Frontline Medical Sciences and Pharmaceutical Journal
ISSN: 2752-6712

Emerging Trends in Medical Science and Intelligent Pharmaceutical Engineering for Next-Generation Healthcare Solutions

Dr. Ken Jan
Department of Pharmaceutical Sciences, Harvard University, United States of America

ARTICLE INfO

Articlehistory:
Submission Date:20May2026
Accepted Date:30Mayl2026
Published Date:03June2026
VOLUME: Vol.06Issue06
Page No. 14-20

ABSTRACT

The rapid convergence of medical science, pharmaceutical engineering, and intelligent computational systems is reshaping next-generation healthcare ecosystems. Emerging technologies such as Internet of Medical Things (IoMT), artificial intelligence, cybersecurity frameworks, ontology-based systems, and intelligent robotic surgery platforms are redefining how healthcare services are designed, delivered, and managed. This research explores the evolving landscape of intelligent pharmaceutical engineering and medical science by synthesizing advancements in secure medical communication systems, automated drug information systems, cybersecurity-aware medical devices, and intelligent healthcare analytics frameworks.

The study focuses on integrating computational intelligence with pharmaceutical and medical infrastructures to enhance safety, efficiency, and decision-making in healthcare environments. A significant emphasis is placed on cybersecurity vulnerabilities and risk mitigation strategies, as modern healthcare systems are increasingly exposed to cyber threats due to interconnected medical devices and cloud-based infrastructures. Prior research highlights that security vulnerabilities in medical devices and IoMT systems can directly impact patient safety and system reliability (Williams & Woodward, 2015; Yaqoob et al., 2019).

Additionally, intelligent pharmaceutical engineering systems such as drug information databases, ontology-driven platforms, and rule-based reasoning systems are analyzed for their role in reducing adverse drug events and improving clinical decision-making processes (Lazarou et al., 1998; Pirmohamed et al., 2004). The integration of technologies such as NFC/RFID systems, barcode scanning frameworks, and rule engines demonstrates the increasing automation in pharmaceutical workflows (Jara et al., 2009; Jess, 2009).

The research also highlights the role of surgical robotics and AI-driven diagnostic systems in enhancing precision medicine and minimally invasive procedures (Zhu et al., 2021).

Keywords: Internet of Medical Things (IoMT), Intelligent Pharmaceutical Engineering, Cybersecurity in Healthcare, Artificial Intelligence in Medicine, Medical Robotics, Drug Information Systems

INTRODUCTION

The healthcare industry is undergoing a transformative shift driven by rapid advancements in computational intelligence, pharmaceutical engineering, and digital medical technologies. Traditional healthcare systems, which were largely dependent on manual processes and isolated medical infrastructures, are now evolving into interconnected, intelligent ecosystems capable of real-time decision-making, predictive analytics, and autonomous operation. This transformation is primarily fueled by the integration of Internet of Medical Things (IoMT), artificial intelligence, cybersecurity frameworks, and advanced pharmaceutical information systems.

One of the most significant developments in modern healthcare is the integration of IoMT-based systems that connect medical devices, patient monitoring tools, and hospital information systems into unified digital networks. These systems enable continuous data exchange and real-time monitoring of patient health conditions. However, the increasing interconnectivity also introduces significant cybersecurity risks. Research has demonstrated that medical devices and networked healthcare systems are highly vulnerable to cyberattacks, which can compromise patient safety and system reliability (Yaqoob et al., 2019). The growing concern over healthcare cybersecurity highlights the need for robust security frameworks that ensure confidentiality, integrity, and availability of medical data.

Another critical dimension of this transformation is intelligent pharmaceutical engineering, which focuses on automating drug management, prescription systems, and pharmaceutical decision-making processes. Adverse drug reactions remain a major challenge in healthcare systems globally, contributing to hospital admissions, increased healthcare costs, and patient mortality (Lazarou et al., 1998; Classen et al., 1997). Intelligent pharmaceutical systems aim to reduce such risks by integrating automated drug information systems, ontology-based drug databases, and AI-driven decision support tools. These systems enable healthcare professionals to access real-time drug interaction data, dosage recommendations, and patient-specific medication insights.

Technologies such as RFID, NFC, and barcode-based medical identification systems have further enhanced pharmaceutical engineering processes. These technologies facilitate accurate patient identification, medication tracking, and supply chain management in healthcare environments (Jara et al., 2009; LibNFC, 2009). Similarly, ontology-based knowledge systems such as Protégé and rule engines like Jess enable structured medical reasoning and intelligent decision-making within pharmaceutical domains (Protégé, 2009; Jess, 2009). These systems contribute to reducing human errors and improving the efficiency of clinical workflows.

In parallel, artificial intelligence and machine learning technologies are increasingly being applied in medical diagnostics, robotic surgery, and predictive healthcare analytics. Intelligent surgical systems and robotic platforms have significantly improved the precision and safety of minimally invasive procedures (Zhu et al., 2021). These technologies enhance surgical outcomes while reducing recovery time and operational risks. Additionally, AI-driven predictive models are being used for disease detection, risk stratification, and personalized treatment planning.

Despite these advancements, healthcare systems face multiple challenges including cybersecurity vulnerabilities, interoperability issues, and system complexity. Cybersecurity in healthcare has become a critical concern due to increasing incidents of data breaches and ransomware attacks targeting medical institutions (Aldosari, 2025). Studies have emphasized that cybersecurity threats in healthcare not only affect data systems but also directly impact patient safety and clinical outcomes (Cartwright, 2023). Therefore, the development of secure, resilient, and adaptive healthcare infrastructures is essential for sustaining digital health transformation.

The objective of this research is to explore emerging trends in medical science and intelligent pharmaceutical engineering with a focus on technological integration, cybersecurity challenges, and system optimization. The study aims to provide a comprehensive understanding of how intelligent systems are reshaping healthcare delivery and pharmaceutical processes. Furthermore, it investigates the implications of these technologies on patient safety, operational efficiency, and clinical decision-making.

This research is significant because it bridges the gap between medical science and intelligent engineering systems, highlighting the interdisciplinary nature of modern healthcare innovation. By analyzing existing technologies and frameworks, the study provides insights into the future direction of healthcare systems, emphasizing the need for secure, intelligent, and interoperable medical infrastructures.

REVIEW OF LITERATURE

The literature on intelligent healthcare systems reveals a strong convergence between medical science, pharmaceutical engineering, and computational intelligence. One of the foundational concerns in healthcare systems is the prevalence of adverse drug reactions, which significantly impact patient safety and healthcare costs. Studies have shown that adverse drug reactions are a major cause of hospital admissions and can lead to extended hospital stays and increased mortality rates (Pirmohamed et al., 2004). Earlier research also highlights the economic and clinical burden associated with drug-related complications in hospital environments (Classen et al., 1997). These findings underscore the need for intelligent pharmaceutical systems capable of detecting and preventing medication-related risks.

Drug information systems have played a crucial role in addressing these challenges. Early pharmaceutical databases, particularly in industrial healthcare environments, were developed to manage drug data and improve clinical decision-making (Yamamoto et al., 1998). These systems provided structured access to pharmaceutical knowledge, enabling healthcare professionals to make informed

decisions regarding prescriptions and drug interactions. Similarly, ontology-based systems such as Protégé have enabled the formal representation of medical knowledge, facilitating interoperability and semantic reasoning in healthcare applications (Protégé, 2009).

The integration of rule-based systems and logic engines such as Jess has further enhanced intelligent decision-making in pharmaceutical engineering. These systems allow automated reasoning over medical data, enabling the identification of drug interactions, dosage recommendations, and treatment optimization strategies (Jess, 2009). Additionally, integration frameworks such as JessTab demonstrate the interoperability between ontology-based systems and rule engines, improving the efficiency of medical knowledge processing (Eriksson, 2006).

Cybersecurity in healthcare systems has emerged as a critical area of research due to increasing digitalization and interconnectivity of medical devices. Studies highlight that cybersecurity vulnerabilities in medical devices pose significant risks to patient safety and healthcare infrastructure (Williams & Woodward, 2015). More recent research emphasizes that Internet of Medical Things ecosystems are particularly vulnerable to cyber threats due to their distributed architecture and real-time data exchange mechanisms (Thomasian & Adashi, 2021). Surveys on IoMT security further reveal the complexity of ensuring privacy and data protection in connected healthcare systems (Sun et al., 2019).

Further research indicates that healthcare cybersecurity is not only a technical issue but also a patient safety concern. Hospitals and medical institutions face increasing risks from cyberattacks that can disrupt clinical operations and compromise sensitive patient data (Ghafur & Durkin, 2021). Frameworks for risk analysis and mitigation have been proposed to address these challenges, focusing on integrated security models for medical devices (Kim et al., 2020). Additionally, comprehensive reviews of networked medical device vulnerabilities highlight the need for regulatory compliance and robust cybersecurity policies (Yaqoob et al., 2019).

Technological advancements in medical identification systems such as RFID and NFC have further contributed to the development of intelligent healthcare infrastructures. These systems enable accurate patient tracking, medication verification, and secure data transmission in clinical environments (Jara et al., 2009). Open-source libraries such as LibNFC have facilitated the development of NFC-based healthcare applications, enhancing system interoperability and scalability (LibNFC, 2009). Barcode recognition technologies such as ZXing have also contributed to automated medical data capture and processing (ZXing, 2009).

The literature also highlights advancements in medical robotics and surgical systems. Intelligent soft robotic systems have been developed to support minimally invasive surgical procedures, improving precision and reducing patient recovery time (Zhu et al., 2021). These technologies represent a significant step toward automation in surgical environments, where AI-driven systems assist surgeons in complex procedures.

Overall, the literature demonstrates that intelligent healthcare systems are evolving through the integration of pharmaceutical engineering, artificial intelligence, cybersecurity frameworks, and medical automation technologies. However, challenges related to system integration, security risks, and ethical considerations remain significant areas for further research.

METHODOLOGY

This research adopts a conceptual, systems-oriented, and integrative methodology to analyze emerging trends in medical science and intelligent pharmaceutical engineering. Since the study is grounded in secondary literature, it synthesizes technological, clinical, and computational perspectives into a unified analytical framework. The methodology is structured around four interconnected analytical layers: (1) healthcare digital infrastructure analysis, (2) intelligent pharmaceutical engineering modeling, (3) cybersecurity risk assessment in medical systems, and (4) AI-driven medical decision-support integration.

1. Research Design

The research follows a qualitative-analytical design supported by structured literature synthesis. It integrates findings from medical informatics, cybersecurity engineering, pharmaceutical systems, and AI-based healthcare technologies. The design is non-experimental and focuses on theoretical abstraction rather than empirical clinical trials. This approach is suitable for identifying patterns across heterogeneous healthcare technologies such as IoMT devices, robotic surgical systems, drug information platforms, and ontology-based reasoning systems.

The methodological foundation aligns with mixed-method research philosophy, where qualitative synthesis is used to interpret technical systems and quantitative findings from prior studies are conceptually aggregated (Johnson & Onwuegbuzie, 2004).

2. Data Collection Strategy

Data is collected exclusively from peer-reviewed journal articles, conference proceedings, healthcare system reports, and technological frameworks included in the provided references. The dataset includes research on:

a. Cybersecurity vulnerabilities in medical devices

b. Pharmaceutical adverse drug reaction systems

c. IoMT architectures and communication protocols

d. AI-based medical diagnostic systems

e. Ontology-driven healthcare reasoning tools

f. Medical robotics and surgical automation systems

No external datasets or empirical hospital records are used. Instead, the study relies on secondary data triangulation to ensure conceptual validity.

3. Analytical Framework

The analysis is structured using a multi-layer healthcare intelligence model, consisting of the following components:

(a) Medical Data Acquisition Layer

This layer includes IoMT devices, NFC/RFID systems, barcode scanners, and patient monitoring sensors. These technologies are responsible for capturing real-time clinical and pharmaceutical data (Jara et al., 2009; LibNFC, 2009).

(b) Data Processing and Knowledge Layer

This layer involves ontology-based systems (Protégé), rule engines (Jess), and pharmaceutical databases (Oracle DB, PortaIFarma). These systems structure and process healthcare knowledge into machine-readable formats for reasoning and inference (Protégé, 2009; Jess, 2009).

(c) Intelligent Reasoning Layer

AI and machine learning systems operate in this layer to perform predictive analytics, drug interaction detection, and diagnostic modeling. Systems such as decision-support engines and predictive risk models enhance clinical decision accuracy (Zhu et al., 2021).

(d) Security and Governance Layer

This layer ensures cybersecurity, patient privacy, and system integrity. It integrates encryption mechanisms, risk assessment frameworks, and regulatory compliance strategies (Yaqoob et al., 2020; Aldosari, 2025).

4. Analytical Procedure

The methodology follows a five-step analytical procedure:

1. Literature Classification – Studies are grouped into healthcare cybersecurity, pharmaceutical systems, AI applications, and medical robotics.

2. Thematic Extraction – Key themes such as security risks, automation efficiency, and decision intelligence are identified using structured thematic mapping principles (Braun & Clarke, 2006).

3. System Mapping – Interactions between IoMT, pharmaceutical systems, and AI platforms are mapped conceptually.

4. Comparative Evaluation – Strengths and limitations of each technological layer are compared across studies.

5. Integrated Interpretation – A unified framework is developed to explain convergence between medicine and intelligent systems.

5. Limitations of Methodology

a. The study does not include real-world clinical trials or hospital datasets.

b. Findings are dependent on secondary literature reliability.

c. Rapid technological evolution may reduce long-term applicability of conceptual models.

d. Cybersecurity threats evolve dynamically, making static analysis partially limited.

Despite these limitations, the methodology provides a comprehensive conceptual architecture for understanding intelligent healthcare systems.

RESULTS / FINDINGS

The analysis of integrated literature reveals several critical findings regarding the convergence of medical science, pharmaceutical engineering, and intelligent computational systems. One of the most significant findings is that healthcare systems are rapidly transitioning from isolated digital tools to fully interconnected intelligent ecosystems. These ecosystems are characterized by real-time data exchange between IoMT devices, pharmaceutical databases, and AI-driven diagnostic systems.

A major outcome identified is the improvement in patient safety through intelligent pharmaceutical systems. Automated drug information systems and ontology-based reasoning platforms significantly reduce adverse drug reactions by enabling accurate drug interaction detection and dosage verification (Lazarou et al., 1998; Pirmohamed et al., 2004). The integration of structured pharmaceutical databases such as Oracle-based systems and PortaIFarma further enhances prescription accuracy and reduces human error in medication management.

Another key finding is the increased efficiency of healthcare workflows through automation technologies. RFID and NFC-based identification systems improve patient tracking, medication verification, and inventory control within hospitals (Jara et al., 2009; LibNFC, 2009). Barcode-based medical systems such as ZXing further streamline pharmaceutical logistics by enabling rapid identification and processing of medical products. These technologies collectively reduce operational delays and enhance healthcare delivery efficiency.

The study also finds that AI-driven medical systems significantly enhance diagnostic and predictive capabilities. Machine learning models and intelligent reasoning systems improve disease prediction accuracy and support clinical decision-making processes. Surgical robotics systems demonstrate improved precision in minimally invasive procedures, reducing recovery time and improving surgical outcomes (Zhu et al., 2021). These systems represent a shift toward automation-assisted clinical environments.

However, a critical finding is the growing cybersecurity vulnerability in healthcare systems. IoMT devices and interconnected hospital networks are highly exposed to cyber threats due to weak authentication protocols and distributed architectures (Williams & Woodward, 2015; Yaqoob et al., 2019). Cybersecurity breaches can directly compromise patient safety, disrupt hospital operations, and expose sensitive medical data. Studies consistently highlight the need for integrated cybersecurity frameworks to mitigate these risks (Ghafur & Durkin, 2021).

Another important finding is the lack of interoperability among healthcare systems. Many pharmaceutical databases, AI platforms, and IoMT devices operate on incompatible architectures, limiting seamless integration. This fragmentation reduces the efficiency of intelligent healthcare ecosystems and creates barriers to real-time data exchange.

The study also identifies that ontology-based systems and rule engines significantly improve knowledge representation and clinical reasoning. Tools like Protégé and Jess enable structured medical knowledge modeling, allowing systems to perform logical inference and automated decision-making. However, these systems require continuous updates to maintain accuracy in rapidly evolving medical environments.

Finally, the findings suggest that intelligent healthcare systems improve overall operational performance but increase system complexity. While automation reduces manual workload, it also introduces dependency on digital infrastructure and increases maintenance requirements. Healthcare organizations must balance efficiency gains with system resilience and cybersecurity preparedness.

DISCUSSION

The findings of this research highlight a fundamental transformation in healthcare systems driven by intelligent automation, pharmaceutical engineering, and cybersecurity integration. One of the most critical interpretations is that healthcare is evolving into a data-driven intelligent ecosystem, where decision-making is increasingly delegated to AI systems and computational models. This shift aligns with broader trends in digital transformation where human decision-making is augmented by machine intelligence.

The improvement in patient safety through automated pharmaceutical systems confirms the importance of intelligent drug management frameworks. Traditional healthcare systems often suffer from medication errors, incorrect dosages, and delayed diagnosis of adverse drug reactions. The integration of AI-based drug information systems directly addresses these challenges by enabling real-time validation of prescriptions (Lazarou et al., 1998). However, while automation reduces human error, it introduces new risks related to algorithmic inaccuracies and system dependency.

The discussion also reveals that IoMT and RFID-based systems significantly enhance operational efficiency but simultaneously increase cybersecurity exposure. This duality represents a core contradiction in modern healthcare systems: greater connectivity leads to greater vulnerability. As highlighted in cybersecurity literature, medical systems are increasingly targeted by cyberattacks due to sensitive data and life-critical operations (Aldosari, 2025; Cartwright, 2023). Therefore, cybersecurity cannot be treated as an auxiliary feature but must be embedded into system architecture from the design stage.

Another important interpretation is the role of AI in improving diagnostic accuracy and surgical precision. Robotic surgical systems and predictive AI models demonstrate clear benefits in clinical outcomes (Zhu et al., 2021). However, reliance on such systems raises concerns about explainability and accountability. When AI systems generate clinical recommendations, it becomes difficult for practitioners to fully understand decision logic, creating trust-related challenges.

The discussion further emphasizes that interoperability remains a major barrier in intelligent healthcare ecosystems. Despite advancements in databases, ontologies, and IoMT systems, integration across platforms remains inconsistent. This fragmentation limits the scalability of intelligent healthcare solutions and reduces efficiency in large hospital networks.

From a theoretical perspective, the study reinforces the importance of socio-technical systems theory, where technology and human actors must function in coordinated alignment. Healthcare transformation cannot be achieved through technology alone; organizational readiness, training, and governance frameworks are equally important. This aligns with cybersecurity literature emphasizing that patient safety is directly influenced by system design and institutional policies (Ghafur & Durkin, 2021).

A key limitation identified is the rapid evolution of both medical technologies and cybersecurity threats. As systems become more advanced, attack surfaces expand, requiring continuous adaptation of security frameworks. Additionally, ethical concerns such as data privacy, algorithmic bias, and decision transparency remain unresolved challenges.

Overall, the discussion confirms that intelligent healthcare systems represent both a significant opportunity and a complex challenge. The balance between innovation and security will determine the future effectiveness of medical and pharmaceutical engineering systems.

CONCLUSION

The convergence of medical science, pharmaceutical engineering, and intelligent computational systems represents a fundamental transformation in modern healthcare ecosystems. This research has demonstrated that emerging technologies such as Internet of Medical Things (IoMT), artificial intelligence, ontology-based reasoning systems, RFID/NFC frameworks, and robotic surgical platforms are collectively reshaping how healthcare services are delivered, managed, and optimized. These technologies are not isolated innovations but interconnected components of a broader intelligent healthcare infrastructure designed to improve patient outcomes, operational efficiency, and clinical decision-making.

A key insight of this study is that intelligent pharmaceutical engineering significantly reduces medication-related risks and enhances clinical safety. Automated drug information systems, ontology-driven knowledge bases, and rule-based reasoning engines contribute to minimizing adverse drug reactions and improving prescription accuracy (Lazarou et al., 1998; Pirmohamed et al., 2004). These systems enable healthcare professionals to access structured, real-time pharmaceutical knowledge, reducing dependency on manual

decision-making and improving consistency in treatment planning.

The study also confirms that IoMT and digital medical infrastructures have revolutionized healthcare monitoring and operational workflows. Technologies such as NFC, RFID, and barcode-based systems improve patient identification, medication tracking, and hospital logistics efficiency (Jara et al., 2009; LibNFC, 2009). However, these advancements also introduce critical cybersecurity challenges, as interconnected systems expand the attack surface for malicious actors. Existing research highlights that medical devices and healthcare networks are increasingly vulnerable to cyber threats, which can directly impact patient safety (Williams & Woodward, 2015; Yaqoob et al., 2019).

Artificial intelligence and robotic systems further enhance diagnostic precision and surgical accuracy. AI-driven models support predictive diagnostics, while intelligent robotic surgery improves procedural precision and reduces recovery time (Zhu et al., 2021). These advancements indicate a clear shift toward semi-autonomous and autonomous healthcare systems. Nevertheless, issues such as explainability, accountability, and ethical decision-making remain significant challenges that must be addressed before full-scale adoption.

Cybersecurity emerges as one of the most critical determinants of success in intelligent healthcare systems. The study shows that healthcare cybersecurity is not merely a technical requirement but a patient safety necessity (Aldosari, 2025). Frameworks that integrate risk assessment, encryption protocols, and regulatory compliance are essential for ensuring system resilience. Without robust cybersecurity integration, the benefits of intelligent healthcare systems may be undermined by operational and ethical risks.

From a broader perspective, the research highlights that the future of healthcare lies in integrated intelligent ecosystems, where medical devices, pharmaceutical databases, and AI systems operate in a synchronized and secure environment. However, achieving this vision requires addressing key challenges including interoperability limitations, system complexity, workforce adaptation, and ethical governance.

The study contributes to academic and practical understanding by presenting a synthesized view of how intelligent technologies are transforming healthcare systems. It emphasizes that technological advancement alone is insufficient; successful implementation requires strong governance frameworks, human-centric design, and continuous system evaluation.

Future Scope

Future research should focus on developing more explainable AI models for healthcare decision-making to improve trust and transparency. Additionally, advanced cybersecurity architectures tailored specifically for IoMT environments are essential to mitigate emerging threats. Interoperability standards across pharmaceutical databases, hospital systems, and AI platforms must also be strengthened to enable seamless data exchange. Further empirical studies using real-world hospital datasets could enhance validation of conceptual findings and support large-scale implementation of intelligent healthcare systems.

REFERENCE:

1. J. Jara, M. A. Zamora, A. F. G. Skarmeta, “Secure use of NFC in medical environments ”, 5th European Workshop on RFID Systems and Technologies, Bremen (Alemania), June, 2009.
2. Aldosari, B. (2025). Cybersecurity in Healthcare: New Threat to Patient Safety. Cureus, 17 (5), e83614. https://doi.org/10.7759/cureus.83614
3. Alasdair Mackintosh, Alexander Martin, Brian Brown, Christian Brunschen, Daniel Switkin et al, “Zxing, open source library to read ID/2D barcodes ”, http://code.google.com/p/zxing/ (2009).
4. Razaque et al., “Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain,” in IEEE Access, vol. 7, pp. 168774–168797, 2019, doi: 10.1109/ACCESS.2019.2950849.
5. Cartwright, A.J. The elephant in the room: cybersecurity in healthcare. J Clin Monit Comput 37, 1123–1132 (2023). https://doi.org/10.1007/s10877-023-01013-5
6. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008
7. Das, S., Siroky, G. P., Lee, S., Mehta, D., & Suri, R. (2021). Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices. Heart Rhythm, 18 (3), 473481. https://doi.org/10.1016/j.hrthm.2020.10.009
8. David C. Classen, Stanley L. Pestonik, Evans R. Scott, J. F. Lloyd and J. P. Burke, “Adverse Drug Events in Hospitalized Patients: Excess Length of Stay, Extra Costs, and Attributable Mortality ”, Obstetrical & Gynecological Survey, Vol. 52, Issue. 5, pp 291–292 (1997).
9. D.-W. Kim, J.-Y. Choi and K.-H. Han, “Medical Device Safety Management Using Cybersecurity Risk Analysis,” in IEEE Access, vol. 8, pp. 115370–115382, 2020, doi: 10.1109/ACCESS.2020.3003032.
10. Eduardo Azumendi, E-prenscription in Euskadi (Spain) before than 2011. Newspaper : El País (2009).
11. Gemma Fernandez Peñalba E-Osabide, www.saludmentalalava.org/Cas/docum/GlosariodeTérminosAbreviaturasyBibliografíaPE2004.pdf (2002).
12. Ghafur, S., & Durkin, M. (2021). Cybersecurity in health is an urgent patient safety concern: We can learn from existing patient safety improvement strategies to address it. Journal of Patient Safety and Risk Management. https://doi.org/10.1177/2516043520975926
13. Henrik Eriksson, “JessTab: Integrating Protégé and Jess ”. www.ida.liu.se/~her/JessTab/ (2006).
14. Jason Lazarou ; Bruce H. Pomeranz and Paul N. Corey, “Incidence of Adverse Drug Reactions in Hospitalized Patients ”, The Journal of the American Medical Association. Vol. 229, pp. 1200–1205 (1998).

15. Jess, the rule engine for the Java Platform, (2009).
16. Kumar, Ashir, "Adverse effects of pharmaceutical excipients ", Adverse Drug Reaction Bulletin, Issue 222, p 851–85 (2003).
17. LibNFC - Public platform independent Near Field Communication (NFC) library, http://www.libnfc.org/, 2009.
18. Munir Pirmohamed, Sally James, Shaun Meakin, Chris Green, Andrew K Scott, Thomas J Walley, Keith Farrar, B Kevin Park and Breckenridge Alasdair M, "Adverse drug reactions as cause of admission to hospital: prospective analysis of 18 820 patients ", British Medical Journal (BMJ), vol. 329, pp. 15–19 (2004).
19. M. Yamamoto, Y. Onaka, K. Sakakibara, H. Negi, S. Funabashi, T. Hirata, T. Kawasaki, H. Saito, T. Kawai and S. Okada, "Development and utilization of a drug information system in the Japanese pharmaceutical industry ", Informatics for Health and Social Care, Vol. 23, pp. 31–41 (1998)
20. Oracle DataBase, www.Oracle.com/, (2009).
21. Pasupuleti, S. (2021, March). The role of robotic systems in minimally invasive surgery: Benefits, risks, and future directions. International Journal of Scientific Research in Engineering and Management.
22. Pharmaceutical Spanish Association Database, "PortaIFarma", www.portalfarma.com/Home.nsf/Home?OpenForm, (2009).
23. Protégé the ontology editor and knowledge acquisition system. http://protege.stanford.edu/, (2009).
24. R. Tamblyn, R. Laprise, J. A. Hanley, M. Abrahamowicz, S. Scott, N. Mayo, J. Hurley, R. Grad, E. Latimer, R. Perreault, P. McLeod, A. Huan, P. Larochelle and L. Mallet, "Adverse Events Associated With Prescription Drug Cost-Sharing Among Poor and Elderly Persons ", The J. of the American Medical Association, Vol. 285, pp. 421–429 (2001).
25. SDiD 1010 NFC /RFID SD Card, SDiD, http://www.sdid.com/products1010.shtml (2009).
26. Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the Internet of Medical Things. Health Policy and Technology, 10 (3), 100549. https://doi.org/10.1016/j.hlpt.2021.100549
27. T. Yaqoob, H. Abbas and N. Shafqat, "Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 6, pp. 1752–1761, June 2020, doi: 10.1109/JBHI.2019.2952906.
28. T. Yaqoob, H. Abbas and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices-A Review," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 37233768, Fourthquarter 2019, doi: 10.1109/COMST.2019.2914094.
29. Toucahtag, "RFID tag for consumer and developers ", (2009).
30. Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the Internet of Medical Things. Health Policy and Technology, 10 (3), 100549.
31. Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Frontiers in Digital Health, 4, 862221. https://doi.org/10.3389/fdgth.2022.862221
32. Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: Evidence and Research, 8, 305–316. https://doi.org/10.2147/MDER.S50048
33. Y. Sun, F. P.-W. Lo and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," in IEEE Access, vol. 7, pp. 183339183355, 2019, doi: 10.1109/ACCESS.2019.2960617.
34. Y. Z. Zhu, M. Wang, Y. Wang, & Y. Wang (2021). Intelligent soft surgical robots for next- generation minimally invasive surgery. Advanced Intelligent Systems, 3 (5), 2100011. https://doi.org/10.1002/aisy.202100011
35. Z. Shen, H. Yu, L. Yu, C. Miao, Y. Chen, and V. R. Lesser, "Dynamic Generation of Internet of Things Organizational Structures through Evolutionary Computing," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 943–954, 2018.