Archives of Advances in Artificial Intelligence & Data Science and Machine Learning
Review Article

Anomaly Detection in IoT Using Machine Learning

Soren Falkner*

Vienna University of Technology, Faculty of Computer Engineering, Vienna, Austria

Citation: *Falkner S. Anomaly Detection in IoT Using Machine Learning. Arch Adv Art Intel Data Sci Mach Learn 2025;1(1):1-11.*

Received Date: May 09, 2025**; Accepted Date** May 13, 2025**; Published Date:** May 15, 2025

***Corresponding author:** Soren Falkner, Vienna University of Technology, Faculty of Computer Engineering, Vienna, Austria

ABSTRACT

The proliferation of Internet of Things (IoT) devices has introduced unprecedented connectivity and data generation, but also significant security challenges. Traditional security mechanisms often prove inadequate for the dynamic and resource-constrained nature of IoT networks. Anomaly detection, leveraging the power of machine learning, offers a promising approach to identify unusual or malicious behavior within these complex environments. This paper explores the application of various machine learning techniques, including supervised, unsupervised and semi-supervised methods, for detecting anomalies in IoT data streams. We discuss the unique characteristics of IoT data that influence the choice and performance of these algorithms, such as high dimensionality, temporal dependencies and the prevalence of noisy or imbalanced datasets. Furthermore, we examine the challenges and opportunities associated with deploying machine learning-based anomaly detection systems in resource-constrained IoT environments, including model training, real-time inference and data privacy considerations. Finally, we highlight promising research directions and potential advancements in this critical area for securing the future of connected devices.

Keywords: Anomaly detection; Internet of things (IoT); Machine learning; Security; Intrusion detection; Unsupervised learning; Supervised learning; Semi-supervised learning; Time series analysis; Edge computing; Resource constraints; Data security; Cyber security

INTRODUCTION

The Internet of Things (IoT) has rapidly transitioned from a futuristic concept to a pervasive reality, weaving its way into the fabric of our daily lives, industries and critical infrastructures. From smart homes and wearable devices to industrial control systems and connected vehicles, the sheer volume and diversity of interconnected devices are expanding at an exponential rate. This digital transformation promises unprecedented levels of automation, efficiency and convenience, unlocking new possibilities for data-driven decision-making and innovative services. However, this hyper-connectivity also introduces a significantly expanded attack surface, making IoT networks [1-33] increasingly vulnerable to a wide range of cyber threats. The inherent characteristics of many IoT devices, including limited computational resources, diverse communication protocols and often lax security configurations, further exacerbate these vulnerabilities, posing significant risks to data confidentiality, integrity and availability, as well as the physical safety of individuals and systems.

The traditional security paradigms, often relying on perimeter-based defenses and signature-based detection, struggle to effectively address the unique challenges presented by IoT environments. The distributed nature of IoT networks, the heterogeneity of devices and the continuous stream of data generated necessitate more intelligent and adaptive security solutions. Unlike conventional IT systems [34-55] with well-defined boundaries and predictable behavior, IoT ecosystems are often characterized by dynamic topologies, resource-constrained devices incapable of running complex security software and communication patterns that can vary significantly based on context and application. This complexity renders static security rules and signature-based approaches largely ineffective against novel and sophisticated attacks that can easily evade predefined patterns. Consequently, there is a pressing need for advanced security mechanisms capable of detecting subtle deviations from normal behavior and identifying previously unseen threats within these intricate networks.

The promise of machine learning for intelligent IoT security

In response to the evolving threat landscape in IoT, machine learning (ML) has emerged as a powerful paradigm for building intelligent and adaptive security systems. Machine learning algorithms possess the ability to learn complex patterns from large datasets, enabling them to identify anomalies that deviate from established norms without explicit programming of specific attack signatures. This data-driven approach is particularly well-suited for the dynamic and unpredictable nature of IoT environments, where normal operational patterns can vary significantly depending on the specific application, time of day and environmental conditions. By continuously analyzing the vast amounts of data generated by IoT devices, machine learning models can learn the subtle nuances of normal behavior and flag deviations that might indicate malicious activity, system malfunctions or configuration errors.

The application of machine learning in IoT security [56-66] spans a wide spectrum of tasks, including intrusion detection, malware analysis, botnet identification and the detection of insider threats. Various machine learning techniques, ranging from classical statistical methods to advanced deep learning architectures, offer different capabilities in terms of pattern recognition, adaptability and computational requirements. For instance, unsupervised learning algorithms like clustering and anomaly detection techniques can identify unusual data points without requiring prior knowledge of specific attack types, making them particularly valuable for detecting novel threats. Supervised learning methods, on the other hand, can be trained on labeled data to classify network traffic or device behavior as normal or malicious, offering high accuracy in detecting known attack patterns. Furthermore, semi-supervised learning approaches can leverage both labeled and unlabeled data to build robust models even when labeled attack data is scarce, a common challenge in real-world IoT deployments.

The integration of machine learning into IoT security [67-80] frameworks holds the potential to significantly enhance the resilience and trustworthiness of connected devices and networks. By enabling proactive threat detection, automated response mechanisms and adaptive security policies, machine learning can empower security professionals to effectively manage the growing complexities and evolving threats within the IoT ecosystem. However, the successful deployment of machine learning-based security solutions in IoT environments is not without its challenges. Factors such as the heterogeneity of devices and data formats, the resource constraints of edge devices, the need for real-time analysis and concerns about data privacy and model explainability must be carefully considered and addressed. The subsequent sections of this work will delve deeper into the specific applications of machine learning for anomaly detection in IoT, explore the various techniques and their suitability for different IoT scenarios and discuss the key challenges and future directions in this critical and rapidly evolving field.

CHALLENGES

While machine learning offers significant promise for enhancing IoT security through anomaly detection, its practical implementation faces a multitude of challenges stemming from the unique characteristics of IoT environments and the inherent complexities of machine learning itself. Overcoming these hurdles is crucial for realizing the full potential of AI-driven security in the connected world.

One of the primary challenges lies in the heterogeneity and scale of IoT devices and data. The IoT ecosystem encompasses a vast array of devices, from low-power sensors with limited processing capabilities to more sophisticated gateways and edge servers. These devices often employ diverse communication protocols, generate data in various formats and at varying rates and operate under different resource constraints. Training and deploying a single, universal anomaly detection model across such a heterogeneous landscape is impractical. Developing tailored models for specific device types or application domains requires significant effort in data collection, preprocessing and model customization. Furthermore, the sheer volume of data generated by billions of interconnected devices poses significant scalability challenges for both model training and real-time inference. Efficient data management, feature extraction and model optimization techniques are essential to handle the massive data streams without overwhelming computational resources or introducing unacceptable latency.

Resource constraints at the edge present another significant obstacle. Many IoT devices have limited processing power, memory and battery life, making it infeasible to run complex machine learning models directly on the devices themselves. While edge computing paradigms aim to bring computation closer to the data source, deploying even lightweight machine learning models on resource-constrained devices requires careful consideration of model complexity, energy efficiency and memory footprint [81-94]. Techniques like model compression, quantization and distributed learning are being explored to address these limitations, but achieving a balance between model accuracy and resource efficiency remains a critical challenge.

The dynamic and evolving nature of IoT environments also complicates anomaly detection. Normal operational patterns in IoT networks can change over time due to software updates, device deployments, environmental variations and evolving user behavior. Machine learning models trained on historical data may become less effective in detecting novel anomalies or may generate a high number of false positives if they fail to adapt to these dynamic changes. Continuous learning and model retraining mechanisms are necessary to maintain the accuracy and relevance of anomaly detection systems in the face of evolving operational contexts. However, implementing effective online learning strategies in resource-constrained and distributed IoT environments presents its own set of technical challenges.

Furthermore, the scarcity of labeled anomaly data poses a significant hurdle for supervised learning approaches. While vast amounts of normal operational data are typically available in IoT deployments, instances of actual cyberattacks or system failures are often rare. Training accurate supervised models requires a sufficient amount of labeled data representing various types of anomalies. Obtaining such labeled data can be challenging, time-consuming and costly, often requiring manual analysis and expert knowledge. This data imbalance problem can lead to biased models that are more adept at recognizing normal behavior but struggle to detect rare but critical anomalies. Techniques like anomaly generation, transfer learning and semi-supervised learning are being investigated to mitigate the impact of limited labeled data.

Data privacy and security concerns are also paramount in IoT [95-109] environments. Many IoT devices collect sensitive personal or operational data and transmitting this data to a centralized server for training machine learning models raises significant privacy risks. Federated learning, where models are trained locally on individual devices and only model updates are shared with a central server, offers a promising approach to address these privacy concerns. However, implementing federated learning in heterogeneous and resource-constrained IoT environments presents technical challenges related to data distribution, communication efficiency and model aggregation.

Finally, the interpretability and explainability of machine learning models can be a challenge, particularly for complex deep learning architectures. Understanding why a particular behavior is flagged as anomalous is crucial for effective security analysis and incident response. Black-box models that lack transparency can hinder trust and make it difficult for security analysts to validate alerts and take appropriate actions. Developing more interpretable machine learning models or employing post-hoc explanation techniques is essential for building confidence in AI-driven anomaly detection systems.

Future Works and Research Directions in Machine Learning for IoT Anomaly Detection

The field of applying machine learning for anomaly detection in IoT is still rapidly evolving, with numerous promising avenues for future research and development. Addressing the challenges outlined previously and pushing the boundaries of current techniques will be crucial for building more robust, efficient and trustworthy AI-powered security solutions for the Internet of Things. Several key areas warrant significant attention in future works:

Enhanced feature engineering and selection for diverse IoT data

Future research should focus on developing more sophisticated and automated feature engineering techniques capable of extracting meaningful insights from the diverse data streams generated by IoT devices. This includes exploring methods for handling heterogeneous data types (e.g., time-series sensor data, network traffic logs, device metadata), dealing with missing or noisy data and identifying relevant features that are indicative of anomalous behavior across different IoT applications. Techniques like graph-based feature engineering and the incorporation of domain-specific knowledge could prove valuable in capturing complex relationships and contextual information. Furthermore, developing efficient feature selection methods that can adapt to the dynamic nature of IoT data and reduce the dimensionality for resource-constrained devices will be critical.

Development of lightweight and efficient machine learning models for edge deployment

A significant direction for future work involves the creation of more lightweight and energy-efficient machine learning models suitable for deployment on resource-constrained IoT devices. This includes exploring techniques such as model compression (e.g., pruning, quantization), knowledge distillation and the design of novel neural network architectures optimized for low-power hardware. Furthermore, research into distributed learning paradigms like federated learning and split learning needs to continue, focusing on addressing challenges related to communication efficiency, data heterogeneity across devices and ensuring the security and privacy of local model training.

Addressing concept drift and model adaptation in dynamic IOT environments

Future research must tackle the challenge of concept drift, where the statistical properties of the data and the definition of "normal" behavior change over time. This includes developing online learning algorithms that can continuously adapt models to evolving operational patterns without requiring complete retraining. Techniques for detecting concept drift and triggering model updates efficiently in resource-constrained environments are also crucial. Exploring meta-learning approaches that enable models to quickly adapt to new environments or device types with limited data could also be highly beneficial.

Advancing Few-Shot and Zero-Shot Anomaly Detection Techniques

Given the scarcity of labeled anomaly data in many IoT scenarios, future work should focus on advancing few-shot and zero-shot learning techniques for anomaly detection. This includes exploring methods that can learn to detect novel anomalies based on very few or even no prior examples of attacks. Techniques like meta-learning for anomaly detection, generative adversarial networks (GANs) for synthesizing anomalous data and transfer learning from related domains could play a significant role in addressing the labeled data bottleneck.

Enhancing the interpretability and explainability of anomaly detection models

Improving the interpretability and explainability of machine learning models is crucial for building trust and facilitating effective security analysis. Future research should explore the application of explainable AI (XAI) techniques to anomaly detection in IoT, enabling security analysts to understand why a particular behavior is flagged as anomalous. This includes developing methods for feature importance analysis, generating visual explanations and providing contextual information that aids in understanding the detected anomalies and their potential impact.

Integration of machine learning with existing security frameworks and threat intelligence

Future work should focus on seamlessly integrating machine learning-based anomaly detection systems with existing security information and event management (SIEM) systems, intrusion detection/prevention systems (IDS/IPS) and threat intelligence platforms. This includes developing standardized data formats and communication protocols for sharing anomaly alerts and contextual information. Leveraging threat intelligence feeds to inform the training and adaptation of machine learning models can also enhance their ability to detect known and emerging threats.

CONCLUSION

The escalating proliferation of Internet of Things devices has ushered in an era of unprecedented connectivity and data-driven opportunities. However, this hyper-connected landscape is fraught with burgeoning security challenges that traditional defense mechanisms struggle to address effectively. The inherent characteristics of IoT environments - their heterogeneity, resource constraints and dynamic nature - necessitate a paradigm shift towards more intelligent and adaptive security solutions.

Machine learning has emerged as a powerful enabler in this transition, offering the capability to learn complex patterns from vast amounts of IoT data and detect subtle anomalies indicative of malicious activity, system malfunctions or configuration errors. By leveraging various machine learning techniques, from unsupervised methods for novel threat discovery to supervised approaches for known attack identification, we can build more proactive and resilient security systems for the Internet of Things.

However, the journey towards fully realizing the potential of machine learning for IoT anomaly detection is not without its complexities. Challenges related to data heterogeneity and scale, resource limitations at the edge, the dynamic nature of IoT environments, the scarcity of labeled anomaly data, privacy concerns and the need for model interpretability must be diligently addressed.

REFERENCES

1. Gholizadeh M, Panah O. Система исследований в информационных системах управления здравоохранением. Sciencia Scripts Publishing. 2021.
2. Ostovar L, Vatan KK, Panahi O. Clinical Outcome of Thrombolytic Therapy. Scholars Press Academic Publishing. 2020.
3. Panahi O. Integrating dental and cardiac patient data for comprehensive health insights using AI. Ann Cardiolol. 2025;2:1007.
4. Panahi O. The Future of Medicine: Converging Technologies and Human Health. J Bio-Med Clin Res. 2025;2(1).
5. Panahi O. The Age of Longevity: Medical Advances and The Extension of Human Life. J Bio Med Clin Res. 2025;2.

6. Panahi O. Nanomedicine: Tiny Technologies, Big Impact on Health. J Bio Med Clin Res Publishers. 2025;2(1).
7. Panahi O. The evolving partnership: surgeons and robots in the maxillofacial operating room of the future. J Dent Sci Oral Care. 2025;1(1):1-7.
8. Panahi O. Nanotechnology, Regenerative Medicine and Tissue Bioengineering. Scholars Press Academic Publishing. 2019.
9. Zarei S, Panahi O, Bahador N. Antibacterial activity of aqueous extract of eucalyptus camaldulensis against Vibrio harveyi (PTCC1755) and Vibrio alginolyticus (MK641453.1). Saarbucken: LAP. Lambert Academic Publishing. 2019.
10. Zarei S, Panahi O. Eucalyptus camaldulensis Extract as a Preventive to the Vibriosis, Scholars Press Academic Publishing. 2019.
11. Panahi O. Dental Implants the Rise of AI. On J Dent Oral Health. 2024;8(1).
12. Omid P, Sevil Farrokh E. Bioengineering Innovations in Dental Implantology. Curr Trends Biomedical Eng, Bio sci. 2025;23(3):556111.
13. Panahi P, Bayılmış C, Çavuşoğlu U, Kaçar S. Performance evaluation of lightweight encryption algorithms for IoT-based applications. Arabian J Sci Eng. 2021;46(4):4015-4037.
14. Panahi U, Bayılmış C. Enabling secure data transmission for wireless sensor networks based IoT applications. Ain Shams Eng J. 2023;14(2):101866.
15. Panahi O, Panahi U. AI-Powered IoT: Transforming Diagnostics and Treatment Planning in Oral Implantology. J Adv Artif Intell Mach Learn. 2025;1(1):1-4.
16. Panahi O, Esmaili F, Kargarnezhad S. Искусственный интеллект в стоматологии. SCIENCIA SCRIPTS Publishing. 2024.
17. Esmaielzadeh S, Panahi O, Çay FK. Application of Clay's in Drug Delivery in Dental Medicine. Scholars Press Academic Publishing. 2020.
18. Gholizadeh M, Panahi O. Investigating System in Health Management Information Systems. Scholars Press Academic Publishing. 2021.
19. Gholizadeh M, Panahi O. Untersuchungssystem im Gesund heits management Informations system. Unser wissen Publishing. 2021.
20. Gholizadeh M, Panahi O. Sistema de investigación en sistemas de información de gestión sanitaria, Nuestro Conoc. MENTO Publishing. 2021.
21. Gholizadeh M, Panahi O. Système d'investigation dans les systèmes d'information de gestion de la santé. EDITION NOTRE SAVOIR Publishing. 2021.
22. Gholizadeh M, Panahi O. Indagare il sistema nei sistemi informativi di gestione della salute. SAPIENZA Publishing. 2021.
23. Gholizadeh M, Panahi O. Systeemonderzoek in Informatiesystemen voor Gezondheidsbeheer. ONZE KENNIS Publishing. 2021.
24. Gholizadeh M, Panahi O. System badawczy w systemach informacyjnych zarządzania zdrowiem. NAZSA WIEDZA Publishing. 2021.

25. Panahi O, Azarfardin A. Computer-Aided Implant Planning: Utilizing AI for Precise Placement and Predictable Outcomes. J Dentistry Oral Health. 2(1).
26. Gholizadeh M, Panahi O. Sistema de Investigação em Sistemas de Informação de Gestão de Saúde. NOSSO CONHECIMENTO Publishing. 2021.
27. Panahi O. The Algorithmic Healer: AI's Impact on Public Health Delivery. Medi Clin Case Rep J. 2025;3(1):759-762.
28. Panahi O. The Future of Healthcare: AI, Public Health and the Digital Revolution. MediClin Case Rep J. 2025;3(1):763-766.
29. Panahi O, Raouf MF, Patrik K. The evaluation between pregnancy and peridontal therapy Int J Acad Res. 2011;3:1057-1058.
30. Panahi O, Melody FR, Kennet P, Tamson MK. Drug induced (calcium channel blockers) gingival hyperplasia. JMBS. 2011;2(1):10-12.
31. Omid P. Relevance between gingival hyperplasia and leukemia. Int J Acad Res. 2011;3:493-494.
32. Panahi O, Çay FK. Nano Technology, Regenerative Medicine and, Tissue Bio-Engineering. Acta Scientific Dental Sciences. 2023;7(4):118-122.
33. Panahi O. Dental Pulp Stem Cells: A Review. Acta Scientific Dental Sci. 2024;8(2):22-24.
34. Panahi U. AD HOC Networks: Applications, Challenges, Future Directions. Scholars' Press. 2025.
35. Panahi P. Artificial intelligence in Dentistry, Scholars Press. Academic Publishing.
36. Panahi O. Smart Robotics for Personalized Dental Implant Solutions. Dental. 2025;7(1):21.
37. Panahi P, Freund M. Safety Application Schema for Vehicular Virtual Ad Hoc Grid Networks, Int J Academic Res. 2011;3(2).
38. Panahi P. New Plan for Hardware Resource Utilization in Multimedia Applications Over Multi Processor Based System, MIPRO 2009. 32nd Int Convention Conf GRID AND VISUALIZATION SYSTEMS (GVS) 2009:256-260.
39. Panahi O, Eslamlou SF. Peridontium: Struktur, Funktion und klinisches Management.
40. Panahi O, Eslamlou SF. Peridoncio: Estructura, función y manejo clínico.
41. Panahi O, Eslamlou SF. Le péridontium: Structure, fonction et gestion Clinique.
42. Panahi O, Eslamlou SF. Peridonio: Struttura, funzione e gestione clinica.
43. Panahi O, Eslamlou SF. Peridontium: Struktura, funkcja i postępowanie kliniczne.
44. Pejmanpanahi B. Kalman Filtering of Link Quality Indicator Values for Position Detection by Using WSNS. Int J Computing, Communications Instrumentation Eng. 2014;1.
45. Panahi O. The Algorithmic Healer: AI's Impact on Public Health Delivery. Med Clin Case Rep J. 2025;3(1):759-762.
46. Panahi O. The Future of Healthcare: AI, Public Health and the Digital Revolution. Med Clin Case Rep J. 2025;3(1):763-766.
47. Panahi O. Comparison between unripe Makopa fruit extract on bleeding and clotting time. Int J Paediatric Dentistry. 2013;23:205.
48. Panahi O, Arab MS, Tamson KM. Gingival Enlargement and Relevance with Leukemia. Int J Academic Res. 2011;3(2).

49. Panahi O. Stammzellen aus dem Zahnmark 2021.
50. Panahi O. Células madre de la pulpa dental 2021.
51. Panahi O. Стволовые клетки пульпы зуба 2021.
52. Panahi O. Cellules souches de la pulpe dentaire 2021.
53. Panahi O. Cellule staminali della polpa dentaria 2021.
54. Panahi O. Células estaminais de polpa dentária 2021.
55. Panahi O. A Novel Scheme About Extraction Orthodontic and Ortho Therapy. Int J Academic Res. 2011;3(2).
56. Panahi O, Nunag GM, Siyahtan AN. Molecular Pathology: P-115: Correlation of Helicobacter Pylori and Prevalent Infections in Oral Cavity. Cell J Int Student Congress on Cell Molecular Med. 2011;12:91-92.
57. Panahi P, Bayılmış C, Çavuşoğlu U, Kaçar S. Performance Evaluation of L-Block Algorithm for IoT Applications. UluslararasıBilgisayarBilimleri veMühendisliğiKonferansı. 2018:609-612.
58. Panahi P, Bayılmış C, Çavuşoğlu U, Kaçar S. Comparing PRESENT and L Block ciphers over IoT Platform. 12th Int Conf Information Security Cryptology. 2019:66-69.
59. PanahiU. Nesnelerininternetiiçinhafifsıkletkriptolojialgoritmalarınadayalıgüvenlihaberleşmemodelitasarımı. SakaryaÜniversitesi, Fen BilimleriEnstitüsü Sakarya. 2022.
60. Koyuncu B, Panahi P, Varlioglu S. Comparative Indoor Localization by using Landmarc and Cricket Systems. Int J Emerging Techno Adv Eng. 2015;5(6):453-456.
61. Panahi O, Eslamlou SF, Jabbarzadeh M. Digitale Zahnmedizin und künstliche Intelligenz.
62. Panahi O, Eslamlou SF, Jabbarzadeh M. Odontología digital e inteligencia artificial 2025.
63. Panahi O, Eslamlou SF, Jabbarzadeh M. Dentisterie numérique et intelligence artificielle 2025.
64. Panahi O, Eslamlou SF, Jabbarzadeh M. Odontoiatria digitale e intelligenza artificiale 2025.
65. Panahi O, Eslamlou SF, Jabbarzadeh M. Stomatologia cyfrowa i sztuczna inteligencja.
66. Panahi O, Eslamlou SF, Jabbarzadeh M. Medicina dentária digital e inteligência artificial.
67. Panahi O, Jabbarzadeh M. The Expanding Role of Artificial Intelligence in Modern Dentistry. On J Dent Oral Health. 2025;8(3).
68. Omid P, Shabnam D. Mitigating Aflatoxin Contamination in Grains: The Importance of Postharvest Management Practices. Adv Biotech Micro. 2025;18(5):555996.
69. Panahi O, Ezzati A. AI in Dental-Medicine: Current Applications & Future Directions. Open Access J Clin Images. 2025;2(1):1-5.
70. Koyuncu B, Gokce A, Panahi P. Reconstruction of an Archeological site in real time domain by using software techniques. In 2015 Fifth Int Conf Communication Systems Network Technologies. 2015:1350-1354.
71. Omid P, Soren F. The Digital Double: Data Privacy, Security and Consent in AI Implants West J Dent Sci. 2025;2(1):108.
72. Panahi U. Redes AD HOC: Aplicações, Desafios, Direcções Futuras, Edições Nosso Conhecimento.
73. Panahi U. Sieci AD HOC: Zastosowania, wyzwania, przyszłe kierunki, Wydawnictwo Nasza Wiedza.
74. Panahi U. Reti AD HOC: Applicazioni, sfide e direzioni future, Edizioni Sapienza.
75. Panahi O, Eslamlou SF. Peridontium: Estrutura, função e gestão clínica.

76. Panahi O, Dadkhah S. AI in der modernen Zahnmedizin 2022.
77. Panahi O, Dadkhah S. La IA en la odontología moderna 2025.
78. Panahi O, Dadkhah S. L'IA dans la dentisterie modern 2025.
79. Panahi O, Dadkhah S. L'intelligenza artificiale nell'odontoiatria moderna 2025.
80. Panahi O, Dadkhah S. Sztuczna inteligencja w nowoczesnej stomatologii 2025.
81. Panahi O, Dadkhah S. A IA na medicina dentária moderna 2025.
82. Panahi U. Redes AD HOC: Aplicaciones, retos y orientaciones futuras, Ediciones Nuestro Conocimiento.
83. Panahi U. Réseaux AD HOC: Applications, défis et orientations futures. Editions Notre Savoir.
84. Panahi U. AD HOC-Netze: Anwendungen, Herausforderungen, zukünftige Wege, Verlag Unser Wissen.
85. Panahi O. The Role of Artificial Intelligence in Shaping Future Health Planning. Int J Health Policy Plann. 2025;4(1):01-05.
86. Panahi O. AI in Health Policy: Navigating Implementation and Ethical Considerations. Int J Health Policy Plann. 2025;4(1):01-05.
87. Panahi O. Dental Implants & the Rise of AI. On J Dent Oral Health. 2024;8(1).
88. Panahi O, Falkner S. Telemedicine, AI and the Future of Public Health. Western J Med Sci Res. 2025;2(1):102.
89. Panahi O. Innovative Biomaterials for Sustainable Medical Implants: A Circular Economy Approach. European J Innovative Studies Sustainability. 2025;1(2):1-5.
90. Panahi O. Wearable Sensors and Personalized Sustainability: Monitoring Health and Environmental Exposures in Real-Time. European J Innovative Studies Sustainability. 2025;1(2):1-5.
91. Panahi O. AI-Enhanced Case Reports: Integrating Medical Imaging for Diagnostic Insights. J Case Rep Clin Images. 2025;8(1):1161.
92. Panahi O. AI and IT in Medical Imaging: Case Reports. J Case Rep Clin Images. 2025;8(1):1160.
93. Panahi O, Farrokh S, Amirloo A. Robotics in Implant Dentistry: Current Status and Future Prospects. Scientific Archives of Dental Sci. 2022;57(9):55-60.
94. Omid P, Soren F. The Digital Double: Data Privacy, Security and Consent in AI Implants. Digit J Eng Sci Technol. 2025;2:105.
95. Panahi O. Algorithmic Medicine. J Medical Discoveries. 2025;2(1).
96. Panahi O. Deep Learning in Diagnostics. J Med Discoveries. 2025;2(1).
97. Panahi O. AI in Health Policy: Navigating Implementation and Ethical Considerations. Int J Health Policy Plann. 2025;4(1):01-05.
98. Panahi O. The Role of Artificial Intelligence in Shaping Future Health Planning. Int J Health Policy Plann. 2025;4(1):01-05.
99. Panahi O. Secure IoT for Healthcare. European J Innovative Studies, Sustainability. 2025;1(1):1-5.
100. Omid P, Evil Farrokh E. Beyond the Scalpel: AI, Alternative Medicine and the Future of Personalized Dental Care. J Complement Med Alt Healthcare. 2024;13(2):555860.
101. Panahi O, Farrokh S. Ethical Considerations of AI in Implant Dentistry: A Clinical Perspective. J Clin Rev Case Rep. 2025;10(2):01-05.

102. Panahi O, Ezzati A, Zeynali M. Will AI Replace Your Dentist? The Future of Dental Practice. OnJ Dent Oral Health. 2025;8(3).

103. Panahi O. Navigating the AI Landscape in Healthcare and Public Health. Mathews J Nurs. 2025;7(1):56.

104. Panahi O, Esmaili F, Kargarnezhad S. Künstliche Intelligenz in der Zahnmedizin. Unser wissen Publishing 2024.

105. Panahi O, Esmaili F, Kargarnezhad S. Artificial Intelligence in Dentistry, Scholars Press Publishing. 2024.

106. Panahi O, Esmaili F, Kargarnezhad S. Inteligencia artificial en odontología. NUESTRO CONOC MENTO Publishing 2024.

107. Panahi O, Esmaili F, Kargarnezhad S. L'intelligence artificielle dans l'odontologie. EDITION NOTRE SAVOIR Publishing Publishing. 2024.

108. Panahi O, Esmaili F, Kargarnezhad S. Intelligenza artificiale in odontoiatria, SAPIENZA Publishing. 2024.

109. Panahi O, Esmaili F, Kargarnezhad S. Inteligência Artificial em Medicina Dentária, NOSSO CONHECIMENTO Publishing. 2024.