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

Automated Security Response in IoT Networks Using AI

Soren Falkner*

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

Citation: *Falkner S. Automated Security Response in IoT Networks Using AI. Arch Adv Art Intel Data Sci Mach Learn 2025;1(1):1-12.*

Received Date: May 09, 2025**; Accepted Date** May 12, 2025**; Published Date:** May 14, 2025

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

Copyright: ©2025 Falkner S. this is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.

ABSTRACT

The increasing scale and complexity of Internet of Things (IoT) networks necessitate automated security response mechanisms to effectively mitigate threats in a timely manner. Manual intervention often proves insufficient to handle the volume and speed of potential attacks targeting vulnerable IoT devices and infrastructure. Artificial Intelligence (AI) offers a promising avenue for developing intelligent and autonomous security response systems capable of detecting, analyzing and reacting to security incidents in real-time. This paper explores the application of various AI techniques, including machine learning, rule-based expert systems and reinforcement learning, for automating security responses in IoT networks. We discuss the challenges and opportunities associated with implementing such systems, including the need for accurate threat detection, context-aware decision-making, secure actuation and minimizing disruption to normal operations. Furthermore, we examine potential AI-driven automated responses to common IoT threats, such as malware propagation, denial-of-service attacks and data breaches. Finally, we highlight future research directions focused on developing robust, adaptive and trustworthy AI-powered automated security response systems for the evolving IoT landscape.

Keywords: Automated security response; Internet of things (IoT); Artificial intelligence (AI); Machine learning, Reinforcement learning; Expert systems; Intrusion response; Threat mitigation; Security automation; Cyber security; Network security; Edge computing; Real-time response

INTRODUCTION

The Imperative for Automated Security Response in the Expanding IoT Ecosystem

The Internet of Things (IoT) has rapidly transformed the technological landscape, connecting billions of devices across diverse domains, from smart homes and wearable technology to industrial control systems and critical infrastructure. This unprecedented connectivity offers numerous benefits, including enhanced efficiency, automation and data-driven insights. However, the sheer scale and heterogeneity of IoT networks have also created

a significantly expanded attack surface, making them increasingly vulnerable to a wide array of cyber threats. The inherent limitations of many IoT devices [1-34], such as constrained computational resources, diverse communication protocols and often weak built-in security, further exacerbate these vulnerabilities. As the reliance on IoT continues to grow, the potential consequences of successful cyberattacks, ranging from data breaches and service disruptions to physical harm and economic losses, become increasingly severe.

Traditional security approaches, often relying on manual analysis and reactive responses, are proving inadequate to address the dynamic and sophisticated threats targeting IoT environments. The volume and velocity of potential attacks can easily overwhelm human security teams, leading to delayed responses and increased damage. Moreover, the distributed nature of IoT networks and the sheer number of interconnected devices make centralized monitoring and manual intervention impractical. The need for timely and effective threat mitigation in IoT networks necessitates a paradigm shift towards automated security response mechanisms capable of operating at the speed and scale required to protect these complex ecosystems.

Automated security response involves the use of technologies and processes to automatically identify, analyze and react to security incidents without or with minimal human intervention. In the context of IoT [35-48], this capability is crucial for several reasons. Firstly, it enables rapid containment of threats, preventing them from spreading across the network and compromising more devices or data. Secondly, automation can improve the efficiency and effectiveness of security operations by freeing up human analysts to focus on more complex threats and strategic decision-making. Thirdly, automated responses can ensure consistent and timely application of security policies, reducing the risk of human error or delayed action. As IoT environments become more intricate and the threat landscape more sophisticated, the ability to automate security responses will be paramount for maintaining the integrity, availability and safety of these interconnected systems.

The role of artificial intelligence in enabling autonomous IoT security responses

Artificial Intelligence (AI), with its ability to learn, reason and make decisions based on data, offers a powerful toolkit for developing intelligent and autonomous security response systems for IoT networks. Various AI techniques, including machine learning (ML), rule-based expert systems and reinforcement learning (RL), can be leveraged to automate different aspects of the security response lifecycle, from threat detection and analysis to incident containment and recovery.

Machine learning algorithms play a crucial role in enhancing the accuracy and efficiency of threat detection in IoT environments. By learning patterns of normal and anomalous behavior from vast amounts of network traffic, device logs and sensor data, ML models can identify potential security incidents that might be missed by traditional signature-based or rule-based systems. Once a threat is detected, AI [49-60] can assist in the analysis phase by automatically correlating events, identifying affected devices and assessing the potential impact of the incident. This automated analysis can provide security teams with valuable context and insights, enabling them to make more informed decisions about the appropriate response actions.

Rule-based expert systems, while less adaptive than machine learning models, can be effective for automating responses to well-defined and known threats. These systems utilize predefined rules based on expert knowledge to trigger specific actions when certain security events occur. For instance, a rule could automatically isolate a device exhibiting known malicious behavior or block traffic from a blacklisted IP address. While lacking the learning capabilities of ML, expert systems can provide deterministic and predictable responses to common attack patterns.
Reinforcement learning offers a promising approach for developing adaptive and autonomous security response policies in dynamic IoT environments [61-78]. RL agents can learn optimal response strategies by interacting with the environment and receiving feedback (rewards or penalties) based on the outcomes of their actions. This allows the system to learn how to effectively mitigate threats in complex and uncertain situations, potentially even discovering novel response strategies that might not be explicitly programmed. For example, an RL agent could learn the most effective sequence of actions to contain a distributed denial-of-service (DDoS) attack targeting a network of IoT devices.

The integration of these AI techniques [79-90] holds the potential to revolutionize security response in IoT networks. By automating the detection, analysis and reaction to security incidents, AI-powered systems can significantly reduce response times, minimize the impact of attacks and improve the overall security posture of the connected world. However, the successful implementation of automated security response in IoT environments requires careful consideration of several critical factors, including the need for accurate and reliable threat detection, the ability to make context-aware decisions, the secure actuation of response actions and the minimization of disruptions to normal operations. The subsequent sections of this paper will delve deeper into these considerations and explore the potential of various AI techniques [91-99] for enabling robust and autonomous security response in the evolving landscape of the Internet of Things.

CHALLENGES

While the potential benefits of AI-driven automated security response in IoT networks are significant, realizing this vision presents a complex set of challenges that span technical, operational and ethical domains. Overcoming these hurdles is crucial for building effective and trustworthy autonomous security systems for the Internet of Things.

One of the primary challenges lies in ensuring accurate and reliable threat detection. Automated response systems are only as effective as their ability to correctly identify malicious activity. Relying on flawed or inaccurate threat detection can lead to either missed attacks or, equally problematic, the triggering of unnecessary responses to benign events (false positives). In the context of AI, this requires robust machine learning models that are trained on representative and high-quality data, capable of distinguishing subtle anomalies from normal variations in IoT device behavior and network traffic. Addressing the challenges of data heterogeneity, class imbalance (where normal behavior significantly outweighs malicious activity) and the dynamic nature of IoT threats is paramount for achieving high detection accuracy and minimizing false alarms.

Context-aware decision-making is another critical challenge. Automated response systems must be able to

understand the context of a detected threat and make intelligent decisions about the appropriate course of action [100-109]. A generic response that indiscriminately isolates devices or blocks traffic could disrupt critical IoT functions or even lead to safety hazards in industrial or healthcare settings. AI algorithms need to consider factors such as the type of device, its role in the network, the severity of the threat and the potential impact of different response actions. This requires integrating information from various sources, including network topology, device configurations and application-level data, to make nuanced and contextually appropriate response decisions.

Secure actuation of response actions is paramount in automated security systems. Once a response decision is made, the system must be able to securely and reliably execute the necessary actions on the affected IoT devices or network infrastructure. This involves ensuring the integrity and confidentiality of the commands issued by the AI-powered system and preventing malicious actors from exploiting the response mechanisms themselves. Given the resource constraints and diverse communication protocols prevalent in IoT environments, implementing secure actuation mechanisms across a heterogeneous network presents significant technical complexities. Secure over-the-air updates, authenticated command channels and robust access control mechanisms are essential to prevent unauthorized manipulation of response actions.

Minimizing disruption to normal operations is a crucial consideration for any automated security response system. Overly aggressive or poorly calibrated responses can inadvertently disrupt legitimate IoT functionalities, leading to service outages or operational inefficiencies. AI algorithms need to be designed to implement responses that are proportionate to the threat and minimize collateral damage. This requires careful tuning of response thresholds, the ability to implement granular and targeted actions and mechanisms for rollback or remediation in case of unintended consequences. Ensuring the resilience and availability of critical IoT services while automatically responding to threats is a delicate balancing act.

Furthermore, the diversity and resource constraints of IoT devices pose significant challenges for deploying and managing automated response capabilities at the edge. Many low-power IoT devices lack the computational resources to run complex AI models or execute sophisticated response actions locally. This necessitates exploring distributed architectures where threat detection and response decisions might be made at more capable edge devices or gateways, which then orchestrate actions on the end nodes. However, this introduces challenges related to communication latency, coordination across multiple devices and ensuring consistent security policies throughout the network.

The lack of standardized protocols and data formats across the IoT ecosystem also hinders the development and deployment of interoperable automated security response systems. The fragmented nature of the IoT market, with numerous vendors and proprietary technologies, makes it difficult to collect and analyze data consistently and to implement uniform response actions across different device types and platforms. The development and adoption of open standards and common data models would significantly facilitate the creation of more integrated and effective automated security solutions.

Finally, ethical considerations and the potential for unintended consequences must be carefully addressed. Automated security response systems operate with a degree of autonomy and their decisions can have significant real-world impacts. It is crucial to ensure that these systems are designed and deployed in a way that is fair, transparent and accountable. Thorough testing, validation and human oversight mechanisms are necessary to mitigate the risk of unintended consequences or biases in the AI algorithms that could lead to inappropriate or harmful actions.

FUTURE WORKS

The field of AI-powered automated security response in IoT is ripe with opportunities for future research and development. Addressing the challenges outlined previously and pushing the boundaries of current capabilities will be crucial for building truly autonomous and effective security systems for the ever-expanding Internet of Things. Several key areas warrant significant attention in future works:

Enhancing contextual awareness and intelligent decision-making

Future research should focus on developing AI algorithms that can achieve a deeper understanding of the context surrounding security events in IoT networks. This includes incorporating knowledge about device functionality, network topology, user behavior and the criticality of different assets. Techniques like knowledge graphs, semantic reasoning and hybrid AI approaches that combine machine learning with symbolic reasoning can enable more nuanced and context-aware response decisions, minimizing disruptions to normal operations while effectively mitigating threats.

Developing adaptive and dynamic response strategies

Future work should explore the use of reinforcement learning and other adaptive control techniques to enable automated response systems to learn and evolve their strategies over time. This includes the ability to dynamically adjust response parameters based on the evolving threat landscape, the characteristics of the attacked network and the observed outcomes of previous actions. Developing multi-agent reinforcement learning approaches could also facilitate coordinated and collaborative responses across multiple devices or network segments.

Ensuring secure and resilient actuation mechanisms

Research is needed to develop more robust and secure mechanisms for actuating automated responses in diverse and resource-constrained IoT environments. This includes exploring secure communication protocols, hardware-based security enclaves for executing critical response actions and decentralized control architectures to prevent single points of failure. Investigating blockchain technologies for maintaining the integrity and auditability of response commands could also be a promising direction.

Minimizing false positives and enhancing response precision

Future work should focus on improving the accuracy of AI-driven threat detection to minimize false positives, which can lead to unnecessary disruptions and erode trust in automated response systems. This includes exploring advanced anomaly detection techniques, incorporating explainable AI (XAI) methods to understand the reasoning

behind alerts and developing feedback mechanisms that allow security analysts to refine the system's detection and response policies over time.

Addressing the challenges of edge-based automated response

Research is needed to develop efficient and lightweight AI models and response mechanisms that can be deployed and executed directly on resource-constrained IoT devices or edge gateways. This includes exploring model compression techniques, federated learning for collaborative model training at the edge and the development of specialized hardware accelerators for AI inference on IoT devices.

Fostering interoperability and standardization

Future efforts should promote the development and adoption of open standards and common data formats for security events and response actions in IoT. This would facilitate the interoperability of different security tools and enable the creation of more integrated and effective automated response systems across heterogeneous IoT deployments. Collaboration between industry consortia, research institutions and standardization bodies is crucial in this regard.

Incorporating human oversight and explainability

While the goal is to automate security responses, maintaining appropriate levels of human oversight and ensuring the explainability of AI-driven decisions remain critical. Future research should explore methods for providing security analysts with clear and concise explanations of why certain response actions were taken, allowing for human review and intervention when necessary. Developing mechanisms for seamless human-machine collaboration in incident response workflows is also essential.

Addressing privacy and security of automated response systems

Future work must address the privacy and security implications of deploying AI-powered automated response systems. This includes ensuring the confidentiality and integrity of the data used for training and decision-making, protecting the AI models themselves from adversarial attacks and adhering to relevant data privacy regulations. Exploring privacy-preserving AI techniques and secure model deployment strategies is crucial.

Developing comprehensive evaluation frameworks and benchmarks

The lack of standardized evaluation frameworks and benchmarks hinders the comparison and progress of automated security response techniques for IoT. Future research should focus on creating realistic and diverse testbeds and metrics that can effectively evaluate the performance, security and resilience of these systems under various attack scenarios and operational conditions.

Exploring novel AI paradigms for automated response

Future work could explore the application of emerging AI paradigms, such as neuromorphic computing for

energy-efficient real-time response and bio-inspired algorithms for developing robust and adaptive security strategies in complex IoT environments.

CONCLUSION

The imperative for automated security response in Internet of Things (IoT) networks has become undeniable. The sheer scale, heterogeneity and dynamic nature of these interconnected ecosystems render traditional, manual security approaches increasingly inadequate in the face of evolving and sophisticated cyber threats. Artificial Intelligence offers a transformative potential, enabling the development of intelligent and autonomous systems capable of detecting, analyzing and reacting to security incidents with the speed and scale required to protect the vast and expanding IoT landscape.

By leveraging the power of machine learning for enhanced threat detection, expert systems for rule-based responses and reinforcement learning for adaptive strategies, we can move towards a future where IoT networks are more resilient and self-defending. Automated security response promises faster incident containment, improved operational efficiency for security teams and consistent enforcement of security policies, ultimately reducing the risks associated with the growing attack surface of the IoT.

However, the journey towards fully autonomous IoT security is fraught with significant challenges. Ensuring accurate threat detection, achieving context-aware decision-making, implementing secure actuation mechanisms, minimizing operational disruptions, addressing device diversity and resource constraints, fostering interoperability and maintaining necessary human oversight are all critical hurdles that must be overcome. Furthermore, ethical considerations and the potential for unintended consequences demand careful attention throughout the design and deployment of these AI-powered systems.

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. Nesnelerininternetiiçinhafifsıkletkriptolojialgoritmalarınadayalıgüvenlihaberleşmemodelitasarı mı. 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 CONOCMENTO 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.