

CYBERSECURITY FOR SUSTAINABLE INTERNET OF THINGS IMPLEMENTATION IN HEALTHCARE

Teodora Bakardjieva^{1✉}, Antonina Ivanova¹, Yanko Yankov²,
Zhivko Zhekov³

Received on December 11, 2024

Presented by Ch. Roumenin, Member of BAS, on February 25, 2025

Abstract

This systematic review aims to summarize and analyze the impact and implications of the Internet of Things (IoT) in the healthcare sector. A comprehensive electronic search was conducted using Google Scholar, PubMed, and Scopus, covering articles published between January 1, 2019, and July 1, 2024, following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. The review examines cybersecurity threats in IoT-based healthcare infrastructure and applications that support smart healthcare services. The integration of IoT in medical data collection and storage offers valuable opportunities for data analysis, enhancing risk factor identification, disease diagnosis, treatment, and remote monitoring. This, in turn, facilitates reliable self-monitoring for patients. The study evaluates both the advantages and risks associated with IoT in healthcare and provides recommendations for further research.

Key words: cybersecurity, Internet of Things (IoT), healthcare, vulnerabilities, threats

Introduction. The Internet of Things (IoT) is a transformative trend driving the continuous digitization and integration of information technology into various sectors in unprecedented ways. The number of IoT-enabled devices is rapidly increasing and is expected to double by 2030 [1].

<https://doi.org/10.7546/CRABS.2025.04.09>

Cybersecurity risks are a major concern for the widespread adoption of IoT in healthcare. Key challenges include safeguarding patient data, preventing unauthorized tracking, and mitigating hacking threats. Ensuring the security of medical information is essential to prevent data breaches and protect patient privacy [2].

The primary objective of this study is to outline the cybersecurity threats associated with IoT implementation in healthcare and to address the following 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 [3].

The search “cybersecurity AND IoT AND healthcare OR IoHT AND cyber-attacks” included only articles in English published from January 1, 2019, to July 1, 2024. The inclusion criteria were: articles that discuss cybersecurity and the Internet of Things (IoT) in healthcare or articles that describe the Internet of Healthcare Things (IoHT) and cyber-attacks. The exclusion criteria were: articles before January 1, 2019; not full-text articles and citations; and articles in languages different from English.

Results and discussion. The initial search found 23 862 relevant studies (Google Scholar – 4680 results; PubMed – 18 results; Scopus – 975 results). Figure 1 illustrates the PRISMA flow diagram, outlining the screening and selection process.

This study has certain limitations that should be acknowledged. The first 100 search results from both Google Scholar and Scopus, along with all 18 studies from PubMed, were selected for evaluation. A total of 25 duplicate records were excluded, resulting in 193 records being screened and assessed for eligibility. Ultimately, 16 relevant articles were included in this study.

To enhance methodological rigour, quality assessment criteria have been incorporated into the study, as detailed in Table 1 (Quality assessment framework).

Each study was scored between 1 (low quality) and 5 (high quality) on each criterion. A study must score at least 3 in each category to be included in the analysis. The characteristics of the review articles that met the eligibility criteria and were included in the current study are presented in Table 2.

The 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. Strengthening the resilience and security of medical data and connected devices requires identifying potential vulnerabilities and implementing comprehensive cybersecurity frameworks [20].

A word frequency count of key terms from the reviewed articles is presented in Fig. 2.

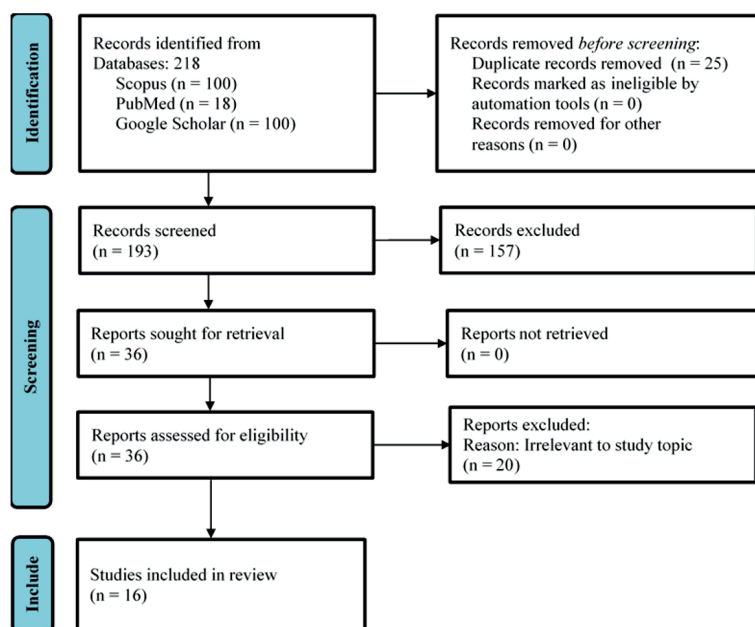


Fig. 1. The PRISMA flow diagram

T a b l e 1

Quality assessment framework

Criteria	Description	Score
Study design	Systematic review, experimental, case study, survey, opinion-based, etc.	1–5
Relevance to research question	Direct relevance to IoT healthcare cybersecurity issues	1–5
Methodological rigour	Clarity of methodology, sample size, data reliability	1–5
Evaluation of solutions	Feasibility, scalability, and effectiveness of cybersecurity solutions proposed	1–5
Quality of reporting	Clarity, transparency, and presence of any bias/conflict of interest	1–5

The quantitative synthesis of reviewed papers reveals that the most common cybersecurity challenge across the reviewed papers is the risk of data breaches. These findings emphasize that while the cybersecurity of IoT devices in healthcare has improved over time, challenges remain, particularly in data protection, authentication, and availability.

Regarding technologies proposed in the literature a majority of studies advocate for multi-layered security measures such as combining encryption, firewalls, access control, and authentication protocols. The proposed solutions demonstrate that IoT healthcare systems need to adopt a multi-layered defense approach, com-

T a b l e 2

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

Reference	Title	Year	Recap	Average score (1–5)
Cartwright et al. [4]	The elephant in the room: cybersecurity in healthcare	2023	Cybersecurity is essential for protecting healthcare systems and patient data. The article emphasizes the need for proactive measures like security.	4
Mazhar et al. [5]	Analysis of IoT security challenges and its solutions using artificial intelligence	2023	AI-driven approaches can significantly enhance IoT security in healthcare by detecting threats quickly and effectively.	5
Bhukya et al. [6]	Cybersecurity in internet of medical vehicles: state-of-the-art analysis, research challenges and future perspectives	2023	IoMV systems are highly vulnerable to cyber threats due to their mobility and connectivity. It calls for enhanced security frameworks.	3
Hussain et al. [7]	A framework for malicious traffic detection in IoT healthcare environment	2021	The proposed framework effectively detects malicious traffic, improving the security posture of healthcare IoT networks.	4
Almalawi et al. [8]	Managing security of healthcare data for a modern healthcare system	2023	Multi-layered approach, including encryption, access control, and regular audits is essential for managing healthcare data security effectively.	4
Mejía-Granda et al. [9]	Security vulnerabilities in healthcare: an analysis of medical devices and software	2024	The study calls for the implementation of stricter security standards, regular vulnerability testing, and enhanced collaboration between manufacturers and healthcare providers.	4
Hurrah et al. [10]	CADEN: cellular automata and DNA based secure framework for privacy preserving in IoT based healthcare	2023	CADEN framework provides strong privacy and data security measures for IoT healthcare environments. Further development and testing are recommended to enhance its defense against advanced cyber threats.	3
Ahouanmenou et al. [11]	Information security and privacy in hospitals: a literature mapping and review of research gaps	2023	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 and shows the research gaps.	4
Khatiwada et al. [12]	An overview on security and privacy of data in IoMT devices: performance metrics, merits, demerits, and challenges	2022	IoMT devices provide significant benefits to healthcare, they come with major security and privacy risks. It suggests balancing performance with enhanced measures.	4

T a b l e 2

(continued)

Nayak et al. [13]	Extreme learning machine and Bayesian optimization-driven intelligent framework for IoMT cyber-attack detection	2022	An effective framework for detecting cyber-attacks in IoMT systems is proposed, demonstrating high accuracy and low false positive rates. It recommends testing for real-world applications.	5
Bughio et al. [14]	Developing a novel ontology for cybersecurity in internet of medical things-enabled remote patient monitoring	2024	The proposed ontology framework helps systematically address cybersecurity concerns in remote patient monitoring, improving threat identification.	3
Sparrell D. [15]	Cyber-safety in health-care IOT	2019	Healthcare IoT systems are highly vulnerable to cyber threats, stressing the need for robust security protocols and ongoing monitoring.	3
Rahman et al. [16]	An investigation of vulnerabilities in internet of health things	2022	The study identifies security weaknesses in IoHT devices that could be exploited by attackers and recommends enhanced security measures.	4
Javaid et al. [17]	Towards insighting cybersecurity for healthcare domains: a comprehensive review of recent practices and trends	2023	Although there have been improvements in healthcare cybersecurity, many vulnerabilities remain. The paper emphasizes the need for innovative solutions.	4
AboulEla S. et al. [18]	Navigating the cyber threat landscape: an in-depth analysis of attack detection within IoT ecosystems	2024	Effective cyber-attack detection in IoT requires advanced machine learning techniques, and continuous system monitoring and suggests further research to refine detection methods.	5
Sousa R. [19]	Cyber threats to healthcare technology services: a case study	2024	Healthcare technology services are frequently targeted by advanced cyber threats. It highlights the critical need for cybersecurity frameworks.	4

binning traditional methods like encryption and authentication with newer technologies such as AI and blockchain.

Key findings. The deployment of IoT in healthcare has brought new challenges in terms of cybersecurity. Malicious attacks, such as DDoS (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.

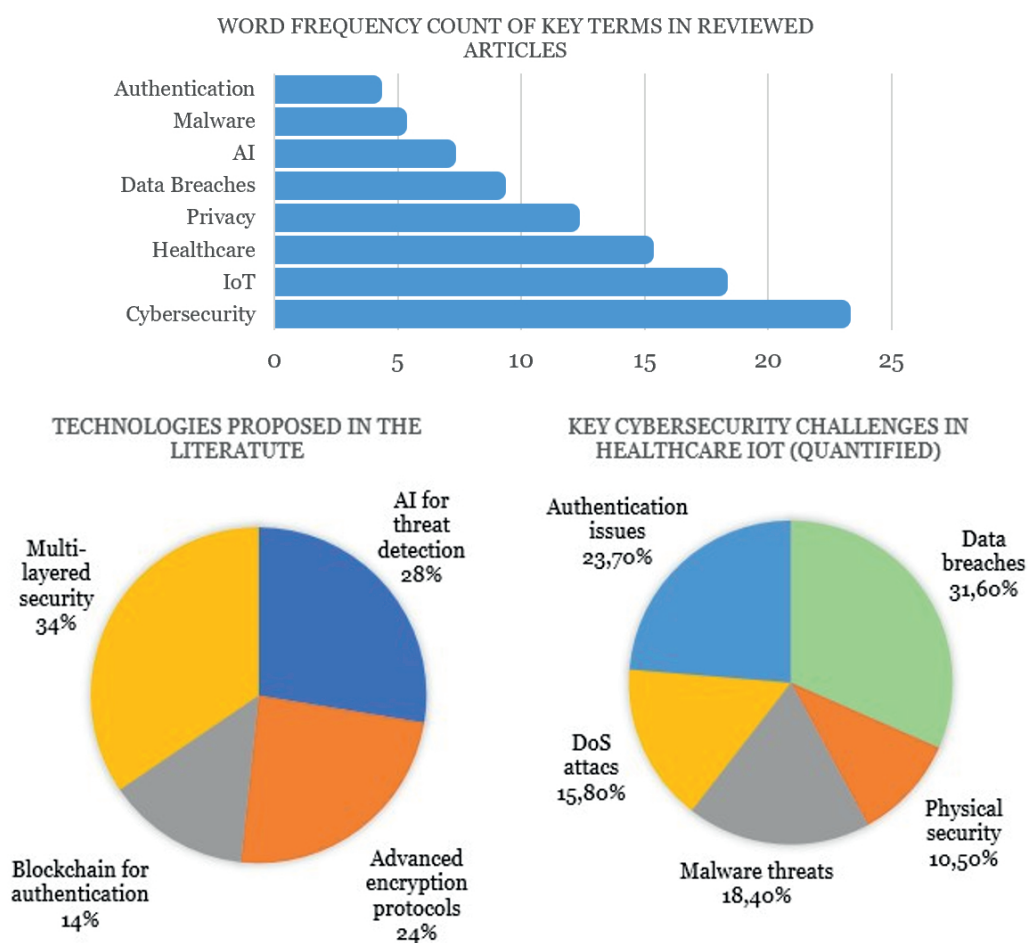


Fig. 2. Quantitative synthesis of reviewed papers

Specific recommendations that could be summarized include:

- Developing IoT-specific cybersecurity regulations and standards.
- Implementation of layered security strategies and continuous staff training.
- Investment in AI-based detection, blockchain for authentication, and IoT device security.
- Research focuses on device vulnerabilities and developing scalable, cloud-based solutions.
- Promotion of industry-wide collaboration and knowledge sharing for more comprehensive cybersecurity strategies

This paper is moving beyond just reviewing existing research allowing for a nuanced view of the issues, focusing on gaps and limitations in existing studies, and suggesting recommendations and improvements.

Conclusion. The study indicates a need for more research and development in healthcare IoT cybersecurity. In particular, there is a necessity 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.

Bulgaria has been transitioning to digital health records, e-prescriptions, and remote monitoring technologies. However, the lack of comprehensive cybersecurity frameworks for these technologies makes healthcare systems more susceptible to attacks. Cybersecurity in the Bulgarian healthcare sector requires significant improvements, especially in light of the increasing adoption of IoT devices and digital health records. The challenges are manifold, including outdated infrastructure, lack of training, and the fragmented nature of the cybersecurity landscape. However, through collaboration, infrastructure modernization, training, and implementation of national standards, Bulgaria can strengthen the cybersecurity of its healthcare system, ensuring the safety of patient data and the integrity of critical healthcare services.

REFERENCES

- [1] IoT Analytics (2024) INSIGHTS RELEASE – Number of connected IoT devices, <https://iot-analytics.com/wp/wp-content/uploads/2024/09/INSIGHTS-RELEASE-Number-of-connected-IoT-devices-vf.pdf> (Accessed: December 2, 2024).
- [2] NIST (2024) Product development cybersecurity handbook: concepts and considerations for IoT product manufacturers, <https://csrc.nist.gov/pubs/cswp/33/product-development-cybersecurity-handbook/ipd> (Accessed: September 19, 2024).
- [3] PAGE M. J., J. E. MCKENZIE, P. M. BOSSUYT et al. (2021) The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, *BMJ*, **372**, n71, <https://doi.org/10.1136/bmj.n71>.
- [4] CARTWRIGHT A. J. (2023) The elephant in the room: cybersecurity in healthcare, *J. Clin. Monit. Comput.*, **37**, 1123–1132, <https://doi.org/10.1007/s10877-023-01013-5>.

- [5] MAZHAR T., D. B. TALPUR, T. A. SHLOUL et al. (2023) Analysis of IoT security challenges and its solutions using artificial intelligence, *Brain Sci.*, **13**, 683, <https://doi.org/10.3390/brainsci13040683>.
- [6] 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 (Basel)*, **23**, 8107, <https://doi.org/10.3390/s23198107>.
- [7] HUSSAIN F., S. G. ABBAS, G. A. SHAH et al. (2021) A framework for malicious traffic detection in IoT healthcare environment, *Sensors (Basel)*, **21**, 3025, <https://doi.org/10.3390/s21093025>.
- [8] ALMALAWI A., A. I. KHAN, F. ALSOLAMI et al. (2023) Managing security of healthcare data for a modern healthcare system, *Sensors (Basel)*, **23**, 3612, <https://doi.org/10.3390/s23073612>.
- [9] MEJÍA-GRANDA C. M., J. L. FERNÁNDEZ-ALEMÁN, J. M. CARRILLO-DE-GEA, J. A. GARCÍA-BERNÁ (2024) Security vulnerabilities in healthcare: an analysis of medical devices and software, *Med. Biol. Eng. Comput.*, **62**, 257–273, <https://doi.org/10.1007/s11517-023-02912-0>.
- [10] HURRAH N. N., E. KHAN, U. KHAN (2023) CADEN: cellular automata and DNA based secure framework for privacy preserving in IoT based healthcare, *J. Ambient Intell. Humaniz. Comput.*, **14**, 2631–2643, <https://doi.org/10.1007/s12652-022-04510-8>.
- [11] AHOUANMENOU S., A. VAN LOOY, G. POELS (2023) Information security and privacy in hospitals: a literature mapping and review of research gaps, *Inform. Health Soc. Care*, **48**, 30–46, <https://doi.org/10.1080/17538157.2022.2049274>.
- [12] KHATIWADA P., B. YANG (2022) An overview on security and privacy of data in IoMT devices: performance metrics, merits, demerits, and challenges, *Stud. Health Technol. Inform.*, **299**, 126–136, <https://doi.org/10.3233/SHTI220970>.
- [13] NAYAK J., S. K. MEHER, A. SOURI et al. (2022) Extreme learning machine and Bayesian optimization-driven intelligent framework for IoMT cyber-attack detection, *J. Supercomput.*, **78**, 14866–14891, <https://doi.org/10.1007/s11227-022-04453-z>.
- [14] 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 (Basel)*, **24**, 2804, <https://doi.org/10.3390/s24092804>.
- [15] SPARRELL D. (2019) Cyber-safety in healthcare IoT, *ITU Kaleidoscope: Challenges for a Data-Driven Society*, Atlanta, GA, USA, 2019, 1–6, <https://doi.org/10.23919/ITUK48006.2019.8996148>.
- [16] RAHMAN S., T. SULESKI, M. AHMED, A. S. M. KAYES (2022) An investigation of vulnerabilities in internet of health things, *Lecture Notes of the Institute for Computer Sciences, Social Informatics, and Telecommunications Engineering (LNICST)*, **427**, 296–306, https://doi.org/10.1007/978-3-030-98002-3_22.
- [17] 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>.
- [18] ABOULELA S., N. IBRAHIM, S. SHEHMIR et al. (2024) Navigating the cyber threat landscape: an in-depth analysis of attack detection within IoT ecosystems, *AI*, **5**, 704–732, <https://doi.org/10.3390/ai5020037>.

- [19] SOUSA R. (2024) Cyber threats to healthcare technology services: a case study, *Adv. Res. Inf. Systems*, **4**, 35–46, <https://doi.org/10.56394/aris2.v4i1.38>.
- [20] VAIDYA S. (2024) Enhancing cybersecurity in healthcare IoT ecosystems: a comprehensive framework for securing medical data and devices, *Educ. Adm.: Theory Pract.*, **30**, 270–277, [https://doi.org/10.53555/kuey.v30i6\(S\).5371](https://doi.org/10.53555/kuey.v30i6(S).5371).

¹*Department of Computer Science, Varna Free University “Chernorizets Hrabar”,
84 Yanko Slavchev St, 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 St, 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 St, 9002 Varna, Bulgaria
e-mail: zhivko.zhekov@mu-varna.bg*