrol, vol. 193, pp. 127–136, 2018, doi: 10.1159/000484969.

[29] A. Almashrafi, M. Elmontsri, and P. Aylin, "Systematic review of factors influencing length of stay in ICU after adult cardiac surgery," *BMC Health Serv Res*, vol. 16, no. 1, pp. 1–12, Jul. 2016, doi: 10.1186/S12913-016-1591-3/TABLES/5.

[30] X. Han, J. Li, P. Zeng, C. Luo, and D. Zhou, "Effect of the Kanghuier Transparent Hydrocolloid Dressing in Preventing Central Venous Catheter Infection and Phlebitis after Cardiac Surgery," *Comput Math Methods Med*, vol. 2022, 2022, doi: 10.1155/2022/4700257.

[31] K. Yang *et al.*, "Perioperative psychological issues and nursing care among patients undergoing minimally invasive surgeries," *Laparosc Endosc Robot Surg*, vol. 5, no. 3, pp. 92–99, Sep. 2022, doi: 10.1016/J.LERS.2022.06.001.

[32] L. Raymond, A. Castonguay, O. Doyon, and G. Paré, "Nurse practitioners' involvement and experience with AI-based health technologies: A systematic review," *Applied Nursing Research*, vol. 66, Aug. 2022, doi: 10.1016/J.APNR.2022.151604.

[33] P. Friedman *et al.*, "Efficacy and Safety of an Extravascular Implantable Cardioverter–Defibrillator," *New England Journal of Medicine*, vol. 387, no. 14, pp. 1292–1302, Oct. 2022, doi: 10.1056/NEJMOA2206485/SUPPL_FILE/NEJMOA2206485_DATA-SHARING.PDF.

[34] P. J. Bhatt *et al.*, "Infections due to multidrug-resistant organisms following heart transplantation: Epidemiology, microbiology, and outcomes," *Transpl Infect Dis*, vol. 22, no. 1, p. e13215, Feb. 2020, doi: 10.1111/tid.13215.

[35] M. K. H. Tan, O. A. Jarral, Y. Salmasi, M. Sabetai, and T. Athanasiou, "Thoracic Aortic Surgery," *Patient Reported Outcomes and Quality of Life in Cardiovascular Interventions*, pp. 49–81, 2022, doi: 10.1007/978-3-031-09815-4_4.

[36] L. H. Cohn and D. H. Adams, "Cardiac Surgery in the Adult," p. 1454, 2017, Accessed: Dec. 22, 2022. [Online]. Available: https://lib.hpu.edu.vn/handle/123456789/32478

[37] J. J. Pérez, E. Nadal, E. Berjano, and A. González-Suárez, "Computer modeling of radiofrequency cardiac ablation including heartbeat-induced electrode displacement," *Comput Biol Med*, vol. 144, p. 105346, May 2022, doi: 10.1016/J.COMPBIOMED.2022.105346.

[38] A. Marelli *et al.*, "Canadian Cardiovascular Society 2022 Guidelines for Cardiovascular Interventions in Adults With Congenital Heart Disease," *Canadian Journal of Cardiology*, vol. 38, no. 7, pp. 862–896, Jul. 2022, doi: 10.1016/J.CJCA.2022.03.021.

[39] A. J. Poovathoor, J. Ali, and M. Berman, "Patient Reported Outcomes and Quality of Life following Heart Transplantation," *Patient Reported Outcomes and Quality of Life in Cardiovascular Interventions*, pp. 83–107, 2022, doi: 10.1007/978-3-031-09815-4_5.

[40] "Patient Reported Outcomes and Quality of Life in Cardiovascular Interventions," *Patient Reported Outcomes and Quality of Life in Cardiovascular Interventions*, 2022, doi: 10.1007/978- 3-031-09815-4.

[41] N. di Bari, M. Moscarelli, G. Nasso, and G. Speziale, "Quality of Life After Mitral Valve and Tricuspid Valve Surgery," *Patient Reported Outcomes and Quality of Life in Cardiovascular Interventions*, pp. 211–216, 2022, doi: 10.1007/978-3-031-09815-4_11.

[42] K. A. Horvath *et al.*, "Blood Transfusion and Infection After Cardiac Surgery," *Ann Thorac Surg*, vol. 95, no. 6, pp. 2194–2201, Jun. 2013, doi: 10.1016/J.ATHORACSUR.2012.11.078.

[43] F. E. Aslan, A. Badir, S. K. Arli, and H. Cakmakci, "Patients' experience of pain after cardiac surgery," *Contemp Nurse*, vol. 34, no. 1, pp. 48–54, 2009, doi: 10.5172/CONU.2009.34.1.048.

[44] M. Leegaard, J. Watt-Watson, M. McGillion, J. Costello, J. Elgie-Watson, and K. Partridge, "Nurses' educational needs for pain management of post-cardiac surgery patients: a qualitative study," *J Cardiovasc Nurs*, vol. 26, no. 4, pp. 312–320, Jul. 2011, doi: 10.1097/JCN.0B013E3181F806BC.

[45] K. W. Ene, G. Nordberg, I. Bergh, F. G. Johansson, and B. Sjöström, "Postoperative pain management - The influence of surgical ward nurses," *J Clin Nurs*, vol. 17, no. 15, pp. 2042–2050, Aug. 2008, doi: 10.1111/j.1365-2702.2008.02278.x.

[46] Kumar, R., Gupta, M., Agarwal, A., & Nayyar, A. (2024). CBAR-UNet: A novel methodology for segmentation of cardiac magnetic resonance images using block attention-based deep residual neural network. *Multimedia Tools and Applications*, 1-17.

[47] Singh, P., Kumar, R., Gupta, M., & Al-Turjman, F. (2024). SegEIR-Net: A Robust Histopathology Image Analysis Framework for Accurate Breast Cancer Classification. *Current Medical Imaging*.

[48] Juneja, A., Kumar, R., & Gupta, M. (2022, July). Smart Healthcare Ecosystems backed by IoT and Connected Biomedical Technologies. In *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 230-235). IEEE.

[49] Kaur, R., Kumar, R., & Gupta, M. (2024). Lifestyle and Dietary Management Associated with Chronic Diseases in Women Using Deep Learning. *Combating Women's Health Issues with Machine Learning*, 59-73.

[50] Kumar, R., Gupta, M., & Abraham, A. (2024). A Critical Analysis on Vertebra Identification and Cobb Angle Estimation Using Deep Learning for Scoliosis Detection. *IEEE Access*.

Network Security in Architectures for Software Defined Networking (SDN)

Ramiz Salama [1*], Chadi Altrjman [2], Fadi Al-Turjman [3]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT, Near East University, Nicosia, Mersin 10 – Turkey

[2]Department of Chemical Engineering, Waterloo University, ON N2L 3G1, Canada

[3]Artificial Intelligence, Software, and Information Systems Engineering Departments, Research Center for AI and IoT, AI and Robotics Institute, Near East University, Nicosia, Mersin10, Turkey

*Corresponding author Email: ramiz.salama@neu.edu.tr

Abstract: SDN (Software Defined Networking) is a new network design that separates the control and data planes, allowing for better network management and centralized control. This decoupling makes networks more programmable, scalable, and flexible, which is critical for meeting the changing requirements of modern digital environments. Although SDN streamlines network administration, it also adds new security risks, such as the possibility of centralized control failures, expanded attack surfaces, and vulnerability to multiple network attack types. SDN architectures must include network security to mitigate these dangers. This includes setting up automated responses to detect and remove threats, as well as implementing security capabilities like real-time traffic monitoring into the SDN controller. Furthermore, SDN's programmability allows for the dynamic deployment of security policies across the network, increasing the network's ability to respond to emerging threats. A more robust and flexible security posture can be achieved by effectively managing and coordinating security solutions like as intrusion detection systems (IDS), firewalls, and distributed denial of service (DDoS) mitigation with SDN controllers. This paper examines many techniques to incorporate network security into SDN systems, highlighting the benefits of centralized policy enforcement, real-time monitoring, and SDN's agility in implementing security measures. Along with future advances such as the use of AI and machine learning for automated incident response and predictive threat analysis, the challenges and restrictions of safeguarding SDN configurations are discussed. To deal with the rising complexity and sophistication of assaults in SDN-based networks, the study underlines the importance of continuous innovation in security mechanism.

Keywords: network security, network design, cybersecurity, network management, software-defined networking (SDN), and SDN controllers

1. Introduction

The integration of network security into software defined networking (SDN) designs is a rapidly evolving field. SDN increases the flexibility and dynamic nature of network administration by separating the control plane from the data plane. By analyzing the mythology and technology used to integrate security measures into SDN systems, this study addresses the inherent flaws and offers better security strategies. As the population ages, more people are selecting comfortable, eco-friendly networking options. Because of its programmability and centralized network control, software application defined as networking, or SDN, has emerged as a practical solution to this need. However, as the size of SDN architecture increases, the need for strong community protection becomes even more important. The integration of network security into software defined networking (SDN) designs is a rapidly evolving field. SDN increases the

flexibility and dynamic nature of network administration by separating the control plane from the data plane. By analyzing the mythology and technology used to integrate security measures into SDN systems, this study addresses the inherent flaws and offers better security strategies [1]. As the population ages, more people are selecting comfortable, eco-friendly networking options. Because of its programmability and centralized network control, software application defined as networking, or SDN, has emerged as a practical solution to this need. However, as the size of SDN architecture increases, the need for strong community protection becomes even more important. By virtualizing and controlling community factors with a centralized controller, SDN facilitates cybercriminals' ability to take advantage of vulnerabilities and obtain an advantage through unauthorized access to a community [2–11]. In order to ensure the community's dependability and elegant protection, community safety must be incorporated into SDN architecture [12]. One important component of community safety that SDN design seeks to protect is the right of access to govern. Protocol. Record encryption is becoming an essential part of network security due to the growing threat of cyberattacks and truth breaches. To ensure that all network website visitors are secure and encrypted, the centralized controller of SDNs can provide abs at case communications channels for community devices to use encryption protocols. Network segmentation is another important component of network security that must be considered in SDN architecture [5]. SDN adds extra security by making it simple to split networks into smaller virtual networks.
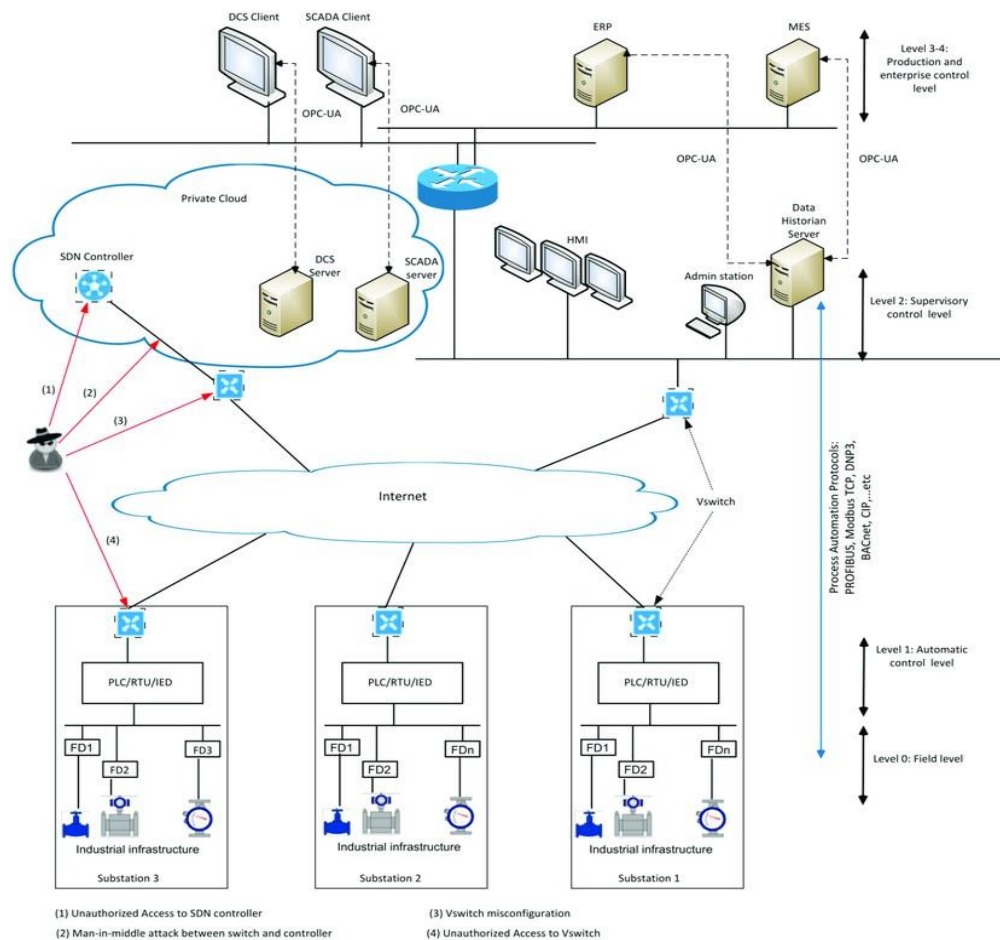

Figure 1. Software-defined networking (SDN)-based ICS architecture.

1.1 Streamlined protection administration
Incorporating network protection into SDN architecture enables a centralized, secure control method. Because security policies and processes can be easily communicated, executed, and managed from a single location, security becomes more environmentally friendly and less prone to human mistake.

1.2 Adaptive reaction to danger
SDNs can respond to safe threats instantly since they are programmable and dynamic.

1.3 Improved command and visibility
SDN protection makes it easier for community administrators to view and manage network traffic. By detecting and stopping security threats at many network layers, including the utility layer, this makes it possible to take a more comprehensive approach to network protection [13].

1.4 Flexibility and growth
While considering the intended rollout of new security solutions and technologies, SDN offers a flexible and scalable framework for integrating security [14].

2. Amount of Work Previously Published;
An explanation of the software program because it provides a dynamic, flexible, and programmable network infrastructure, networking is a new method of networking that has been more and more popular recently. It separates the information plane from the manage plane by considering centralized network management via a separate controller [15–17]. This separation of the facts and control planes has many benefits.

3. The recommended model
The proposed version seeks to include community safe frosty into the software package with an emphasis on SDN architecture. SDN is a community structure that separates the controlled aircraft from the plane of the record while taking into account centralized administration and management of the community [18–20]. This model shows how the SDN controller, which is in charge of overseeing and controlling society, might incorporate safety.

3.1 Construction
Information aircraft and community management are separated by the new networking paradigm known as software networking. In order to manipulate communities with centralized controllers and enable efficient and dynamic resource allocation and control, SDN is essential. There are several difficult situations when integrating network security with SDN design. Installing traditional security measures like firewalls and intrusion detection systems is challenging due to the dynamic nature of the SDN environment. This is because the community topology may change in real-time in SDN, requiring standard protection methods to be adjusted to the dynamic SDN environment. The second challenge in SDN is the retrained visibility of visitors to community sites. Because safety algorithms can search for the most efficient means to gain access to the network, it can be challenging to peep at network traffic at different layers in consensual networks. Therefore, a safety mechanism that works with the SDN controller should be developed to ensure the networks' security.
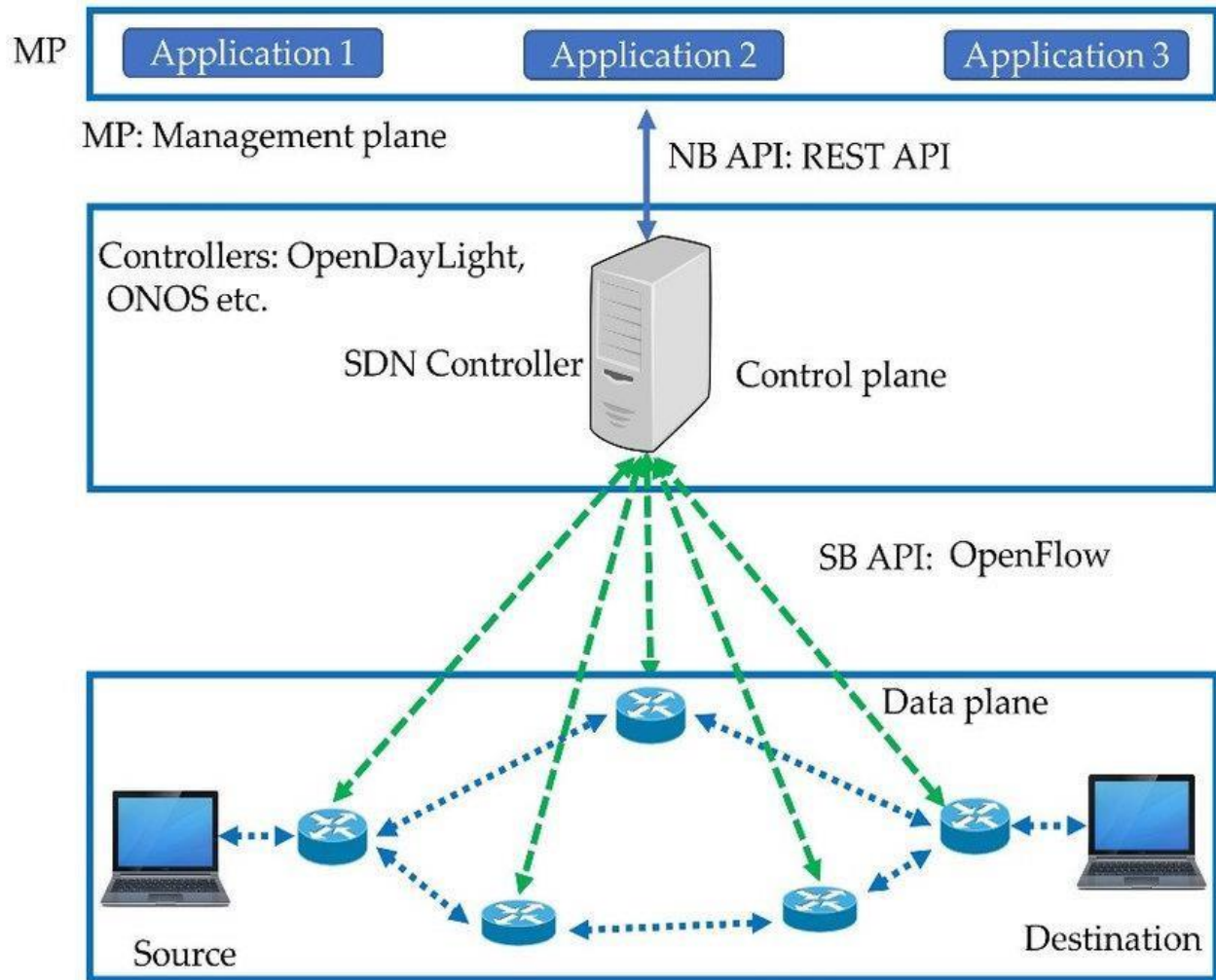
Figure 2. An overview of SDN (software-defined networking) architecture

3.2 Operational Principle

A network structure technique called software program defined networking (SDN) separates the control plane from the records aircraft while taking community programmability and centralized control into account. This architecture, which mostly relies on software to manage and configure the network, provides flexibility, performance, and scalability. Network safety can be incorporated into SDN architecture by adding safety rules and features to the SDN controller, which acts as the community's central brain and is in charge of overseeing all community resources.

4. Materials and methods

This study looks at a variety of scholarly works, conference proceedings, and technical reports about SDN and network security using a systematic review methodology [21]. Threat mitigation techniques, intrusion detection systems, the application of security policies, and the impact of security measures on network performance are among the crucial components

that are evaluated [22–24]. Discussion and comparison are based on the experimental settings, case studies, and simulation results found in the reviewed literature [25].

5. Results and Discussion

Integrating network safety into software applications, or networking architectures, is one of the most crucial elements in guaranteeing current security. Although SDN is an amazing new technology that provides a flexible and dynamic method of network management, it also poses new security threats. By integrating network protection into SDN systems, companies can ensure that their networks are competitive against both established and new threats. Instead of relying on external security devices and solutions, this is achieved by immediately incorporating safety policies and controls within the SDN architecture. Additionally, more efficient and novice safety manipulation is made possible by integrating community protection into SDN architecture. Because SDN enables centralized management, it is simple to build and administer protection rules for the duration of the network in order to configure and handle character devices. Detecting and responding to security incidents is more authentic when safety is combined with enhanced visibility and control over community visits [26][27]. Combining community security and software program security Numerous benefits and difficult situations are provided by networking architectures. By allowing centralized and programmable control of network protection rules, it greatly simplifies the management and deployment of security functions throughout the whole network. This centralized approach also offers improved visibility and control over traffic to community websites, which could help detect and mitigate capacity problems [28][29]. The proposed method has been contrasted with the existing software-defined networking framework (SDNF), deep learning-based intrusion detection (DLID), intelligent optimization framework (IOF), and Harris-hawk-optimization (HHO).
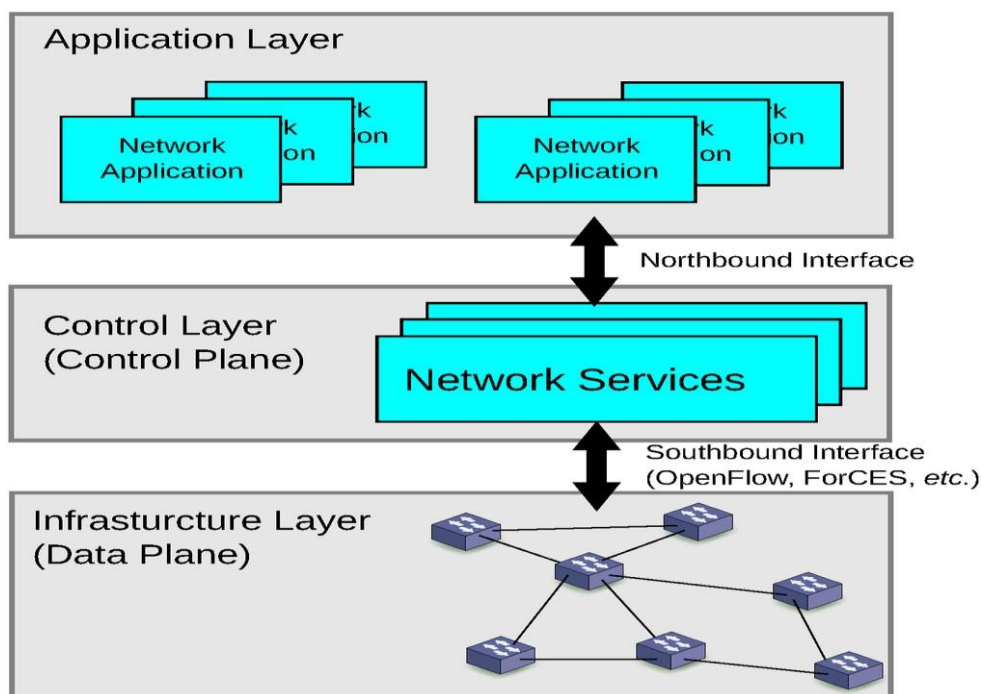

Figure 3. Software Defined Networking (SDN) and OpenFlow Architecture Interview Questions and Answers

5.1 DETAILS

Networking is defined by software as a network architectural technique that divides the record aircraft of a community device from the manage plane. This makes it easier to control and customize by enabling programmable, centralized network management. SDN's decentralized architecture does, however, also provide a special set of protection-demanding circumstances. Thus, it is essential to incorporate network protection into SDN design in order to guarantee SDN network security. The requirement for unified, centralized security coverage is one of the most crucial and technically challenging scenarios during the integration of community security into SDN architecture. Figure 3. Demonstrate the fight for specificity.

6. Conclusion

Building robust, adaptable, and flexible networks that can successfully fend off contemporary cyberthreats requires the integration of network security into Software Defined Networking (SDN) designs. The special capabilities of SDN, like network programmability, centralized control, and dynamic policy management, present previously unheard-of chances to improve security. Network administrators can create a more resilient and flexible defensive system by utilizing these capabilities to deploy automated response systems, adaptive security rules, and real-time threat detection. SDN's centralization, however, may potentially result in additional attack surfaces and single points of failure, among other possible security flaws. Strong authentication procedures, encryption techniques, and redundant and distributed SDN controllers are essential for mitigating these hazards. Furthermore, by enabling automated incident response and predictive threat analysis, the integration of artificial intelligence (AI) and machine learning (ML) technologies can improve the security framework even more. This will minimize the need for human interaction and cut down on the amount of time required to mitigate risks. In summary, SDN designs offer a potential framework for integrating network security, but in order to stay up with the always changing threat landscape, constant innovation and adaptation are needed. To create a truly safe and intelligent SDN environment, future research should concentrate on creating increasingly complex security algorithms, improving controller resilience, and investigating the possibilities of AI-driven solutions. Next-generation networks that are more dependable and safe may eventually be made possible by the effective integration of network security into SDN.

References

[1] H. Sharma, R. Kumar and M. Gupta, "A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/INOCON57975.2023.10101044.

[2] Pillai, S. E. V. S., & Polimetla, K. (2024, February). Integrating Network Security into Software Defined Networking (SDN) Architectures. In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-6). IEEE.

[3] Huang, X., Zheng, K., Chen, S., & He, Z. (2024). Construction of switch information security protection system based on software-defined networking. Transactions on Emerging Telecommunications Technologies, 35(9), e5033.

[4] Fartitchou, M., Lamaakal, I., Maleh, Y., El Makkaoui, K., El Allali, Z., Pławiak, P., ... & A. Abd El-Latif, A. (2024). IOTASDN: IOTA 2.0 smart contracts for securing software-defined networking ecosystem. Sensors, 24(17), 5716.

[5] Akinola, O. I., Olaniyi, O. O., Ogungbemi, O. S., Oladoyinbo, O. B., & Olisa, A. O. (2024). Resilience and recovery mechanisms for software-defined networking (SDN) and cloud networks. Journal of Engineering Research and Reports, 26(8), 112-134.

[6] Al-Shareeda, M. A., Alsadhan, A. A., Qasim, H. H., & Manickam, S. (2024). Software defined networking for internet of things: review, techniques, challenges, and future directions. Bulletin of Electrical Engineering and Informatics, 13(1), 638-647.

[7] Jafarian, T., Ghaffari, A., Seyfollahi, A., & Arasteh, B. (2025). Detecting and mitigating security anomalies in Software-Defined Networking (SDN) using Gradient-Boosted Trees and Floodlight Controller characteristics. Computer Standards & Interfaces, 91, 103871.

[8] Agnew, D., Boamah, S., Bretas, A., & McNair, J. (2024). Network Security Challenges and Countermeasures for Software-Defined Smart Grids: A Survey. Smart Cities, 7(4), 2131-2181.

[9] AbdulRaheem, M., Oladipo, I. D., Imoize, A. L., Awotunde, J. B., Lee, C. C., Balogun, G. B., & Adeoti, J. O. (2024). Machine learning assisted snort and zeek in detecting DDoS attacks in software-defined networking. International Journal of Information Technology, 16(3), 1627-1643.

[10] Maheswaran, N., Bose, S., & Natarajan, B. (2024). An adaptive multistage intrusion detection and prevention system in software defined networking environment. Automatika, 65(4), 1364-1378.

[11] Jain, A. K., Kumari, P., Dhull, R., Jindal, K., & Raza, S. (2024). Enhancing Software-Defined Networking With Dynamic Load Balancing and Fault Tolerance Using a Q- Learning Approach. Concurrency and Computation: Practice and Experience, e8298.

[12] Al-Ibraheemi, F. A., Hazzaa, F., Jabbar, M. S., Tawfeq, J. F., Sekhar, R., Shah, P., & Parihar, S. (2024). Intrusion detection in software-defined networks: leveraging deep reinforcement learning with graph convolutional networks for resilient infrastructure. Fusion: Practice and Applications, 15(1), 78-88.

[13] M. Gupta, R. Kumar, M. Maheshwari and R. Kumar, "Drones and Networks: Ensuring safe and secure operations using 5g mobile network," *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India, 2023, pp. 1239-1242, doi: 10.1109/ICAC3N60023.2023.10541654.

[14] S. Luthra, R. Kumar, M. Gupta and A. J. Obaid, "Exploring Link Prediction Techniques in Social Network Analysis for Community Detection," 2024 3rd International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Phuket, Thailand, 2024, pp. 107-113, doi: 10.1109/ICCMSO61761.2024.00034.

[15] Mahar, I. A., Libing, W., Maher, Z. A., & Rahu, G. A. (2024, January). A Comprehensive Survey of Software Defined Networking and its Security Threats. In 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) (pp. 1-5). IEEE.

[16] Setitra, M. A., Fan, M., Benkhaddra, I., & Bensalem, Z. E. A. (2024). DoS/DDoS attacks in Software Defined Networks: Current situation, challenges and future directions. Computer Communications.

[17] Cherednichenko, O., Sharonova, N., Pliekhova, G., & Babkova, N. (2024). Intelligent Methods of Secure Routing in Software-Defined Networks. In COLINS (1) (pp. 342-351).

[18] Kumar, R., & Agrawal, N. (2024). Software defined networks (SDNs) for environmental surveillance: A Survey. Multimedia Tools and Applications, 83(4), 11323-11365.

[19] Li, D. C., Tu, H. H., & Chou, L. D. (2024). Cross-layer detection and defence mechanism against DDoS and DRDoS attacks in software-defined networks using P4 switches. Computers and Electrical Engineering, 118, 109307.

[20] Zhou, Q. (2024). Smart library architecture based on internet of things (IoT) and software defined networking (SDN). Heliyon, 10(3).

[21] Bodapati, V., Kranthi, S., & Baji, S. S. (2024, February). Preventing Network Attacks using Support Vector Machine (SVM) and Software Defined Networking (SDN) Integration. In 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE) (pp. 1-8). IEEE.

[22] P. Kaur, R. Kumar, and H. Kaur, "The Survey of Various Types of Wireless Sensor Network and Paser Protocol," Int J Sci Res Sci Technol, vol. 3, no. 7, pp. 1049 –1052, Oct. 2017, doi: 10.32628/IJSRST117374.

[23] Raza, M., Saeed, M. J., Riaz, M. B., & Sattar, M. A. (2024). Federated Learning for Privacy Preserving Intrusion Detection in Software Defined Networks. IEEE Access.

[24] Ram, A., & Chakraborty, S. K. (2024). Analysis of Software-Defined Networking (SDN) Performance in Wired and Wireless Networks Across Various Topologies, Including Single, Linear, and Tree Structures. Indian Journal of Information Sources and Services, 14(1), 39-50.

[25] Kumar, D., & Gupta, M. (2018). Implementation of firewall & intrusion detection system using pfSense to enhance network security. *International Journal of Electrical Electronics & Computer Science Engineering*, *1*, 2454-1222.

[26] Gupta, D., Kaur, H., & Kumar, R. (2016). Detection of sink hole attack in wireless sensor network using advanced secure AODV routing protocol. *International Journal of Computer Applications*, *156*(11).

[27] Bawa, H., Singh, P., & Kumar, R. (2012). An efficient novel key management scheme using nchoosek algorithm for wireless sensor networks. *International Journal of Computer Networks & Communications*, *4*(6), 121.

[28] Sharma, H., Kumar, R., & Gupta, M. (2023, March). A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network. In *2023 2nd International Conference for Innovation in Technology (INOCON)* (pp. 1-5). IEEE.

[29] Chaki, S. K., Kumar, R., & Gupta, M. (2022, March). Satellite-Based Estimation of Air Quality in South Asian Countries Using Neural Networks: A Review. In *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)* (Vol. 1, pp. 725-728). IEEE.

Comparative Analysis of Anesthetic Methods and Their Influence on Postoperative Outcomes

Efe Precious Onakpojeruo[1], Yesim Cetintas[2], Ozlem Balcioglu[3,1], Berna Uzun[4,1,5], Christiana Chioma Efe[1], Ezedom Theresa[6], Dilber Uzun Ozsahin[7,1]

[1]Operational Research Centre in Healthcare, Near East University, Nicosia, TRNC, Mersin 10, Turkey

[2]Department of Anesthesiology, Near East University, Nicosia, TRNC, Mersin 10, Turkey

[3]Department of Cardiovascular Surgery, Near East University, Nicosia, TRNC, Mersin 10, Turkey

[4]Carlos III University of Madrid, Statistics Department, Getafe, Madrid, Spain

[5]Near East University, Faculty of Arts and Sciences, Department of Mathematics, Nicosia, TRNC, Mersin 10, Turkey

[6]Department of Medical Biochemistry, Delta State University, Abraka, Nigeria

[7]University of Sharjah, Medical Diagnostic Imaging Department, College of Health Science, Sharjah, United Arab Emirates

efeprecious.onakpojeruo@neu.edu.tr, yesimcetintas@yahoo.com, ozlem.balcioglu@neu.edu.tr, berna.uzun@neu.edu.tr, ilker.ozsahin@neu.edu.tr, 20227178@std.neu.edu.tr, ezedomt@delsu.edu.ng, dilber.uzunozsahin@neu.edu.tr

* Correspondence: efeprecious.onakpojeruo@neu.edu.tr

Abstract- Anesthesia is used as a neural blocker capable of preventing nociceptive impulses from entering the nervous system, before, during, and after surgery. Anesthetic agents should be able to enhance recovery processes, potencies, and relaxation of the muscles, including a wide range of safety, free from toxicity, reactivity problems, and possibilities of adverse effects. The objective of this study was to apply a multi-criteria decision-making method (MCDM) called fuzzy PROMETHEE (Preference Ranking Organization Method for Enrichment of Evaluations) method to evaluate, compare, and rank 5 different types of anesthesia used for surgical operations including (general anesthesia, spinal anesthesia, epidural anesthesia, peripheral nerve blocks, and sedation) based on professionally selected parameters, to determine the preferred analgesic agent for specific patients. The results show that peripheral nerve blocks with a net flow of 0.0321 are among the most preferred anesthesia for patients with the considered contraindications and based on the selected criteria, assigned weights, and set preferences, followed by sedation with a net flow of 0.0083. Epidural anesthesia is ranked the lowest with a negative net flow of -0.0300. Expert opinion is always needed when assigning weights to criteria, and grading alternatives is the major challenge in multi-criteria decision-making studies. Fuzzy PROMETHEE is proposed to solve a multi-criteria decision-making problem in selecting anesthesia used for surgical operations.

Keywords: Anesthesia, Analgesic-agent, Pain-reduction, Surgical Operations, Fuzzy-PROMETHEE, Decision-making

1. Introduction

Anesthesia is a pain-reducing medication induced through incision needles or inhalation to cause a loss of sensation, to significantly decrease the severity of incisional pain during surgery,

movement-associated pains, and pains due to pressure amounted to the surgery site [1,2]. Anesthesia is used as a neural blocker capable of preventing nociceptive impulses from entering the nervous system, before, during, and after surgery[1]. Anesthetic agents should be able to enhance recovery processes, potencies, and relaxation of the muscles, including a wide range of safety, free from toxicity, reactivity problems, and possibilities of adverse effects [2,3]. Prior to reviewed studies, local anesthesia, sedation, peripheral nerve blocks, epidural, spinal, and general anesthesia have been proven to be very effective in decreasing the severity of pain [1–3]. Anesthesia was first introduced into medicine by William Morton in 1846 when he demonstrated that inhalation of ether can cause loss of sensation to pains associated with surgery [4]. This has led to the explosive exposure of surgical operations in different respects [4]. However, different factors are considered for selecting the preferred anesthesia depending on the type and duration of the operation [2]. The choice of anesthesia administered through inhalation and injection is dependent on factors such as the side effects, the cost, the patient's medical history, possibilities of reactivity, cardiac and pulmonary functions, and characteristics like age, weight, sex, etc. [2,5,6]. The age difference is an important factor to be considered when selecting the preferred anesthetic agent [2]. Due to differences in body mass index, body compositions, metabolic reaction rates, and cardiac outputs of patients, keen evaluation is needed for the proper administration of anesthetic agents to avoid toxicities and adverse effects possible through overestimation, as a result of pharmacodynamics and pharmacokinetics differences [2,7]. It is observed that elderly patients require surgery more than patients in other age groups [1,8], this makes it very important for individual evaluations to be carried out on patients before the selection of anesthetic agents is done. Some other related factors that are important when selecting the anesthetic agents of choice according to the American Society of Anesthesiologists (ASA), physical conditions classification system of vital signs, patient's medical conditions, patient's lifestyle such as (tobacco usage, obesity, diabetic, etc.) and patient's consent [2,7,8]. When considering these factors, it is possible to apply multi-criteria decision-making algorithms that are founded on human knowledge to the process of selecting different types of anesthetic agents used for surgical operations.

The fuzzy Preference Ranking Organization Method for Enrichment of Evaluations (PROMETHEE) decision-making method is a concept that is based on the evaluation and comparison of complex and multiple criteria [9,10]. In contrast to other multi-criteria decision-making systems, it has the advantage of being easy to implement [2,11]. To the best of my knowledge, the fuzzy PROMETHEE approach for the determination of anesthetic agents has only been applied in one study, which was carried out by [2]. The applications of this methodology have been offered in the existing literature. According to the study's findings, fuzzy PROMETHEE was used to compare, evaluate, and rank general anesthesia based on the physical criteria and the importance typically attributed to regularly used medications. However, the author has failed to compare general anesthesia with other available types of anesthesia. Thus, to cover the research gap, this study is aimed at proposing the use of Fuzzy PROMETHEE to compare, evaluate, and rank 5 different types of anesthesia used for surgical operations which include (general anesthesia, spinal anesthesia, epidural anesthesia, peripheral nerve blocks, and sedation) based on the physical parameters, contraindications of anesthetic agents and assigned importance weight of criteria based on expert's opinion which include; Patient refusal, medical conditions that are not optimized prior to surgery, Severe heart valve disease, significant pulmonary disease, congestive heart failure, age, mental illness, infection at the injection site, type of surgery, complicated surgery, anesthesiologist experience, increased nausea and vomiting, history of malignant hyperthermia, systemic infection (sepsis), coagulopathy or bleeding disorders, major spinal deformities (like

kyphoscoliosis, and arthritis), previous lumber, surgery, long surgical procedures, elevated intracranial pressure, patients with a risk of vomiting, Neuromuscular diseases, and cost.

1.1 General Anesthesia

The use of anesthetic agents during surgery is currently of paramount importance as patients indicated for surgical treatments, experience high risk/rates of morbidity, mortality, and complications especially related to pulmonary and cardiovascular disabilities [2,15,16]. Therefore, it is of urgent medical importance to improve factors that would reduce the risks associated with surgical operations. General anesthesia has been a proposed anesthetic agent that has been hypothesized to facilitate rehabilitation and reduce the risks associated with postoperative complications during surgical operations [15,17,18]. General anesthesia offers improved hemodynamic stability, decreases blood loss to an extent, and gives an outcome of improved analgesia [18]. The effectiveness of general anesthetic agents has been compared with different anesthetic agents in different studies. A study by [15] examined about 18,158 patients indicated for hip fracture surgery in 126 hospitals in New York. 5,254 which is (29%) of the total number were administered epidural or spinal (regional) anesthesia. The efficacy of epidural anesthesia and spinal anesthesia was compared with general anesthesia using morbidity, mortality, and pulmonary complications as discharge criteria for comparison. It was concluded from the study that regional anesthesia has an improved survival rate and fewer pulmonary complications when compared with general anesthesia. Another study by [18] compared general anesthesia with spinal anesthesia in a randomized study of 120 patients indicated to undergo total knee arthroplasty. The criteria for comparison were; recovery time from total knee arthroplasty (46 vs 52h), nausea and vomiting, pain reduction rate, and less dizziness. It was concluded from the study that general anesthesia outperformed spinal anesthesia by meeting the discharge criteria in a shorter time compared to spinal anesthesia. This conclusion contradicts previous recommendations regarding regional anesthesia for surgical operations [15] [19].

1.2 Spinal Anesthesia

Spinal anesthesia has uniquely gained prominence with reference to landmark studies proving the superiority of spinal anesthesia over general anesthesia in terms of reducing complications associated with surgical operations [5] [20,21]. Efficacy in rehabilitation has been broadly observed with the use of spinal anesthesia, improvements in general anesthesia in terms of a decrease in blood loss, improved pain relief rate, improvements in blood flow, reduced pulmonary complications, shorter recovery time, and a drastic reduction in surgical stress response [22,23]. Spinal anesthesia has greatly challenged general anesthesia, although not totally without complications and various risks, that relatively occur in rare cases [5]. Some possible side effects of spinal anesthesia noticed are; spinal hematoma, infections, abscesses, longer stay in the post-anesthesia care unit, and risk of overdosing [24].

1.3 Epidural Anesthesia:

Epidural anesthesia is administered by injecting neuraxial blockade into the epidural space surrounding the spinal fluid sac [21,24]. It has been observed that epidural anesthesia is associated with numerous benefits compared to general anesthesia[24]. Epidural anesthesia has been proven to reduce morbidity and mortality rates, increase postoperative analgesia, enhance cost-effectiveness, and reduction of surgical stress-related responses [25]. Epidural anesthesia has been observed to be associated with after-effects relating to nerve injury and other possible side effects

such as renal failure, respiratory depression, pneumonia, infections, deep vein thrombosis, myocardial infarction, pulmonary embolism, and loss of blood that may result in transfusion requirements [21]. A study conducted by [21] containing 141 trials and 9559 patients, obtained a reliable estimate of the effects of epidural anesthesia. The result of the study showed that overall morbidity and mortality rate was reduced, the odds of deep vein thrombosis was reduced by 44%, pulmonary embolism was reduced by 55%, respiratory depression was reduced by 59%, pneumonia was reduced by 39%, transfusion requirements were reduced by 50%, renal failure, and myocardial infarction was also reduced when the neuraxial blockade was injected [21].

1.4 Peripheral Nerve Blocks

Peripheral nerve block anesthesia is a superior type of anesthesia with efficient analgesic properties for the effective management of postoperative pain [26,27]. Peripheral nerve blocks increase patient satisfaction and decrease the stay in the post-anesthesia care unit and total stay in the hospital [27]. A study conducted by [26] comparing spinal anesthesia with peripheral nerve blocks against general anesthesia with peripheral nerve blocks concluded that peripheral nerve blocks shortened the length of stay in the post-anesthesia care unit and total stays in the hospital. The study strongly recommended the use of peripheral nerve blocks with general anesthesia for surgeries, especially for elective foot and ankle operations. Another study by [28] compared peripheral nerve blocks with general anesthesia for efficacy in pain management. A total of 14 randomized trials with 851 patients were included in the study. The meta-analysis demonstrated that peripheral nerve blocks are associated with a significant and massive reduction in pain compared to general anesthesia. A recent study compared peripheral nerve blocks with spinal anesthesia in terms of postoperative mortality and walking ability in aged patients indicated for hip fracture surgery. Patients above 65 years were included in the study and analysis was performed using the Kaplan-Meier method. Results from the study indicated that 360 patients were included; 200 received spinal anesthesia and 116 received peripheral nerve blocks. When evaluated and compared, peripheral nerve blocks outperformed spinal anesthesia and showed a lower risk of mortality but higher hospitalization costs [29].

1.5 Sedation

Sedation is simply a state of consciousness during a drug-induced depression [30]. Sedation can either be minimal (normal response to verbal stimulation), moderate (purposeful response to verbal stimulation), or deep sedation (purposeful response after repeated or painful stimulation) [30]. Sedation combined with interscalene block has been successfully used as an alternative analgesic agent [31]. When compared with general anesthesia in patients undergoing shoulder surgery and endovascular therapy of basilar artery occlusions in a study by [31,32], efficacy in analgesic properties was observed. The technique provided excellent intraoperative muscle relaxation, faster post-anesthesia care unit and hospital discharge times, and a decreased tendency for nausea and vomiting [31,32]. Sedation minimizes drops in blood pressure, especially during endovascular therapy and it enables assessment of neurological functions but with difficulty in immobility with risk in pulmonary aspirations [32]. When recommending sedation, patients' health status, age, concurrent medications, anxiety levels, pain tolerance, and procedural variables are all checked to achieve the desired results [33]. Usually, for patients with long-term narcotic habits, sedation is generally accompanied by general anesthesia to manage difficulties [31]. Patients suffering from obesity or obstructive sleep apnea are at a high risk of hypoxemia when administered deep sedation [31,33].

2. Material And Methods
2.1 Fuzzy PROMETHEE and Applications

The term "fuzzy-PROMETHEE" refers to the combination of two separate concepts, namely fuzzy logic, and PROMETHEE. At one time, researchers merely scratched the surface of this conceptual combination in a very small fraction of its total iterations. The PROMETHEE has been demonstrated to be an efficient tool for comparing several alternative approaches using essential parameters (criteria) in order to evaluate their level of performance. The criteria, in order to be characterized as lingual data, are transformed into fuzzy scales using the weight of individual criteria. The end result will provide a ranking of the options, from the one with the most favorable outcomes to the least alternative. Many researchers for example, [34–37] have applied the fuzzy PROMETHEE methodology in their studies. An ultimate example of a multi-criteria decision-making (MCDM) approach is the fuzzy-PROMETHEE, which analyses multi-criteria scenarios, thereby creating a ranking organizational methodology aimed at comparing and evaluating alternatives [38]. Comparative decision-making is a complicated process, such as the one described above, that is typically difficult to achieve; however, due to the prevalence of such complications, fuzzy-PROMETHEE was designed to solve them. By translating language variables into mathematical quantitative variables, both numbers and non-numerical data [10,39].

In this study, the fuzzy PROMETHEE method was deployed to compare and evaluate 5 types of anesthesia used respectively during surgical operations and to identify and determine the most preferred analgesic agent based on applied parameters. To achieve this aim, the aforementioned parameters in Table 1 were collected. These parameters were determined professionally by an anesthesiologist and from searched literature. Thereafter, the parameters were normalized to obtain a triangular linguistic fuzzy scale showing the importance weight of each criterion and the min/max preference as seen in Table 2. In addition, the Yagar index was applied to de-fuzzified the fuzzy values. Finally, the visual PROMETHEE program was deployed using the Gaussian preference functions.

Table 1. Linguistic Fuzzy Scale for the importance of criteria

Linguistic scale for ranking	Triangular Fuzzy Scale	Importance ratings of criteria
Very High (VH)	(0.75, 1, 1)	Patient refusal, medical conditions that are not optimized prior to surgery, Severe heart valve disease, significant pulmonary disease, congestive heart failure, Age, mental illness, infection at the injection site, Type of surgery, complicated surgery, Anesthesiologist experience, increased nausea, and vomiting
High (H)	(0.50, 0.75, 1)	history of malignant hyperthermia, systemic infection (sepsis), coagulopathy or bleeding disorders, major spinal deformities (Like Kyphoscoliosis, and arthritis), previous lumber, surgery, long surgical procedures, elevated intracranial pressure,
Medium (M)	(0.25, 0.50, 0.75)	patients with a risk of vomiting, Neuromuscular diseases,
Low (L)	(0, 0.25, 0.50)	cost

Very Low (VL)	(0, 0, 0.25)

2.2 3-Case scenarios applied to the study

1. A 35 years old male patient without any underlying health challenges got involved in a fatal traffic accident [41] while returning from a night party. He had a fractured forearm in between the elbow and the wrist and had to be given immediate surgical care due to compromised perfusion of the arm [42]. The question is; which anesthetic technique is optimum for this patient? (Spinal or Epidural anesthesia would not be appropriate due to the affected site that needs a surgical operation. Spinal or epidural may be difficult as an application of pressure or elevation of the limb and exsanguination is usually accompanied by intense pain. And again, to avoid reactivities that may lead to drug toxicity, seizures, dizziness, coma, cardiac arrhythmias, and possible hypotension or loss of consciousness. These risks could be overcome with the administration of Peripheral nerve blocks [40]. General anesthesia would also be risky due to the patient's full stomach which could risk aspiration of the lungs during anesthesia induction. A peripheral nerve block would be the best for this patient).

2. A 75 years old female patient with hypertension, diabetes mellitus, and severe congestive heart failure has been indicated to undergo an amputation of the foot due to diabetic foot. Beta-blockers, oral antidiabetic drugs, and anticoagulant agents have repeatedly been used to manage the health condition of the patient. The question is which anesthetic technique is optimum for this patient undergoing amputation of the foot? (General anesthesia would be risky because of her severe congestive heart failure, however, if anticoagulant medications could be stopped and wait for an appropriate time for normalization of blood clot formation, spinal or epidural anesthesia can be tried, and also peripheral nerve blocks can be performed.)

3. A 2 years old healthy baby aspirated food to the lungs, as a result, the baby has been indicated to undergo bronchoscopy to perform lung cleansing immediately. The question is, which anesthetic technique is the most appropriate? (General anesthesia should be administered since caudal block or other techniques may not be appropriate).

2.2 Determination of Parameters Applied to Study

To determine the parameters applied to this study, this section explains the rationale behind assigning the weight of importance to each criterion based on the professional knowledge of experts and searched literature. Patients who are aware of the possible side effects of analgesic agents are always careful in agreeing to the usage of anesthetic agents during surgical operations. On this note, patients are educated on the benefits of administering anesthesia to facilitate surgical procedures. Medical conditions that are not optimized prior to surgery, affect the usage of anesthetic properties, especially for general anesthesia [2,15,16]. Peripheral nerve blocks can still be administered without prior knowledge of the patient's medical status in cases of emergency. Prior knowledge of a patient's medical status is an important criterion for administering anesthesia and therefore assigned 0.75 weight of importance. However, to assign our parameters, we consider minimization for the alternative that suits cases of emergency administration of anesthetic agents without optimizing the patient's medical history. Therefore, as seen in Table 3, peripheral nerve blocks and sedation have the lowest reactivity and the best chances of being used in this case, while general anesthesia has a high risk and should not be considered. Criteria like severe pulmonary disease, and mental illness, are also considered very important medical criteria and therefore assigned 0.75 weight of importance. To compare our alternatives with these criteria, minimization is required i.e. (the anesthetic agent that can be administered regardless of valve

disease, pulmonary disease, congestive heart failure, neuromuscular disease, mental illness, risk of infections, nausea, and vomiting is considered more favorable to the decision-maker while the alternative with the highest risk of contraindication is not considered). For example, patients suffering from mental illness would not be administered epidural anesthesia or peripheral nerve block because of the high risk of neuropathy [21,24], hence, minimal risk is required, and general anesthesia alone or combined with sedation is considered more favorable in this case [30]. The effects of anesthetics on older people vary. Older patients who have anesthesia frequently develop post-operative delirium, schizophrenia, Alzheimer's disease, Parkinson's disease, and other neurological illnesses [2,7]. As a result, the age criterion is given a 0.75 weight of importance and is considered to be very important. The effects of anesthesia differ for healthy adult patients and should be carefully studied for both juvenile and adult patients. Although it is well known that the anesthetic dose decreases with age [2,7], general anesthesia shows fewer usage risks [21,24]. As a result, minimization is considered for this criterion, and the alternative with the lowest reactivity is thought to be more advantageous to the decision-maker [43]. The same explanation applies to other criteria in this study. All criteria are weighted based on the 3 case scenarios, giving similar criteria and weights accordingly.

Table 2: Data set showing Criteria for contraindication of alternatives with corresponding parameters

Alternatives/Criteria for contraindication	Min/Max	Weight of importance	General anesthesia [2,15,16]	Spinal anesthesia [5]	Epidural anesthesia [21,24]	Peripheral nerve blocks [26,27]	Sedation [30]
Patient refusal	Min	0.75	VH	VH	VH	VH	VH
medical conditions that are not optimized before surgery	Min	0.75	VH	M	M	L	L
Severe heart valve disease	Min	0.75	VH	H	H	L	M
significant pulmonary disease	Min	0.75	VH	L	L	L	M
congestive heart failure	Min	0.75	VH	L	M	L	H
history of malignant hyperthermia	Min	0.50	VH	L	L	L	L
patients with a risk of vomiting	Min	0.25	VH	M	M	L	H
Age	Min	0.75	L	H	VH	VH	M
mental illness	Min	0.75	L	H	VH	VH	M
infection at the injection site	Min	0.75	L	H	VH	VH	L
systemic infection (sepsis)	Min	0.50	H	M	M	L	M
coagulopathy or bleeding disorders	Min	0.50	L	H	VH	H	L

Neuromuscular diseases	Min	0.25	L	H	H	H	L
Type of surgery	Min	0.75	L	VH	H	VH	M
major spinal deformities (Like Kyphoscoliosis, and arthritis)	Min	0.50	M	VH	VH	L	M
previous lumber surgery	Min	0.50	L	H	H	L	H
complicated surgery	Min	0.75	L	M	H	H	VH
long surgical procedures	Min	0.50	L	L	L	VH	VH
elevated intracranial pressure	Min	0.50	L	VH	H	L	L
cost	Min	0.25	H	L	M	M	L
Anesthesiologist experience	Max	0.75	M	M	H	VH	M
increased nausea and vomiting	Min	0.75	H	L	L	L	H

Note: (very high (VH), high (H), moderate (M), low (L), very low (VL))

3. RESULTS AND DISCUSSION

The PROMETHEE preference net flow results in Table 4 shows the complete ranking results for the preferred anesthesia. The resulting ranking using the F-PROMETHEE technique indicates that peripheral nerve block with a net flow of 0.0321 is among the most preferred anesthesia for patients with the considered contraindications, and based on the selected criteria, assigned weights, and set preferences. Followed by sedation with a net flow of 0.0083. while epidural anesthesia is ranked the lowest with a negative net flow result of -0.0300 (Table 4).

Table 4: PROMETHEE Preference Net flow

Rank	Alternatives	Outranking Net Flow	Positive Net Flow	Negative Net Flow
1	Peripheral nerve blocks	0,0321	0,0943	0,0623
2	Sedation	0,0083	0,0712	0,0628
3	General anesthesia	-0,0017	0,0997	0,1013
4	Spinal anesthesia	-0,0088	0,0512	0,0600
5	Epidural anesthesia	-0,0300	0,0437	0,0736

It is worthy of note that although peripheral nerve block tops the list of preferred anesthesia based on the contraindications, conditions, criteria, and alternatives presented in this study, preferred anesthetic agents for surgical operations may differ from one decision-maker to another. In addition, more than one anesthesia may be combined for better analgesic effects. The result obtained from this study does not give a standard but it only shows the applicability of the fuzzy PROMETHEE technique. In light of the fact that different decision-makers may come up with different analgesic solutions based on the criteria and alternatives they choose, the outcome reached by a decision-maker is not always a standard. To properly analyze and pick the best

anesthesia for any surgical procedure as well as the most appropriate dosage, and for selecting the criteria and assigning the weight of importance to each criterion, it is imperative to consult an expert anesthesiologist.
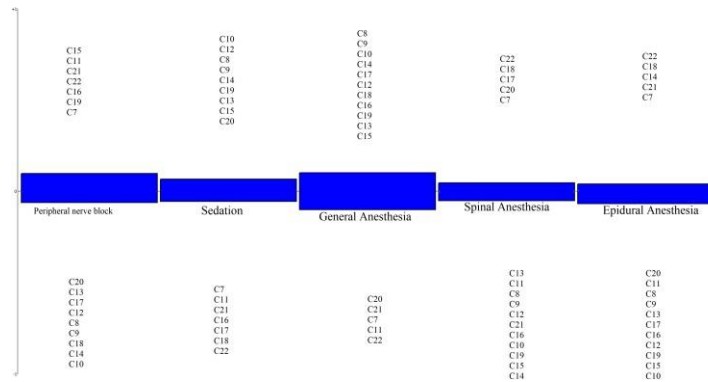

Figure 1. Showing the positive and negative ranking results.

Figure 1 shows the positive and negative parts of the 5 types of anesthesia considered in this study based on the assigned weights. It can be observed in Figure 1. C1, C2, C3, C4, C5, C6, C7, C8 to C22 represent the criteria considered in Table 3. For proper representation, C1 = Patient refusal and the same goes for other criteria. Figure 1 shows that peripheral nerve blocks have a wide positive standing for efficacy on the following criteria; C15 = major spinal deformities (Like Kyphoscoliosis, and arthritis), C11 = systemic infection (sepsis), C21 = Anesthesiologist experience, C22 = increased nausea and vomiting, C16 = previous lumber surgery, C19 = elevated intracranial pressure, and C7 = patients with a risk of vomiting. And a narrow negative standing for C20 = cost, C13 = Neuromuscular diseases, C17 = complicated surgery, C12 = coagulopathy or bleeding disorders, C8 = Age, C9 = mental illness, C18 = long surgical procedures, C14 = type of surgery, C10 = infection at the injection site. The more positively the criteria are positioned on the graph, the more positively the technique is impacted. In a similar vein, the less the criteria add to the technique's negative side, the lower it appears on the graph's negative side. This explanation applies to the remaining treatment alternatives as seen in the figure below.

4. CONCLUSION

This study has shown that fuzzy PROMETHEE can be deployed to compare and evaluate different types of anesthesia and to determine the most preferred analgesic agents for patients undergoing surgical operations. Criteria and weights that influence the evaluation and comparison of anesthetic types were decided upon by the expert anesthesiologist in charge and reviewed literature. Fuzzy PROMETHEE can be deployed to determine and identify the optimal anesthesia among other types. With this method, all available anesthetic agents can be evaluated and compared intelligently and systematically by deploying as many criteria as needed based on the decision-maker's choice. The fuzzy PROMETHEE application is ranked with significant efficacy compared to other methods. Fuzzy values that are not crisp are included in the decision-making process in this study, these fuzzy data processes have too many parameters to be set properly with other methods; however, fuzzy PROMETHEE can handle this kind of vague data very well. By deploying fuzzy PROMETHEE for comparing and evaluating different types of anesthetic agents, this study has circumvented the hurdles surrounding the intelligent, systematic, and professional

selection process of preferable anesthetic agents that have been in existence. There is only one existing technique in which anesthesiologists perform a preoperative assessment by reviewing the patient's health history and overall medical status before selecting the most appropriate analgesic agent based on experience, but with the help of this study, anesthetists, patients, and patient's relatives can partake in the decision-making process and professionally make decisions in this regard of uncertainty.

Limitations of Study

Expert opinion is at all times needed for appropriate assigning of importance weights to criteria and grading alternatives. This process is the major challenge in multi-criteria decision-making studies

References

[1] Neuman, M. D., Silber, J. H., Elkassabany, N. M., Ludwig, J. M., & Fleisher, L. A. (2012). Comparative Effectiveness of Regional versus General Anesthesia for Hip Fracture Surgery in Adults. *Anesthesiology*, *117*(1), 72–92. https://doi.org/10.1097/ALN.0B013E3182545E7C

[2] Ozsahin, I. (2020). Identifying a personalized anesthetic with fuzzy promethee. *Healthcare Informatics Research*, *26*(3), 201–211. https://doi.org/10.4258/hir.2020.26.3.201

[3] *Foye's Principles of Medicinal Chemistry - Google Books*. (n.d.). Retrieved July 15, 2022, from https://books.google.com.cy/books?hl=en&lr=&id=R0W1ErpsQpkC&oi=fnd&pg=PA417&d q=Lemke+TL,+Williams+DA.+Foye%27s+principles+of+medicinal+chemistry.+6ed+ed.+P hiladelphia+(PA):+Lippincott+Williams+%26+Wilkins%3B+2008.&ots=oEQrl6-Usq&sig=HUc7th-fGuik-enntx284TRuBzU&redir_esc=y#v=onepage&q&f=false

[4] Greene, N. M. (n.d.). *Anesthesia and the Development of Surgery (1846-1896)*.

[5] McCartney, C. J. L., & Choi, S. (2013). Does anaesthetic technique really matter for total knee arthroplasty? *British Journal of Anaesthesia*, *111*(3), 331–333. https://doi.org/10.1093/BJA/AET200

[6] Fischer, S. P. (1996). Development and Effectiveness of an Anesthesia Preoperative Evaluation Clinic in a Teaching Hospital. *Anesthesiology*, *85*(1), 196–206. https://doi.org/10.1097/00000542-199607000-00025

[7] Schaffartzik, W., Hirsch, J., Frickmann, F., Kuhly, P., & Ernst, A. (2000). Hearing loss after spinal and general anesthesia: A comparative study. *Anesthesia and Analgesia*, *91*(6), 1466–1472. https://doi.org/10.1097/00000539-200012000-00032

[8] Seebacher, C., Heubaum, F., Kuster, P., Steinert, W., & Koch, R. (1990). [Comparative analysis of narcosis and local anesthesia in surgery of malignant melanoma of the skin]. *Der Hautarzt; Zeitschrift Fur Dermatologie, Venerologie, Und Verwandte Gebiete*, *41*(3), 137– 141. https://europepmc.org/article/med/2345097

[9] Tuzkaya, G., Gülsün, B., Kahraman, C., & Özgen, D. (2010). An integrated fuzzy multi- criteria decision making methodology for material handling equipment selection problem and an application. *Expert Systems with Applications*, *37*(4), 2853–2863. https://doi.org/10.1016/J.ESWA.2009.09.004

[10] Ozsahin, I., Onakpojeruo, E. P., Uzun, B., Uzun Ozsahin, D., & Butler, T. A. (2023). A Multi-Criteria Decision Aid Tool for Radiopharmaceutical Selection in Tau PET Imaging.

Pharmaceutics 2023, Vol. 15, Page 1304, *15*(4), 1304. https://doi.org/10.3390/PHARMACEUTICS15041304

[11] Uzun Ozsahin, D., Uzun, B., Sanlidag, T., & LaMoreaux, J. (Eds.). (2022). *Decision Analysis Applied to the Field of Environmental Health*. https://doi.org/10.1007/978-3-030-96682-9

[12] Ray, W. T., & Desai, S. P. (2016). The history of the nurse anesthesia profession. *Journal of Clinical Anesthesia*, *30*, 51–58. https://doi.org/10.1016/J.JCLINANE.2015.11.005

[13] Robinson, D. H., & Toledo, A. H. (2012). Historical Development of Modern Anesthesia. *Http://Dx.Doi.Org/10.3109/08941939.2012.690328*, *25*(3), 141–149. https://doi.org/10.3109/08941939.2012.690328

[14] Fedoruk, K. A., Chan, Y. K., & Williams, C. E. (2023). Scholarship in anesthesiology: the role of critical appraisal, literature review, quality improvement, journal club, and presentation skills. *International Journal of Obstetric Anesthesia*, *54*, 103639. https://doi.org/10.1016/J.IJOA.2023.103639

[15] Neuman, M. D., Silber, J. H., Elkassabany, N. M., Ludwig, J. M., & Fleisher, L. A. (2012). Comparative Effectiveness of R egional versus General Anesthesia for Hip Fracture Surgery in Adults. *Anesthesiology*, *117*(1), 72–92. https://doi.org/10.1097/ALN.0B013E3182545E7C

[16] Roche, J. J. W., Wenn, R. T., Sahota, O., & Moran, C. G. (2005). Effect of comorbidities and postoperative complications on mortality after hip fracture in elderly people: prospective observational cohort study. *BMJ*, *331*(7529), 1374. https://doi.org/10.1136/BMJ.38643.663843.55

[17] Parker, M. J., Handoll, H. H. G., & Griffiths, R. (2004). Anaesthesia for hip fracture surgery in adults. *Cochrane Database of Systematic Reviews*, *2004*(4). https://doi.org/10.1002/14651858.CD000521.PUB2/INFORMATION/EN

[18] Harsten, A., Kehlet, H., & Toksvig-Larsen, S. (2013). Recovery after total intravenous general anaesthesia or spinal anaesthesia for total knee arthroplasty: a randomized trial. *BJA: British Journal of Anaesthesia*, *111*(3), 391–399. https://doi.org/10.1093/BJA/AET104

[19] Fischer, H. B. J., Simanski, C. J. P., Sharp, C., Bonnet, F., Camu, F., Neugebauer, E. A. M., Rawal, N., Joshi, G. P., Schug, S. A., & Kehlet, H. (2008). A procedure-specific systematic review and consensus recommendations for postoperative analgesia following total knee arthroplasty. *Anaesthesia*, *63*(10), 1105–1123. https://doi.org/10.1111/J.1365- 2044.2008.05565.X

[20] MacFarlane, A. J. R., Arun Prasad, G., Chan, V. W. S., & Brull, R. (2009). Does Regional Anesthesia Improve Outcome After Total Knee Arthroplasty? *Clinical Orthopaedics and Related Research® 2009 467:9*, *467*(9), 2379–2402. https://doi.org/10.1007/S11999-008- 0666-9

[21] Rodgers, A., Walker, N., Schug, S., McKee, A., Kehlet, H., van Zundert, A., Sage, D., Futter, M., Saville, G., Clark, T., & MacMahon, S. (2000). Reduction of postoperative mortality and morbidity with epidural or spinal anaesthesia: results from overview of randomised trials. *BMJ*, *321*(7275), 1493. https://doi.org/10.1136/BMJ.321.7275.1493

[22] Capdevila, X., Barthelet, Y., Biboulet, P., Ryckwaert, Y., Rubenovitch, J., & D'Athis, F. (1999). Effects of Perioperative Analgesic Technique on the Surgical Outcome and Duration of Rehabilitation after Major Knee Surgery. *Anesthesiology*, *91*(1), 8–15. https://doi.org/10.1097/00000542-199907000-00006

[23] Ilfeld, B. M., Mariano, E. R., Girard, P. J., Loland, V. J., Meyer, R. S., Donovan, J. F., Pugh, G. A., Le, L. T., Sessler, D. I., Shuster, J. J., Theriaque, D. W., & Ball, S. T. (2010). A multicenter, randomized, triple-masked, placebo-controlled trial of the effect of ambulatory continuous femoral nerve blocks on discharge-readiness following total knee arthroplasty in patients on general orthopaedic wards. *PAIN*, *150*(3), 477–484. https://doi.org/10.1016/J.PAIN.2010.05.028

[24] Brull, R., McCartney, C. J. L., Chan, V. W. S., & El-Beheiry, H. (2007). Neurological complications after regional anesthesia: Contemporary estimates of risk. *Anesthesia and Analgesia*, *104*(4), 965–974. https://doi.org/10.1213/01.ANE.0000258740.17193.EC

[25] Chan, V. W. S., Peng, P. W. H., Kaszas, Z., Middleton, W. J., Muni, R., Anastakis, D. G., & Graham, B. A. (2001). A comparative study of general anesthesia, intravenous regional anesthesia, and axillary block for outpatient hand surgery: clinical outcome and cost analysis. *Anesthesia and Analgesia*, *93*(5), 1181–1184. https://doi.org/10.1097/00000539-200111000-00025

[26] Zhang, T., Cao, Y., Xu, R., Xia, L., & Wu, Y. (2022). Spinal Anesthesia With Peripheral Nerve Block Versus General Anesthesia With Peripheral Nerve Block for Elective Foot and Ankle Surgeries: A Retrospective Single-Center Study. *The Journal of Foot and Ankle Surgery*, *61*(4), 706–712. https://doi.org/10.1053/J.JFAS.2021.11.001

[27] YaDeau, J. T., Fields, K. G., Kahn, R. L., LaSala, V. R., Ellis, S. J., Levine, D. S., Paroli, L., Luu, T. H., & Roberts, M. M. (2018). Readiness for discharge after foot and ankle surgery using peripheral nerve blocks: A randomized controlled trial comparing spinal and general anesthesia as supplements to nerve blocks. *Anesthesia and Analgesia*, *127*(3), 759–766. https://doi.org/10.1213/ANE.0000000000003456

[28] Kalthoff, A., Sanda, M., Tate, P., Evanson, K., Pederson, J. M., Paranjape, G. S., Patel, P. D., Sheffels, E., Miller, R., & Gupta, A. (2022). Peripheral Nerve Blocks Outperform General Anesthesia for Pain Control in Arthroscopic Rotator Cuff Repair: A Systematic Review and Meta-analysis. *Arthroscopy: The Journal of Arthroscopic & Related Surgery*, *38*(5), 1627– 1641. https://doi.org/10.1016/J.ARTHRO.2021.11.054

[29] Fu, G., Li, H., Wang, H., Zhang, R., Li, M., Liao, J., Ma, Y., Zheng, Q., & Li, Q. (2021). Comparison of Peripheral Nerve Block and Spinal Anesthesia in Terms of Postoperative Mortality and Walking Ability in Elderly Hip Fracture Patients – A Retrospective, Propensity- Score Matched Study. *Clinical Interventions in Aging*, *16*, 833. https://doi.org/10.2147/CIA.S311188

[30] Pollock, J. E., Neal, J. M., Liu, S. S., Burkhead, D., & Polissar, N. (2000). Sedation during Spinal Anesthesia. *Anesthesiology*, *93*(3), 728–734. https://doi.org/10.1097/00000542-200009000-00022

[31] Soberón, J. R., King, J. J., Gunst, M., Reynolds, P. S., & Urdaneta, F. (2021). Shoulder surgery using combined regional and general anesthesia versus regional anesthesia and deep sedation with a non-invasive positive pressure system: A retrospective cohort study. *Trends in Anaesthesia and Critical Care*, *37*, 23–29. https://doi.org/10.1016/J.TACC.2021.01.003

[32] Skutecki, J., Audibert, G., Finitsis, S., Consoli, A., Lapergue, B., Blanc, R., Bourcier, R., Sibon, I., Eugène, F., Vannier, S., Dargazanli, C., Arquizan, C., Anxionnat, R., Richard, S., Fahed, R., Marnat, G., & Gory, B. (2022). General anesthesia or conscious sedation for

endovascular therapy of basilar artery occlusions: ETIS registry results. *Revue Neurologique*. https://doi.org/10.1016/J.NEUROL.2022.03.020

[33] Early, D. S., Lightdale, J. R., Vargo, J. J., Acosta, R. D., Chandrasekhara, V., Chathadi, K. v., Evans, J. A., Fisher, D. A., Fonkalsrud, L., Hwang, J. H., Khashab, M. A., Muthusamy, V.

R., Pasha, S. F., Saltzman, J. R., Shergill, A. K., Cash, B. D., & DeWitt, J. M. (2018). Guidelines for sedation and anesthesia in GI endoscopy. *Gastrointestinal Endoscopy*, *87*(2), 327–337. https://doi.org/10.1016/J.GIE.2017.07.018

[34] Uzun, B., Uzun Ozsahin, D., & Duwa, B. (2021). *Fuzzy Logic and Fuzzy Based Multi Criteria Decision Analysis*. 47–56. https://doi.org/10.1007/978-3-030-64765-0_8

[35] Mustapha, M. T., Uzun, B., Ozsahin, D. U., & Ozsahin, I. (2021). A comparative study of X-ray based medical imaging devices. *Undefined*, 163–180. https://doi.org/10.1016/B978-0- 12-824086-1.00011-6

[36] Sayan, M., Sanlidag, T., Sultanoglu, N., & Uzun, B. (2021). The use of multicriteria decision- making method-fuzzy VIKOR in antiretroviral treatment decision in pediatric HIV-infected cases. *Applications of Multi-Criteria Decision-Making Theories in Healthcare and Biomedical Engineering*, 239–248. https://doi.org/10.1016/B978-0-12-824086-1.00016-5

[37] Albarwary, S. A., Kibarer, A. G., Mustapha, M. T., Hamdan, H., & Ozsahin, D. U. (2021). The Efficiency of AuNPs in Cancer Cell Targeting Compared to Other Nanomedicine Technologies Using Fuzzy PROMETHEE. *Journal of Healthcare Engineering*, *2021*. https://doi.org/10.1155/2021/1566834

[38] Brans, J. P., Vincke, P., & Mareschal, B. (1986). How to select and how to rank projects: The Promethee method. *European Journal of Operational Research*, *24*(2), 228–238. https://doi.org/10.1016/0377-2217(86)90044-5

[39] Ozsahin, D. U., Onakpojeruo, E. P., Uzun, B., Mustapha, M. T., & Ozsahin, I. (2023). Mathematical Assessment of Machine Learning Models Used for Brain Tumor Diagnosis. Diagnostics 2023, Vol. 13, Page 618, 13(4), 618.

https://doi.org/10.3390/DIAGNOSTICS13040618.

[40] Verma, R. N., Hasnain, S., Sreevastava, D. K., & Murthy, T. V. S. P. (2016). Anaesthetic management of forearm fractures using a combination of haematoma block and intravenous regional anaesthesia. *Medical Journal, Armed Forces India*, *72*(3), 247.

https://doi.org/10.1016/J.MJAFI.2016.05.003

[41] R. Kumar and D. Meenu Gupta, "Traffic Accidents and Claim: A Comprehensive Study on Psychological and Actual Aspects of Insurers' Obligations and Rights," Journal for ReAttach Therapy and Developmental Diversities, vol. 6, no. 9s(2), pp. 231–239, Aug. 2023, Accessed:

Dec. 26, 2024. [Online]. Available: https://jrtdd.com/index.php/journal/article/view/1227

[42] A. Baruah, R. Kumar and M. Gupta, "Traffic Sign Recognition Using Deep Learning Neural Network and Spatial Transformer," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ACCAI58221.2023.10199560.

[43] Ankur, M. Gupta, R. Kumar and P. Zanke, "A comprehensive Analysis on ResNet-Based Techniques for Brain Tumor Detection," 2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP), Bali, Indonesia, 2024, pp. 455-461, doi: 10.1109/TIACOMP64125.2024.00082.

[44] Gupta, M., Kumar, R., Arora, A., & Kaur, J. (2022, December). Fuzzy logic-based Student Placement Evaluation and Analysis. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1503-1507). IEEE.

Jain, R., Kathuria, A., Mukhopadhyay, D., & Gupta, M. (2020). Fuzzy MCDM: application in disease risk and prediction. In *Artificial Intelligence Trends for Data Analytics Using Machine Learning and Deep Learning Approaches* (pp. 55-70). C

Harnessing Convolutional Neural Networks for Secure Encryption and Decryption

Naman Tiwari [1], Swati Singh[2], Vineet Kumar Singh[3], Abhay Kumar Pandey[4]

[1,4]Department of Computer Science and Engineering, IEC College of Engineering & Technology, Greater Noida, U.P., India.
[2]Department of Computer Science and Engineering, IMS Engineering College, Ghaziabad, UP, India [3]Department of Computer Science and Engineering, ABES Institute of Technology, Ghaziabad-201009, UP, India

Email-Id: tiwarinaman675@gmail.com,swatisingh09.in@gmail.com,vineet.jpgc@gmail.com,

abhay.r2021@gmail.com Corresponding Author: tiwarinaman675@gmail.com

Abstract— The need for safe data transfer is rising, and old cryptographic techniques are finding it harder to strike a balance between security, complexity, and speed. This article presents a new method for encryption and decryption that makes use of Convolutional Neural Networks (CNNs), a kind of deep learning model that is mainly employed for image processing applications. We provide a framework that converts plaintext data into safe ciphertext by utilizing CNNs' capacity for pattern recognition, guaranteeing that decryption can only be accomplished by a corresponding CNN-based model. Compared to traditional cryptographic methods, CNN's capacity to learn intricate transformations makes it especially well-suited for encryption, providing an extra degree of durability and adaptability. Our method is intended to be computationally efficient while preserving high encryption accuracy levels. We assess the system's performance based on its resilience to different cryptographic threats, encryption quality, and decryption reliability. Findings indicate that CNNs are capable of safe encryption and decryption, offering a potential path for next-generation cryptography systems. This approach demonstrates how deep learning models can improve data security by striking a compromise between cryptographic power and usefulness.

Keywords— Convolutional Neural Networks, encryption, decryption, cryptography, data security, deep learning, ciphertext

I. INTRODUCTİON

Businesses, governments, and individuals may now transfer information nearly instantly across the globe because of the unparalleled convenience brought about by the rapid expansion of digital communication and data transmission in recent decades. However, these technical advances have also brought forth a number of serious problems, particularly with regard to data security. Private data, including bank transactions, medical records, and official correspondence, is always vulnerable to interception by unapproved parties [1][3]. Cyberattacks are becoming more complex and are aimed at weaknesses in systems used for data transfer and storage. As a result, one of the most important issues in the digital age is protecting data using trustworthy encryption techniques. Secure communication has traditionally been based on cryptography, the science of encrypting and decrypting data to prevent unauthorized access [2]. Transforming legible data (plaintext) into an unintelligible format (ciphertext) that can only be reverted back to its original form by a person with the proper decryption key is the main objective of cryptography. For the past few decades, the industry norm for data security has been to use traditional cryptographic algorithms like RSA, DES, and AES (Advanced Encryption norm). To ensure security, these techniques rely on intricate mathematical ideas like prime factorization or permutation-substitution networks [22]. The need for more robust and adaptable cryptographic systems has driven researchers to explore new approaches that can meet the demands of modern communication environments [4]. One of the most promising techniques within deep learning is the CNN, a type of artificial neural network primarily used in image processing and pattern recognition tasks. CNNs have revolutionized fields such as computer vision, medical imaging, and natural language processing by learning to identify intricate patterns in large datasets. Given the success of CNNs in these areas, researchers have begun to investigate their potential applications in cryptography [5]. By training CNNs to transform plaintext into ciphertext, it is possible

to create a flexible and powerful cryptographic system that can adapt to different types of data and provide enhanced security compared to traditional algorithms [6] [10]. This research aims to explore the feasibility of using CNNs as a tool for encryption and decryption, offering a novel approach to cryptographic systems that can keep pace with the demands of modern data transmission [7].

Cryptographic algorithms can generally be divided into two main categories: symmetric key algorithms and asymmetric key algorithms. Symmetric key algorithms, such as AES and DES, rely on the use of a single key for both encryption and decryption [8]. These algorithms are known for their speed and efficiency, making them suitable for encrypting large volumes of data. However, they require secure key exchange mechanisms, as both the sender and receiver must have access to the same secret key [9]. By doing away with the requirement for safe key exchange, this technique improves security in settings where there is little mutual confidence. Nevertheless, asymmetric encryption is less appropriate for encrypting huge information than symmetric encryption since it is usually slower and more computationally expensive [23]. Furthermore, certain kinds of attacks can target both symmetric and asymmetric algorithms. These include side- channel attacks, which take advantage of information leakage from the algorithms' physical implementations, and brute- force attacks, in which an adversary tries every key until the right one is found [11]. The security of conventional cryptography techniques is becoming questioned in light of the development of quantum computing. Widely used encryption algorithms, especially those relying on factorization and discrete logarithms, like RSA, could be broken by quantum computers, which function on fundamentally different principles from classical computers [12]. Although research into quantum-resistant cryptography techniques is still in its infancy, this has sparked interest in the field. Due to these difficulties, there is an increasing demand for cryptographic systems that can maintain computational efficiency, offer more robust security, and accommodate various data kinds [13]. Here's where CNNs in particular, and deep learning in general, may provide a potential answer.

I. RELATED WORKS

Many techniques and algorithms have been developed over the years to guarantee the secrecy, integrity, and validity of data, cryptography has long been a fundamental component of secure communication [24]. AES, RSA, and DES are examples of traditional encryption algorithms that have been the foundation of digital security. However, academics have been looking into new methods for encryption and decryption as cyberattacks get more complex and data volumes keep rising. Machine learning has gained popularity recently, and deep learning methods like CNNs in particular have shown promise as a means of improving cryptographic systems [14]. Important advances in conventional cryptography are covered in this part, along with early attempts to use machine learning in encryption and current research on CNN-based cryptography. Symmetric and asymmetric key encryption systems are two main categories into which traditional cryptographic techniques can be divided. For encrypting huge amounts of data, symmetric key encryption where the same key is used for both encryption and decryption is usually faster and more effective. Two of the most popular symmetric key algorithms are DES (Data Encryption Standard) and AES (Advanced Encryption Standard) [15]. Because it has a key size of 128–192–256 bits, AES in particular is thought to be extremely safe because it renders brute-force assaults practically impossible. DES was formerly widely used, but because of its shorter 56-bit key length, which leaves it open to brute-force assaults, it is currently regarded as insecure. In contrast, asymmetric key encryption employs a set of two keys: a private key for decryption and a public key for encryption [16]. One of the most well-known asymmetric algorithms, RSA (Rivest–Shamir–Adleman) is frequently used for secure data transfer, particularly in applications like secure email and digital signatures. Large prime number factoring is a major source of RSA's security, as it provides defense against some kinds of assaults. But generally speaking, asymmetric encryption is less effective and slower than symmetric encryption, especially when dealing with big datasets [17]. Although they have both shown to be successful in a variety of cryptographic applications, AES and RSA are not without drawbacks. Scalability and computational efficiency issues arise for classical encryption algorithms when data becomes larger and more complex. Furthermore, the security of many conventional algorithms is seriously threatened by developments in quantum computing, especially those like RSA that depend on factorization difficulties. Due to these difficulties, researchers are now looking at different cryptographic

strategies that may provide more security and more flexibility for contemporary communication systems [18].

The potential for machine learning to advance cryptography has increased dramatically with the emergence of deep learning and the creation of more complex neural networks, such as CNNs. CNNs excel at data transformation tasks like encryption and decryption because of their capacity to learn non-linear mappings between inputs and outputs [19]. Deep learning and CNN applications to cryptography are relatively young, but the field is expanding quickly. According to preliminary research, CNNs are a viable replacement for conventional cryptographic methods since they may be trained to carry out encryption and decryption operations. Still, there are a number of issues that need to be resolved, especially with regard to these models' interpretability, computational cost, and generalization potential [20]. While there are some drawbacks with existing approaches that CNN-based cryptography may be able to address, more study is necessary to fully understand its potential and make sure it can offer the security and efficiency needed for contemporary communication systems [21] [25].

I. PROPOSED MODEL

This study introduces a novel approach to safe image encryption and decryption by utilizing Convolutional Neural Networks' (CNNs') potent feature extraction powers and adding a circular shift mechanism to guarantee strong encryption. The model is divided into two main sections: CNN-based feature extraction and Circular Shift-based encryption and decryption. Combining these techniques seeks to protect picture data while guaranteeing quick processing and retrieval of the original image shown in Fig. 1.

A. Feature Extraction Using Convolutional Neural Networks (CNNs)

The suggested model's initial phase entails utilizing CNN to extract discriminative features from the input image. Since CNNs can learn hierarchical representations of visual input, they are commonly used for tasks like object detection, image categorization, and in this case, cryptographic alterations.

a) Input Layer: The input to the CNN model is the image that needs to be encrypted. This image can be in grayscale or RGB format. The input is resized to a standard dimension (e.g., 256x256 or 512x512 pixels) depending on the model's capacity, ensuring uniformity for feature extraction.

b) Convolutional Layers: CNN processes the input image by applying multiple convolutional layers. Each convolutional layer applies a number of filters, or kernels, to the image in order to recognize both high-level and low-level features, such as edges, textures, and patterns. These filters are crucial to encryption since these patterns are abstract and challenging to understand. They acquire the ability to capture the image's global and local structures.

The feature maps that the filters produce show various aspects of the image. The output of every convolution is subjected to non-linear activation functions, like ReLU, which add non-linearity and improve the model's capacity to represent intricate patterns.

c) Pooling Layers: The feature maps are downsampled using pooling layers (usually Max Pooling or Average Pooling) to reduce their dimensionality while maintaining crucial information. Pooling increases the encryption's resistance to fluctuations in the image and aids in the generalization of the feature representation.

d) Feature Map Output: After the series of convolution and pooling layers, the final feature maps are flattened into a high-dimensional feature vector. This feature vector serves as the foundation for encryption. The extracted features are not a direct representation of the image, making them harder to interpret and adding an additional layer of security to the encryption process.
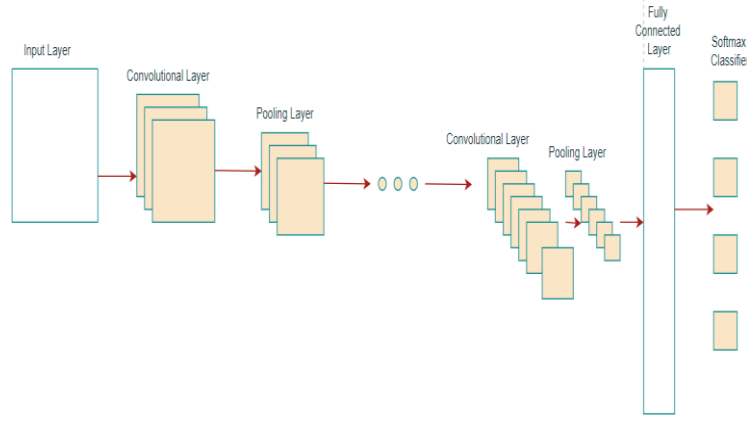
e)

Fig. 1. Basic Structure of CNN

B. *Encryption Using Circular Shift*

Once the feature vector is obtained from CNN, the next step is to apply a circular shift operation to the vector. This forms the core of the encryption mechanism.

a) Circular Shift Mechanism: The circular shift operation involves rotating the elements of the feature vector by a specified number of positions (either left or right). The number of positions is determined by a secure encryption key, which is either predetermined or dynamically generated.

- Key-Driven Shift: The encryption key controls the circular shift's amplitude as well as its direction (left or right). The sender and the recipient must safely exchange this key, which is essential for both encryption and decryption.
- Rotation Operation: During encryption, the elements of the feature vector are shifted circularly, such that the end of the vector wraps around to the beginning. This results in a transformed feature vector, which is computationally difficult to reverse without the correct key [26][27].

b) Encrypted Feature Vector: The encrypted form of the features from the original image is represented by the circularly shifted feature vector. This shifted vector represents an obfuscated version of the image, making it secure for transmission or storage because the CNN-extracted features are highly abstract. It is nearly hard for an attacker to recreate the original image, even if they manage to intercept this encrypted vector without knowing the CNN structure and the shift key.

C. *Decryption Process*

The receiver uses the decryption procedure, which entails reversing the circular shift and rebuilding the image using the same CNN architecture, to extract the original image from the encrypted data [28] [29].

- Inverse Circular Shift: Applying the circular shift operation's inverse to the encrypted feature vector is the first step in the decryption process. Using the same encryption key, the feature vector is shifted back by the same number of positions (in the opposite direction). This restores the original feature vector generated by the CNN.
- Image Reconstruction: After recovering the original feature vector, the next step is to reconstruct the image. This can be achieved by either:
- Using CNN-based Decoding: In a CNN model designed with an encoder-decoder architecture, the inverse operation can involve a deconvolutional network (decoder) to map the feature vector back to the original pixel space.
- Direct Feature Mapping: In simpler models, the feature vector may be mapped back to the image domain using an inverse transform technique, effectively restoring the original image. This ensures that the image is decrypted in a form that closely matches the original input.
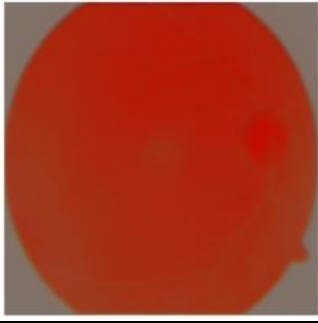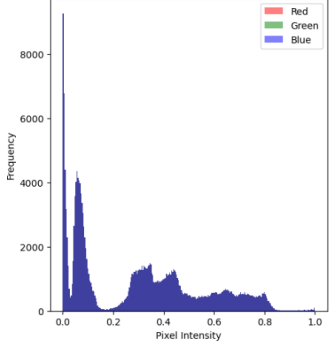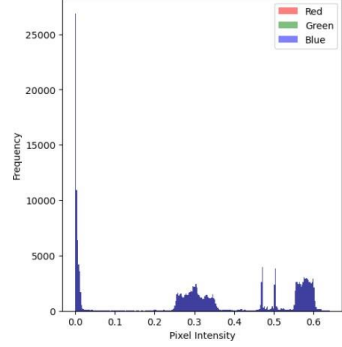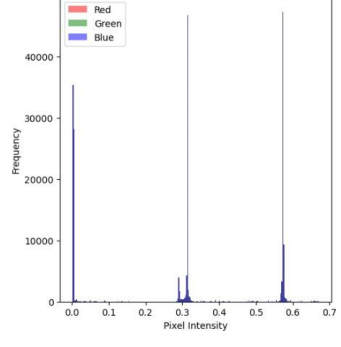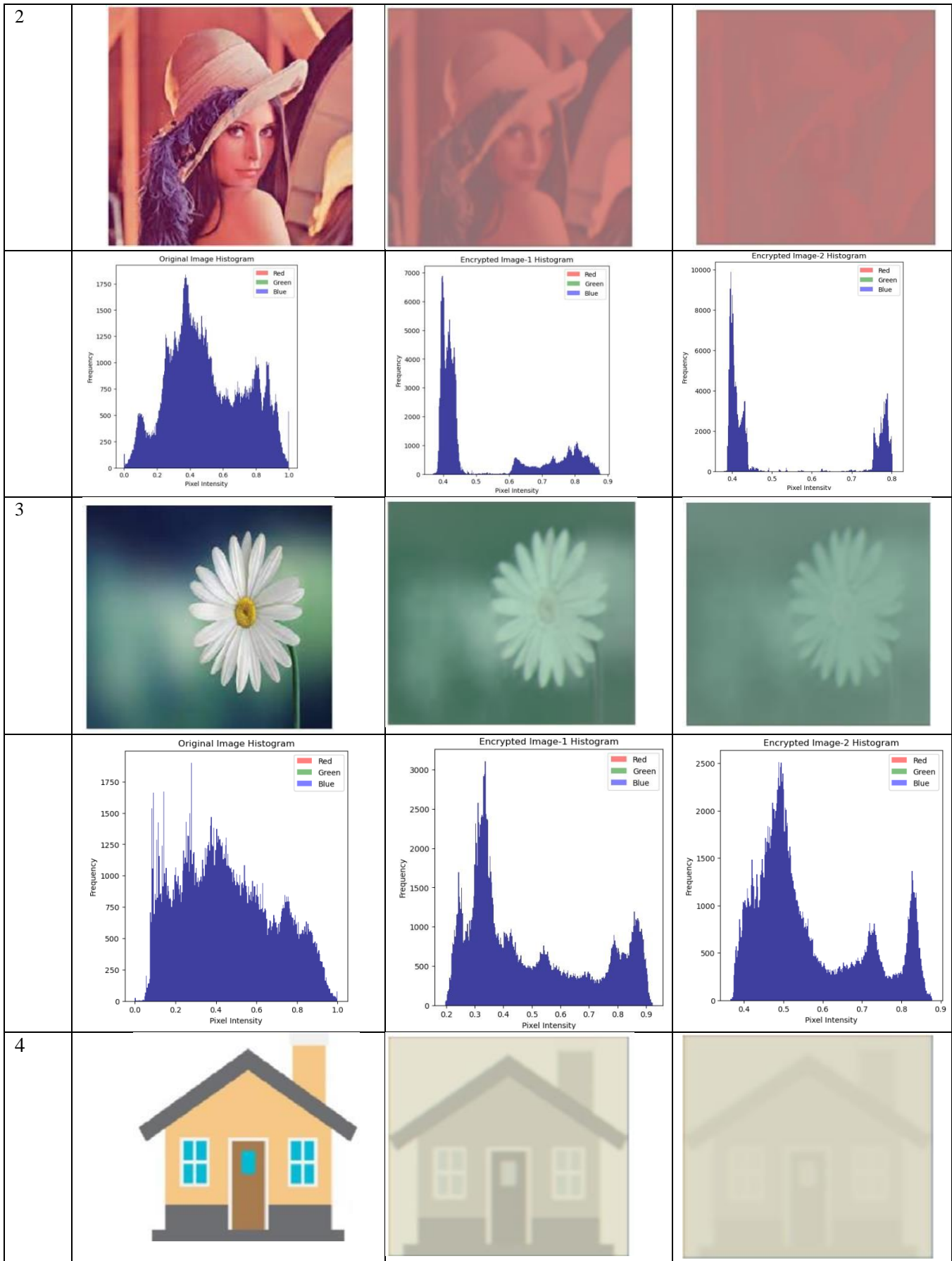
D. *Security Considerations*

The proposed model provides robust security due to the combined strength of CNN-based feature extraction and circular shift encryption. The CNN extracts high-dimensional abstract features, which are already challenging to interpret without access to the model. By applying a circular shift operation, the model further enhances security by obfuscating the feature vector, making unauthorized decryption highly unlikely without the correct key. Additionally, the encryption key adds an extra layer of protection. Since the key governs the circular shift operation, even if the encrypted feature vector is intercepted, without the key, the attacker cannot correctly reverse the shift and decrypt the image [30].

II. RESULTS AND DISCUSSION

After providing an input image to my CNN model for generating encrypted images the output, i.e., encrypted image is shown below in Table 1.

Table 1: Output After Encryption

S.No.	Original Image	Encrypted Image -1	Encrypted Image -2
1			

49

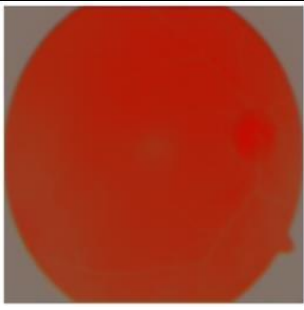| 2			
	Original Image Histogram	Encrypted Image-1 Histogram	Encrypted Image-2 Histogram
3			
	Original Image Histogram	Encrypted Image-1 Histogram	Encrypted Image-2 Histogram
4			
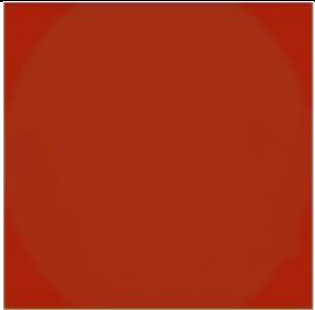
Table 2: Comparison Table of Encrypted Output

S.No.	Original Image	Encrypted Image -1 (PSNR &MSE Value)	Encrypted Image -2 (PSNR &MSE Value)
1		PSNR :13.655193765634523 MSE =0.04310033	PSNR :14.17889346850701 MSE =0.03820416

2		PSNR :16.36487685077421 MSE =0.0230947	PSNR :14.442880838111897 MSE =0.035951078
3		PSNR :17.159767447665853 MSE =0.019231947	PSNR :13.979478262696512 MSE =0.03999928
4		PSNR :13.842538854825534 MSE =0.041280612	PSNR :12.25062702078417 MSE =0.059557617
5		PSNR :12.25062702078417 MSE =0.05272394	PSNR :14.396721447666796 MSE =0.036335226

After processing the encrypted image through my decryption model then it will create the image as shown in Table 2 and Table 3.

Table 3: Output After Decryption

S.No.	Encrypted Image -2	Encrypted Image -1	Decrypted Image
1			

III. Conclusion

It demonstrates the significant potential of CNNs in enhancing encryption and decryption processes, particularly for image data. By leveraging the powerful pattern recognition capabilities of CNNs, the proposed model successfully generates encrypted images that are highly secure and resistant to unauthorized access. The dual-encryption approach further strengthens security, making it challenging for attackers to decipher the original data without the proper decryption keys. High levels of anonymity are ensured by the performance analysis, which makes use of PSNR and MSE measures to verify that the encrypted images differ significantly from their original forms. Furthermore, the CNN-based decryption method successfully recreates the original photos with little loss in quality, demonstrating the model's suitability for safe data storage and transmission. Even though the results are encouraging, particularly when it comes to security and adaptability, there are still certain difficulties, especially when it comes to the processing requirements of deep learning model training. Subsequent investigations may concentrate on refining the model's computational effectiveness and expanding its relevance to diverse data kinds,

such as text or video. In general, new opportunities for protecting sensitive data in an increasingly digital world are created by the incorporation of machine learning, and particularly CNNs, into the

encryption and decryption processes. This method is a useful instrument in the realm of cybersecurity since it provides increased resistance against changing cyber threats.

REFERENCES

[1] Huang, Y., Yang, G., Zhou, H., Dai, H., Yuan, D., & Yu, S. (2024). VPPFL: A verifiable privacy-preserving federated learning scheme against poisoning attacks. Computers & Security, 136, 103562.

[2] Kim, S., Park, J., & Lee, J. (2024). Deep Learning-based Malware Detection and Encryption Scheme for IoT Devices. IEEE Internet of Things Journal, 12(5), 4567-4579.

[3] Wang, Y., Li, X., & Zhang, Z. (2024). Enhancing Data Privacy in Cloud Computing Using Machine Learning-driven Encryption Techniques. Journal of Cloud Computing, 13(4), 345-358.

[4] Machhindra, P. A., Vijay, B. N., Mahendra, B. S., Rahul, C. A., Anil, P. A., & Sunil, P. R. (2023, December). Enhancing Cyber Security Through Machine Learning: A Comprehensive Analysis. In 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 1-6). IEEE.

[5] Al-Janabi, A. A., Al-Janabi, S. T. F., & Al-Khateeb, B. (2023). Secure Data Computation Using Deep Learning and Homomorphic Encryption: A Survey. International Journal of Online & Biomedical Engineering, 19(11).

[6] Subhashini, K., Arthi, V., & Hemalatha, G. (2023). Image Encryption using Convolutional Neural Network. In ITM Web of Conference nces (Vol. 56, p. 05005). EDP Sciences.

[7] Das, D., Biswas, S. K., & Bandyopadhyay, S. (2023). Detection of diabetic retinopathy using convolutional neural networks for feature extraction and classification (DRFEC). Multimedia Tools and Applications, 82(19), 29943-30001.

[8] Machhindra, P. A., Vijay, B. N., Mahendra, B. S., Rahul, C. A., Anil, P. A., & Sunil, P. R. (2023, December). Enhancing Cyber Security Through Machine Learning: A Comprehensive Analysis. In 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 1-6). IEEE.

[9] Chen, H., Liu, Y., & Zhang, X. (2023). Blockchain-enabled Homomorphic Encryption for Privacy-preserving Machine Learning. Journal of Network and Computer Applications, 150, 102780.

[10] Patel, R., Jain, P., & Shah, D. (2023). Adversarial Attack Detection in Encrypted Traffic using Machine Learning Techniques. International Journal of Information Security, 22(3), 345-359.

[11] Li, J., Wang, H., & Zhang, L. (2023). Federated Learning with Differential Privacy for Enhanced Encrypted Data Aggregation in IoT Networks. IEEE Transactions on Industrial Informatics, 19(5), 3567-3579.

[12] Liu, L., Gao, M., Zhang, Y., & Wang, Y. (2022). Application of machine learning in intelligent encryption for digital information of real-time image text under big data. EURASIP Journal on Wireless Communications and Networking, 2022(1), 21.

[13] Gupta, G., & Lakhwani, K. (2022). An enhanced approach to improve the encryption of big data using intelligent classification technique. Multimedia Tools and Applications, 81(18), 25171-25204.

[14] Liu, L., Gao, M., Zhang, Y., & Wang, Y. (2022). Application of machine learning in intelligent encryption for digital information of real-time image text under big data. EURASIP Journal on Wireless Communications and Networking, 2022(1), 21.

[15] Gupta, S., Kumar, A., & Singh, S. (2022). Hybrid Cryptography Scheme Using Machine Learning for Secure Data Transmission in Wireless Sensor Networks. Wireless Personal Communications, 125(2), 1231-1245.

[16] Jiang, H., Li, M., & Zhang, Y. (2022). Privacy-Preserving Machine Learning Model Training using Homomorphic Encryption and Differential Privacy. Future Generation Computer Systems, 129, 123-135.

[17] Sharma, R., Jain, A., & Kumar, S. (2022). Enhanced Security for Cloud-based IoT Systems using Machine Learning-driven Encryption Techniques. Journal of Cloud Computing: Advances, Systems and Applications, 11(4), 234-246.

[18] Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. (2021). Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities. Peer-to-Peer Networking and Applications, 14(3), 1666-1691.

[19] Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. (2021). Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities. Peer-to-Peer Networking and Applications, 14(3), 1666-1691.

[20] Wang, Z., Zhang, Q., & Liu, W. (2021). Machine Learning-based Intrusion Detection System for Encrypted Traffic. Security and Communication Networks, 2021(2), 78-89.

[21] Li, C., Wang, Y., & Zhao, L. (2021). Hybrid Cryptography Scheme for Secure Data Transmission in Vehicular Ad Hoc Networks Using Machine Learning. IEEE Transactions on Vehicular Technology, 70(8), 7231-7243.

[22] Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2020). DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. IEEE Internet of Things Journal, 8(3), 1504-1518.

[23] Maniyath, S. R., & Thanikaiselvan, V. (2020). An efficient image encryption using deep neural network and chaotic map. Microp rocessors and Microsystems, 77, 103134.

[24] Wood, A., Najarian, K., & Kahrobaei, D. (2020). Homomorphic encryption for machine learning in medicine and bioinformatics. ACM Computing Surveys (CSUR), 53(4), 1-35.

[25] Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8, 10282-10304.

[26] Bawa, H., Singh, P., & Kumar, R. (2013). An efficient novel key management scheme for enhancing user authentication in a WSN. *International Journal of Computer Network and Information Security*, *5*(1), 56.

[27] Gupta, D., Kaur, H., & Kumar, R. (2016). Detection of sink hole attack in wireless sensor network using advanced secure AODV routing protocol. *International Journal of Computer Applications*, *156*(11).

[28] Gupta, M., Kumar, R., Maheshwari, M., & Kumar, R. (2023, December). Drones and Networks: Ensuring safe and secure operations using 5g mobile network. In *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1239- 1242). IEEE.

[29] Kumar, D., & Gupta, M. (2018). Implementation of firewall & intrusion detection system using pfSense to enhance network security. *International Journal of Electrical Electronics & Computer Science Engineering*, *1*, 2454-1222.

[30] Gupta, M., Gupta, A., & Arora, S. (2022). Addressing the Security, Privacy, and Trust Issues in IoT-Enabled CPS. In *Handbook of Research of Internet of Things and Cyber-Physical Systems* (pp. 433-452). Apple Academic Press.

Reinforcement Learning Models in Stock Trading

Efe Precious Onakpojeruo[1,2] [0000-0001-8582-409X], Berna Uzun [1,3] [0000-0002-5438-8608], Fadi Al-Turjman[4]

[1] Operational Research Center in Healthcare, Department of Biomedical Engineering, Near East University, Nicosia 99138, Mersin 10, Turkey.

[2] Department of Biomedical Engineering, Near East University, Nicosia 99138, Mersin 10, Turkey

[3] Department of Mathematics, Near East University, Nicosia 99138, Mersin 10, Turkey.

[4] Artificial Intelligence Engineering Department, Research Centre for AI and IoT, AI and Robotics Institute, Near East University, Mersin 10, Turkey.

Correspondence: E.P.O.: efeprecious.onakpojeruo@neu.edu.tr

Abstract: Many researchers and professional stock traders have struggled with the specialty of figuring out stock prices. The study area of stock value prediction has piqued financial experts' interest greatly. Many speculators are adept at predicting the stock market's future direction, which allows for decent and profitable speculation. Brokers, speculators, and professional traders can provide crucial information on the stock market's future direction with the use of tremendous and strong prediction frameworks for the stock market. In this study, Reinforcement Learning (RL) models are shown to have the best predictive and trading signal accuracy for the stock market. The Preference Ranking Organization Method for Enrichment Evaluation (fuzzy PROMETHEE) multicriteria decision-making (MCDM) method was used to evaluate the RL models developed in this study. the following; accuracy, precision, consistency in making profits, simplicity in implementation, profit optimization rate, volatility rate/speed, reliability, and speed were employed to evaluate the performance of the models. The results from this study showed that with a net flow of 0.0823, DDQN was determined as the most favorable and preferred RL model in stock trading. DQN, Dueling QN, and CNN came second, third, and fourth, with net flows of 0.0364, −0.0142, and −0.0465, respectively. RNN-LSTM with a net flow of −0.0581 was the least preferred alternative. The obtained result illustrates the applicability and usage of the MCDM approach in model selection.

Keywords: Reinforcement Learning (RL), Models, Fuzzy PROMETHEE, Decision Making, Stock Trading, Stock Market, MCDM

1. Introduction

The stock market plays a critical role in the overall financial market [1]. For a long time, researchers have been trying to figure out how to get useful trading signals during the transaction process in order to maximize the gains. The financial markets' price predictions are a hot topic in today's research as researchers look for reliable models that are simple to deploy, and are consistent in predicting accurate signals for trading the stock market to optimize profits and returns. Stock price prediction is one of the most challenging tasks in the field of financial market forecasting [2,3]. Technical analysis and fundamental analysis are the two main methods used to evaluate and forecast stock prices [1,2,4]. But this has been greatly challenged. The technical analysis only looks at past market data to forecast the future. Contrarily, the fundamental analysis considers additional data such as the condition of the economy, headlines, financial statements, meeting notes from discussions between Chief executives, etc. The efficient market hypothesis is a foundation for technical analysis [1,2,4,5]. According to the efficient market hypothesis, stock prices will quickly react to market fluctuations. In reality, the price can change in a matter of milliseconds, resulting in extremely high stock liquidity [4]. Technical analysis has received a lot of attention recently for the straightforward reason that we can gather enough information by simply looking at the historical stock market, which is open to the public and well-organized, as opposed to fundamental analysis, where we must examine unstructured datasets [1,2,4,6]. Both technical and fundamental analysis performed by humans has been greatly challenged by the inability to consistently optimize profits returns and the prediction of future outcomes [1,2,4,6]. The major goal of stock trading is to maximize returns while trying to avoid high risks[6,7].

Given the rapid growth of the deep learning community, deep learning techniques have recently been the most popularly chosen techniques because it is believed that deep reinforcement learning algorithms can outperform human players and other traditional statistical learning algorithms [1,2,8]. The non-stationarity and non-linearity of the stock markets are other factors that traditional statistical learning algorithms cannot handle [1,2]. The need to create something novel has arisen as modern artificial intelligence techniques have gotten closer to how people think and act. Human cognition and learning are stimulated by deep reinforcement Learning, which combines the perception of deep learning with the capacity for decision-making of reinforcement learning. This technique can output actions directly through the simulation of a deep neural network, which can be directly controlled according to the input image without the need for external constant monitoring, and it can input vision and other high-dimensional and multidimensional resource information[1,2]. By extracting the input data from the higher dimension, a deep neural network can automatically locate the corresponding representation of the lower dimension. Integrating respondent bias into the hierarchical neural network architecture is at the heart of deep learning [1,2]. Deep Learning and reinforcement learning, therefore, have strong feature extraction and perception capabilities [1,2,9]. Its weakness is that it is incapable of making decisions [5,8,10]. Reinforcement learning can be used directly for decision-making, i.e. to decide how to buy, hold or sell any stock. But it has difficulties fully expressing perception [1,2,4–8,10,11]. Stock price prediction and stock trading are the two main uses of deep learning and reinforcement learning in the stock markets [1,2]. Price regression and stock trend prediction are the two subsets of applications for stock price prediction. In the first application, numerical prices are precisely predicted, typically using a stock's closing price or day-wise price. In the second method, the turning point of a stock price, or when it changes direction from up to down or vice versa, is typically predicted [12]. Due to the stock market's non-stationary and non-linear nature, traditional methods of stock market forecasting based on fundamental and technical analysis are typically difficult. Deep learning, both supervised and unsupervised techniques, have been utilized to combine fundamental and technical analysis for stock price prediction

and stock trading [7,8,12]. Numerous studies using reinforcement learning have been reported in literature [1,2,7,8,10–16].

It is already a known fact that reinforcement learning models can be deployed to predict the stock market, but the question is, which model is more effective and reliable? Which model is simple to deploy? Which model is stable and consistent in profit optimization? These questions have been left unanswered even though many existing works of literature have deployed different reinforcement models with their respective potentials. This has motivated us to evaluate common reinforcement learning models that have been deployed in different literature for stock trading based on well-defined reinforcement algorithms, and then, we compared them based on their performance using a hybrid multicriteria decision-making method called Fuzzy PROMETHEE, by establishing our comparison based on important criteria and factors that determine the applicability of reinforcement learning models for the prediction of the stock exchange market. This integrated approach is a unique approach that can provide a scheme for the construction of a sophisticated cognitive decision-making system for reinforcement learning models. Additionally, no existing research has integrated this approach to evaluate, compare, and rank reinforcement learning models used in trading stock.
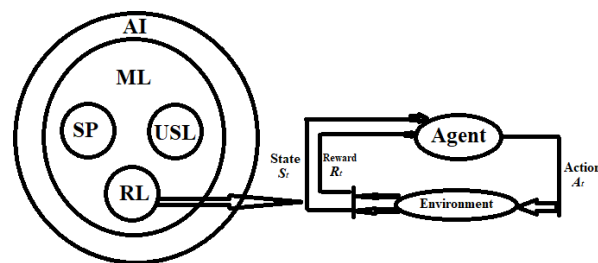

Fig. 1: The relationship between Artificial Intelligence (AI), Machine learning (ML), Supervised Learning (SL), Unsupervised Learning, and Reinforcement Learning (RL)
The diagram of the relationship between Artificial Intelligence (AI), Machine learning (ML), Supervised Learning (SL), Unsupervised Learning, and Reinforcement Learning (RL) is shown in Figure 1.

2. Reinforcement Learning in Stock Trading

Reinforcement learning as visualized in Figure 1, is a subset of machine learning [17,18]. Reinforcement learning learns how to take what kind of actions are suitable for a particular situation in order to maximize rewards to reach a specific goal [1,2]. It is different from supervised and unsupervised learning in way that supervised learning learns to predict from corresponding labels or output values associated with it, while unsupervised learning learns the underlying patterns or distributions that govern a given set of data. But in reinforcement learning, the agent (i.e. a piece of software you are training) learns through discovering actions that yield the most rewards through its experience. This is only done when agents repeatedly interact with the environment (i.e. the surrounding area where the agent interacts) [19]. Reinforcement learning has been used in playing games, wind energy optimization, industrial robotics, video game designs, fraud detection, autonomous driving, and in stock trading. Reinforcement learning has been very effective in stock trading [15,19,20]. As seen in Figure 1, consider the agent to be a stock trader, and the environment to be the stock market. The agent takes an action and is rewarded at time step t. Then, the environment changes to a new state. The agent must learn how to respond to its environment so that it can maximize its overall reward [1]. The models analyzed in this study are depicted in Figure 2.
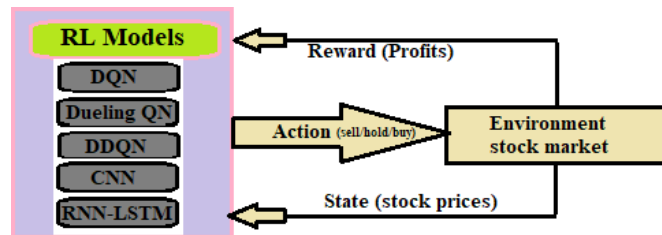
Fig. 2: Overview of RL models in stock trading

2.1. Deep Q Network (DQN)

One of the most well-known and effective reinforcement learning algorithms is Deep Q Network (DQN) [1,2,15]. It is a multi-layered neural network that generates a vector of action values for a given input state [2]. DQN is a particular type of network that employs a neural network to forecast Q value and continuously modifies the neural network to discover the maximum Q value. In the DQN, there are two neural networks: The Target Network, which is used to obtain the target value and has relatively fixed parameters, and the Current Q-Network, which assesses the current Q value. The actions (a), rewards (r), and outcomes of the next state (s, a, r, and s′) are recorded in replay memory, from which the training data is randomly taken [1,2]. Networks regularly update their parameters in response to environmental changes, and replay memory does the same. The Q value in DQN stands for the most recent learned experience. Learning the q-value function is essential to the DQN model in order to converge and successfully predict the Q value of each action in a range of states [2]. A study by [21] developed a DQN that is able to combine reinforcement learning with a class of artificial neural networks to evaluate the performance efficiency of DQN over others in games. The Atari 2600 platform which offers a diverse array of tasks, and is difficult for human players was used to evaluate the DQN agent. The DQN was compared with other efficiently performing reinforcement learning models along with a human game tester that is highly proficient in playing under controlled conditions. The study showed that the DQN method outperforms the best existing reinforcement learning methods. Another study by [22] developed a DQN for automated stock trading to make automatic decisions and achieve long-term stable profits. When DQN was compared with benchmarks of buy and hold and random action-selected DQN trade, the results showed that DQN outperforms the benchmarks. Other two classic models in deep reinforcement learning modified by the DQN models are; Double Deep Q-Network (DDQN), and Dueling Double Deep Q-Network (Dueling DDQN).

2.2 Double Deep Q-Network (DDQN)

DDQN is the combination of an old neural network and a new neural network, where the new neural network has an updated internal parameter with a time difference [2,23]. The DQN optimal Q value has been known to do the selection and evaluation of actions, this has often led to choosing an overestimated value which usually leads to an overestimation of the Q value. This overestimation of the Q value leads to an accumulated error with the increase in the number of iterations. Van Hasselt et al. [21] proposed the DDQN model to solve this overestimation problem. In the DDQN model, one of the Q networks chooses the action and the other evaluates the action. The new neural network helps to optimize the influence of error and solve the deviation problems that exist in DQN by modifying the generating of the target Q value [23]. A study by [22] showed that DDQN outperforms human beings in many fields such as playing Atari games and also in making trading decisions. When DDQN was compared to other proficient models, the results showed that the DDQN outperforms all models and even the DQN model. The DDQN model is able to discover and exploit profitable patterns more than other models. A study by [23] showed that the DDQN outperforms the DQN both in accuracy and policy quality. In trading stock, [24] proved the effectiveness of DDQN in

predicting accurate trade signals and executing trade positions. Another study by [25] also proved that DDQN is able to solve the overestimation problems of DQN and therefore, it is a more robust model in reinforcement learning. Finally, Kim et al. [26] performed a comparative study and compared the performance efficacy of the DDQN model with the DQN model in stock trading. Results from the study showed that DDQN outperforms DQN and guaranteed increased and stable trading returns.

2.3 Dueling Q-Network

This dueling network is a single Q network with two streams that substitutes the typical one-stream Q network in existing techniques like Deep Q-Networks. Without any additional supervision, the dueling network automatically generates independent estimations of the state value function and advantage function. Depending on the impact of various actions, the value functions of the state action pairs in many DRL functions vary. The size of the value function, however, may differ depending on the state in some cases. In light of this, Wang et al. [27] suggested adding Dueling DQN to the DQN network pattern. Dueling DQN combines DQN and Dueling Network [27]. The performance capacity of the dueling Q-network was presented in a study by [28] based on 10 Indian stock datasets. The dataset contained the trade histories, and trade volumes of index NIFTY 50. The result from the study shows that the dueling Q-network model outperforms the DDQN and DQN models. Another study by [29] also proved that the dueling Q-network model is an efficient model in reinforcement learning which can be deployed in intraday trading of the stock market.

2.4 Convolutional Neural Network (CNN)

Convolutional neural networks (CNNs) are one kind of deep learning network that perform best at image processing tasks [30]. CNN models can be used to generate feature map visualizations to determine where the neural network is placing its attention on the candlestick images. CNN can switch its attention from all the candles in a candlestick image to the more recent ones in the image based on an event in the trading market. Computer vision and image classification tasks have both made extensive use of this network. In order to convert a pixel to a signal and train AI to play the game, CNN is also used. The result is a classification of different signal types. A convolutional layer and a subsampling layer are the two different types of layers that make up CNN [30,31]. These various layers will connect one after the other. Convolution will be performed in the convolutional layer, and the results will be passed on to the following layer. The representation size and parameter will be decreased until the data are a one-dimensional vector in the subsampling layer. CNN has proven to be very efficient in stock trading. A study by [30] trained a CNN model to make stock predictions. Preprocessed stock data were input into the model for an improved result of the model. The result from the study indicated that the CNN model is a robust model that can be deployed in making predictions in stock trading. Another study by [31] proposed an algorithmic CNN-TA trading model using a 2-D CNN that has a high image processing capacity. When compared with other common trading systems, the result indicated better performance for the CNN-TA model in buying, holding, and selling stock instruments. Finally, a study by [32] and [33] also proved the performance efficiency of the CNN models over LSTM and other common trading strategies [34].

2.5 Recurrent Neural Network (RNN)- Long Short-Term Memory Model (LSTM)

A Recurrent Neural Network (RNN) is a sort of NN that uses previous layers/information to extract current information and predict future trends [35,36]. To predict future trends, the RNN recalls the earlier extracted and stored information, in this case, the hidden layer serves as a repository for historical data from the sequential data. Due to the difficulties in storing long-

term memory for RNNs, long short-term memory is used (LSTM) [37]. The memory line-based LSTM performed exceptionally well in forecasting scenarios including protracted data. An LSTM contains gates along the memory line that can be used to memorize previous information. The LSTM is a unique type of RNN because it can memorize data sequences [36]. A set of cells responsible for storing passed data streams must be present in every LSTM node. LSTM is one sort of RNN that can capture data from earlier stages and use it to make predictions for the future. The RNN-LSTM model has been very assistive in predicting the stock market. A research study by [38] and [39] deployed the LSTM model for predicting stock prices. The result showed that the LSTM model performed very well in generating profits. Another study by [40] presented the RNN-LSTM model to deal with anticipated stock market files. Results proved to be very efficient with the LSTM model. The performance accuracy was equated to about 97%. Finally, a research study by [41] optimized the LSTM model to prove its feasibility and performance in generating trade signals. When tested with six U.S market stocks, an average accuracy of 59.5% was obtained. The model was able to generate a total profit of $4143,233.33 with a $6,000,000 initial investment capital.

3. Methodology

The evaluation, assessment, and comparison of models have historically been based on performance evaluation metrics like mean absolute percentage error (MAPE), accuracy, F1 score, log loss, precision, recall, specificity, and so forth. None have increased the number of significant metrics or performance evaluation metrics to evaluate models that are more reliable, flexible, and less compromising. Consequently, there are several research questions, such as what happens if a decision-maker requires significant key aspects that are not covered by performance evaluation metrics.

This research study takes a novel approach to evaluate reinforcement models used in stock trading by using the Multicriteria decision-making method (MCDM) called fuzzy PROMETHEE based on certain selected criteria. This methodology has never been deployed in evaluating reinforcement learning models in stock trading. Therefore, this method is unique in its kind to this study.

Performance metrics must be used to evaluate the model's predictive ability after reinforcement learning models have been developed. Accuracy and precision in performance are the focus of these metrics. However, none mentions other crucial aspects including the model's applicability, functioning, and the effects of different factors on the model. The question of whether an "accurate model" can manage redundant and irrelevant market variables and if a precise model can be applied to a large dataset can be reduced to this. These are crucial factors for decision-makers to consider when selecting a model. Examples of these include the number of training samples needed, the effect of feature scaling, the effect of hyperparameter adjustment, and sensitivity to trivial features. MCDM approaches are crucial in this regard. One of the most important ways to choose the optimal course of action from a variety of options is to use MCDM approaches. It is a powerful tool with tremendous potential in the field of operational research that deals with how to compare a group of options using a variety of criteria [42–44]. We suggest combining and assessing the predictive, adaptability, and usability criteria of reinforcement learning models using MCDM. As a result, decision-makers will have access to resources that will help them make informed decisions when choosing the ideal model for stock trading [45].

3.1 Application of Fuzzy PROMETHEE

PROMETHEE is an MCDM technique that is user-friendly. It can be perfectly applied to real-life problem structures and is known for its efficiency in providing more preferences to decision-makers and fuzzy logic supports the decision-makers considering uncertainty based

on available criteria in the PROMETHEE model [44]. PROMETHEE 1 is a partial ranking structure and PROMETHEE II is the complete ranking structure and (both), is a technique that provides simplicity for ranking the alternatives.

In this study, several criteria were proposed and weights of importance were assigned to each criterion based on expert opinions to evaluate the alternatives. The criteria include; accuracy, precision, consistency in making profits, simplicity in implementation, profit optimization rate, volatility rate, reliability, and speed. To implement fuzzy PROMETHEE, each criterion is simplified using a linguistic scale of relevance as seen in Table 1. RL models were evaluated using the selected criteria and their importance weights as shown in Table 2 using the fuzzy linguistic scale. In addition, the Yager index was applied to de-fuzzified the fuzzy values using Equation 1.

$$(3N - a + b)/3 \tag{1}$$

where N is the center of the set, a is the distance between the center and left bound and b is the distance between the center and the right bound.

The Yager index is a recommended technique for defuzzification since it considers all possible points of the sets for this process [45]. Finally, the PROMETHEE approach was deployed using the Gaussian preference functions for each criterion.

There are 5 main steps of the PROMETHEE method to be applied for the MCDM analysis

Step 1: The preference function Pj(d) of each criteria j should be defined.
Step 2: Importance weights of each criteria wt=(w1, w2, …, wk) should be defined.
Step 3: For each of the alternative pairs a_t, $a_{t'} \in$ A, the outranking relation (π) should be determined by the:

$$\pi(a_t, a_{t'}) = \sum_{k=1}^{K} w_k . [p_k(f_k(a_t) - f_k(a_{t'}))], \ AXA \rightarrow [0,1] \tag{2}$$

where π (a, b) denotes the preference indices, which shows the preference intensity for an alternative a_t in comparison to an alternative $a_{t'}$ while counting all criteria.

Step 4: The positive and negative outranking flows should be determined as follows:

A positive outranking flow of the alternative a_t:

$$\Phi^+(a_t) = \frac{1}{n-1} \sum_{\substack{t'=1 \\ t' \neq t}}^{n} \pi(a_t, a_{t'}) \tag{3}$$

A negative outranking flow of the alternative a_t:

$$\Phi^-(a_t) = \frac{1}{n-1} \sum_{\substack{t'=1 \\ t' \neq t}}^{n} \pi(a_{t'}, a_t) \tag{4}$$

n denotes the number of the alternatives. The $\Phi^+(a_t)$ defines the strength of alternative $a_t \in$ A, while the negative outranking flow $\Phi^-(a_t)$ defines the weakness of alternative $a_t \in$ A.

PROMETHEE I determine the partial pre-order of the alternatives while PROMETHEE II determines the net ranking to alternatives. The partial pre-order of the options can be determined based on the following statements:

Via PROMETHEE I, alternative a_t is selected to alternative $a_{t'}$ ($a_t P a_{t'}$) if it satisfies either of the statements given below.

$$\Phi^+(a_t) \geq \Phi^+(a_{t'}) \ and \ \Phi^-(a_t) < \Phi^-(a_{t'})$$
$$\{\Phi^+(a_t) > \Phi^+(a_{t'}) \ and \ \Phi^-(a_t) = \Phi^-(a_{t'}) \tag{5}$$

a_t is indifferent to alternative $a_{t'}$ ($a_t I a_{t'}$) if:

$$\Phi^+(a_t) = \Phi^+(a_{t'}) \ and \ \Phi^-(a_t) = \Phi^-(a_{t'}) \tag{6}$$

And at is incomparable to $a_{t'}$ ($a_t R a_{t'}$) if:

$$\{\begin{matrix} \Phi^+(a_t) > \Phi^+(a_{t'}) \ and \ \Phi^-(a_t) > \Phi^-(a_{t'}) \\ \Phi^+(a_t) < \Phi^+(a_{t'}) \ and \ \Phi^-(a_t) < \Phi^-(a_{t'}) \end{matrix} \tag{7}$$

Step 5: The net outranking flow can be calculated for each alternative by using the Eq. (8).

$$\Phi^{net}(a_t) = \Phi^+(a_t) - \Phi^-(a_t) \tag{8}$$

Via PROMETHEE II, the complete order with net flow can be determined as:

a_t is preferred to $a_{t'}$ ($a_t P a_{t'}$) if $\Phi^{net}(a_t) > \Phi^{net}(a_{t'})$ (9)

a_t is indifferent to $a_{t'}$ ($a_t I a_{t'}$) if $\Phi^{net}(a_t) = \Phi^{net}(a_{t'})$ (10)

The higher $\Phi^{net}(a_t)$ value provides the better alternative.

The criteria that were used to evaluate alternatives during the decision-making process were carefully chosen. It is necessary to give weights in order to determine the relative significance levels of each criterion because not all criteria are equally relevant. The most crucial criteria are given more weight, while the least crucial criteria are given less weight. The fuzzy PROMETHEE approach relies on the applied criteria, weighted criteria, and defined preferences to rank particular alternatives. Different decision-makers may have different preferred alternatives and criteria and the outcomes can be updated accordingly. Diverse decision-makers may come up with different ideas based on predetermined preferences to compare, analyze, and rank outcomes when the necessity to choose criteria occurs. Expert opinion is crucial and required to obtain the most ideal solution to selection problems containing multiple parameters.

Knowing whether or not a reinforcement learning model predicts trade signals correctly is critical because it will significantly affect profit optimization. If a model is not consistent in producing correct signals and accurate rewards, a decision-maker will not want to start the deployment of the model [46] [47]. A decision-maker will also be interested in knowing the number of incorrect predictions generated by the model. When analyzing RL models used in stock trading, some of the most often utilized evaluation metrics include accuracy, reliability, precision, and consistency in optimizing profits. They serve as the primary performance indicators for the model, highlighting successfully and erroneously classified values. As a result, they were assigned a very high weight as shown in Table 1. The rate at which profits are optimized is also important because no decision-maker will like to deploy a model that generates negative returns. Thus, the profit optimization rate was assigned a high weight. Some instruments in stock trading are known to have high volatility/liquidity rates, common examples are the National Association of Securities Dealers Automated Quotations (Nasdaq 100) and the Standard & Poor's 500 Index (S & P 500). A slow model will not be able to accurately generate profitable signals. Therefore, volatility rate/speed significantly impacts model performance and was also assigned a medium weight.

Table 1. Linguistic Fuzzy Scale and assigned weights of importance to the criteria.

Linguistic scale for ranking	Triangular Fuzzy Scale	Importance ratings of criteria
Very High (VH)	(0.75, 1, 1)	Accuracy, precision, consistency in making profits, reliability
High (H)	(0.50, 0.75, 1)	Profit optimization rate
Medium (M)	(0.25, 0.50, 0.75)	Volatility rate/Speed
Low (L)	(0, 0.25, 0.50)	
Very Low (VL)	(0, 0, 0.25)	

Table 2: Data set for evaluating RL models

Aim	Max	Max	Max	Max	Max	Max
Alternatives/ Criteria	Accuracy	Precision	Consistency in making profits	Reliability	Profit optimization rate	Volatility rate/Speed
DQN [1,2,15]	VH	H	H	YES	H	M
DDQN [2,23]	VH	H	VH	YES	VH	VH
Dueling QN [27]	H	H	M	NO	H	H
CNN [30,31]	M	M	H	YES	M	H
RNN-LSTM [34,35]	M	M	M	YES	H	H

4. Results and Discussions

DDQN outperformed other models with the highest accuracy, precision, reliability, consistency in profit optimization, and speed whereas naive CNN and RNN-LSTM have the lowest accuracy, precision, profit optimization, and speed. The results obtained were satisfactory. This makes the RL models entirely appropriate and satisfactory to implement in predicting the stock market. When compared with previous studies employing the models in stock trading, our approach for ranking RL models is reliable in decision-making.

With a net flow of 0.0823, DDQN was determined as the most favorable and preferred RL model in stock trading using the fuzzy PROMETHEE method of decision-making. DQN, Dueling QN, and CNN came second, third, and fourth, with net flows of 0.0364, −0.0142, and −0.0465, respectively. RNN-LSTM with a net flow of −0.0581 was the least preferred alternative, as shown in Table 3. However, the results may differ if a different weight is assigned to the criteria.

Table 3: PROMETHEE Flow Table

Rank	Alternatives	Outranking NetFlow	Positive NetFlow	Negative NetFlow
1	DDQN	0.0823	0.0823	0.000
2	DQN	0.0364	0.0451	0.0087
3	Dueling QN	-0.0142	0.0189	0.0331

| 4 | CNN | -0.0465 | 0.0078 | 0.0542 |
| 5 | RNN-LSTM | -0.0581 | 0.0073 | 0.0654 |

Fig. 3 displays the evaluation results of the models, highlighting their advantages and disadvantages as well as the final order of available options. Each model is represented in this graph from most to least preferred. The parameters above the 0 threshold denote the advantages of the alternative, while the parameters below the 0 threshold denote the disadvantages of those alternatives. The net flow values are shown in the diagram, where options are arranged from left to right according to rank. A vertical bar made up of criteria shows the alternatives. This bar illustrates the contribution of each criterion to the final net flow value of an alternative. The height of the vertical bar, multiplied by the appropriate weight of the given criterion, displays the difference between the positive and negative preference flow. The highest positive values are displayed by the indications at the top of the vertical bar, while the highest negative values are displayed by the indicators at the bottom of the vertical bar. As a result, the PROMETHEE diagram offers a thorough picture of all options and requirements, together with an assessment of their relative weight [48].
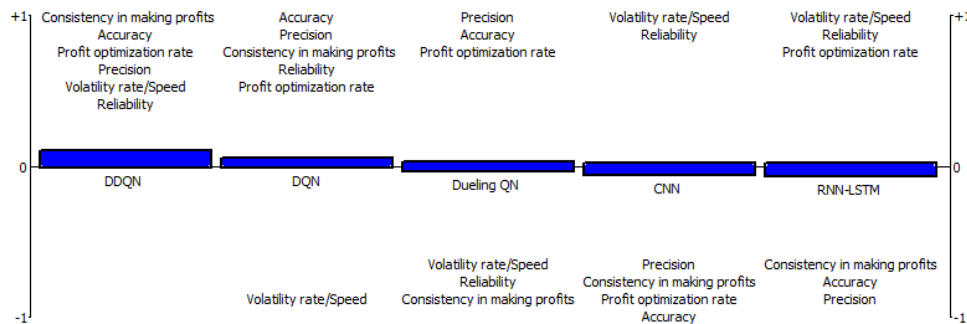

Fig. 3: PROMETHEE Evaluation ranking of RL algorithms.

5. Conclusion

This study suggests a novel method for selecting the best RL model for signal generation and prediction in stock trading. By including more variables than only the often-used key metrics, this innovative technique advances the evaluation of RL models and thereby creates a new path for model evaluation. Important factors including accuracy, precision, consistency in producing profits, ease of implementation, profit optimization rate, volatility rate/speed, reliability, and speed were considered in this study. These criteria are important, as demonstrated by the study's findings. With this study, existing literature relating to RL models for stock trading has been verified, and it is aimed to inform stock traders that are uncertain about the best RL models for predicting the stock market.

The findings of this study show that the deployed method is useful and effective for evaluating RL model performance. The result might change if the weights given to the various criteria are changed. The obtained result illustrates the applicability and usage of the MCDM approach in model selection.

References

[1] "Reinforcement Learning in Stock Trading", Accessed: Oct. 01, 2022. [Online]. Available: https://hal.archives-ouvertes.fr/hal-02306522

[2] Y. Li, P. Ni, and V. Chang, "Application of Deep Reinforcement Learning in Stock Trading Strategies and Stock Forecasting".

[3] E. Kiral and B. Uzun, "Forecasting Closing Returns Of Borsa Istanbul Index With Markov Chain Process Of The Fuzzy States," Journal of Economics, Finance and Accounting-JEFA, vol. 4, no. 1, pp. 15–24, 2017, doi: 10.17261/Pressacademia.2017.362.

[4] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, "Proximal Policy Optimization Algorithms," Jul. 2017, Accessed: Oct. 01, 2022. [Online]. Available: https://towardsdatascience.com/deep-reinforcement-learning-for-automated-stock-trading-f1dad0126a02

[5] B. M. Henrique, V. A. Sobreiro, and H. Kimura, "Literature review," Expert Syst Appl, vol. 124, pp. 226–251, Jun. 2019, doi: 10.1016/J.ESWA.2019.01.012.

[6] "Stock Market Prediction, The Planetary Barometer and How to Use It (Reprint of 1948 Edition) by Bradley, Donald A.: Very Good Soft cover (1948) Reprint | Alanpuri Trading." https://www.abebooks.com/Stock-Market-Prediction-Planetary-Barometer-Use/9811061811/bd (accessed Oct. 01, 2022).

[7] Y. Zuo and E. Kita, "Stock price forecast using Bayesian network," Expert Syst Appl, vol. 39, no. 8, pp. 6729–6737, Jun. 2012, doi: 10.1016/J.ESWA.2011.12.035.

[8] M. Hiransha, E. A. Gopalakrishnan, V. K. Menon, and K. P. Soman, "NSE Stock Market Prediction Using Deep-Learning Models," Procedia Comput Sci, vol. 132, pp. 1351–1362, Jan. 2018, doi: 10.1016/J.PROCS.2018.05.050.

[9] M. Ballings, D. van den Poel, N. Hespeels, and R. Gryp, "Evaluating multiple classifiers for stock price direction prediction," Expert Syst Appl, vol. 42, no. 20, pp. 7046–7056, Jun. 2015, doi: 10.1016/J.ESWA.2015.05.013.

[10] X. dan Zhang, A. Li, and R. Pan, "Stock trend prediction based on a new status box method and AdaBoost probabilistic support vector machine," Appl Soft Comput, vol. 49, pp. 385–398, Dec. 2016, doi: 10.1016/J.ASOC.2016.08.026.

[11] E. J. Elton, M. J. Gruber, S. J. Brown, and W. N. Goetzmann, "Modern portfolio theory and investment analysis," p. 738, Accessed: Oct. 01, 2022. [Online]. Available: https://www.wiley.com/en-us/Modern+Portfolio+Theory+and+Investment+Analysis%2C+9th+Edition-p-9781118469941

[12] B. ; Krollner, B. ; Vanstone, G. Finnie, B. Krollner, and B. Vanstone, "Financial time series forecasting with machine learning techniques A survey Financial time series forecasting with machine learning techniques: A survey Financial Time Series Forecasting with Machine Learning Techniques: A Survey," pp. 25–30, 2010, Accessed: Oct. 01, 2022. [Online]. Available: http://epublications.bond.edu.au/infotech_pubs/110

[13] F. Abtahi, Z. Zhu, and A. M. Burry, "A Deep Reinforcement Learning Approach to Character Segmentation of License Plate Images," 2015.

[14] "Reinforcement Learning For Trading Applications." https://alphaarchitect.com/2020/02/reinforcement-learning-for-trading/ (accessed Oct. 01, 2022).

[15] A. Brim and N. S. Flann, "Deep reinforcement learning stock market trading, utilizing a CNN with candlestick images," PLoS One, vol. 17, no. 2, p. e0263181, Feb. 2022, doi: 10.1371/JOURNAL.PONE.0263181.

[16] V. François-Lavet, P. Henderson, R. Islam, M. G. Bellemare, and J. Pineau, "An Introduction to Deep Reinforcement Learning," Foundations and Trends® in Machine Learning, vol. 11, no. 3–4, pp. 219–354, Dec. 2018, doi: 10.1561/2200000071.

[17] A. Leite, M. Candadai, and E. J. Izquierdo, "Reinforcement learning beyond the Bellman equation: Exploring critic objectives using evolution," pp. 441–449, Jul. 2020, doi: 10.1162/ISAL_A_00338.

[18] P. Carrera Flórez De Quiñones, V. Laparra, P.-M. Jordi, and M. Marí, "Reinforcement Learning in Stock Market".

[19] J. W. Scholars and Y. Liu, "ScholarlyCommons ScholarlyCommons Reinforcement Learning Applications in Real Time Trading Reinforcement Learning Applications in Real Time Trading," 2019, Accessed: Oct. 03, 2022. [Online]. Available: https://repository.upenn.edu/joseph_wharton_scholars/

[20] V. Mnih et al., "Human-level control through deep reinforcement learning," Nature 2015 518:7540, vol. 518, no. 7540, pp. 529–533, Feb. 2015, doi: 10.1038/nature14236.

[21] L. Chen and Q. Gao, "Application of Deep Reinforcement Learning on Automated Stock Trading," undefined, vol. 2019-October, pp. 29–33, Oct. 2019, doi: 10.1109/ICSESS47205.2019.9040728.

[22] H. van Hasselt, A. Guez, and D. Silver, "Deep Reinforcement Learning with Double Q-Learning," Proceedings of the AAAI Conference on Artificial Intelligence, vol. 30, no. 1, pp. 2094–2100, Mar. 2016, doi: 10.1609/AAAI.V30I1.10295.

[23] L. Chen and Q. Gao, "Application of Deep Reinforcement Learning on Automated Stock Trading," undefined, vol. 2019-October, pp. 29–33, Oct. 2019, doi: 10.1109/ICSESS47205.2019.9040728.

[24] "DEEP REINFORCEMENT LEARNING IN ALGORITHMIC TRADING (Part- II) | by Astarag Mohapatra | Analytics Vidhya | Medium." https://medium.com/analytics-vidhya/deep-reinforcement-learning-in-algorithmic-trading-part-ii-b78db754961c (accessed Oct. 04, 2022).

[25] M. T. Kim and K. B. Wook, "Trading Bot Implementation and Performance Comparison Using DQN and DDQN," 전기학회논문지, vol. 70, no. 1, pp. 158–167, 2021.

[26] Z. Wang, T. Schaul, M. Hessel, H. van Hasselt, M. Lanctot, and N. de Frcitas, "Dueling Network Architectures for Deep Reinforcement Learning," 33rd International Conference on Machine Learning, ICML 2016, vol. 4, pp. 2939–2947, Nov. 2015, doi: 10.48550/arxiv.1511.06581.

[27] S. Bajpai, "APPLICATION OF DEEP REINFORCEMENT LEARNING FOR INDIAN STOCK TRADING AUTOMATION A PREPRINT," 2021.

[28] L. Zhang et al., "You may also like Multi-input Convolutional Neural Network Fault Diagnosis Algorithm Based on the Hydraulic Pump Research on Image Classification Algorithm Based on Convolutional Neural Network Lihua Luo-Symptomatically Brain Tumor Detection Using Convolutional Neural Networks Stock Prediction Using Convolutional Neural Network", doi: 10.1088/1757-899X/435/1/012026.

[29] O. B. Sezer and A. M. Ozbayoglu, "Algorithmic financial trading with deep convolutional neural networks: Time series to image conversion approach," Appl Soft Comput, vol. 70, pp. 525–538, Sep. 2018, doi: 10.1016/J.ASOC.2018.04.024.

[30] S. K. Chandar, "Convolutional neural network for stock trading using technical indicators," Automated Software Engineering, vol. 29, no. 1, pp. 1–14, May 2022, doi: 10.1007/S10515-021-00303-Z/FIGURES/8.

[31] A. Moghar and M. Hamiche, "Stock Market Prediction Using LSTM Recurrent Neural Network," Procedia Comput Sci, vol. 170, pp. 1168–1173, 2020, doi: 10.1016/J.PROCS.2020.03.049.

[32] K. Narang, M. Gupta, R. Kumar and A. J. Obaid, "Channel Attention Based on ResNet-50 Model for Image Classification of DFUs Using CNN," 2024 5th International Conference for Emerging Technology (INCET), Belgaum, India, 2024, pp. 1-6, doi: 10.1109/INCET61516.2024.10593169.

[33] Z. Zou and Z. Qu, "Using LSTM in Stock prediction and Quantitative Trading".

[34] A. Pandey, "Prediction of Stock Price using RNN's LSTM-Based Deep Learning Model,"

Int J Res Appl Sci Eng Technol, vol. 9, no. 8, pp. 2469–2474, Aug. 2021, doi: 10.22214/IJRASET.2021.37791.

[35] D. Singh, M. Gupta, and R. Kumar, "BGR Images-Based Human Fall Detection Using ResNet-50 and LSTM," Lecture Notes in Networks and Systems, vol. 608, pp. 175–186, 2023, doi: 10.1007/978-981-19-9225-4_14.

[36] N. Mottaghi and S. Farhangdoost, "Stock Price Forecasting in Presence of Covid-19 Pandemic and Evaluating Performances of Machine Learning Models for Time-Series Forecasting," May 2021, Accessed: Oct. 06, 2022. [Online]. Available: http://arxiv.org/abs/2105.02785

[37] K. POTHUGANTI, "Long Short-Term Memory (LSTM) Algorithm Based Prediction of Stock Market Exchange," SSRN Electronic Journal, Jan. 2021, doi: 10.2139/SSRN.3770184.

[38] Q. Gao, Z. He, and T. Supervisor, "STOCK MARKET FORECASTING USING RECURRENT NEURAL NETWORK," 2016.

[39] E. Precious Onakpojeruo, B. Uzun, and D. Uzun Ozsahin, "Hydrogel-Based Drug Delivery Nanoparticles with Conventional Treatment Approaches for Cancer Tumors; A comparative study using MCDM Technique," 2022, doi: 10.21203/rs.3.rs-2116197/v1.

[40] E. Precious Onakpojeruo, B. Uzun, and D. Uzun Ozsahin, "Evaluation of the Treatment Alternatives for Spinal Cord Tumors Using Analytical Evaluation Models," 2022, doi: 10.21203/rs.3.rs-2009799/v1.

[41] B. Duwa, E. Precious Onakpojeruo, B. Uzun, and D. Uzun Ozsahin, "Comparative Evaluation of 3D Filaments, Used in Additive Manufacturing of Biomedical Tools; Using Fuzzy Promethee," 2022, doi: 10.21203/rs.3.rs-2020207/v1.

[42] I. Ozsahin, T. Sharif, D. U. Ozsahin, and B. Uzun, "Evaluation of solid-state detectors in medical imaging with fuzzy PROMETHEE," Journal of Instrumentation, vol. 14, no. 01, p. C01019, Jan. 2019, doi: 10.1088/1748-0221/14/01/C01019.

[43] V. Ahuja, U. Singh, M. Gupta, and R. Kumar, "A Critical Analysis of Artificial Intelligence in Stock Market Prediction: A Literature Review," NEU Journal for Artificial Intelligence and Internet of Things, vol. 1, no. 2, Oct. 2023, Accessed: Dec. 26, 2024. [Online]. Available: https://dergi.neu.edu.tr/index.php/aiit/article/view/798

[44] Di. U. Ozsahin, K. Nyakuwanikwa, T. Wallace, and I. Ozsahin, "Evaluation and Simulation of Colon Cancer Treatment Techniques with Fuzzy PROMETHEE," 2019 Advances in Science and Engineering Technology International Conferences, ASET 2019, May 2019, doi: 10.1109/ICASET.2019.8714509.

[45] D. Kumar, M. Gupta and R. Kumar, "Tata Steel Stock Forecasting Using Deep Learning," 2023 2nd International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Bali, Indonesia, 2023, pp. 33-39, doi: 10.1109/ICCMSO59960.2023.00020.

[46] Gupta, M., Kumar, R., Chaudhary, R. K., & Kumari, J. (2021, December). IoT based voice controlled autonomous robotic vehicle through google assistant. In *2021 3rd international conference on advances in computing, communication control and networking (ICAC3N)* (pp. 713-717). IEEE.

[47] Gupta, M., Kumar, R., Walia, H., & Kaur, G. (2021, October). Airlines based twitter sentiment analysis using deep learning. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE.

[48] Kumar, R., Gupta, M., Ahmed, S., Alhumam, A., & Aggarwal, T. (2022). Intelligent Audio Signal Processing for Detecting Rainforest Species Using Deep Learning. *Intelligent Automation & Soft Computing*, *31*(2).

Addressing Cybersecurity Vulnerabilities with Cloud Security

Ramiz Salama[1*], Fadi Al-Turjman[2, 3]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT,
Near East University Nicosia, Mersin 10, Turkey

[2]Artificial Intelligence, Software, and Information Systems Engineering Departments, AI and Robotics Institute,
Near East University, Nicosia, Mersin10, Turkey

[3]Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin10, Turkey

*Corresponding author Email: ramiz.salama@neu.edu.tr

Abstract: In today's increasingly digital environment, the rapid adoption of cloud technology has transformed data storage, access, and management. However, this transition has created new cyber security weaknesses, exposing private information to prospective assaults and invasions. This study looks at the major security concerns that cloud-based enterprises must deal with, including insider threats, sophisticated persistent attacks, data breaches, and misconfiguration difficulties. We explore how these vulnerabilities develop, how they affect an organization's security posture, and the unique characteristics of cloud infrastructures that make these risks more and less severe. We look at a number of cloud security best practices and solutions to these issues.These include data encryption, multi-factor authentication, identity and access management (IAM), zero-trust architecture, and continuous monitoring. We also highlight the importance of regulatory compliance and governance mechanisms in enhancing cloud security. The research also examines upcoming technologies such as AI- driven threat identification and automated remediation, which have the potential to improve cloud security. Organizations may successfully preserve their data and maximize the promise of cloud computing by installing strong security measures and taking a proactive approach. This study underlines the importance of an organized, multi-layered security strategy to secure digital assets and maintain resilience in an ever-changing cyber world.

Keywords: cloud computing, threat detection, remediation techniques, cybersecurity vulnerabilities, cloud security.

1. Introduction

The rise of cloud computing has caused a fundamental shift in how businesses handle their IT operations. Cloud services enable organizations to grow quickly without having to make large investments in physical infrastructure by providing on-demand access to computer resources. This change has been essential in encouraging efficiency and creativity across numerous industries. Businesses must address the unique cybersecurity challenges posed by the cloud migration in order to protect sensitive data and maintain consumer trust. Cloud computing has drastically changed how companies manage their IT resources since it provides unparalleled scalability, flexibility, and cost savings. However, there are significant security dangers associated with these benefits. Due to their shared nature and complexity, cloud systems pose several cybersecurity vulnerabilities that may lead to data breaches and service disruptions. This study examines the many types of cloud system vulnerabilities and looks at workable remedial methods to safeguard data and apps [1–5]. By looking at case studies and recent research, this report analyzes the evolving threat landscape and provides best practices for lowering risks associated with cloud-based infrastructures.

Figure.1 Top Cloud Security Issues: Threats, Risks, Challenges & Solutions

1.1 The Development of Cloud Computing

Cloud computing has evolved from simple storage solutions to complex, multifaceted systems that offer a range of services, including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).One characteristic of this development has been the emergence of cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), which offer a wide range of tools and services designed to satisfy various business needs. The usage of cloud computing has allowed organizations to expand their global reach, reduce operating costs, and operate more effectively.

1.2 Security Concerns in Cloud Environments

Despite all of the advantages of cloud computing, there remain significant cybersecurity threats. To protect sensitive data and maintain system integrity, organizations need to address the additional attack vectors and vulnerabilities brought about by the shift from traditional on-

premises infrastructure to cloud-based solutions.Because of their shared responsibility model, complexity, and dynamic nature, cloud environments pose unique security challenges.

1.3 Complexity and Dynamic Nature

Cloud infrastructures are inherently complex due to the several layers of networking, storage, and virtualization technologies they contain. Because cloud environments are dynamic and resources are constantly being added, removed, and modified, misconfigurations and security vulnerabilities may arise. Businesses must have a solid understanding of their cloud architecture because cloud services are interconnected and a problem in one area could affect the entire system.

1.4 The Shared Responsibility Model

The shared responsibility paradigm in cloud security describes how security responsibilities are divided between cloud service providers and their customers. While providers are responsible for safeguarding the underlying infrastructure, customers are responsible for protecting their data, apps, and user access within the cloud [6–10]. Misunderstandings and security breaches could result from improper understanding and application of this paradigm. Organizations must ensure they fully understand their responsibilities and implement robust security procedures to protect their assets.

1.5 The Significance of Cloud Security

In the contemporary digital era, one of an organization's most valuable assets is data. Because cloud computing is so widely used, large amounts of sensitive data are now handled and kept there, making it a favorite target for hackers. Data breaches can result in significant financial losses, reputational damage, legal ramifications, and a reduction in customer trust [11–15]. As a result, cloud environment security is crucial for maintaining business continuity and safeguarding data.

2. Number of Previous Articles

• *Misconfigurations and Data Breaches:* Data breaches remain a top concern for cloud users. Configuration problems, such as unprotected storage buckets and insufficient access limitations, are frequently cited as the primary causes of data disclosure. For example, a 2023 study by Johnson et al. found that 45% of data breaches in cloud environments were due to misconfigurations.

• *Insecure APIs:* Application Programming Interfaces (APIs) play a major role in cloud service integration and interaction. Attackers might, however, leverage weak APIs as entry points. Patel's (2024) recent research highlights the importance of developing and deploying APIs securely to prevent unauthorized access.

• *Internal Dangers:* Insider threats continue to be a major worry in cloud systems. Employees or contractors with access to confidential data may inadvertently or intentionally compromise security. A Thompson (2021) study emphasizes the need for careful access management and monitoring to lessen insider threats.

• *New Dangers:* New attack techniques and vulnerabilities are always emerging, resulting in a constantly shifting danger landscape. Williams (2023) discusses the rise in sophisticated attacks that target cloud infrastructure, including ransomware and advanced persistent threats (APTs).

• *Case Studies:* Up-to-date case studies provide useful details on real security incidents and their consequences. For example, the 2019 Capital One data breach exposed the private information of over 100 million customers due to a misconfigured firewall.

How concerned are you about the security of public clouds?

95%

of organizations are moderately to extremely concerned about cloud security

35%	41%	19%	4%	1%
Extremely concerned	Very concerned	Moderately concerned	Slightly concerned	Not at all concerned

Figure.2 Public cloud security concern rate (Cybersecurity Insiders), cloud vulnerabilities

3. Supplies and Methods
3.1 Method

By carefully examining the corpus of recent literature and case studies, this work employs a qualitative research methodology to identify common vulnerabilities and repair methods in cloud computing [16]. The research focuses on reviewing reports from cybersecurity organizations, academic journals, and industry publications to gather knowledge about current threats and best practices.
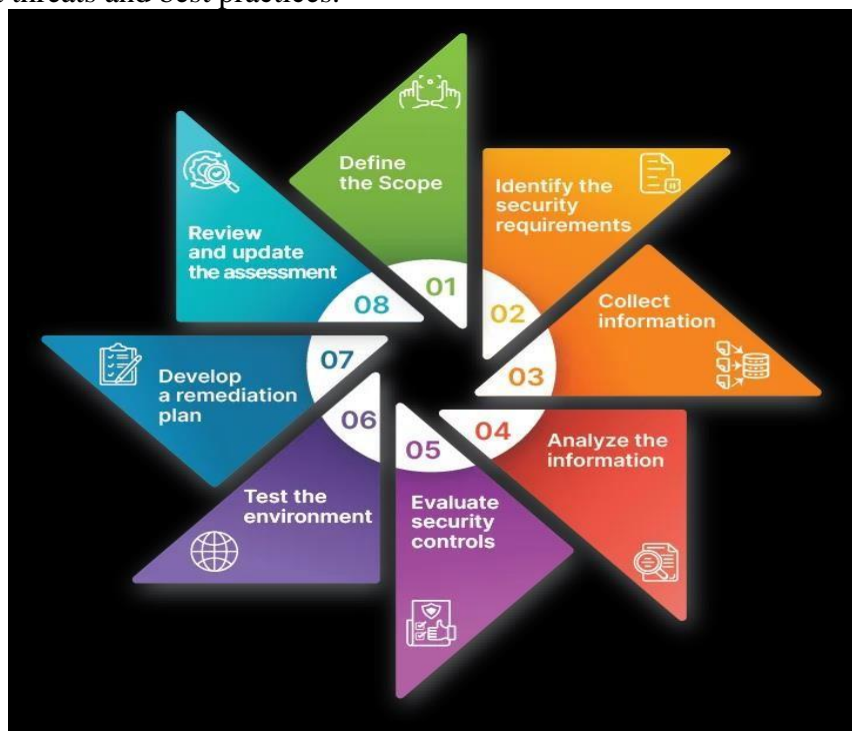

Figure 3. The Cloud Security Assessment Process

3.2 Research Tools and Frameworks

NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) provides a well-known framework for improving cybersecurity practices [17]. The assessment and enhancement of cloud security measures are guided by this framework.

CVE Database: The Common Vulnerabilities and Exposures (CVE) database is searched to identify current vulnerability disclosures and trends. This database contains a comprehensive list of known cybersecurity vulnerabilities.

Security Audits and Assessments: A range of security audit approaches and processes are used to evaluate the security posture of cloud infrastructure and identify any vulnerabilities.

4. Crucial Elements Influencing Cloud Adoption

• *Flexibility and Scalability:* Businesses may easily adapt their IT assets to meet demand thanks to cloud services' unparalleled scalability. This flexibility may be quite helpful for businesses that cope with fluctuating workloads or seasonal variations in traffic [18].

• *Cost Savings:* By doing away with the need for physical infrastructure and the associated maintenance costs, cloud computing helps organizations reduce their operating and capital expenditures. The pay-as-you-go pricing approach further increases cost effectiveness by aligning costs with real consumption [19] .

• *Speed and Agility:* The cloud's rapid resource provisioning and app delivery enable businesses to grow and respond to market shifts more rapidly. This adaptability is a crucial competitive advantage in the fast-paced business world of today.

• *Collaboration and Accessibility:* Cloud services enable remote teams to work together effortlessly by providing easy access to shared resources and apps from any location with an internet connection. This ability is particularly important in a workforce that is growing increasingly distant and global.
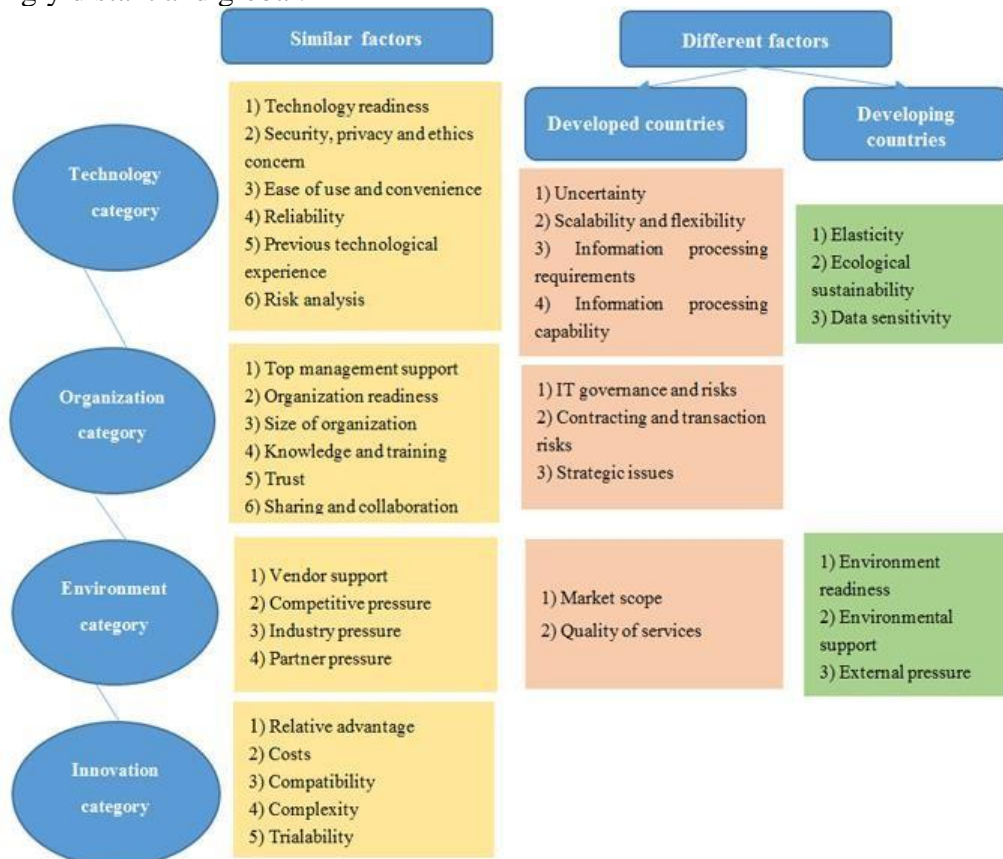

Figure 4. Factors affecting the adoption of cloud computing by firms.

5. Risks and Challenges of Cloud Computing

Despite all of its benefits, cloud computing comes with a unique set of risks and challenges that companies must handle to ensure security and compliance [20–22]. The complexity and dynamic nature of cloud infrastructures make these challenges worse and may create vulnerabilities that hackers could exploit.

6. Common Security Problems

1. Data Privacy and Protection: Businesses place a high value on data privacy and protection because sensitive data is handled and kept in the cloud. Following laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) makes managing cloud data even more difficult.

2. Regulatory Compliance: Companies operating in regulated industries, such as healthcare and finance, must ensure that their cloud deployments comply with industry-specific regulations and standards. Failure to comply with compliance duties may result in severe legal and financial consequences.

3. Multi-tenancy risks: Cloud services are often multi-tenant, meaning that multiple businesses use a single physical infrastructure. This system saves money, but it also raises security concerns because defects in one tenant's surroundings could affect others.

4. Vendor Lock-In: Businesses that depend on a single cloud provider may encounter vendor lock-in, which makes switching providers or putting a multi-cloud strategy into practice difficult. This dependence might hinder flexibility and innovation since companies may be constrained by the capabilities and limitations of the service they have chosen. The cybersecurity threat landscape is always evolving due to the daily emergence of new threats and attack techniques. The methodologies used by cybercriminals to target cloud infrastructures and exploit vulnerabilities are becoming increasingly sophisticated.

New Risks

• Ransomware Attacks: Ransomware attacks, in which hackers encrypt an organization's data and demand payment to unlock it, have increased in frequency in cloud environments. Particularly if backup data is also affected, these attacks have the potential to cause significant disruptions in operations and monetary losses.

• Advanced Persistent Threats (APTs) are highly targeted attacks designed to get continuous access to a network in order to steal sensitive information. The massive amounts of data and resources in cloud systems attract APTs.

• *Insider Threats:* Insider threats pose a significant risk to cloud security, whether they are intentional or not. Employees or contractors with permission to use cloud resources may accidentally reveal personal data or actively breach security for personal gain.

• *Misconfigurations and Human Error:* In cloud environments, data breaches are often caused by misconfigurations, such as improperly configured access controls or unprotected storage buckets. Human error, which often results from ignorance or insufficient training, can also lead to security problems.

The Value of Robust Cloud Security

Given these risks and challenges, organizations need to have robust cloud security measures in place to protect against unwanted access and exploitation of their data and systems. Effective cloud security requires a holistic approach that includes technical solutions, policies, and practices meant to lower risks and increase resilience.

Figure 5 Here are the most common types of security incidents that pose a threat to organizations' security and security incident management measures.

7. Identity management and access control

Are crucial components of cloud security [23]. Strong access controls and identity management systems must be put in place to guarantee that only authorized users can access cloud resources [24–29]. This includes regular user authorization audits, multi-factor authentication (MFA), and the implementation of role-based access controls (RBAC) .

• Encrypting data: Data must be encrypted both in transit and at rest to prevent unauthorized access to private information [30]. A secure encryption key management system must include regular key rotation and strict access restrictions [31].

8. Results and Discussion
8.1 Findings

The report identifies some significant issues that are commonly seen in cloud environments:

Inadequate encryption, loose access controls, and improper settings are common causes of data breaches. Financial and reputational damage can result from data breaches. APIs that are not sufficiently secured can pose a risk, even if they are essential for connecting cloud services.Common issues include inadequate input validation, inadequate authorization and authentication, and inadequate logging and monitoring.

Insider Dangers: Insiders who have been granted permission to access cloud resources pose significant risks. These dangers could be purposeful, like data theft or sabotage, or inadvertent, such accidental data disclosure.

Configuration errors: Cloud services such as storage buckets, databases, and virtual machines may be set up incorrectly, exposing personal data and making systems vulnerable to invasions.

Focused, extremely skilled attacks known as Advanced Persistent Threats, or APTs, seek to gain continuous access to a network. Cloud environments might be attractive targets due to their amount of data [32][33].

8.2 Talk

The findings indicate that while cloud computing offers numerous advantages, there are still some security concerns that require attention. Numerous vulnerabilities are mostly caused by human error and configuration, which emphasizes the need for comprehensive security protocols and employee training. Additionally, AI and ML show promise in automating threat detection; nevertheless, careful application is required to avoid creating new security issues.

The shared responsibility model of cloud security is crucial because it specifies the security obligations of both clients and cloud service providers. Both sides must understand their responsibilities and cooperate in order to ensure a secure cloud environment. While service providers are frequently in charge of protecting the underlying infrastructure, customers are responsible for safeguarding their data and apps within the cloud.

9. Conclusion

Because cloud computing offers enterprises flexibility, scalability, and cost savings, it continues to transform IT infrastructure. However, these benefits do come with a responsibility to reduce the associated cybersecurity risks. By understanding common hazards and implementing effective repair processes, businesses can protect their assets and maintain customer trust. Effective cloud security requires a multi-layered approach that includes technology solutions, clear policies, and ongoing education and training. By integrating AI and ML into cloud security protocols, there are intriguing prospects to enhance threat detection and response capabilities. Care must be taken while using these technologies to avoid introducing new vulnerabilities. Future research should focus on developing complex security frameworks that include AI technology to manage threats in real time. Additionally, as the threat landscape evolves, businesses need to stay vigilant and adapt their security procedures to address new threats.

Referencess

[1] Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2(1), 129-171.

[2] Alquwayzani, A., Aldossri, R., & Frikha, M. (2024). Prominent Security Vulnerabilities in Cloud Computing. International Journal of Advanced Computer Science & Applications, 15(2).

[3] Raja, V. (2024). Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 4(1), 121-144.

[4] Raja, V. (2024). Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 4(1), 121-144.

[5] Ahmadi, S. (2024). Challenges and Solutions in Network Security for Serverless Computing. International Journal of Current Science Research and Review, 7(01), 218-229.

[6] Kumar, S., Dwivedi, M., Kumar, M., & Gill, S. S. (2024). A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services. Computer Science Review, 53, 100661.

[7] Agarwal, P., & Gupta, A. (2024, May). Cybersecurity strategies for safe erp/crm implementation. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.

[8] Ajiga, D., Okeleke, P. A., Folorunsho, S. O., & Ezeigweneme, C. (2024). Designing cybersecurity measures for enterprise software applications to protect data integrity.

[9] Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. Journal of medical internet research, 26, e46904.

[10] Shafik, W. (2024). Dissecting the Role of Women in Cybersecurity and Information Technology: A Medical Perspective. In Next-Generation Cybersecurity: AI, ML, and Blockchain (pp. 325-350). Singapore: Springer Nature Singapore.

[11] Devipriya, A., Rosaline, R. A. A., Prabhu, M. R., Nancy, P., Karthick, V., & Kadumbadi, V. (2024, April). Algorithmic Approaches to Securing Cloud Environments in the Realm of Cybersecurity. In 2024 10th International Conference on Communication and Signal Processing (ICCSP) (pp. 697-702). IEEE.

[12] Moses, O. O., & Ehizuenlen, E. P. (2024). The Future of Cyber Security: Examining the Security Challenges and Trends in Smart Technology. Journal of Energy Technology and Environment, 6(1), 56-67.

[13] Zhang, Y., Xu, X., & Shi, Y. (2024). Construction and Analysis of Network Cloud Security Situation Awareness System Based on DBN-DE Algorithm. Journal of Cyber Security and Mobility, 439-460.

[14] Khoshaba, F. S., Askar, S., Hamad, S., & Maghdid, S. (2024). Cyber Security Challenges in Industry 4.0: A Review. Indonesian Journal of Computer Science, 13(2).

[15] Mohamed, M., Elmor, A., Smarandache, F., & Metwaly, A. A. (2024). An efficient superhypersoft framework for evaluating llms-based secure blockchain platforms. Neutrosophic Sets and Systems, 72, 1-21.

[16] Andrews, L. J. B., Alagappan, A., Sarathkumar, D., Fathima, M., Venkatachary, S. K., Rajeshkanna, R., & Raj, R. A. (2024, February). Investigations on Cyber Security Vulnerability using Distribution Analysis. In 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) (pp. 1-6). IEEE.

[17] Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2024). Thriving in the era of hybrid work: raising cybersecurity awareness using serious games in industry trainings. Journal of Systems and Software, 210, 111946.

[18] Nisha and M. Gupta, "A novel scheme to manage the e-healthcare system using cloud computing and the internet of things," Computational Intelligence in Healthcare, pp. 81–97, Feb. 2023, doi: 10.1201/9781003305347-5.

[19] H. Sharma, R. Kumar and M. Gupta, "A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/INOCON57975.2023.10101044.

[20] Singh, N., Buyya, R., & Kim, H. (2024). IoT in the Cloud: Exploring Security Challenges and Mitigations for a Connected World. arXiv preprint arXiv:2402.00356, 1-27.

[21] Memon, S., Memon, S., Das, L., & Memon, B. R. (2024, January). Cyber Security Risk Assessment Methods for Smart Healthcare. In 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) (pp. 1-6). IEEE.

[22] Takale, D. G., Mahalle, P. N., & Sule, B. (2024). Cyber Security Challenges in Generative AI Technology. Journal of Network Security Computer Networks, 10(1), 28-34.

[23] "Kumar, G., Saini, D. K., & Cuong, N. H. H. (Eds.). (2020). Cyber Defense Mechanisms: Security, Privacy, and Challenges. CRC Press.

[24] Tihanyi, N., Ferrag, M. A., Jain, R., Bisztray, T., & Debbah, M. (2024, September). CyberMetric:

A Benchmark Dataset based on Retrieval-Augmented Generation for Evaluating LLMs in Cybersecurity Knowledge. In 2024 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 296-302). IEEE.

[25]   Rahman, A., Ashrafuzzaman, M., Jim, M. M. I., & Sultana, R. (2024). Cloud Security Posture Management Automating Risk Identification and Response In Cloud Infrastructures. Academic Journal on Science, Technology, Engineering & Mathematics Education, 4(03), 151-162.

[26]   Radanliev, P. (2024). Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. Frontiers in Blockchain, 7, 1359130.

[27]   Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future Horizons: AI- Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. International Journal of Multidisciplinary Sciences and Arts, 3(1), 242-251.

[28]   Suriya, B. J., Amarnath, B. K., Raghuraman, A. R., & Arumugam, C. (2024, March). Cloud Security: Upgradation in CSPM Configuration Setting. In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-4). IEEE.

[29]   Tripathi, R., & Tripathi, S. (2024). Frauds and Cyber Security Issues in the Finance Sector. In Transforming the Financial Landscape With ICTs (pp. 165-189). IGI Global.

[30]   H. Bawa, P. Singh, and R. Kumar, "An Efficient Novel Key Management Scheme for Enhancing User Authentication in A WSN," International Journal of Computer Network and Information Security, vol. 5, no. 1, pp. 56–64, Jan. 2013, doi: 10.5815/ijcnis.2013.01.07.

[31]   M. Gupta, A. Gupta, and S. Arora, "Addressing the Security, Privacy, and Trust Issues in IoT-Enabled CPS," Handbook of Research of Internet of Things and Cyber-Physical Systems, pp. 433–452, Jun. 2022, doi: 10.1201/9781003277323-22.

[32]   Gupta, D., Kaur, H., & Kumar, R. (2016). Detection of sink hole attack in wireless sensor network using advanced secure AODV routing protocol. International Journal of Computer Applications, 156(11).

[33]   Bawa, H., Singh, P., & Kumar, R. (2012). An efficient novel key management scheme using nchoosek algorithm for wireless sensor networks. International Journal of Computer Networks & Communications, 4(6), 121.

Personalized Learning in Education through AIoT: Adaptive Systems for Student Engagement and Performance

Anupriya Sharma Ghai[1], Ramesh Chander Sharma[1], Zehra Altinay[2], Fahriye Altinay[3], Gokmen Dagli[4], Sanjay Jasola[1]

[1]Department of Computer Applications, Graphic Era Hill University, Dehradun - 248002, India,
[2]Department of Educational Sciences, Societal Research and Development Center, Near East University, Nicosia
[3]Department of Computer Education and Instructional Technology, Societal Research and Development Center, Near East University, Nicosia
[4]Faculty of Education, University of Kyrenia

anupriya@gehu.ac.in, rcsharma@gehu.ac.in, zehra.altinaygazi@neu.edu.tr, fahriye.altinay@neu.edu.tr, gokmen.dagli@kyrenia.edu.tr, sjasola@yahoo.com

Abstract : With the integration of artificial intelligence (AI) and the Internet of Things (IoT), AIoT has transformed education and specifically improved student engagement and subsequent academic performance through adaptive systems. AIoT is a fusion of the processing powers of artificial intelligence and the connectivity of the IoT to create interactive learning experiences that adjust in real-time based on the needs of different learners. This article outlines how AIoT contributes to active and inclusive learning as evidence has illustrated that adaptive systems note student behaviour and performance to provide customized assistance. They motivate the students by changing the content and teachings with real-time feedback, thereby improving their learning. AIoT can make education more equitable by providing personalized learning experiences without geographical or socioeconomic barriers. It fosters digital literacy and essential 21st-century skills, preparing students for future workplaces and highlighting its long-term role in education. The following review will detail AIoT's continued impact on education and the evolution of how its birth will transform student-centric learning to open access to quality education further everywhere.

Keywords: Artificial Intelligence of Things, personalized learning, adaptive systems, student engagement, academic performance, educational technology

1. Introduction

Personalized learning refers to an educational approach that tailors instructional content, pace, and delivery methods to meet individual students' unique needs, learning styles, and preferences. Unlike traditional, one-size-fits-all teaching, personalized learning seeks to optimize each learner's experience and outcomes by recognizing and adapting to diverse learning needs. Adaptive systems play a crucial role in this approach, using real-time data to adjust content and engagement strategies based on student's performance, preferences, and areas of improvement [1]. This responsiveness fosters a more inclusive and engaging learning environment, enhancing

student motivation and academic performance by addressing personal challenges and strengths, a strategy increasingly favoured in higher education [2].

AIoT represents a technological advancement that integrates AI's decision-making abilities with IoT data collection capabilities. In educational settings, AIoT encompasses a range of tools and platforms—from wearable sensors and smart classrooms to predictive learning algorithms—that continuously gather and analyze data on students' activities, behaviors, and performance. Through machine learning and real-time data processing, AIoT systems create individualized learning paths and provide educators with insights for immediate intervention and support, thereby enhancing personalized education [3]. These adaptive and responsive systems enable data-driven teaching methods, allowing students to engage with material at their optimal level of challenge and understanding.

AIoT is becoming indispensable for developing student-centered and flexible learning environments, offering solutions to cater to the heterogeneous nature of learning needs. By leveraging AIoT-driven insights, educators can make informed decisions, continuously adapting content and instructional methods to align with each student's progress and engagement levels. This approach not only enhances student learning outcomes but also promotes an inclusive, student-centered atmosphere in which students feel more supported and valued [4].Through AIoT, learning environments evolve beyond static frameworks, enabling dynamic educational experiences that are both interactive and aligned with individual student goals, ultimately advancing the quality and accessibility of education in a digital age.

2. Understanding AIoT in Education

In educational contexts, AIoT comprises four key components: AI algorithms, IoT devices, data processing units, and network infrastructure. AI algorithms analyze data to identify patterns, make predictions, and customize learning experiences [5]. IoT devices—such as smart sensors, wearables, and interactive displays—gather continuous data on students' behaviors, engagement, and performance. Data processing units process and organize this data, enabling seamless communication between devices and systems. Finally, network infrastructure ensures the real-time transfer of data, facilitating uninterrupted connections among devices, learning platforms, and educational applications [6]. Together, these components create a cohesive system that adapts dynamically to student needs, setting the foundation for highly personalized learning environments.

AIoT's capacity to continuously monitor and analyze data allows educational systems to generate valuable insights into students' progress, engagement, and learning behaviors. These data-driven insights provide educators with actionable information, such as identifying students who may require additional support or are excelling and ready for advanced material [7]. Automated interventions, driven by AI algorithms, can adjust content difficulty, provide instant feedback, or recommend supplementary resources, catering to individual learning paces without educator intervention. Additionally, real-time responses enable systems to react promptly to students' needs—for example, by modifying content delivery or assessing engagement levels to prevent

potential learning fatigue. AIoT's responsiveness supports more efficient, effective learning processes, optimizing student outcomes while reducing the cognitive load on educators.

2.1 AIoT in Reshaping Educational Experiences

AIoT has the potential to redefine educational experiences by making learning environments more interactive, accessible, and student-centered. Increased interactivity is achieved as AIoT devices, such as augmented reality headsets and adaptive learning platforms, allow students to engage in immersive, hands-on activities, which cater to different learning preferences and stimulate deeper engagement [8]. Moreover, AIoT-driven accessibility features, such as language translation tools and real-time captioning, can reduce learning barriers, providing equitable access to educational resources for students with disabilities or language challenges. By reshaping the structure of learning experiences to be more interactive and adaptive, AIoT promotes inclusive education, where every student has the opportunity to engage in meaningful, personalized learning.

4. Adaptive Systems for Student Engagement

Adaptive learning systems are designed to adjust instructional content and methodologies to suit individual student needs. These systems employ algorithms and real-time data to continuously evaluate students' understanding and learning pace, allowing for dynamic modifications in content delivery. For example, if a student exhibits difficulty in a specific topic, the system may present additional exercises, offer multimedia resources for diverse learning preferences, or break down complex information into simpler segments. Alternatively, when students demonstrate mastery, adaptive systems can introduce more challenging material or facilitate peer-to-peer interactions for collaborative learning [9]. By responding to students' unique progress, adaptive learning systems foster personalized educational experiences that increase engagement, accommodate different learning styles, and improve comprehension.

IoT devices play a pivotal role in monitoring student engagement through sensors that track specific behaviors, such as eye movement, posture, and device interaction. In smart classrooms or remote learning setups, sensors embedded in devices like cameras, wearables, and computers capture and analyze behavioral indicators in real-time. For instance, eye-tracking sensors gauge where a student's gaze is focused, providing insights into attention and engagement levels. Posture sensors in chairs or wearables monitor physical fatigue or restlessness, while device interaction metrics—such as the frequency and intensity of clicks, keystrokes, or screen touches—provide information on engagement patterns. These data points allow teachers and adaptive learning systems to detect signs of disengagement, such as prolonged inactivity or signs of frustration [10]. By capturing detailed, nuanced engagement data, IoT enables a deeper understanding of each student's attentiveness and overall engagement, offering opportunities for timely intervention.

5. Improving Student Performance with AIoT

AIoT technology supports targeted learning interventions by continuously monitoring and assessing students' performance in real time. Through IoT devices, data on students' progress, response accuracy, and interaction patterns is collected and processed by AI algorithms [11]. This analysis identifies specific learning needs, allowing AIoT systems to provide immediate,

personalized support. For example, if a student consistently struggles with certain concepts, AIoT may recommend focused resources, such as tutorials or visual aids, to address these areas. Additionally, for students showing signs of disengagement or fatigue, AIoT systems might introduce shorter, interactive tasks to re-engage them [12]. By using performance data to target interventions adaptively, AIoT technology enhances the learning process and promotes mastery by addressing challenges as they arise, ultimately leading to improved academic outcomes [13].

6. Case Studies and Practical Examples

In educational settings, AIoT has facilitated the creation of "smart campuses" and has led to enhanced student experiences through personalized learning, optimized instructional practices, and real-time monitoring of resources [14]. Below are real-world applications of AIoT in education, including examples of institutions leveraging these solutions to improve learning outcomes and engagement.

6.1. Smart Classrooms: Enhancing Learning Environments

The University of California, Berkeley, has implemented AIoT-driven environmental controls in several classrooms to optimize air quality, temperature, and lighting based on student presence and time of day. This has created more comfortable learning environments and reportedly improved student focus and comfort levels during sessions.

Research has shown that when students are physically comfortable, their engagement and comprehension levels increase. By creating an optimized, distraction-free setting, smart classrooms help students concentrate, leading to improved academic performance [15].

6.2. Student Monitoring and Personalized Learning Support

At the Indian Institute of Technology (IIT) in Delhi, an AIoT-enabled platform tracks students' real-time engagement, adapting content to students based on attention patterns. This is particularly beneficial for students who require additional support, as the AI component flags when students are struggling and automatically recommends resources or schedules consultations [16]. This personalized approach has increased engagement levels by adapting the learning experience to students' immediate needs. Data-driven insights allow instructors to provide targeted assistance, increasing retention rates and academic performance.

6.3. Smart Libraries: Resource Management and Enhanced Learning Spaces

Singapore Management University (SMU) has developed a smart library where students use IoT-enabled cards to find study spaces, check the availability of resources, and receive AI-driven recommendations on relevant reading materials based on their course profiles [17]. AIoT-enabled smart libraries optimize resource utilization, streamline access, and promote effective study habits. Students benefit from having easier access to resources, which enhances academic support and enriches the learning experience.

6.4. AIoT in MOOC Platforms: Personalized Content Delivery

In collaboration with Georgia Tech, Udacity has introduced AIoT-enabled features that track student progress and send reminders or additional resources to students who fall behind. This has

led to a noticeable increase in completion rates. The AIoT-enabled MOOC environment provides timely feedback and support, keeping students on track and enhancing completion rates. Personalized content recommendations make learning more relevant, aiding in knowledge retention and skill acquisition [18].

6.5. Real-Time Analytics for Educators and Administrators

At Stanford University, AIoT platforms have been implemented to aggregate data on student performance and engagement, allowing faculty to adapt teaching strategies in real time. This dynamic adjustment has improved learning outcomes, particularly in high-difficulty courses. Real-time insights enable institutions to make data-informed decisions, adapting resources and instructional approaches based on current needs. This feedback loop promotes effective teaching strategies and identifies areas where students may need more support [19].

7. Challenges and Consideration

AIoT integration into education presents transformative opportunities, but significant challenges must be managed to ensure ethical, secure, and equitable usage. Addressing issues such as data privacy, security, technical limitations, and equity is essential to maximize the potential of AIoT systems in education while safeguarding student rights and access.

Data privacy and security represent a core concern in AIoT-based education systems. These systems collect extensive student data, including academic records, behavioral patterns, and engagement metrics, to create personalized learning experiences [20]. However, such data can be sensitive and vulnerable to misuse if not properly secured. Legal frameworks like the General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA) provide foundational guidelines for data protection, yet implementing these within complex AIoT infrastructures can be challenging [21]. Schools and universities must ensure that student data is securely stored, accessed only by authorized personnel, and anonymized whenever possible to protect identities. Additionally, secure communication protocols and regular audits can help maintain compliance and minimize risks, but these requirements may be financially and technically burdensome for many institutions [22].

Implementing AIoT in education often requires advanced technological infrastructure, including high-speed internet, compatible devices, and reliable cloud-based systems. Many educational institutions, particularly in developing regions, face challenges in establishing this infrastructure due to limited budgets and a lack of technical expertise [23]. Furthermore, the sophistication of AIoT systems demands ongoing maintenance and updates, which can strain the resources of smaller institutions. For example, IoT devices require consistent connectivity and compatibility with existing systems, while AI components may need specialized software and hardware that not all institutions can afford [24]. Addressing these infrastructural gaps is essential for widespread AIoT adoption, and partnerships with governments or private sectors may play a crucial role in providing necessary resources [25].

8. Future Trends in AIoT-Driven Personalized Learning

Emerging trends in personalized education are set to be reshaped by autonomous learning systems and AI-driven tutors [26]. These technologies offer tailored instruction by analyzing student performance, engagement, and learning styles in real-time, allowing the system to adjust lesson difficulty, pacing, and resources to suit each individual's needs. For instance, if a student excels in a topic, the system introduces advanced content; if they encounter challenges, it provides targeted support. AI-based tutors also play a vital role engaging students in interactive dialogue, providing explanations, and encouraging active participation [27] [28]. Together, these tools foster a more adaptive, responsive learning environment, enhancing engagement and improving outcomes across diverse learning profiles.

9. Conclusion

In conclusion, the integration of AIoT in education represents a significant advancement, offering the transformative potential to personalize learning experiences, improve student engagement, and optimize educational outcomes. AIoT's adaptive systems, which respond to individual student needs and learning styles, are poised to reshape traditional educational models by providing targeted support and promoting active participation. By enhancing the ability to monitor, analyze, and respond to student progress in real time, AIoT enables educators to create more engaging, responsive, and inclusive learning environments. This article has highlighted both the considerable benefits and the challenges posed by AIoT, from technical and infrastructural requirements to ethical considerations surrounding data privacy and equity. As AIoT continues to evolve, institutions need to approach its implementation with responsibility, ensuring that adaptive systems are accessible and beneficial for all students. By adopting a balanced approach that emphasizes ethical frameworks and inclusivity, educators can harness AIoT to drive meaningful improvements in student outcomes, ultimately setting the stage for an increasingly adaptive and personalized future in education.

References

[1] Tetzlaff, L., Schmiedek, F., & Brod, G. (2021). Developing personalized education: A dynamic framework. Educational Psychology Review, 33(3), 863–882. https://doi.org/10.1007/s10648-020-09570-w

[2] Bernacki, M. L., Greene, M. J., & Lobczowski, N. G. (2021). A systematic review of research on personalized learning: Personalized by whom, to what, how, and for what purpose(s)? Educational Psychology Review, 33(4), 1675–1715. https://doi.org/10.1007/s10648-021-09615-8

[3] El Dandachi, I. (2023). AI-Powered Personalized Learning: Toward Sustainable Education. In Advances in Artificial Intelligence and Data Engineering (pp. 45-60). Springer. https://doi.org/10.1007/978-981-99-8572-2_5

[4] Dimitriadou, E., & Lanitis, A. (2023). A critical evaluation, challenges, and future perspectives of using artificial intelligence and emerging technologies in smart classrooms. Smart Learning Environments, 10(1), 1-15. https://doi.org/10.1186/s40561-023-00231-3

[5] Gupta, M., Kumar, R., Chaudhary, R. K., & Kumari, J. (2021, December). IoT based voice controlled autonomous robotic vehicle through google assistant. In 2021 3rd international conference on advances in computing, communication control and networking (ICAC3N) (pp. 713-717). IEEE.

[6] Li, X., & Slotta, J. D. (2019). Internet of Things for Sustainable Smart Education: An Overview. Sustainability, 14(7), 4293. https://doi.org/10.3390/su14074293

[7] Sharma Ghai, A., Sharma, R. C., Jasola, S., & Zamfiroiu, A. (2024). Intelligent sustainable development in online learning - Insights from higher education and industry 5.0. In A. Mutawa (Ed.), Impacts of generative AI on the future of research and education (Chapter 17, pp). IGI Global. https://doi.org/10.4018/979-8-3693-0884-4

[8] Altınay, Z., Ghai, A. S., Sharma, R. C., Baştas, M., Jasola, S., Dağlı, G., & Kohli, D. (2024). Embracing digital transformation in learning organizations using blended learning for academic excellence. Pakistan Journal of Life and Social Sciences, 22(1), 6754-6762. https://doi.org/10.57239/PJLSS-2024-22.1.00492Chen, X., & Xie, H. (2024). AI and personalized learning: Bridging the gap with modern educational goals. Journal of Educational Technology & Society, 27(4), 123-135. https://doi.org/10.1007/s41239-024-00448-3

[9] Yu, H., Miao, C., Leung, C., & White, T. J. (2017). Towards AI-powered personalization in MOOC learning. npj Science of Learning, 2(15). https://doi.org/10.1038/s41539-017-0016-3

[10] Kamruzzaman, M. M., Alanazi, S., Alruwaili, M., Alshammari, N., Elaiwat, S., Abu-Zanona, M., Innab, N., & Elzaghmouri, B. M. (2023). AI- and IoT-Assisted Sustainable Education Systems during Pandemics, such as COVID-19, for Smart Cities. Sustainability, 15(10), 8354. https://doi.org/10.3390/su15108354

[11] Larhgotra, A., Kumar, R., & Gupta, M. (2022, November). Traffic monitoring and management system for congestion comtrol using iot and ai. In 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 641-646). IEEE.

[12] Walter, Y. (2024). Embracing the future of Artificial Intelligence in the classroom: The relevance of AI literacy, prompt engineering, and critical thinking in modern education. International Journal of Educational Technology in Higher Education, 21(1), 15. https://doi.org/10.1186/s41239-024-00448-3

[13] S. Dewari, M. Gupta, R. Kumar, A. J. Obaid, and M. R. AL-Hameed, "A Review Analysis on Measuring the Soil Characteristic in Agriculture Using Artificial Intelligence and IOT," Lecture Notes in Networks and Systems, vol. 617 LNNS, pp. 325–334, 2023, doi: 10.1007/978-981-19-9512-5_30.

[14] El-Sabagh, H. A. (2021). Adaptive e-learning environment based on learning styles and its impact on development students' engagement. International Journal of Educational Technology in Higher Education, 18(1), 53. https://doi.org/10.1186/s41239-021-00289-4

[15] Gul, S., & Bano, S. (2019). Smart libraries: An emerging and innovative technological habitat of 21st century. The Electronic Library, 37(5), 764-783. https://doi.org/10.1108/EL-02-2019-0052

[16] Yu, H., Miao, C., Leung, C., & White, T. J. (2017). Towards AI-powered personalization in MOOC learning. npj Science of Learning, 2(15). https://doi.org/10.1038/s41539-017-0016-3

[17] Mougiakou, S., Vinatsella, D., Sampson, D., Papamitsiou, Z., & Giannakos, M. (2023). Educational Data Analytics for Teachers and School Leaders. Advances in Analytics for Learning and Teaching. https://doi.org/10.1007/978-3-031-15266-5

[18] Khan, A. U., Ma, Z., Li, M., Zhi, L., & Hu, W. (2023). From traditional to emerging technologies in supporting smart libraries: A bibliometric and thematic approach from 2013 to 2022. Library Hi Tech, 41(1), 792. https://doi.org/10.1108/lht-07-2023-0280

[19] Tabuenca, B., Uche-Soria, M., Greller, W., Hernández-Leo, D., Balcells-Falgueras, P., Gloor, P., & Garbajosa, J. (2023). Greening smart learning environments with Artificial Intelligence of Things. Internet of Things, 101051. https://doi.org/10.1016/j.iot.2023.101051

[20] Sethi, S. S., & Jain, K. (2024). AI technologies for social emotional learning: Recent research and future directions. Journal of Research in Innovative Teaching & Learning, 17(2), 213-225. https://doi.org/10.1108/JRIT-03-2024-0073

[21] Khan, A. U., Ma, Z., Li, M., Zhi, L., & Hu, W. (2023). From traditional to emerging technologies in supporting smart libraries: A bibliometric and thematic approach from 2013 to 2022. Library Hi Tech, 41(1), 792. https://doi.org/10.1108/lht-07-2023-0280

[22] Williamson, B. (2015). Digital education governance: Data visualization, predictive analytics, and 'real-time' policy instruments. Journal of Education Policy, 31(2), 123-141. https://doi.org/10.1080/02680939.2015.1035758

[23] Alazab, M., Gupta, M., & Ahmed, S. (2023). AIoT technologies and applications for smart environments. Institution of Engineering and Technology. https://shop.theiet.org/editors/mamoun-alazab-meenu-gupta-shakeel-ahmed

[24] Kour, S., Kumar, R., & Gupta, M. (2021, September). Analysis of student performance using Machine learning Algorithms. *In 2021 Third International Conference on Inventive Research in Computing Applications* (ICIRCA) (pp. 1395-1403). IEEE.

[25] Gupta, M., Kumar, R., Arora, A., & Kaur, J. (2022, December). Fuzzy logic-based Student Placement Evaluation and Analysis. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1503-1507). IEEE.

[26] Gupta, M., Kumar, R., Chaudhary, R. K., & Kumari, J. (2021, December). IoT based voice controlled autonomous robotic vehicle through google assistant. In *2021 3rd international conference on advances in computing, communication control and networking (ICAC3N)* (pp. 713-717). IEEE.

[27] Gupta, M., Thakur, N., Bansal, D., Chaudhary, G., Davaasambuu, B., & Hua, Q. (2022). [Retracted] CNN-LSTM Hybrid Real-Time IoT-Based Cognitive Approaches for ISLR with WebRTC: Auditory Impaired Assistive Technology. *Journal of healthcare engineering*, *2022*(1), 3978627.

[28] Kaur, G., Gupta, M., & Kumar, R. (2021). IoT based smart healthcare monitoring system: A systematic review. *Annals of the Romanian Society for Cell Biology*, 3721-3728.

6G Advanced Communication and Sensing: Essential Enabling Technologies, Issues, and Challenges

Ramiz Salama[1]*, Sinem Alturjman[2], Fadi Al-Turjman[2]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT,
Near East University Nicosia, Mersin 10, Turkey

[2]Artificial Intelligence, Software, and Information Systems Engineering Departments, Research Center for AI and IoT, AI and Robotics Institute, Near East University, Nicosia, Mersin10, Turkey

*Corresponding author Email: ramiz.salama@neu.edu.tr

Abstract: The impending sixth generation (6G) of wireless communication technology is set to transform the digital world by combining improved communication and sensor capabilities. It will allow for ultra-reliable, high-speed data transfers, huge networking, and seamless integration of intelligent devices and applications. This confluence will pave the way for future applications including holographic telepresence, extended reality (XR), autonomous systems, and digital twins. Terahertz (THz) communication, reconfigurable intelligent surfaces (RIS), integrated sensing and communication (ISAC), AI-driven networking, quantum communication, and edge computing are all critical 6G enablers. These technologies strive to meet the rapidly increasing demand for data throughput, dependability, and latency requirements while also providing extremely accurate and efficient sensing capabilities. Furthermore, breakthroughs in non-terrestrial networks (NTN), blockchain-based security frameworks, and novel antenna designs would be required for broad 6G implementation. Despite this promise, 6G development and implementation confront considerable obstacles. These include technological difficulties like as overcoming high route loss in THz bands, creating energy-efficient designs, and dealing with spectrum scarcity. With widespread data generation and networking, security and privacy problems grow in importance. In addition, there are governmental and societal difficulties, such as standardization, ethical concerns about data usage, and the potential digital gap caused by uneven access to 6G infrastructure. The purpose of this study is to investigate the essential technologies that will power 6G communication and sensing systems, identify the primary barriers to adoption, and describe the multifarious problems that must be overcome in order to achieve a robust, secure, and inclusive 6G ecosystem.

Keywords: Standards, Difficulties, Integrated Sensing and Communication (ISAC), 6G, and Key Enabling Technologies

1. Introductıon

A move toward investigating new technologies that can support sixth generation (6G) wireless networks has been made possible by the continuous standardization and deployment of fifth generation (SG) wireless networks. A 6G terrestrial wireless network roadmap has been developed to provide users and machine-type devices with continuous connectivity. For instance, the new recommendation for the vision of international mobile telecommunications 2030 IMT-2030(6G) was successfully written by the International Telecommunications Union's (ITU-R) radio communication section. One of the primary use cases for IMAR - 2030/6G, according to the International Telecommunication Union's (ITU-R) radio

communication section, is integrated sensing and communication (Isac). It is anticipated that ISAc will be essential to the next wireless generation standard. We combine a number of critical standpoints in this work, such as academic and industrial advancement. This page specifically outlines 6G requirements and the Isac-enabled vision, covering integration issues, advantages of Isac coexistence, and different facets of 6G standardization. Furthermore, we introduce important enabling technologies, such as orthogonal time frequency space (OTFS) waveform design and interference management for ISAC, as well as intelligent meta surfaces- assisted ISAC. In order to open up a variety of research prospects and problems regarding ISAC technology toward 6G wireless communication, future aspects are finally covered. approved in the June 2023 summit in Geneva.Tthrough sophisticated surface sense that can be reconfigured and improved. Comprehend the transmission environment and the actual world. Given the significance and growth of ISAC in the next generation of wireless technology, we have highlighted a number of crucial and cutting-edge features of ISAC technology for the 6G standards domain [1-10]. In particular, this work can be concluded as follows: This article summarizes the needs for 6G and the goals of ISAC integration, discussing issues related to 6G standardization, the benefits of ISAC coexistence, and associated difficulties. b) It also highlights important enabling technologies, such as intelligent metasurface-: ISAC, and provides the OTFS waveform design for Is. c) In addition, the paper has examined potential future directions that could lead to other research directions for ISAC technology for 6G wireless communication.

As a key component of upcoming 6G networks, integrating sensing and communication (ISAC) is the subject of the paper Towards Integrated Sensing and Communication for 6G: Key Enabling Technologies, Standardization, and Challenges. It emphasizes how improved resource usage, reduced latency, and improved spectrum efficiency might result from the convergence of various technologies.
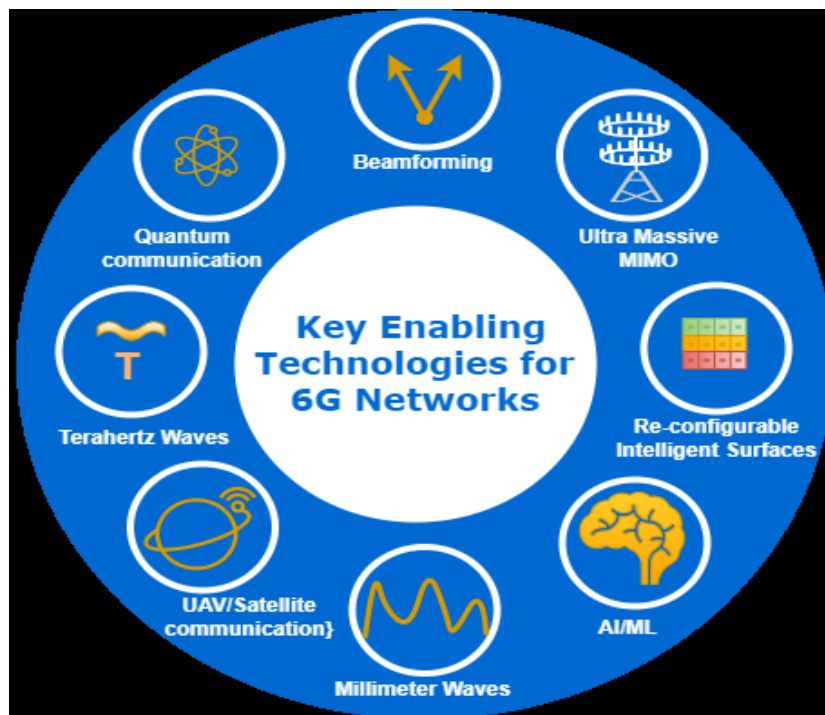

Figure 1. Key Enabling Technologies for 6G Networks

In order to enable ISAC capabilities, the authors talk about enabling technologies such as intelligent metasurfaces and Orthogonal Time Frequency Space (OTFS) waveforms. The difficulties in standardizing and incorporating ISAC into current and developing wireless communication frameworks are also covered in the article. Waveform design, interference control, and unifying disparate use cases under a single standard are major challenges. The study emphasizes how crucial interdisciplinary cooperation is to overcoming these obstacles and successfully advancing 6G technology.

2. ISAC and its significant impact on future generations.

Take integrated positioning and recognition, for instance. It is anticipated that imagination and reconstruction would offer complementary qualities that will be useful in intelligence. thriving social governance and industrial progress. Future wireless generations will be led by network-centric development of the wireless framework core. The development of current skills is made possible by the lessons learned from the preceding generation. 6G aims to outperform its predecessor and open up new possibilities by utilizing advancements in spectrum efficiency, network capacity, etc [11-15]. A higher order MIMO, for instance, is designed to use more antennas, allowing for improved performance.

2.1 Intelligent air interface

Unlike wireless generation, which uses advanced logistics and processing. Utilizing the smart air interface at the transceiver end will enable 6G technology by making it easy to adjust the wireless channel for better propagation conditions.[2]Help from RIS is one of the possible methods. THZ communication and holographic radio.Indeed, RIS support is a new feature of the 6G smart interface.
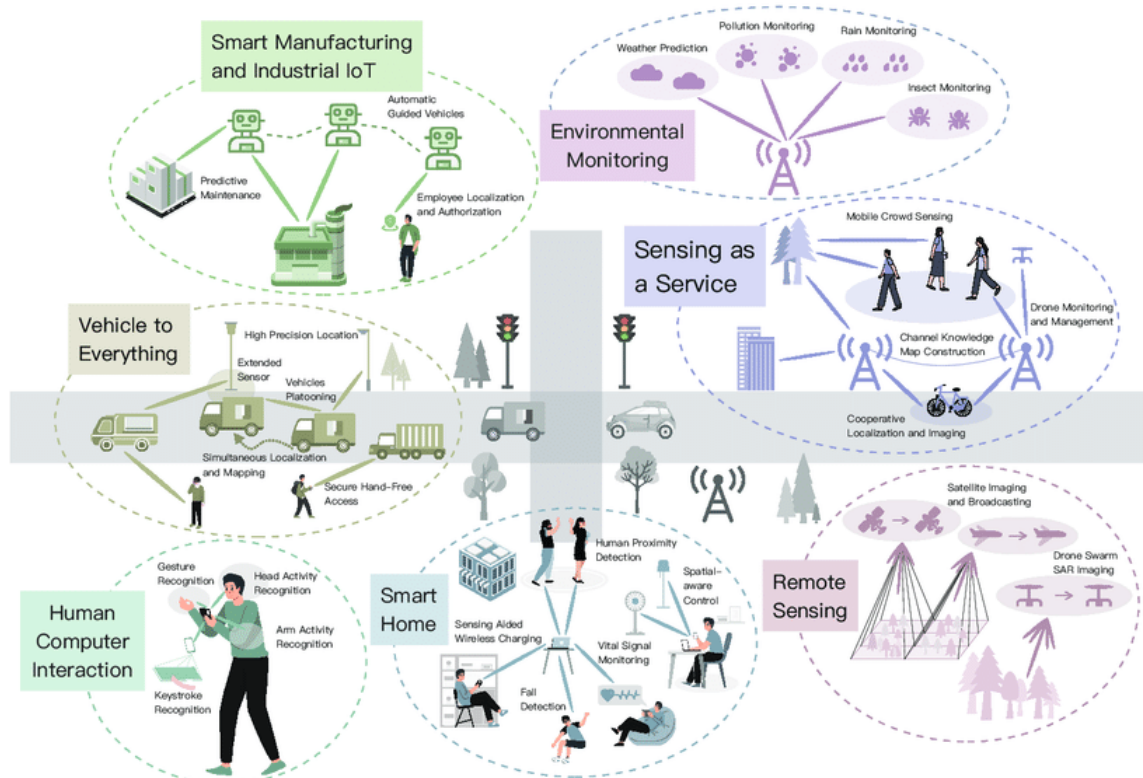

Figure 2 ISAC technology for future wireless networks

2.2 User-assisted improvements

The goal of 6G frontier is to leverage end users' computing capabilities without appreciably increasing the network system's total cost, size, or power consumption. Edge computing: by placing a typical computational load on the user's end, a number of advantages could be realized, such as: a) moving data storage and computation closer to the network edge,
b) lowering end-user latency, c) having real-time processing capabilities, and d) enabling context-aware services. 6G networks can support a wide variety of applications [16].

3. ISAC co-existence and 6G standardization

By creating a consistent platform for productive collaboration amongst developers, academics, and industries, standardization is essential to the advancement of ISAC. A thorough set of standards promotes scalability and interoperability and makes it easier to incorporate new technologies into already-existing ecosystems [17-21].

A. Initiatives and Establishments: Adopting standardization will enable ISAC to reach its full potential and open the door to a future that is sensor-driven, intelligent, and connected. *Project B: Third Generation Partnership (3GPP):* As the scope of 5G-Advanced expands following the initial phase of the 5G standard, interest in ISAC is steadily growing.

While the primary function of the traditional SG was to provide solely communication services, ISAC can play a significant role in its role by supporting new services that are aided by communication. Three main scenarios—object recognition and tracking, environment monitoring, and motion monitoring—are examined in order to find such new ISAC service possibilities.
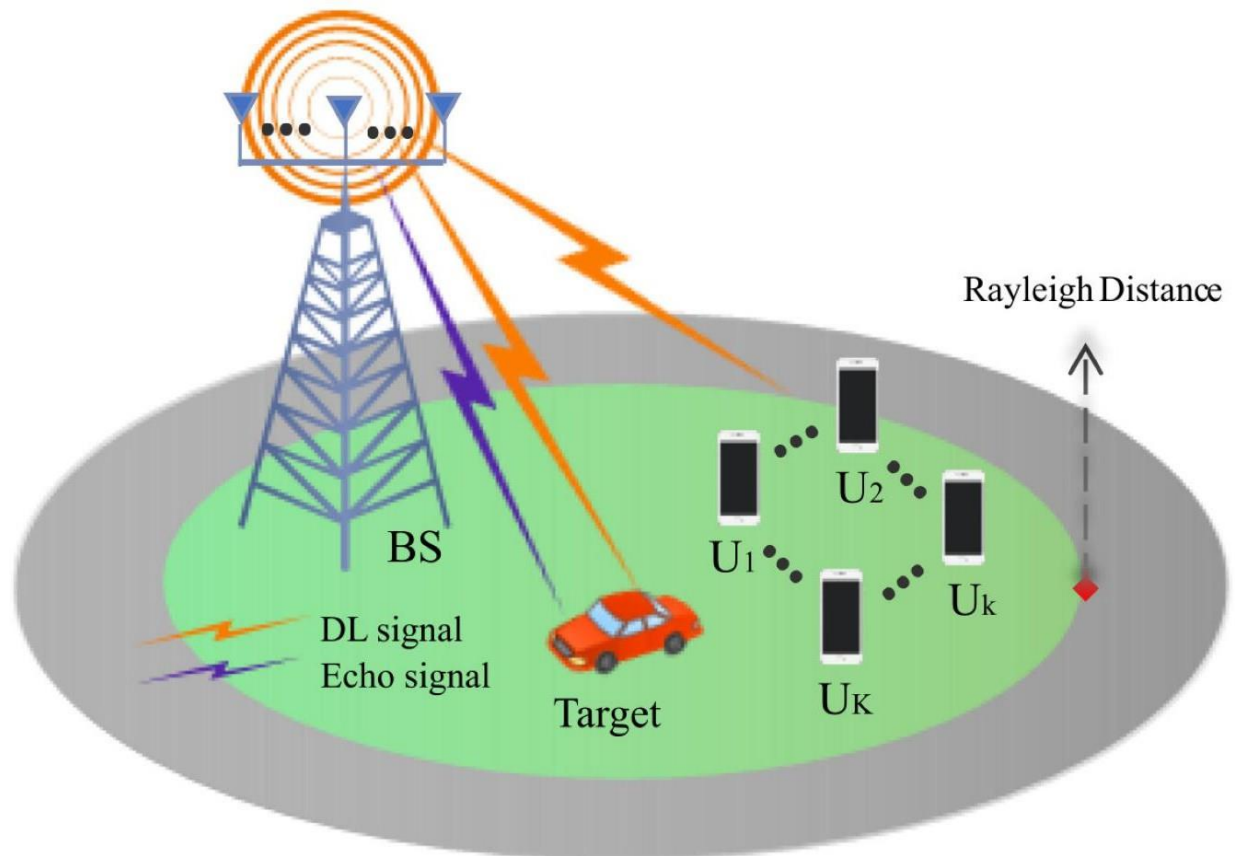

Figure 3. System model of DL NOMA empowered ISAC.

4. Previous publications

• *Literature review overview:* give a thorough analysis of the body of knowledge about ISAC in 6G, emphasizing studies that were published in 2022–2024 [22-26].

Categorization by theme: Important enabling technologies: talk about the function of edge computing, reconfigurable intelligent surfaces (RIS), terahertz (THz) communication, artificial intelligence (AI), and machine learning . • Standardization initiatives: examine the contributions made by organizations like as IEEE, 3Gpp, and ITU in purchasing the 6G standard, especially for ISAC.

• *Difficulties:* emphasize studies tackling issues including interoperability, latency security, and spectrum allocation.
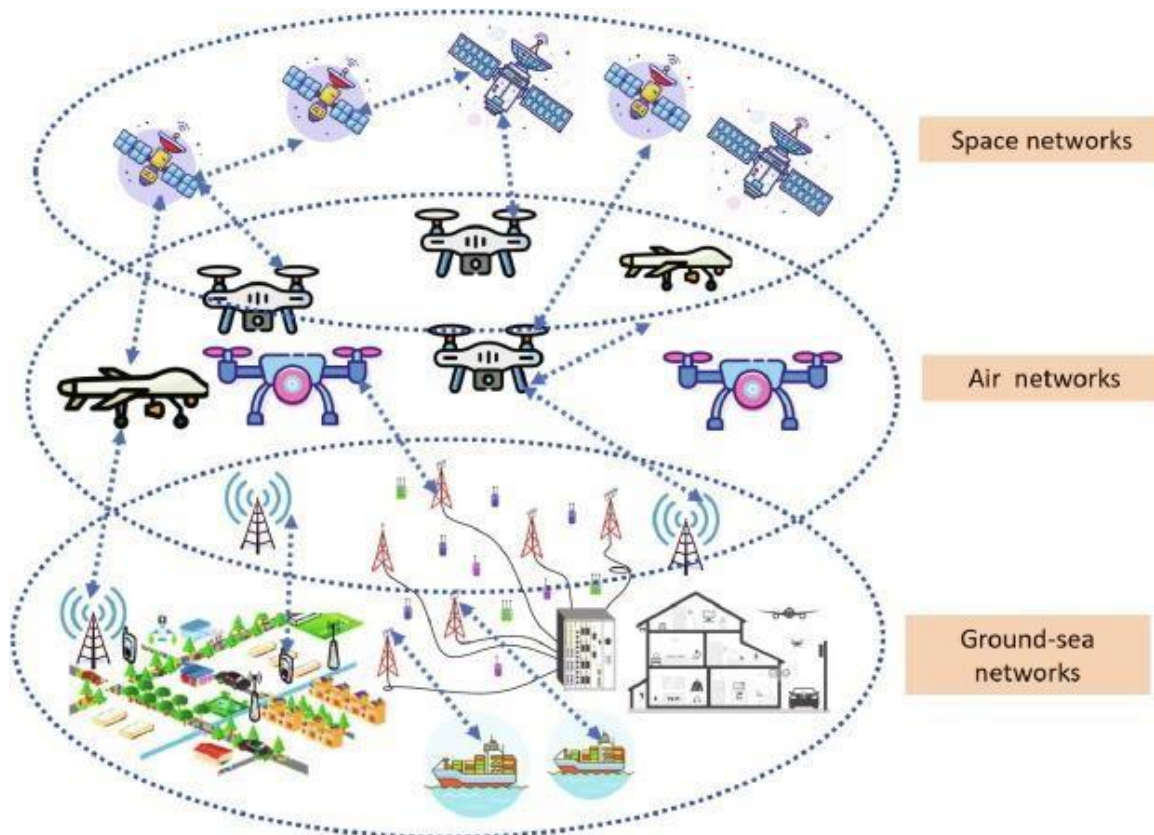
Figur.4 The integrated ground-sea-air-space 6G expected network.

5. Content and technique

Methodology: describe the methical process used to collect and examine study data [27-31].

Data sources: enumerate the databases, journals, and conference proceedings (such as IEE xplore and AÇMA digital library science direct) that were used to compile pertinent literature [32].

Theoretical framework: if any, describe any simulations or model frameworks that are used to examine how sensing and communication are integrated in 6G [33] .

Evaluation criteria: describe the standards by which the enabling technologies, standardization procedures, and difficulties are judged.

6. Results and discussion

• Talk about how AI and machine learning improve 6G network security, efficiency, and adaptability.
• Examine how Examine Rix can enhance connection and optimize signal propagation with reconfigurable intelligent surfaces (RIS) [34][35].
• Cutting-edge computing Examine how edge computing and latency reduction can support real-time applications in 6G [36] [37].
• Standardization initiatives: • 3GPP and IEEE contribution: describe the state of 6G standardization at the moment, with an emphasis on ISAC.
• Standardization with an emphasis on ISAC
The role of international cooperation in creating unified 6 GB standards was explored.

7. Conclusion

Towards Integrated Sensing and Communication for 6G: Essential Facilitating Technologies, Standardization, and Difficulties concluding highlights how important integrated sensing and communication (ISAC) will be in forming wireless technology for the sixth generation (6G). The authors emphasize how ISAC can improve overall system efficiency, save infrastructure costs, and maximize spectrum utilization. Notwithstanding its potential, ISAC's effective implementation depends on resolving a number of technical and standardization challenges, such as the creation of uniform international standards, sophisticated waveform designs, and interference control. In order to fully exploit the potential of ISAC technologies and to clear the path for reliable 6G implementations that meet a variety of use cases and criteria, the study urges ongoing multidisciplinary research and cooperation among academia, industry, and standardization bodies.

References

[1] Sharma, S., Popli, R., Singh, S., Chhabra, G., Saini, G. S., Singh, M., ... & Kumar, R. (2024). The Role of 6G Technologies in Advancing Smart City Applications: Opportunities and Challenges. Sustainability, 16(16), 7039.
[2] Kaushik, A., Singh, R., Dayarathna, S., Senanayake, R., Di Renzo, M., Dajer, M., ... & Shin, W. (2024). Toward Integrated Sensing and Communications for 6G: Key Enabling Technologies, Standardization, and Challenges. IEEE Communications Standards Magazine, 8(2), 52-59.
[3] Chataut, R., Nankya, M., & Akl, R. (2024). 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. Sensors, 24(6), 1888.
[4] Jha, A. V., Appasani, B., Khan, M. S., Zeadally, S., & Katib, I. (2024). 6G for intelligent transportation systems: standards, technologies, and challenges. Telecommunication Systems, 1-28.
[5] Jiang, W., Zhou, Q., He, J., Habibi, M. A., Melnyk, S., El-Absi, M., ... & Leung, V. C. (2024). Terahertz communications and sensing for 6G and beyond: A comprehensive review. IEEE Communications Surveys & Tutorials.
[6] Singh, R., Kaushik, A., Shin, W., Di Renzo, M., Sciancalepore, V., Lee, D., ... & Dobre, O. A. (2024). Towards 6G Evolution: Three Enhancements, Three Innovations, and Three Major Challenges. arXiv preprint arXiv:2402.10781.

[7] Ishteyaq, I., Muzaffar, K., Shafi, N., & Alathbah, M. A. (2024). Unleashing the Power of Tomorrow: Exploration of Next Frontier with 6G Networks and Cutting Edge Technologies. IEEE Access.

[8] Siddiky, M. N. A., Rahman, M. E., & Uzzal, M. S. (2024). Beyond 5G: A Comprehensive Exploration of 6G Wireless Communication Technologies.

[9] Liu, R., Hua, M., Guan, K., Wang, X., Zhang, L., Mao, T., ... & Jamalipour, A. (2024). 6G enabled advanced transportation systems. IEEE Transactions on Intelligent Transportation Systems.

[10] Anvigh, A. A., Khavan, Y., & Pourghebleh, B. (2024). Transforming Vehicular Networks: How 6G can Revolutionize Intelligent Transportation?. Science, Engineering and Technology, 4(1), 80-93

[11] Rafi, S., Akbar, M. A., & Mahmood, S. (2024, July). A conceptual framework for quantum integration challenges in 6g technology. In Proceedings of the 1st ACM International Workshop on Quantum Software Engineering: The Next Evolution (pp. 19 - 26).

[12] Rachakonda, L. P., Siddula, M., & Sathya, V. (2024). A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). High-Confidence Computing, 100220.

[13] Alonistioti, N., Cardona, N., Waldemar, P., & Trivisonno, R. (2024). Establish an Open Platform to Foster 6G Innovation and Research. IEEE Communications Magazine, 62(1), 8-10.

[14] Zhuo, Y., Mao, T., Li, H., Sun, C., Wang, Z., Han, Z., & Chen, S. (2024). Multi-Beam Integrated Sensing and Communication: State-of-the-Art, Challenges and Opportunities. arXiv preprint arXiv:2405.20595.

[15] Houssein, E. H., Othman, M. A., Mohamed, W. M., & Younan, M. (2024). Internet of Things in Smart Cities: Comprehensive Review, Open Issues and Challenges. IEEE Internet of Things Journal.

[16] "6G-Enabled IoT and AI for Smart Healthcare: Challenges, Impact, and Analysis - Google Books." Accessed: Dec. 26, 2024. [Online]. Available: https://books.google.co.in/books?hl=en&lr=&id=wRG8EAAAQBAJ&oi=fnd&pg=PT9&dq =info:BVCQG0WSbwkJ:scholar.google.com&ots=sJe0NZjDXT&sig=d4QIVVU0OoazsAhd UsxhZV5gDRc&redir_esc=y#v=onepage&q&f=false

[17] Gupta, P., Gill, R., Singh, S., Sharma, S., & Bhathal, U. S. 5G-Oriented Positioning Technology. In 5G Enabled Technology for Smart City and Urbanization System (pp. 70 - 83). Chapman and Hall/CRC.

[18] Sefati, S. S., Haq, A. U., Craciunescu, R., Halunga, S., Mihovska, A., & Fratu, O. (2024). A Comprehensive Survey on Resource Management in 6G Network Based on Internet of Things. IEEE Access.

[19] Wang, X., Guo, Q., Ning, Z., Guo, L., Wang, G., Gao, X., & Zhang, Y. (2024). Integration of Sensing, Communication, and Computing for Metaverse: A Survey. ACM Computing Surveys, 56(10), 1-38.

[20] Rafique, W., & Qadir, J. (2024). Internet of everything meets the metaverse: Bridging physical and virtual worlds with blockchain. Computer Science Review, 54, 100678.

[21] Oliveri, G., Zardi, F., Benoni, A., Salucci, M., Massa, A., Cianca, E., ... & Natalizio, E. (2024). 6G Wireless Architectures. In The Road towards 6G: Opportunities, Challenges,

and Applications: A Comprehensive View of the Enabling Technologies (pp. 115 -154). Cham: Springer Nature Switzerland.

[22] Elsadig, M., Alohali, M. A., Ibrahim, A. O., & Abulfaraj, A. W. (2024). Roles of Blockchain in the Metaverse: Concepts, Taxonomy, Recent Advances, Enabling Technologies, and Open Research Issues. IEEE Access, 12, 38410-38435.

[23] Wang, S., Qureshi, M. A., Miralles-Pechuán, L., Huynh-The, T., Gadekallu, T. R., & Liyanage, M. (2024). Explainable AI for 6G Use Cases: Technical Aspects and Research Challenges. IEEE Open Journal of the Communications Society.

[24] Rodriguez, E., Masip-Bruin, X., Martrat, J., Diaz, R., Jukan, A., Granelli, F., ... & Xilouris, G. (2024). A Security Services Management Architecture Toward Resilient 6G Wireless and Computing Ecosystems. IEEE access.

[25] Tian, W., Gu, C., Guo, M., He, S., Kang, J., Niyato, D., & Chen, J. (2024). Large-Scale Deterministic Networks: Architecture, Enabling Technologies, Case Study and Future Directions. IEEE Network.

[26] He, Z., Xu, W., Yang, Z., Shen, H., Fu, N., Huang, Y., ... & You, X. (2024). Unlocking potentials of near-field propagation: ELAA-empowered integrated sensing and communication. arXiv preprint arXiv:2404.18587.

[27] Pachouri, V., Singh, R., Gehlot, A., Pandey, S., Akram, S. V., & Abbas, M. (2024). Empowering sustainability in the built environment: A technological Lens on industry 4.0 Enablers. Technology in Society, 76, 102427.

[28] Parra-Ullauri, J. M., Zhang, X., Bravalheri, A., Moazzeni, S., Wu, Y., Nejabati, R., & Simeonidou, D. (2024). Federated Analytics for 6G Networks: Applications, Challenges, and Opportunities. IEEE Network.

[29] Krupas, M., Kajati, E., Liu, C., & Zolotova, I. (2024). Towards a Human-Centric Digital Twin for Human–Machine Collaboration: A Review on Enabling Technologies and Methods. Sensors, 24(7), 2232.

[30] Piccarozzi, M., Silvestri, L., Silvestri, C., & Ruggieri, A. (2024). Roadmap to Industry 5.0: Enabling technologies, challenges, and opportunities towards a holistic definition in management studies. Technological Forecasting and Social Change, 205, 123467.

[31] Kalør, A. E., Durisi, G., Coleri, S., Parkvall, S., Yu, W., Mueller, A., & Popovski, P. (2024). Wireless 6G connectivity for massive number of devices and critical services. arXiv preprint arXiv:2401.01127.

[32] M. Gupta, C. Ved, and M. Kumari, "Emergence of Blockchain Applications with the 6G-Enabled IoT-Based Smart City," Blockchain for 6G-Enabled Network-Based Applications, pp. 213–235, Aug. 2022, doi: 10.1201/9781003264392-9.

[33] Gargrish, S., Chauhan, S., Gupta, M., & Obaid, A. J. (2023). 6G-Enabled IoT Wearable Devices for Elderly Healthcare. In *6G-Enabled IoT and AI for Smart Healthcare* (pp. 157-169). CRC Press.

[34] Kaur, R., Kumar, R., & Gupta, M. (2024). Lifestyle and Dietary Management Associated with Chronic Diseases in Women Using Deep Learning. *Combating Women's Health Issues with Machine Learning*, 59-73.

[35] Juneja, A., Kumar, R., & Gupta, M. (2022, July). Smart Healthcare Ecosystems backed by IoT and Connected Biomedical Technologies. In *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 230-235). IEEE.

[36] Yadav, A., Kumar, R., & Gupta, M. (2024, March). An analysis of convolutional neural network and conventional machine learning for multiclass brain tumor detection. In *AIP Conference Proceedings* (Vol. 3072, No. 1). AIP Publishing.

[37] Gupta, M., Kumar, R., & Abraham, A. (2024). Adversarial Network-Based Classification for Alzheimer's Disease Using Multimodal Brain Images: A Critical Analysis. *IEEE Access*.