Cybersecurity for Sustainable Internet of Things Implementation in Healthcare

Teodora Bakardjieva[1*], Antonina Ivanova[1], Yanko Yankov[2], Zhivko Zhekov[3]

[1]*Department of Computer Science,*
Varna Free University "Chernorizets Hrabar"
84 Yanko Slavchev Str., Chaika Resort, 9007 Varna, Bulgaria
E-mails: bakardjieva@vfu.bg, antonina.ivanova@vfu.bg

[2]*Department of General and Operative Surgery,*
Medical University "Prof. Dr. Paraskev Stoyanov"
55 Marin Drinov Str., 9002 Varna, Bulgaria
E-mail: yanko.yankov@mu-varna.bg

[3]*Department of Obstetrics and Gynecology,*
Medical University "Prof. Dr. Paraskev Stoyanov"
55 Marin Drinov Str., 9002 Varna, Bulgaria
E-mail: zhivko.zhekov@mu-varna.bg

[*]*Corresponding author*

Received: January 06, 2025 **Accepted: June 10, 2025**

Published: June 30, 2025

Abstract: *The current systematic review aims to summarise and discuss the impact and implications of the Internet of Things (IoT) in the healthcare sector. An electronic search for articles using Google Scholar, PubMed, and Scopus was conducted from January 1, 2019, up to July 1, 2024, under Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. The review presents cybersecurity threats in IoT-based healthcare infrastructure and applications that enable smart healthcare services to operate. When collecting and storing medical data from IoT sensors, there is an opportunity to analyse this data, which can improve the identification of risk factors, diagnosis of diseases, treatment, and remote monitoring, which creates prerequisites for reliable self-monitoring by patients. Advantages and risks have been evaluated, and recommendations for further research have been suggested. IoT provides an opportunity to improve the quality and efficiency of the entire service delivery ecosystem, including hospital management, medical asset management, staff workflow monitoring, and optimisation of medical resources based on patient flow.*

Keywords: *Cybersecurity, Internet of Things, IoT, Healthcare, Vulnerabilities, Threats.*

Introduction

The Internet of Things (IoT) is a trend that is driving the continued digitisation and penetration of information technology in many new and amazing ways. Self-driving cars, autonomous manufacturing robots, and remote medical devices that allow doctors to diagnose patients and even perform surgeries are made possible by these networks of connected things. The number of internet devices is increasing, and it will double by 2030 [4, 23, 31]. The IoT is a network that connects devices or things that can receive, collect, send, and store different kinds of data [24].

Internet of Healthcare Things (IoHT) refers to devices connected to the internet and able to communicate with each other, used in the medical field. These devices transfer information in real time through remote/automatic control. As a result, a high degree of satisfaction of patients' needs is achieved, and the work of medical specialists and healthcare workers is facilitated [30]. Along with the many positives of that technology, there are a lot of security vulnerabilities in existing IoHT implementations, and it is of high importance to discuss them to better understand the resulting security issues [38].

This review aims to summarise, compare, and evaluate IoT applications in healthcare. When collecting and storing medical data from IoT sensors, there is an opportunity to analyse this data, which can improve the identification of risk factors, diagnosis of diseases, treatment, and remote monitoring, which creates prerequisites for reliable self-monitoring by patients.

Cyber risk is of major importance to the wider acceptance of IoT. There are challenges related to the protection of patient data, tracking, and hacking. Information must be secured to prevent data breaches and to protect privacy [39]. Much of the communication in the IoT is wireless, and this creates prerequisites for cyber-attacks, such as sniffing and man-in-the-middle. Also, most of the devices are low energy and do not have good security systems on their own [19].

The main purpose of the present work is to outline cybersecurity threats in IoT implementation in healthcare and to answer the research question: How does the integration of IoT in healthcare impact patient care and operational efficiency, and what cybersecurity measures are necessary to mitigate associated risks?

Materials and methods

An electronic search was made on July 1, 2024, using Google Scholar, PubMed, and Scopus. The current systematic review was conducted under the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines [26, 29].

The search was for "cybersecurity AND IoT AND healthcare OR IoHT AND cyber-attacks" and included only articles in English published from January 1, 2019 to July 1, 2024. The inclusion criteria were: articles that discuss cybersecurity and the IoT in healthcare, or articles that describe the IoHT and cyber-attacks. The exclusion criteria were: articles before January 1, 2019; not full-text articles and citations; and articles in languages other than English.

A review and assessment of compliance with the eligibility criteria was carried out. Duplicate entries have been removed. Inclusion and exclusion criteria were applied.

Results and discussion

The initial search found 23 862 relevant studies (Google Scholar – 4 680 results; PubMed – 18 results; Scopus – 975 results). Table 1 shows the search strategy, and Fig. 1 shows the PRISMA flow diagram.

This study has some potential limitations. The first 100 suggestions from both Google Scholar and Scopus, and all 18 studies from PubMed, were included for evaluation. 25 duplicate records were excluded, and 193 records were screened and evaluated for eligibility. Finally, 16 relevant articles were included in the current study. Also, there is still an insufficient number of studies describing IoT cybersecurity issues in healthcare. The characteristics of the review articles that met the eligibility criteria and were included in the current study are presented in Table 2.

Table 1. Initial search results

Search strategy	Database used	Number of papers identified
"Cybersecurity" AND "IoT" AND "Healthcare" OR "IoHT" AND "cyber-attacks"	Google Scholar	4 680
	PubMed	18
	Scopus	975

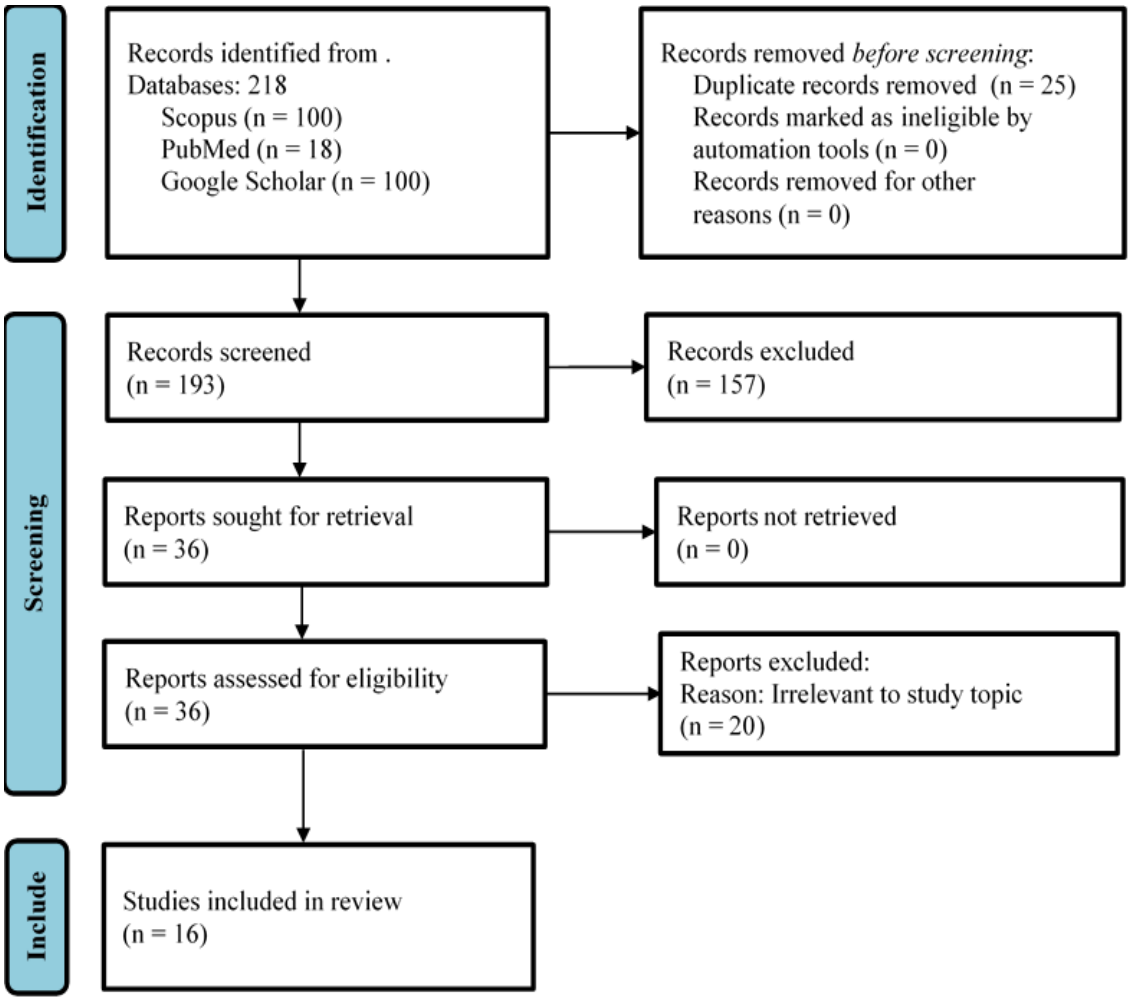

Fig. 1 The PRISMA flow diagram

Table 2. Characteristics of the review articles meeting the eligibility criteria and included in the study

Reference	Title	Year	Objective	Conclusion
Mejía-Granda et al. [22]	Security vulnerabilities in healthcare: an analysis of medical devices and software	2024	To analyse common security vulnerabilities in medical devices and healthcare software, focusing on how these vulnerabilities can be exploited.	The study calls for the implementation of stricter security standards, regular vulnerability testing, and enhanced collaboration between manufacturers and healthcare providers.
Bughio et al. [11]	Developing a novel ontology for cybersecurity in internet of medical things-enabled remote patient monitoring	2024	To develop a specialised ontology framework to enhance cybersecurity for Internet of Medical Things (IoMT) -based remote patient monitoring systems.	The paper concludes that the proposed ontology framework helps systematically address cybersecurity concerns in remote patient monitoring, improving threat identification and mitigation.
AboulEla S. et al. [1]	Navigating the cyber threat landscape: an in-depth analysis of attack detection within IoT ecosystems	2024	To conduct a detailed analysis of attack detection techniques in IoT ecosystems, with a focus on their application to healthcare IoT.	The study concludes that effective cyber-attack detection in IoT requires advanced machine learning techniques, continuous system monitoring and suggests further research to refine detection methods.
Sousa R. [32]	Cyber threats to healthcare technology services: a case study	2024	To analyse specific cyber threats against healthcare technology services through a comprehensive case study approach.	The case study indicates that healthcare technology services are frequently targeted by advanced cyber threats. It highlights the critical need for robust cybersecurity frameworks.
Cartwright [12]	The elephant in the room: cybersecurity in healthcare	2023	To highlight the urgent need for stronger cybersecurity in healthcare, especially with the growing use of IoT devices, which increases vulnerability to cyber-attacks.	Cybersecurity is essential for protecting healthcare systems and patient data. The article emphasises the need for proactive measures like security protocols, system updates, and staff training.
Mazhar et al. [21]	Analysis of IoT security challenges and their solutions	2023	To analyse the security challenges of IoT devices in healthcare and explore how AI can provide effective	The study finds that AI-driven approaches can significantly enhance IoT security in healthcare by

	using artificial intelligence		solutions to these challenges.	detecting threats quickly and effectively.
Bhukya et al. [10]	Cybersecurity in the internet of medical vehicles: state-of-the-art analysis, research challenges and future perspectives	2023	To review current cybersecurity measures for Internet of Medical Vehicles (IoMV), identify existing research gaps, and outline future research directions for improving security in medical vehicle networks.	The paper concludes that IoMV systems are highly vulnerable to cyber threats due to their mobility and connectivity. It calls for enhanced security frameworks, interdisciplinary research, and regulatory measures to mitigate these risks.
Almalawi et al. [7]	Managing the security of healthcare data for a modern healthcare system	2023	To examine the challenges associated with managing the security of healthcare data in modern healthcare systems and propose methods for enhancing protection.	The article concludes that a multi-layered approach, including encryption, access control, and regular audits, is essential for managing healthcare data security effectively.
Hurrah et al. [15]	CADEN: cellular automata and DNA-based secure framework for privacy preserving in IoT-based healthcare	2023	To introduce a new security framework using cellular automata and DNA computing to protect privacy and ensure data security in IoT-based healthcare systems.	The paper concludes that the CADEN framework provides strong privacy and data security measures for IoT healthcare environments. Further development and testing are recommended to enhance its defence against advanced cyber threats.
Ahouanmenou et al. [5]	Information security and privacy in hospitals: a literature mapping and review of research gaps	2023	To map existing research on hospital information security and privacy, identifying gaps and suggesting areas for future study.	The review finds that while there has been considerable research, significant gaps remain in areas like real-time threat detection and privacy-preserving data sharing. It shows the research gaps.
Javaid et al. [18]	Towards insighting cybersecurity for healthcare domains: a comprehensive review of recent practices and trends	2023	To provide a thorough review of current cybersecurity practices and emerging trends in healthcare, highlighting effective strategies and areas needing improvement.	The review concludes that although there have been improvements in healthcare cybersecurity, many vulnerabilities remain. It emphasises the need for innovative solutions and greater collaboration.

Khatiwada and Yang [20]	An overview of security and privacy of data in IoMT devices: performance metrics, merits, demerits, and challenges	2022	To offer a detailed overview of security and privacy concerns in IoMT devices, focusing on key performance metrics, benefits, drawbacks, and challenges.	The study concludes that while IoMT devices provide significant benefits to healthcare, they come with major security and privacy risks. It suggests balancing performance with enhanced measures.
Nayak et al. [25]	Extreme learning machine and Bayesian optimisation-driven intelligent framework for IoMT cyber-attack detection	2022	To design and evaluate an intelligent framework using extreme learning machines and Bayesian optimisation to detect cyber-attacks in IoMT environments.	The research finds that the proposed framework is effective in detecting cyber-attacks in IoMT systems, demonstrating high accuracy and low false positive rates. It recommends further development and testing for real-world applications to improve security.
Rahman et al. [27]	An investigation of vulnerabilities in the Internet of health things	2022	To examine common security vulnerabilities in Internet of Health Things (IoHT) and their potential impact on healthcare infrastructure.	The study identifies security weaknesses in IoHT devices that could be exploited by attackers and recommends enhanced security measures.
Hussain et al. [16]	A framework for malicious traffic detection in an IoT healthcare environment	2021	To propose a framework for detecting and mitigating malicious network traffic specifically targeting IoT devices in healthcare environments.	The study concludes that the proposed framework effectively detects malicious traffic, improving the security posture of healthcare IoT networks.
Sparrell [33]	Cyber-safety in healthcare IoT	2019	To explore the cybersecurity threats and safety concerns related to the use of IoT in a healthcare environment	The study concludes that healthcare IoT systems are highly vulnerable to cyber threats, stressing the need for robust security protocols and ongoing monitoring.

The analysed studies collectively highlight both the opportunities and risks associated with IoT in healthcare, underscoring the critical need for cybersecurity measures to protect sensitive health data and ensure patient safety. Vulnerabilities such as inadequate encryption, poor authentication mechanisms, and a lack of secure communication protocols can be exploited by cybercriminals to gain unauthorized access, steal sensitive patient data, or disrupt healthcare services, leading to potentially life-threatening situations. The literature emphasises the increased connectivity of healthcare devices while improving patient outcomes, which also

opens new avenues for cyber threats [27]. To counter these threats, several studies propose the use of advanced technologies like artificial intelligence (AI), machine learning (ML), and Bayesian optimisation [25]. By automating the process of threat detection, these technologies can significantly enhance the security of IoT healthcare environments, providing a proactive defence against sophisticated cyber-attacks.

The literature strongly advocates for multi-layered security strategies to protect IoT devices and healthcare networks. Implementing comprehensive security measures helps to safeguard against a wide range of cyber threats, from unauthorised access and data breaches to advanced persistent threats [7]. The development of specialised frameworks and ontologies is identified as a key strategy for improving cybersecurity in IoT-based healthcare systems [11]. There is also a significant need for improved privacy-preserving techniques to protect patient data while ensuring that healthcare providers have access to the information they need [20]. There is a lack of standardised security protocols tailored specifically for healthcare IoT environments, and research gaps are particularly evident in the areas of developing advanced cryptographic methods and exploring new AI and ML techniques that can provide security [18].

Future research should aim at developing new AI and ML-based solutions for more effective threat detection and response [1]. There is also a call for increased collaboration among healthcare providers, IT professionals, cybersecurity experts, and policymakers to create a unified approach to cybersecurity and the establishment of standardised protocols and guidelines, along with regular security training for healthcare staff [18, 27, 32].

Cyber risk is the main reason limiting the mass adoption of IoT, and by learning from real-world incidents, healthcare organisations can better respond to cyber threats, ensuring the safety and privacy of their patients [17, 19, 28]. Traditional security measures are not reliable against sophisticated attacks in a complex IoT ecosystem [8, 37]. Additional studies are needed to create a sociotechnical framework that will support cybersecurity in healthcare systems and connect technology, people, and processes in an integrated manner and adaptive multifactor authentication to replace the traditional approaches to authentication [14, 34, 35]. To understand the risks in this new landscape, it is important to know the architecture of the devices, operations, and the social dynamics that may govern their interactions [3]. Enhancing the resilience and security of medical data and connected devices could be realised through the investigation of potential vulnerabilities and the proposal of a comprehensive framework [36].

Cybersecurity for sustainable implementation in healthcare is becoming important not just because of the growing number of threats, vulnerabilities, and bad actors, but because technology is becoming intuitively more sensitive, potentially impacting every area of a person's life [6, 28]. To safeguard patient data and guarantee continuity of service, healthcare institutions have employed specialised cybersecurity staff and deployed cutting-edge security measures [13]. The future in healthcare belongs to the integration of IoT with telemedicine, wearable health technology, and advanced data analytics. Improving patient care could be achieved through IoT-enabled devices, real-time monitoring, and personalised treatment plans [2, 9].

Key findings

The deployment of IoT in healthcare has brought new challenges in terms of cybersecurity. Malicious attacks, such as distributed denial of service attacks, aim to overload network resources and disrupt the operation of IoT devices. To mitigate these threats, healthcare providers must adopt a holistic approach to security that includes proper

risk assessment, implementing security measures, regular network monitoring, and training on cybersecurity practices, together with proper standards. The increased connectivity and data exchange inherent to IoT introduce substantial risks and data breaches. To fully address these challenges, future research should aim to develop standardised and scalable security protocols specifically tailored to the requirements of healthcare IoT environments.

Conclusion

Cybersecurity is a growing concern in healthcare IoT deployments due to the potential exposure of sensitive healthcare information and critical infrastructure. There are several challenges to ensuring the cybersecurity of IoT devices in healthcare, including lax security measures, outdated software configurations, unencrypted communication protocols, and human error.

The current literature indicates a need for more research and development in healthcare IoT cybersecurity. In particular, there is a need to better understand the unique risks associated with different types of IoT devices and applications, and to develop specific strategies to mitigate them. Adopting multi-layered security approaches, leveraging advanced technologies like AI and ML, and addressing existing research gaps are essential steps toward ensuring the security and privacy of healthcare data. Ongoing research, collaboration, and awareness are vital to stay ahead of cyber threats, safeguard patient information, and maintain the integrity of healthcare services in the IoT era. The application of IoT in healthcare will rely on a transparent and sustainable system for data management, privacy, and cybersecurity regarding the use of IoT devices.

More research on cybersecurity for sustainable IoT implementation is needed to specify the level of readiness of all actors in the process of using IoT in healthcare, which ultimately aims to improve patient-centred care.

References

1. AboulEla S., N. Ibrahim, S. Shehmir, A. Yadav, et al. (2024). Navigating the Cyber Threat Landscape: An In-depth Analysis of Attack Detection Within IoT Ecosystems, AI, 5(2), 704-732, https://doi.org/10.3390/ai5020037.
2. Adil M., K. Khan, N. Kumar, M. Attique, et al. (2024). Healthcare Internet of Things: Security Threats, Challenges, and Future Research Directions, IEEE Internet of Things Journal, 11(11), 19046-19069, https://doi.org/10.1109/JIOT.2024.3360289.
3. Affia A. A. O., H. Finch, W. Jung, I. A. Samori, et al. (2023). IoT Health Devices: Exploring Security Risks in the Connected Landscape, IoT, 4(2), 150-182, https://doi.org/10.3390/iot4020009.
4. Ahmed M. U., S. Begum, J. B. Fasquel (2018). Internet of Things (IoT) Technologies for HealthCare, 4th International Conference, Healthy IoT, Springer International Publishing, https://doi.org/10.1007/978-3-319-76213-5.
5. Ahouanmenou S., A. Van Looy, G. Poels (2023). Information Security and Privacy in Hospitals: A Literature Mapping and Review of Research Gaps, Informatics for Health and Social Care, 48(1), 30-46, https://doi.org/10.1080/17538157.2022.2049274.
6. Alanazi A. T., A. Alanazi (2023). Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats, Cureus, 15(10), 47026, https://doi.org/10.7759/cureus.47026.
7. Almalawi A., A. I. Khan, F. Alsolami, Y. B. Abushark, et al. (2023). Managing Security of Healthcare Data for a Modern Healthcare System, Sensors, 23(7), 3612, https://doi.org/10.3390/s23073612.

8. AlSalem T. S., M. A. Almaiah, A. Lutfi (2023). Cybersecurity Risk Analysis in the IoT: A Systematic Review, Electronics, 12(18), 3958, https://doi.org/10.3390/electronics12183958.
9. Altulaihan E., M. A. Almaiah, A. Aljughaiman (2022). Cybersecurity Threats, Countermeasures, and Mitigation Techniques on the IoT: Future Research Directions, Electronics, 11(20), 3330, https://doi.org/10.3390/electronics11203330.
10. Bhukya C. R., P. Thakur, B. R. Mudhivarthi, G. Singh (2023). Cybersecurity in Internet of Medical Vehicles: State-of-the-art Analysis, Research Challenges, and Future Perspectives, Sensors, 23(19), 8107, https://doi.org/10.3390/s23198107.
11. Bughio K. S., D. M. Cook, S. A. A. Shah (2024). Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-enabled Remote Patient Monitoring, Sensors, 24(9), 2804, https://doi.org/10.3390/s24092804.
12. Cartwright A. J. (2023). The Elephant in the Room: Cybersecurity in Healthcare, Journal of Clinical Monitoring and Computing, 37(5), 1123-1132, https://doi.org/10.1007/s10877-023-01013-5.
13. Chataut R., A. Phoummalayvane, R. Akl (2023). Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0, Sensors, 23(16), 7194, https://doi.org/10.3390/s23167194.
14. Ewoh P., T. Vartiainen (2024). Vulnerability to Cyber-attacks and Sociotechnical Solutions for Health Care Systems: Systematic Review, Journal of Medical Internet Research, 26, e46904, https://doi.org/10.2196/46904.
15. Hurrah N. N., E. Khan, U. Khan (2023). CADEN: Cellular Automata and DNA based Secure Framework for Privacy Preserving in IoT based Healthcare, Journal of Ambient Intelligence and Humanized Computing, 14(3), 2631-2643, https://doi.org/10.1007/s12652-022-04510-8.
16. Hussain F., S. G. Abbas, G. A. Shah, I. M. Pires, et al. (2021). A Framework for Malicious Traffic Detection in IoT Healthcare Environment, Sensors, 21(9), 3025, https://doi.org/10.3390/s21093025.
17. Jalali M. S., J. P. Kaiser, M. Siegel, S. Madnick (2019). The Internet of Things Promises New Benefits and Risks: A Systematic Analysis of Adoption Dynamics of IoT Products, IEEE Security & Privacy, 17(2), 39-48, https://doi.org/10.1109/MSEC.2018.2888780.
18. Javaid M., A. Haleem, P. R. Singh, R. Suman (2023). Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends, Cyber Security and Applications, 1, 100016, https://doi.org/10.1016/j.csa.2023.100016.
19. Kelly J. T., K. L. Campbell, E. Gong, P. Scuffham (2020). The Internet of Things: Impact and Implications for Health Care Delivery, Journal of Medical Internet Research, 22(11), e20135, https://doi.org/10.2196/20135.
20. Khatiwada P., B. Yang (2022). An Overview on Security and Privacy of Data in IoMT Devices: Performance Metrics, Merits, Demerits, and Challenges, pHealth, 126-136, https://doi.org/10.3233/SHTI220970.
21. Mazhar T., D. B. Talpur, T. A. Shloul, Y. Y. Ghadi, et al. (2023). Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence, Brain Sciences, 13(4), 683, https://doi.org/10.3390/brainsci13040683.
22. Mejía-Granda C. M., J. Fernández-Alemán, J. Carrillo-de-Gea, J. García-Berná (2024). Security Vulnerabilities in Healthcare: An Analysis of Medical Devices and Software, Medical and Biological Engineering and Computing, 62(1), 257-273, https://doi.org/10.1007/s11517-023-02912-0.
23. Mitchell M., L. Kan (2019). Digital Technology and the Future of Health Systems, Health Systems Reform, 5(2), 113-120, https://doi.org/10.1080/23288604.2019.1583040.

24. Mitchell-Box K., K. L. Braun (2012). Fathers' Thoughts on Breastfeeding and Implications for a Theory-based Intervention, Journal of Obstetric, Gynecologic, and Neonatal Nursing, 41(6), 41-50, https://doi.org/10.1111/j.1552-6909.2012.01399.x.
25. Nayak J., S. K. Meher, A. Souri, B. Naik, S. Vimal (2022). Extreme Learning Machine and Bayesian Optimization-driven Intelligent Framework for IoMT Cyber-attack Detection, Journal of Supercomputing, 78(13), 14866-14891, https://doi.org/10.1007/s11227-022-04453-z.
26. Page M. J., J. E. McKenzie, P. M. Bossuyt, I. Boutron, et al. (2021). The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews, BMJ, 372, https://doi.org/10.1136/bmj.n71.
27. Rahman S., T. Suleski, M. Ahmed, A. S. M. Kayes (2022). An Investigation of Vulnerabilities in Internet of Health Things, International Conference on Cognitive Radio Oriented Wireless Networks, 296-306, https://doi.org/10.1007/978-3-030-98002-3_22.
28. Sadek I., J. Codjo, S. Rehman, B. Abdulrazak (2022). Security and Privacy in the Internet of Things Healthcare Systems: Toward a Robust Solution in Real-life Deployment, Computers in Medicine and Biology Update, 2, 100071, https://doi.org/10.1016/j.cmpbup.2022.100071.
29. Sarkis-Onofre R., F. Catalá-López, E. Aromataris, C. Lockwood (2021). How to Properly Use the PRISMA Statement, Systematic Reviews, 10, 1-3, https://doi.org/10.1186/s13643-021-01671-z.
30. Shahid J., R. Ahmad, A. K. Kiani, T. Ahmad, et al. (2022). Data Protection and Privacy of the Internet of Healthcare Things (IoHTs), Applied Sciences, 12(4), 1927, https://doi.org/10.3390/app12041927.
31. Shewale R. (2024). How Many IoT Devices Are There (2024-2032), IoT Analytics Journal.
32. Sousa R. (2024). Cyber Threats to Healthcare Technology Services: A Case Study, Advanced Research on Information Systems Security, 4(1), 35-46, https://doi.org/10.56394/aris2.v4i1.38.
33. Sparrell D. (2019). Cyber-safety in healthcare IoT, ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K), 1-6, https://doi.org/10.23919/ITUK48006.2019.8996148.
34. Suleski T., M. Ahmed (2023). A Data Taxonomy for Adaptive Multifactor Authentication in the Internet of Health Care Things, Journal of Medical Internet Research, 25, e44114, https://doi.org/10.2196/44114.
35. Tuscano A., S. Joshi (2023). Significance of Cybersecurity of IoT Devices in the Healthcare Sector, Somaiya International Conference on Technology and Information Management, 12-16, https://doi.org/10.1109/SICTIM56495.2023.10104657.
36. Vaidya S. (2024). Enhancing Cybersecurity in Healthcare IoT Ecosystems: A Comprehensive Framework for Securing Medical Data and Devices, Educational Administration: Theory and Practice, 30(6), 270-277, https://doi.org/10.53555/kuey.v30i6(S).5371.
37. Zeadally S., F. Siddiqui, Z. Baig, A. Ibrahim (2020). Smart Healthcare: Challenges and Potential Solutions Using Internet of Things (IoT) and Big Data Analytics, PSU Research Review, 4(2), 149-168, https://doi.org/10.1108/PRR-08-2019-0027.
38. Ziwei H., Z. Dongni, Z. Man, D. Yixin, et al. (2024). The Applications of Internet of Things in Smart Healthcare Sectors: A Bibliometric and Deep Study, Heliyon, 10(3), e25392, https://doi.org/10.1016/j.heliyon.2024.e25392.
39. https://csrc.nist.gov/pubs/cswp/33/product-development-cybersecurity-handbook/ipd (Access date 02 June 2025).

Prof. Teodora Bakardjieva, Ph.D.
E-mail: bakardjieva@vfu.bg

Teodora Bakardjieva earned a degree in Telecommunications Engineering from Varna Technical University, Bulgaria and a Ph.D. degree at Sofia University. She was a Vice Rector for International Affairs and Technological Development at Varna Free University (2015-2019) and Director of its Institute of Technology (2007-2015). Currently, she leads the Cybersecurity and International Business Project Management Master's programs. Her expertise is in the field of cybersecurity, IoT, IT, computer networks, biometric security, and software project management. Since 2023, she has been a Vice Chairman of the Union of Scientists in Bulgaria. Her research focuses on advancing digital security, innovation, and interdisciplinary approaches to technology and business education.

Sen. Assist. Prof. Antonina Ivanova, Ph.D.
E-mail: antonina.ivanova@vfu.bg

Antonina Ivanova earned her degree in Electrotechnics from the Technical University of Dresden, Germany, and later completed her Ph.D. in Computer Science at Varna Free University, Bulgaria. Her academic and professional interests are focused on emerging technologies and their applications in modern digital ecosystems. Her research expertise includes cybersecurity, social network analysis, business process automation, web technologies, e-business, and the internet of things. Over the course of her career, Dr. Ivanova has contributed to numerous research initiatives and interdisciplinary projects. Currently, Dr. Ivanova serves as the Head of the Department of Computer Science at Varna Free University.

Assoc. Prof. Yanko Yankov, Ph.D.
E-mail: yanko.yankov@mu-varna.bg

Yanko Yankov earned his M.Sc. degree in Medicine, M.Sc. degree in Health Management, and a Ph.D. degree from the Medical University "Prof. Dr. Paraskev Stoyanov", Varna, Bulgaria. He began his academic career at the same university, progressing from part-time Assistant in 2019 to full-time Assistant, Senior Assistant Professor, and since 2024, an Associate Professor in Maxillofacial Surgery. His areas of expertise include oral and maxillofacial surgery and aesthetic medicine. Dr. Yankov has been recognised with prestigious awards, including the "Golden Hippocrates" and the "First Degree Award" from the Bulgarian Medical Union in 2014.

Assoc. Prof. Zhivko Zhekov, Ph.D.
E-mail: zhivko.zhekov@mu-varna.bg

Dr. Zhivko Zhekov earned his M.Sc. degree in Medicine and a Ph.D. degree from the Medical University "Prof. Dr. Paraskev Stoyanov", Varna, Bulgaria. His academic career at the same institution includes roles as part-time Assistant, full-time Assistant, and Senior Assistant Professor in Obstetrics and Gynecology from 2017 to 2024. Since 2024, he has been an Associate Professor in the same field. His areas of expertise include laparoscopy in gynecology. In addition to his academic roles, he has been a Head of the Gynecology Department at the Specialised Hospital for Obstetrics and Gynecology for Active Treatment "Prof. Dr. D. Stamatov", Varna, Bulgaria since 2016.