EAI Endorsed Transactions
on Pervasive Health and Technology
Review Article EAI.EU

IoMT and Data Privacy in Alzheimer's Care for Older Adults: A Systematic Review

Fahim Islam Anik[1], Md Mehedi Hasan[2], Juan Rodriguez-Cardenas[2], Richard Beiswanger[2], Masrura Tasnim[2], Mary Ramos[3], Nazmus Sakib[2,*]

[1]Department of Mechanical Engineering, Khulna University of Engineering and Technology, Khulna, Bangladesh
[2]Department of Information Technology, Kennesaw State University, Marietta, Georgia, United States
[3]School of Nursing, Louisiana State University Health Sciences Center New Orleans, New Orleans, LA 70112

Abstract

INTRODUCTION: The use of medical Internet of Things (IoT) devices becomes essential in everyday healthcare routines as the older adults confront an increasing risk of cyber victimization because of Alzheimer's illness. Despite the myriad benefits of IoT devices, escalating concerns about data privacy and cybersecurity loom larger, given the cognitive and physical decline associated with Alzheimer's.
OBJECTIVES: Focusing on the challenges faced by older adults, especially those with Alzheimer's, this study aims to investigate the data privacy and security risks and advocates for specialized education and user-friendly interfaces to narrow the digital divide.
METHODS: Eighteen peer-reviewed articles were selected based on predefined inclusion criteria, focusing on older adults or Alzheimer's patients, IoMT in healthcare, and data privacy or security concerns. Searches were conducted in PubMed and IEEE Xplore, following PRISMA 2020 guidelines. A structured data extraction matrix informed by Grounded Theory was used to chart and analyze key themes across selected studies, including types of vulnerabilities, consequences, and proposed solutions.
RESULTS: Recurring vulnerabilities included social engineering, data breaches, weak authentication, and poor access control. Effective mitigation strategies identified include patient and caregiver education, improved informed consent procedures, robust encryption, and data governance reforms.
CONCLUSION: Smart home technology and the digitization of the healthcare field have shown great promise in caring for Alzheimer's patients, positively affecting their ability to live on their own safely. They also create new challenges with the need to protect the sensitive information they gather. Our research emphasizes developing strategies that can create awareness and educate patients and their caregivers to further reduce the risks related to data security.

Keywords: Data Privacy, Smart Health, Alzheimer's, Older Adults, Internet of Medical Things (IoMT).

Received on 27 May 2024, accepted on 06 August 2025, published on 18 September 2025

doi: 10.4108/eetpht.11.6170

1. Introduction

Alzheimer's disease is the most prevalent form of dementia, particularly affecting older adults. In 2021, an estimated 57 million people were living with dementia worldwide, with over 60% residing in low- and middle-income countries. This number is expected to rise significantly in the coming decades, with approximately 10 million new cases emerging annually [1]. The associated cognitive decline, particularly memory loss, impairs patients' decision-making abilities and compromises their capacity for independent self-care [2,3]. Maintaining social interactions and general relations becomes a challenge for these groups of people due to cognitive decline [4]. However, technology can contribute greatly to older adults at home and in healthcare facilities by identifying and monitoring health-related issues, keeping track of health records, and managing personal and financial information [5]. IoT and IoMT devices can be quite useful for older adults to make their lives easier [6–8]. On the other hand, Cognitive decline reduces the ability of older individuals to learn and

understand the proper uses of these technological devices which makes them more vulnerable to cyber victimization [9]. This increased vulnerability leads to serious concern for their data privacy and protection [10–12]. For instance, electronic health records contain highly sensitive information that, if inadequately protected, may be targeted by cybercriminals for financial exploitation [13,14]. Similarly, Internet of Things (IoT) devices used in healthcare are vulnerable to cyberattacks, which can lead to unauthorized access, data breaches, and the manipulation of medical records [15–17]. These risks are particularly concerning for individuals with Alzheimer's disease or related dementias (ADRD), as their cognitive impairments complicate the process of obtaining informed consent for data collection and device usage—posing both ethical and legal challenges [18,19]. Additionally, while the integration of multiple IoT systems is essential for delivering comprehensive and coordinated care, poor management of interoperability between these devices may introduce further security vulnerabilities. Despite these challenges, IoT technologies offer substantial benefits in monitoring the health and well-being of patients with ADRD. These devices can continuously track vital signs, activity levels, and medication adherence, enabling healthcare providers and caregivers to make timely and informed decisions. Features such as geofencing and real-time location tracking further enhance safety by preventing incidents of wandering or disorientation—common risks among individuals living with dementia [20–22].

While much of the existing literature focuses on the general vulnerabilities in IoT healthcare devices [23–25], little investigation has gone into unraveling the disparities in data privacy that older adults face, a crucial issue with broad ramifications in the evolving the smart-health landscape. The younger generation is more likely to be tech-savvy, while the opposite holds true for older adults in adapting to technology. Since most older adults have a lower level of computer literacy and a lack of general understanding related to novel technological devices, they tend to be unaware when it comes to a device's settings. Another matter of concern is their ignorance of how their sensitive information could be exposed and stolen by cybercriminals. Hackers often attempt to gain access to electronic health records which is putting healthcare providers and patients at risk [26]. Moreover, third-party organizations that handle billing and legal procedures are another common target [27]. As a result, it is a complex system that must be maintained to ensure this sensitive data continues to transfer securely while protecting its privacy. It requires cooperation from the companies that manufacture IoMT devices, healthcare providers, and lawmakers to accomplish these safety goals. Addressing disparities in data privacy requires comprehensive strategies and procedures. Taking each step to ensure the security of using IoMT devices will allow their use to bring benefits to patients, especially older adult patients, and the entire healthcare industry.

Considering the information outlined above, this systematic literature review is centered on a crucial point: How can the usage of Internet of Medical Things (IoMT) technologies be investigated to benefit rather than hold potential risk to the older population in healthcare? This Systematic literature review aims to address the gaps in existing research by investigating the security vulnerabilities in devices, also known as the Internet of Medical Things (IoMT) used by older adults. Within this age group, we will explore the challenges arising from factors like literacy, sensory impairments, and the frequent reliance on remote healthcare services. Through an approach involving searches in literature databases, refining keywords, and utilizing the PRISMA table to organize our search results, we narrowed down our focus to 18 research articles found in the database. Upon reviewing these documents, we have carefully examined the issues at hand. Our analysis delves into identifying the vulnerabilities of IoMT and how they impact the data privacy of older individuals. We explore the cybersecurity protocols in place and put forth a variety of new solutions, including policy recommendations and hardware modifications to address these concerns. These efforts ultimately enhance the safety and reliability of healthcare technologies. Our contribution offers actionable insights for healthcare providers, technology developers, and policymakers to develop a robust security framework sensitive to the unique needs of older adults.

The rest of the paper includes 6 sections. Section 2 describes the study identification and selection procedures. Next, the first Research Question (RQ) is addressed in section 3. Section 4 elaborates on IoMT data privacy and security challenges in older adult healthcare. The following two sections (section 5 and section 6) delineates RQ3 and RQ4 subsequently. Finally, section 7 summarizes the study with future work recommendations.

2. Methods

A systematic review approach was adopted due to its rigorous and transparent methodology for identifying, evaluating, and synthesizing relevant evidence across interdisciplinary domains. The objective was to comprehensively assess the cybersecurity and data privacy vulnerabilities associated with Internet of Medical Things (IoMT) technologies in the context of older adults, particularly those with cognitive impairments such as Alzheimer's disease. The review was conducted in accordance with the PRISMA 2020 guidelines [28], ensuring methodological consistency and reproducibility. This section details the research design, eligibility criteria, search strategy, study selection procedures, data extraction process, and synthesis methods employed to analyze and interpret the findings across the selected studies.

2.1. Research Questions

The research questions in this study encompass an examination of the impact of Artificial Intelligence (AI) and Machine Learning (ML) techniques integrated into aging care

using data sourced from Internet of Medical Things (IoMT) devices. Firstly, they aim to discern the AI and ML methodologies that most effectively elevate medical diagnosis, treatment, and interventions tailored to older adult patients. They also explore data privacy and security within IoMT technologies, emphasizing the identification of vulnerabilities specific to older adult healthcare while seeking technical and regulatory measures to mitigate these risks. Furthermore, they navigate the complex landscape of aging care systems, discerning the optimal balance between data privacy safeguards and the necessity of collecting and sharing this essential health information. The specific research questions are as follows:

RQ1: What artificial intelligence and machine learning techniques can be implemented to enhance medical diagnosis, treatment, and interventions for older adult patients using data from the Internet of Medical Things (IoMT) devices?

RQ2: What are the primary data privacy and security vulnerabilities in IoMT technologies for older adult healthcare, and what technical and regulatory safeguards can help mitigate these risks?

RQ3: How can older adult healthcare systems optimally balance robust data privacy and security protections with the need for collecting and sharing essential health information? What factors most influence the acceptance and adoption of these technologies by older adult users, their caregivers, and healthcare providers?

RQ4: How can we infer the findings to prognosticate future healthcare security and privacy issues centered around Alzheimer's patients?

These research questions include an analysis of the factors influencing the acceptance and adoption of these technologies among older adult users, their caregivers, and healthcare providers. The final question prognosticates future implications in a more vulnerable subset, seeking to extrapolate the findings of healthcare security and privacy concerns centered around Alzheimer's patients. This multi-layered approach aims to grasp the current landscape, conceptualize, and proactively address forthcoming challenges in technology and healthcare privacy for older adults.

2.2. Research Design

This study employed a systematic review methodology to rigorously identify, assess, and synthesize existing evidence on cybersecurity and data privacy concerns associated with Internet of Medical Things (IoMT) technologies in older adult healthcare. Systematic reviews are well-suited for answering focused research questions by applying transparent and replicable methods for study selection, data extraction, and analysis. The review was structured in accordance with the PRISMA 2020 guidelines to ensure methodological rigor and clarity.

Although we followed systematic review principles, we acknowledge that the review protocol was not prospectively registered in a public registry such as PROSPERO or OSF. This was due to the retrospective development of the study framework within an interdisciplinary research context. We recognize this as a limitation and have addressed it accordingly in the discussion section.

2.2. Eligibility Criteria

The eligibility criteria for this systematic review were designed to ensure that selected studies addressed the intersection of older adults' interactions with IoT or IoMT healthcare devices and the cybersecurity and privacy challenges that arise in these contexts. Given the growing integration of smart medical technologies into elder care and the increasing frequency of cybersecurity incidents in recent years, we focused specifically on studies published within the past five years that addressed these contemporary risks.

This review emphasizes the examination of high-impact threats such as ransomware attacks, data leaks, and denial-of-service (DoS) attacks, especially as they pertain to older adults and patients with Alzheimer's or related dementias (ADRD). We also sought to explore proactive solutions, such as the application of artificial intelligence, access control mechanisms, and privacy-compliant design practices, to assess how these technologies are being adapted to safeguard sensitive health data. Our approach delves beyond mere usage patterns and develops a preliminary understanding of productive solutions such as the usage of AI, access controls, & other privacy-compliant practices [29]. To ensure thematic relevance and methodological consistency, we developed clear inclusion and exclusion criteria, summarized in Table 1. Studies were eligible for inclusion if they focused on older adults or ADRD patients and addressed healthcare-based IoT applications involving privacy, security, or ethical concerns. Conversely, studies were excluded if they lacked a specific focus on either the target population (older adults), the healthcare setting, or the data protection aspects.

2.3. Information Sources and Search Strategy

To ensure methodological rigor, we followed a systematic, step-by-step process to identify and retrieve relevant literature. The objective was to gather, critically assess, and synthesize peer-reviewed research addressing cybersecurity risks, data privacy, and ethical considerations in the use of Internet of Medical Things (IoMT) technologies for older adults. This process was designed in alignment with PRISMA guidelines We initially developed a comprehensive search strategy incorporating both subject-specific keywords and Boolean operators to maximize sensitivity and precision. The preliminary search string was: *(Older OR Elder OR Senior) AND (Alzheimer OR Dementia OR AD) AND (Security OR Breach OR Cyber OR Data OR Record OR Scam) AND (IoT OR Health OR Medical) AND (Ethics OR Confidentiality OR Privacy OR Compliance).*

Table 1. Inclusion and Exclusion Criteria

Criterion Category	Inclusion Criteria	Exclusion Criteria
Population	Studies involving older adults (typically aged 60 or above), including individuals diagnosed with Alzheimer's disease or related dementias (ADRD).	Studies not involving older adult populations or those without explicit reference to aging or cognitive impairments.
Technology Context	Research focused on Internet of Things (IoT) or Internet of Medical Things (IoMT) applications within healthcare settings.	Studies addressing IoT technologies outside the healthcare context (e.g., industrial, transportation, or agriculture sectors).
Focus of Analysis	Primary emphasis on data privacy, cybersecurity risks, compliance, ethics, or regulatory challenges associated with IoMT use.	Studies that briefly mention security without substantial discussion or that focus solely on technical vulnerabilities without ethical or privacy considerations.
Relevance to Review Objectives	Articles that examine at least two of the following core themes: (1) older adults or ADRD patients, (2) IoMT use in healthcare, (3) data privacy, security, or compliance frameworks.	Articles lacking two or more of the core themes; general discussions unrelated to the systematic review's objectives.
Language and Publication Criteria	Peer-reviewed journal articles or conference proceedings published in English between 2018 and 2023.	Non-English studies, preprints, dissertations, opinion pieces, and publications outside the specified time frame.

While this query retrieved a broad set of results, many articles were focused solely on clinical characteristics of dementia without addressing privacy or security concerns. To refine our scope, we iteratively revised the search strategy by excluding the terms *(Alzheimer OR Dementia OR AD)* and narrowing the technology component to *(IoT OR device)*. The revised and final search query was: *(Older OR Elder OR Senior) AND (Security OR Breach OR Cyber OR Data OR Record OR Scam) AND (IoT OR device) AND (Ethics OR Confidentiality OR Privacy OR Compliance)*.

We applied this final search string to four prominent academic databases: PubMed, IEEE Xplore, ACM Digital Library, and DBLP. Searches were restricted to:

- Publication years: 2018 to 2023
- Language: English
- Document type: Peer-reviewed journal articles and conference proceedings

The final search yielded 122 articles, predominantly from PubMed and IEEE Xplore. Although ACM Digital Library and DBLP were initially included, they did not yield contextually relevant results and were excluded from the final review. Following the search, we implemented a multi-stage screening process:

Title and Abstract Screening: Two reviewers independently evaluated the relevance of each article's title and abstract, resulting in the selection of 40 studies for full-text review.

Full-Text Screening: We applied our predefined eligibility criteria (Table 1, Section 2.2) to determine final inclusion. This phase led to the retention of 13 studies that addressed IoMT usage among older adults, highlighted security and privacy concerns, and presented potential technical or policy solutions.

To further ensure comprehensiveness, we conducted citation chaining by manually reviewing the reference lists of all included studies. Additionally, we employed the Litmaps citation mapping tool [30] to analyze citation networks and identify additional papers cited by, or citing, the initially selected studies. This process led to the identification and inclusion of 5 additional studies, resulting in a final total of 18 studies included in the review.

All selected studies originated from multidisciplinary domains including healthcare, computer science, biomedical engineering, and cybersecurity. Each was evaluated based on methodological quality, innovation, relevance to the research questions, and contribution to understanding IoMT privacy challenges among older adult populations. The complete selection process is visually represented in the PRISMA flow diagram (Figure 1). A subsequent breakdown of publication year and country distribution is shown in Figure 2.

2.4. Data Charting and Analysis Approach

To facilitate a systematic and transparent synthesis of findings, we employed a structured data charting process grounded in qualitative research principles, particularly those informed by Grounded Theory methodology. This approach enabled the iterative identification and refinement of key themes related to the cybersecurity, privacy, and usability of IoMT technologies among older adult populations. We developed a Data Extraction Matrix to guide the collection and comparison of relevant information across the selected studies. The matrix was initially informed by a preliminary literature scan and refined to align directly with our four research questions (RQ1–RQ4).

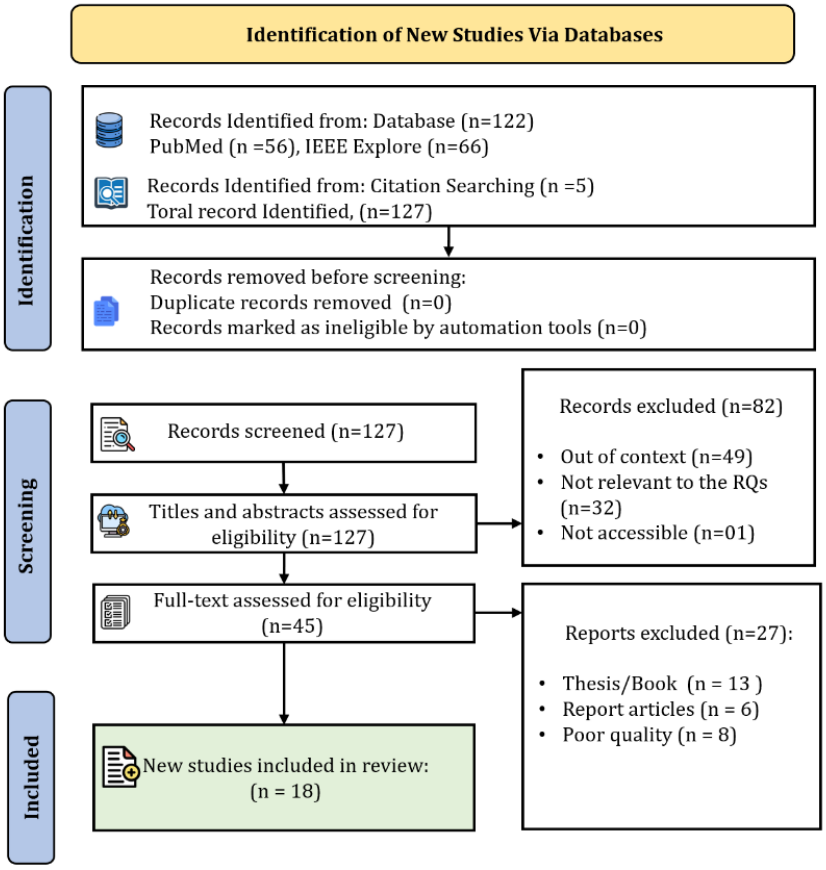

Figure 1. PRISMA flow diagram for study selection in the systematic review

To ensure accuracy and completeness, the charting process underwent three stages of validation:

- Pilot Testing: The matrix was tested on two representative studies to verify that it captured all essential variables. Adjustments were made to include overlooked data points and exclude non-relevant information.
- Expert Review: The matrix was reviewed by interdisciplinary collaborators with expertise in cybersecurity, health informatics, and gerontology. Their feedback was incorporated to enhance the conceptual robustness and completeness of the charting categories.
- Thematic Alignment: We ensured that each variable corresponded to one or more of the core review objectives, specifically targeting issues such as data breaches, patient safety, regulatory compliance, and the ethical implications of IoMT deployment in aging care.

The finalized matrix included the following fields:

- Bibliographic Data: Title, Authors, Year, Institution, Geographic Region
- Study Design and Scope: Methodology, Sample Size, Target Population
- Technology Context: Type of IoT/IoMT Device(s), Deployment Setting
- Cybersecurity Themes: Identified Vulnerabilities, Breach Types (e.g., ransomware, DoS), Impact of Breaches
- Older Adult-Specific Insights: Consequences for Aging Populations, Cognitive or Sensory Barriers
- Solutions and Recommendations: Technical Measures (e.g., encryption, access controls), Policy Proposals, Ethical Considerations
- Key Findings: Relevance to the research questions, Implications for future practice or study

Data were manually extracted and organized using Microsoft Excel, which allowed for uniform comparison across studies and enabled cross-tabulation by technology type, region, and vulnerability type. This structured framework ensured transparency in both the selection and synthesis of evidence.

Following data charting, we conducted a *thematic analysis* to extract patterns, relationships, and recurring constructs from the charted data. Using inductive coding techniques, themes emerged organically and were refined iteratively through comparison and discussion among the research team. These emergent themes were then categorized and mapped

directly to the four predefined research questions, ensuring alignment between data and review objectives. In particular, the synthesis enabled us to:

- Classify the types of AI and ML applications used in IoMT systems for older adults (RQ1)
- Identify and categorize security vulnerabilities and regulatory weaknesses (RQ2)
- Analyze tensions between data-sharing needs and privacy expectations in elder care settings (RQ3)
- Extrapolate findings to predict potential privacy challenges for Alzheimer's patients in future IoMT environments (RQ4)

The combined *charting and analysis process* allowed us to move beyond descriptive summaries toward a more nuanced interpretation of the literature. Table 2 presents a summary of selected studies and their alignment with the thematic categories derived through this process.

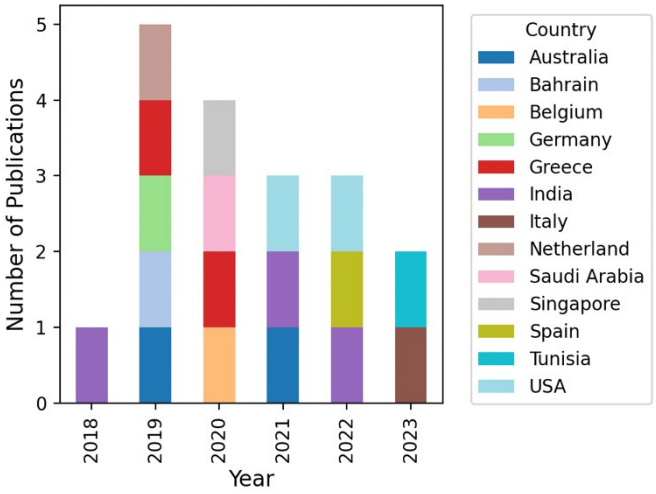

Figure 2. Publications by Year and Country

Table 2. Characteristics and Thematic Summary of Included Studies on IoMT Security and Privacy in Older Adult Healthcare

Ref. & Type of Article	Geography and Year	Population	IoT/IoMT Focus	Identified Vulnerabilities	Impact on Older Adults	Proposed Solutions	Relevance to RQs
[31] Analysis Studies	Global (Theoretical); 2021	Older adults using medical IoT systems	Security-aware data provenance in IoMT	Weak access control, lack of encryption, poor audit mechanisms	Exposure of sensitive health data; reduced autonomy and trust	Multi-factor encryption, fine-grained access controls, audit trails	RQ3
[32] Analysis Studies	USA; 2023	Healthcare providers serving elderly	Medical apps and IoMT data flows	Non-compliance with HIPAA; limited app-level controls	Misuse of personal data; legal and ethical consequences for elder care	Regulatory alignment with HIPAA; stronger app-layer protection mechanisms	RQ2, RQ3
[33] Analysis Studies	Spain; 2022	Elderly patients in clinical environments	Communication protocols in IoMT	Susceptibility to eavesdropping, data manipulation	Risk of medical misinformation and care disruption	Strong protocol-level encryption and real-time verification	RQ2
[34] Experimental Research	India; 2021	Older adults and physically challenged people	Wearable health monitoring IoT	Data interception in transmission; unencrypted device storage	Privacy breaches; unanticipated health interventions	Lightweight encryption, edge computing, local data storage	RQ3
[35] Experimental Research	Saudi Arabia; 2020	Elderly in smart health facilities	Industrial IoT and AI-enabled health sensors	Poor anomaly detection; lack of trust logs; access by unauthorized agents	Physical and psychological harm from incorrect diagnostics	AI-based anomaly detection; blockchain for immutable audit records	RQ3
[36] Experimental Research	Germany; 2019	Older adults with chronic diseases	IoMT for diabetes and cardiovascular monitoring	Limited integration between systems; insecure interfaces	Fragmented care and disease progression	Coordinated care systems; secure API interfaces	RQ1

[37] Experimental Research	Netherlands; 2019	Dementia patients	AI-enhanced exergaming and data streaming via IoMT	No direct focus on vulnerabilities	Cognitive benefit but potential misuse of streamed health data	Ethical AI integration; context-aware data capture	RQ1
[38] Experimental Research	Singapore; 2020	Community-dwelling older adults	IoMT for mental health screening	Weak data handling protocols	Discrimination; anxiety over data exposure	Privacy-conscious mental health AI tools	RQ1
[39] Experimental Research	Italy; 2023	Older adults with cognitive decline	Web-based diagnostic and therapeutic tools	Low digital literacy, phishing, data leakage via app vulnerabilities	Fraud victimization; exploitation via medical interfaces	Education campaigns; secure UI design; minimal data exposure	RQ2
[40] Literature Review	Bahrain; 2019	General elderly healthcare users	Wearables and remote IoT sensors	Insecure communications; lack of firmware updates	Continuous vulnerability to cyberattack	Firmware integrity checking; periodic audits	RQ3
[41] Literature Review	Greece; 2019	Older adults in care homes	IoMT device ecosystem	Broad attack surface; data redundancy risks	Compromised medical records; hindered data sharing	Privacy-by-design architectures; anonymization protocols	RQ2, RQ3
[42] Literature Review	India; 2018	Senior patients	Electronic Health Records + IoMT	Consent fatigue; weak audit trails; poor role separation	Unauthorized data access; degraded trust in digital health	Role-based access, differential privacy, consent management	RQ2, RQ3
[29] Literature Review	Global (Review); 2022	Older adults in smart health systems	General overview of IoMT in geriatric care	Integration complexity; inconsistent privacy protocols	Confusion and resistance to tech use	Standardization and regulatory harmonization	RQ1
[43] Literature Review	USA; 2021	Older adults with dementia	Ambient assisted living IoMT	Lack of monitoring accuracy; data overload	Falls, missed alerts, data misinterpretation	AI-enhanced data filtering; caregiver feedback loops	RQ1
[44] Literature Review	USA; 2022	Elderly with cardiac conditions	Wearable IoMT for anomaly detection	Poor training data; algorithmic bias	False alarms; care plan disruption	Curated dataset training; ethical oversight in AI	RQ1
[45] Literature Review	Belgium; 2020	Older patients on medication regimens	IoMT for medication adherence and disease prediction	Incomplete tracking; privacy leakage via non-secure alerts	Missed doses; embarrassment from alert exposure	Secured notification protocols; ML-driven personalized feedback	RQ1
[46] Literature Review	Australia; 2019	Patients with cognitive impairment	Real-time feedback loops via IoMT	Signal lag; insecure cloud connection	Delay in critical intervention; loss of autonomy	Real-time encryption; adaptive learning systems	RQ1
[47] Survey	Greece; 2020	IoMT developers and healthcare stakeholders	IoMT deployment standardization	Fragmentation across vendors; VPN-based solutions prone to breaches	Inconsistent service quality; exposed networks	Unified frameworks; post-deployment vulnerability testing	RQ2

3. Result

This section presents the key findings of the systematic review, derived from a comprehensive synthesis of 18 selected studies that address the intersection of Internet of Medical Things (IoMT) technologies, cybersecurity, and the healthcare of older adults. The results are organized in alignment with the study's guiding research questions and reflect the thematic analysis conducted during the data charting process. Each subsection corresponds to one of the four research questions, highlighting patterns, vulnerabilities, and proposed solutions as reported across the literature.

3.1 AI and ML techniques for IoMT-enhanced healthcare in older adults (RQ1)

This sub section explores how artificial intelligence (AI) and machine learning (ML) are being integrated with Internet of Medical Things (IoMT) technologies to improve healthcare outcomes for older adults. As IoMT devices increasingly collect diverse health-related data, AI and ML offer powerful tools for interpreting this data, enabling early diagnosis, personalized care, and proactive health management. The following sub-sections highlight key applications and emerging trends, including chronic disease monitoring, fall prevention, and mental health support, as well as the broader shift toward data-driven, preventive care.

3.1.1 Digital Transformation and Data Generation in Healthcare

Healthcare industries are being digitalized to improve the quality of healthcare facilities. IoT companies have brought up different innovative strategies and are developing IoMT devices based on health-related data. IoMT manufacturing companies utilize different types of health-related data to improve the quality of smart home devices and appliances. Different health records such as mobility, biometric measurements, list of medication as well as environmental data are constantly being gathered in these devices [43]. These devices are useful for tracking fitness, monitoring hygiene, and even working as drug dispensers. Wearable IoMT devices usually generate a wealth of information daily. These smart devices operate in real-time or near real-time so that health-related feedback or health updates can be generated. The applications of devices are being updated persistently over a certain period. These IoMT devices are being introduced among people in every age category, especially old adults for the betterment of their health. More people are using more data is being produced [29]. For instance, smart home monitoring systems record and store videos, or personal monitoring devices record health information. However, enormous records of diverse data can cause data deluge which can impact the speed of the process in various devices. Data deluge in older adults' healthcare is shown in Figure 3.

3.1.2 Leveraging AI/ML for Predictive Diagnostics

The expansive datasets generated by IoMT devices serve as valuable inputs for training artificial intelligence (AI) and machine learning (ML) models to enhance diagnostic accuracy. IoMT devices are recording and generating more and more information every day, all over the world. These datasets can be used to train different AI and ML models to level up the accuracy of automatic diagnostics. For example, wearable devices record various levels of the heart rate. Machine learning models can be trained and developed to detect the symptoms of health issues at an early stage before they turn into fatal [44]. The variety of data helps to recognize many complex patterns through machine learning models which was not possible to find the insights through analyzing manually. Therefore, AI systems can primarily suggest personalized treatment plans based on a patient's health history and needs.

3.1.3 Chronic Disease Management with AI and IoMT

In IoMT devices, the application that provides personalized approaches can play a significant role for older adults, especially individuals with chronic diseases. For example, AI-driven approaches can monitor blood sugar levels and address the higher risk associated with chronic diseases like diabetes [36]. By processing data from smartwatches, insulin patches, etc., AI and ML can be used to discover complex patterns that may deliver new insights.

Chronic disease management refers to managing illness such as patient screenings, check-ups, monitoring, coordinating treatment, and often patient education through an integrated care approach. The older population deals with complicated health challenges, and proper treatment and management are necessary. There is potential for a research domain to propose new innovative solutions for better management in this area [36]. Technology like AI and ML hold a significant role here with approaches to help treat various chronic disease conditions like hypertension, chronic obstructive pulmonary disease and arthritis [37]. A remarkable transformation is visible in the healthcare industry with the development of IoMT devices using AI and ML. Many IoMT devices must constantly monitor and collect data on things like physical activity or blood glucose levels [37]. They also generate large amounts of data while monitoring vital signs like heart rate and blood pressure. The scientific community often gathers and processes this data for their research [37]. Through the obtained data, AI and ML approaches can be trained to classify patterns, predict disease exacerbations, and monitor medications and lifestyle trends [45]. IoMT devices can also offer patients real-time feedback for personalized treatment adjustments and proactive health management. As a result, healthcare stakeholders can facilitate this enhanced treatment, which is considered a

significant shift toward preventive care for patients with chronic disease [46].

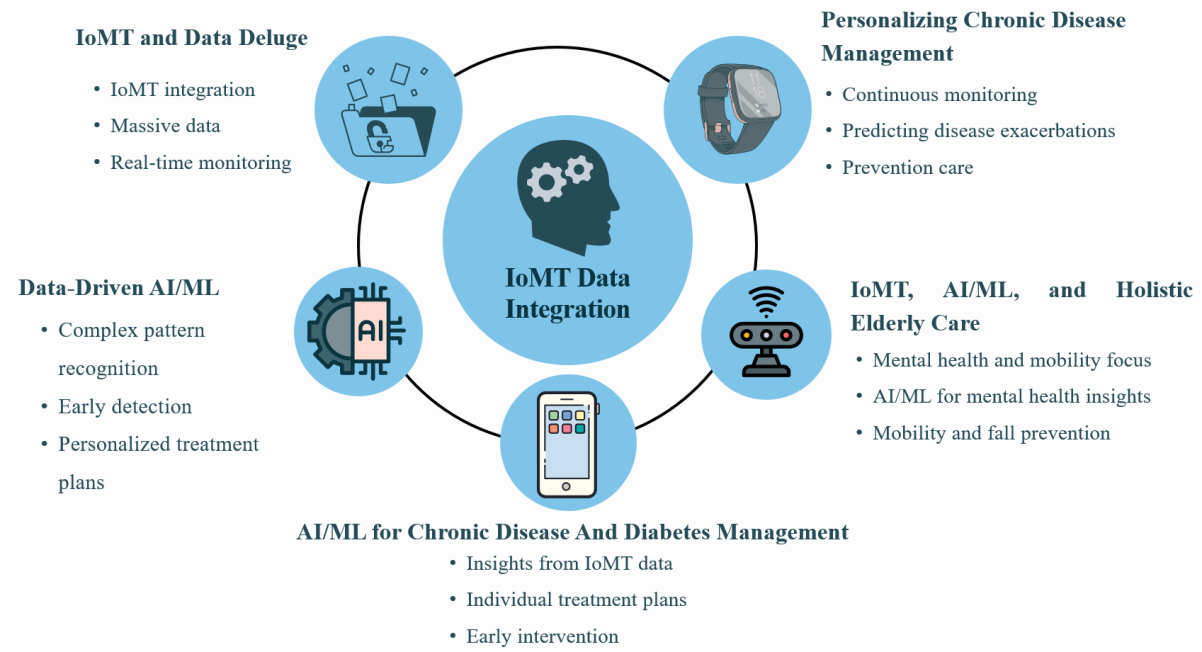

Figure 3. Leveraging AI and ML for Enhanced Medical Care in Older Adults through IoMT Data Integration

3.1.4 Mental Health Monitoring and Fall Prevention

Beyond physical illness, AI and ML applications in IoMT systems are also being explored for mental health and mobility support. The concept of mental health, mobility, and fall prevention is essential in preserving the safety of older adults. Falls are considered a threat to the health of older adults that can cause injuries and reduce their ability to remain independent. AI and ML-driven approaches can be utilized to develop fall prevention systems that continuously assess movement patterns of older adults by analyzing real-time data obtained through cameras and sensors. These kinds of systems can be wearable or non-invasive fitting within living spaces. To help maintain privacy, researchers are developing vibration sensors in place of cameras, that are able to interpret any anomalies or changes in movement identified by these special sensors. The vibration sensor data can then be analyzed to determine potential precursors to falls and take measures for early interventions. Therefore, the healthcare sector can generate valuable data streams by integrating IoMT devices with voice recognition systems and wearable EEG monitors. Utilizing this vast level of data helps AI and ML algorithms to train, analyze, and classify new patterns that enable these systems to provide early warning or alert of cognitive decline of patients. Approaches such as this example allow healthcare stakeholders to take measurements and offer precise therapeutic and medication adjustments, ensuring timely care.

3.2. Addressing IoMT data privacy and security challenges in older adult healthcare (RQ2)

As healthcare systems increasingly adopt Internet of Medical Things (IoMT) technologies, safeguarding the privacy and security of sensitive patient data—particularly for older adults—has become a critical concern. This population is especially vulnerable due to the volume and sensitivity of their medical information and their reliance on digital health tools. Despite advancements in encryption and access controls, frequent breaches and systemic weaknesses underscore the urgent need for comprehensive, user-centered security strategies. This sub-section discusses the major threats to data privacy in IoMT-enabled healthcare, explores recent security incidents, and outlines key approaches to mitigate risks and protect older adult patients.

3.2.1 Increasing Risks to Sensitive Health Data in Aging Populations

In the ever-evolving healthcare landscape, one of the more critical challenges revolves around ensuring data

security, especially concerning the older adult demographic. With the world's population steadily aging, protecting sensitive patient information has become an intricate task that demands utmost precision and diligence. This information, from elaborate medical histories to personal identifiers, requires standard security measures, robust encryption methods, and stringent access controls [41]. The complexity of medical records for older adults showcases the value of their data in the eyes of cybercriminals, making them enticing targets. Integrating advanced encryption algorithms and cutting-edge machine learning models has become necessary to counter this escalating threat. These technologies do not merely protect data; they contribute significantly to creating secure environments within healthcare systems. However, despite these advancements, breaches can still occur, often due to misconfigurations, weak authentication methods, and outdated software. As a result, the personal information of individuals in healthcare databases remains a popular target for cyber threats. This means there is a strong need for vigilance and creative strategies to protect our data.

3.2.2 Common Vulnerabilities and Breach Incidents

The susceptibility of citizens to privacy breaches and data theft in healthcare environments is an issue that requires immediate attention. Human mistakes such as insecure databases and weak passwords pose threats to the security of medical records as illustrated in Figure 4. Furthermore, improperly configured cloud storage and lenient access controls create opportunities for hackers to gain entry, resulting in data breaches that jeopardize the privacy of patients. These incidents highlight the pressing need for special security measures to address the challenges associated with patient data [33]. It is essential to implement protocols that can prevent breaches and uphold the dignity and confidentiality of patients who rely on the healthcare system for their well-being. Ongoing training for staff members and awareness programs can help healthcare professionals remain knowledgeable about security measures that are capable of protecting patient data.

In recent times the healthcare industry has experienced a series of data breaches resulting in legal repercussions. These unfortunate breaches have shed light on the vulnerability of older adult medical information. One case was the 2015 Anthem breach, where hackers accessed millions of records without authorization, causing great concern [42]. Following each breach, healthcare organizations and medical device manufacturers face scrutiny for failing to safeguard sensitive data belonging to older adults. These incidents remind us of the serious responsibility in maintaining data security practices. They highlight legal and financial consequences that healthcare entities encounter when breaches compromise their patient's trust and privacy. Therefore, it has become essential for healthcare organizations to implement security measures that can safeguard the privacy and dignity of their patients. These measures will, in turn, protect the companies themselves from the legal and financial consequences of future potential data breaches.

3.2.3 Technical and Behavioral Attack Vectors

Cyber threats targeting older adult healthcare range from phishing attempts and ransomware to exploitation of outdated IoMT firmware. The specific healthcare requirements of individuals present a range of vulnerabilities covering electronic health records, medical IoT devices, and communication systems dedicated to aging care. Hackers will conduct phishing attempts aimed at older patients and seek out weaknesses in outdated software and medical equipment. Ransomware has become more prominent as well [47]. Once this software is accidentally downloaded onto the victim's system, it blocks access to critical data on that system or the whole system itself. The victim then must pay the attacker to regain access. The perpetrator encrypts the victim's files and locks them out of their system making the data inaccessible. If not adequately protected, IoT devices can serve as entry points for cybercriminals from which healthcare data of individuals passing through those devices is at risk [32]. A comprehensive approach, including periodic security assessments, network segmentation, and regularly scheduled staff training, is essential to protect the healthcare data of older adults and mitigate the risks posed by these malicious attacks.

3.2.4 Digital Literacy and the Human Factor in Security

Older adults are particularly vulnerable due to limited digital literacy, making them susceptible to manipulation and fraud. Their reliance on telehealth platforms, remote monitoring systems, and mobile apps requires intuitive and secure interfaces. Targeted cybersecurity education for older adults, caregivers, and providers is critical to closing this vulnerability gap. To combat these challenges, particularly in the context of older adults, it is crucial to address the unique vulnerabilities they face in the ever-evolving cybersecurity health landscape. Older adults often lack digital literacy, making them susceptible to phishing attacks and other online scams [39]. Moreover, they may rely heavily on healthcare technologies, from telemedicine apps to wearable devices, which, if not properly secured, can serve as entry points for cybercriminals. This heightened risk emphasizes the pressing need for tailored cybersecurity education initiatives designed for older adults. These initiatives should focus on raising awareness about common cyber threats, teaching secure online practices, and offering user-friendly guides on using digital health tools securely. Furthermore, healthcare providers and technology developers must prioritize user-friendly interfaces and robust security features in healthcare applications and devices. Implementing multifactor authentication, encryption, and regular security updates can significantly enhance the defense mechanisms against

data breaches. Collaboration among healthcare organizations, cybersecurity experts, and advocacy groups for adults goes a long way in developing successful cybersecurity guidelines and effective resources. By promoting a culture of learning and adaptability, healthcare professionals and older individuals can stay informed about cybersecurity risks and new recommended strategies.

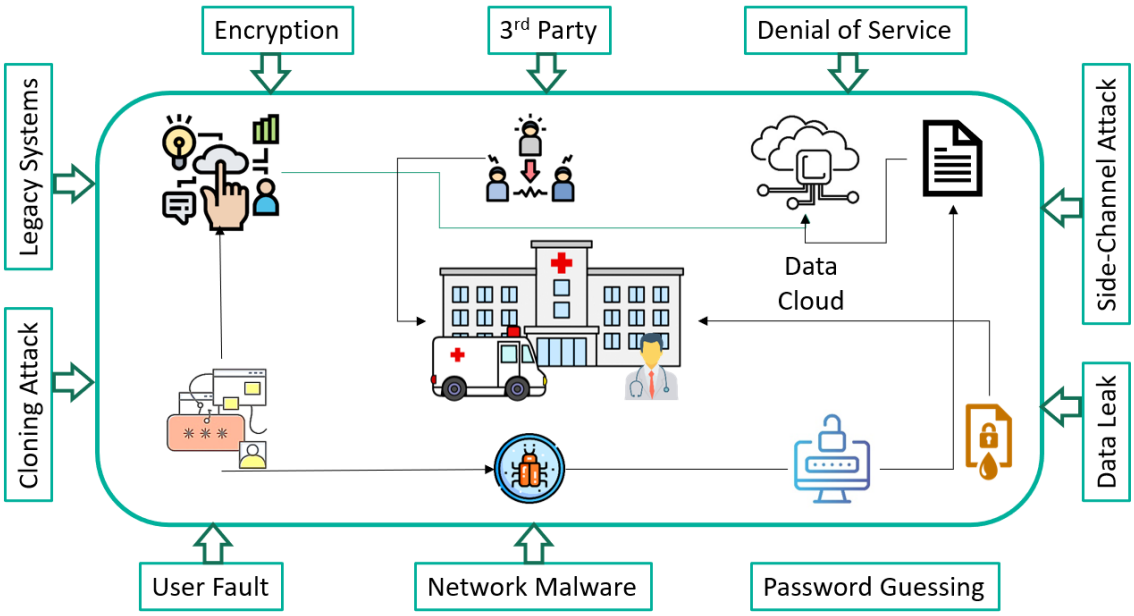

Figure 4. Types of IoMT Vulnerabilities.

3.3. Balancing data security and sharing in older adult healthcare: acceptance and adoption factors (RQ3)

The integration of IoMT devices in older adult healthcare introduces significant opportunities and challenges. While these technologies enable more efficient diagnosis, monitoring, and intervention, they also demand robust data protection mechanisms. Striking a balance between ensuring data privacy and enabling its effective use is critical to both patient safety and healthcare system efficiency. This section examines the key adoption and security concerns, explores emerging solutions, and highlights policy and design strategies that encourage responsible data use without compromising privacy. The discussion is organized into five key subsections.

3.3.1 The Central Dilemma: Utility vs. Security in IoMT Systems

The use of IoMT technologies necessitates constant data exchange for diagnosis, treatment coordination, and monitoring. However, enforcing rigorous security protocols like encryption, access control, and authorization mechanisms may hinder real-time data utility. The challenge lies in enabling effective data sharing without compromising the privacy and independence of older patients. Deploying IoMT devices such as wearables, remote sensors and monitoring systems brings about new cybersecurity issues that require careful consideration in older adult healthcare [40]. There is a constant challenge in finding the proper balance between implementing security measures to protect confidential patient data, and the ability to use the data effectively. The purpose behind IoMTs relies on the ability to gather, analyze, and responsibly disseminate this important health information for accurate diagnosis, treatment coordination, and public health monitoring. Therefore, it's important that security measures do not prevent them from fulfilling their purpose. For example, it's essential to have multifactor encryption, precise access controls, and strict authorization guidelines in place to prevent breaches of personal health data that can jeopardize the privacy, independence, and well-being of patients [31]. Yet, at the same time, healthcare providers require reasonable access to continuously monitor at-risk older adult patients' status via IoMT devices and coordinate urgent care accordingly when issues arise. Healthcare

systems also rely on aggregating and analyzing IoMT data trends for epidemiology and quality improvement. Finding the right balance between watertight security and essential health data sharing is thus critical but highly challenging in the older adult IoMT healthcare context, given the sensitivity of the data involved as seen in Figure 5.

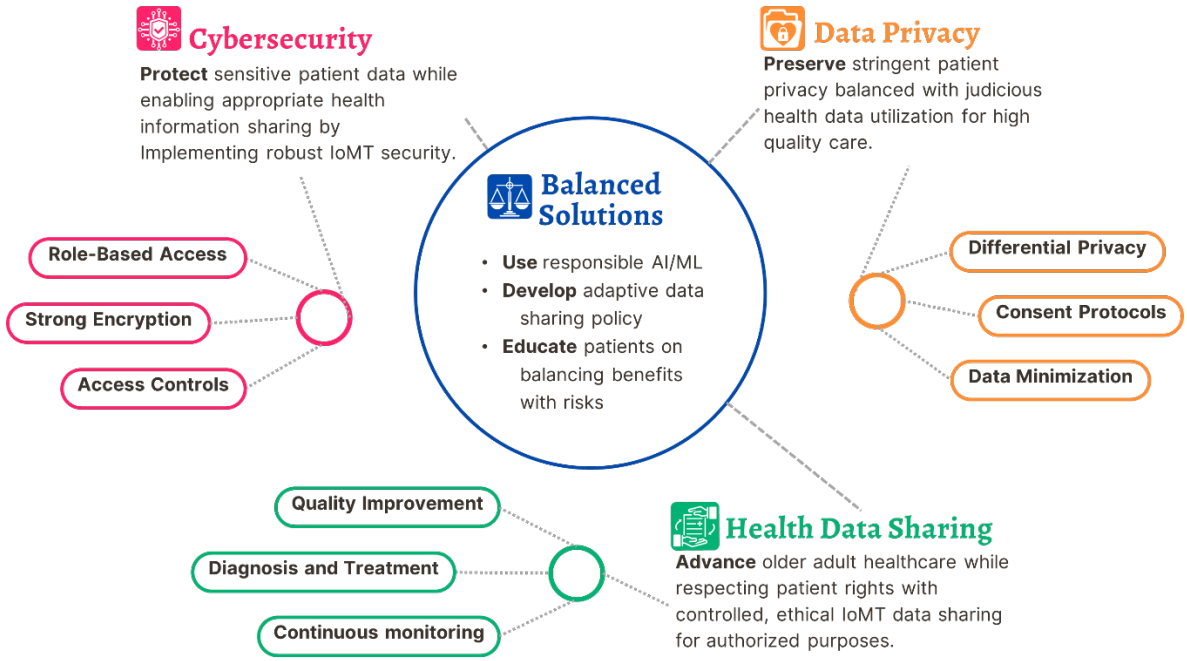

Figure 5. Balancing cybersecurity, data privacy, and health data sharing in older adult healthcare.

3.3.2 Emerging Technological Solutions for Secure Data Use

There are advancements emerging to enhance IoMT security measures that allow for the proper use of health data by authorized individuals and organizations [35]. For example, using access permissions based on roles can ease the sharing of IoMT data with similar parties. Anonymization and data minimization techniques reduce the volume of identifiable data collected and transmitted from IoMT devices. Blockchain-based immutable access logging systems offer tamper-proof auditable records of all data transactions. AI-driven user/entity behavior analytics solutions can identify anomalous or suspicious access attempts to IoMT device data for investigation. When thoughtfully implemented with an emphasis on ethical data usage, striking a reasonable risk balance, and aligning with patient interests, these solutions show promise to enhance IoMT security and privacy while retaining sufficient health data utility for physicians, care coordinators, researchers, and public health authorities to improve older adult healthcare substantially.

3.3.3 The Role of Privacy Regulations and Their Limits

In parallel with cybersecurity, rigorous data privacy protections and policies are equally vital when implementing IoMT monitoring technologies in older adult healthcare environments[41]. IoMT devices can gather remarkably expansive sensitive data from remote patients, including continuous biometrics, location tracking both inside homes and around communities, and extensive behavioral patterns detected by motion sensors and AI algorithms. However, overly stringent privacy restrictions that tightly lock down all IoMT data could inhibit the appropriate availability and analysis of this information that is often needed for timely and effective medical interventions, care coordination, and quality improvement initiatives. Longstanding healthcare privacy regulations like HIPAA generally allow the sharing of IoMT health data for legitimate treatment purposes but still require providers and stewards to implement reasonable administrative, technical, and physical safeguards[32]. In short, securing IoMT technology means finding ways to keep sensitive data safe and usable at the same time. The sheer volume of useful data promises to improve intervention times if it can be processed and observed as it

is collected. Such swift turnarounds would lead to fewer detrimental accidents and increased quality of life for the patients, significantly reducing the time and cost associated with being hospitalized.

3.3.4 Patient-Centered Consent and Control Mechanisms

When using data from IoMT devices, upholding regulations like (HIPAA) or (GDPR) will go a long way to ensuring the data remains protected [42]. Three major steps can help patients by keeping their data safe when in use:

(i) Restrict sensitive data access to specific roles
(ii) Log and monitor when sensitive data is being accessed
(iii) Create user-friendly methods to gain informed consent so patients know when and how their sensitive data is being used

Some data can be collected anonymously and without labeled meta-data so that if it is intercepted, it would not violate any individual's privacy. This method would be highly useful for group data collected en-mass for research purposes. Another possibility is to keep sensitive data in the hands of the patient or their caregivers. Consent to share any sensitive data would be on a case-by-case basis, enhancing transparency. This feeling of control over their own data would enhance the trust between patients and their healthcare providers. It also reduces the frequency with which sensitive data is transmitted between parties, making it less vulnerable to attack. Together, all these protocols work to create a powerful IoMT environment that can keep patients safe and their data private at the same time.

3.3.5 Recommendations for Achieving Ethical and Effective Data Use

Finding a balance between keeping all this sensitive health data safe while being able to use it effectively has been a primary goal in upholding patients' privacy [34]. IoMT devices are able to highly benefit older adult patients when this balance is achieved. According to our research, possible security solutions include using state-of-the-art technologies like AI and blockchain to interpret what data is important to share, help encrypt the data, and track who can access and who is accessing the data. Stop unnecessarily recording and sharing sensitive data and wherever possible, put the data in the control of the patient and their caregiver. Raise awareness by educating all stakeholders on the proper use and protection of the data, and this will help ensure patients are providing informed consent when necessary. Using these new technologies to secure data while following regulation standards for data privacy will be required in the future IoMT landscape. With thoughtful tuning of leading-edge technical controls and adaptive policy levers, IoMT-enabled older adult healthcare can benefit tremendously from data-driven insights while respectfully safeguarding patients' highly sensitive personal health information.

3.4. Prognosticating future security and privacy challenges in Alzheimer's patient care (RQ4)

In the evolving older adult healthcare landscape, the intersection of Alzheimer's care and the security and privacy of their health data emerges as a critical area of concern. As we delve into Research Question 4 (RQ4), our focus shifts to the prognostication of future challenges in safeguarding the privacy and security of healthcare information specific to Alzheimer's patients. This exploration is multifaceted, reflecting the various challenges of Alzheimer's disease and the detrimental ways it interacts with healthcare technologies and practices. The first segment of our inquiry explores the existing technological ecosystem supporting Alzheimer's care. We examine how technologies such as smart home devices and digital health platforms revolutionize care and treatment regimens, contributing to improved patient outcomes. This discussion lays the groundwork for understanding the technological context in which privacy and security issues arise. Subsequently, we address data vulnerability specific to Alzheimer's healthcare. Alzheimer's patients are especially vulnerable to exploitation due to their impaired condition. This makes it even more important to understand these specific vulnerabilities as they pertain to breaches in security and the loss of sensitive information. Further, we delve into the key attack vectors that pose significant threats to these vulnerabilities. Analyzing these exploitable areas gives us insight into the cybersecurity threats prevalent in Alzheimer's patient care. This analysis is crucial for developing strategies to counteract these vulnerabilities. Finally, we conclude by discussing the security and privacy implications Alzheimer's patients face. This section synthesizes the insights gained from the previous parts, highlighting the real-world impacts of security and privacy breaches on Alzheimer's patients. In detailing these implications, we can better define the need for robust, patient-centric solutions that address the unique challenges faced by this vulnerable group as shown in Fig. 6. Through this prognostication, we paint a picture of what the future holds for Alzheimer's patients. This is a brainstorming for insights into the unique solutions required to meet the specific demands of this vulnerable population.

3.4.1. Technology Enabling Alzheimer's Home Care

Modern smart systems—from voice-activated assistants to motion sensors and health monitoring wearables—are reshaping Alzheimer's care. These technologies offer autonomy, enhance safety, and extend the independence of patients by providing real-time alerts, reminders, and remote caregiver support. As a whole, modern technology has produced numerous advantages that can benefit the

Alzheimer population and their care providers. IoMT technology specifically creates improved care environments that are advantageous in caring for Alzheimer's patients. This is because Alzheimer's patients need more care than others, and these technologies can substitute for a large percentage of human care, providing autonomy and safety for longer periods of time, as shown in Figure 6. Smart devices like lights, doorbell cameras and thermostats connected to voice-activated assistants can make life easier for the patient and allow caregivers to interactively support them remotely. Older adults, especially those with memory issues tend to rely on routines to feel safe and secure. Reminders and alarms can speak to them, reminding them to take their medication or do their physical therapy exercises each day. Also, sensors like security cameras and heart monitors can actively track Alzheimer's patients day and night, immediately alerting caregivers or medical personnel when an out-of-the-ordinary situation occurs. Many severe older adult hospitalizations occur because of a fall that wasn't discovered until hours later happens. IoMT technology can prevent that. Therefore, IoMT can help Alzheimer's patients live safer normal lives for longer rather than being restricted to a hospital bed 24/7.

Another way modern technology can help Alzheimer's patients is in the form of digital communications. Doctors and patients can engage in many of their communications through an online portal on a computer or even through the television via telemedical assistance. Alzheimer's patients typically shouldn't be driving to doctor's appointments, but they can attend an online appointment from the comfort of their living room even without a caregiver's support. These user-friendly applications on a computer tablet can also enable Alzheimer's patients and their caregivers to track medications, view lab results, and even engage in cognition games specifically designed to manage their dementia symptoms. All these modern technologies can have a major positive impact on the success of Alzheimer patient care.

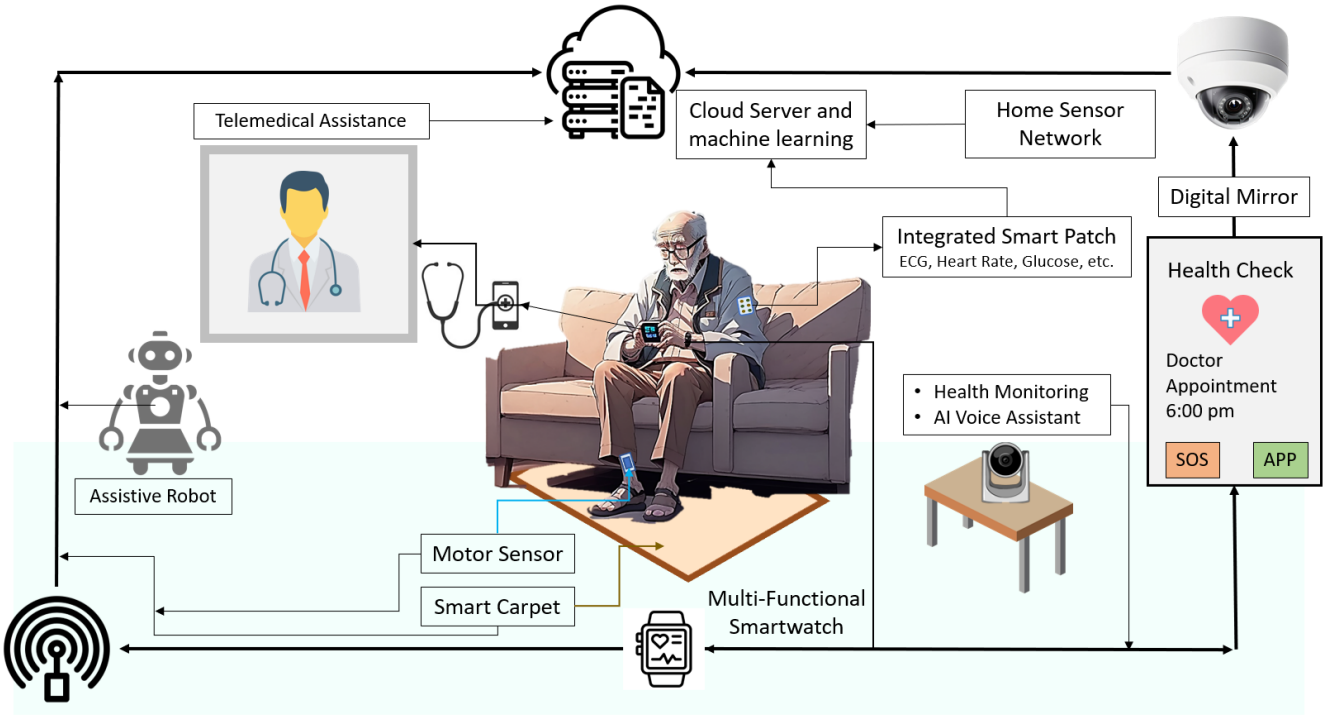

Figure 6. The future of Alzheimer's healthcare in the home setting.

3.4.2. Unique Data Vulnerabilities in Alzheimer's Healthcare

Due to cognitive decline, Alzheimer's patients face increased risk of identity theft, data misuse, and unauthorized data sharing. Their dependency on caregivers and digital systems further amplifies these risks, making sensitive information more widely circulated and vulnerable. There are many vulnerabilities that must be addressed for Alzheimer's patients. Cyberattacks target Alzheimer's patients because mental decline leaves them more vulnerable to prescription, financial, and identity theft. They can be an easy target for phishing attacks and online scams. This is why their sensitive information, like birthdates and social security numbers, must be kept secure. Because these patients need so much extra support,

their information is shared and distributed more than other groups. Medication and consent forms are shared with more people since these patients can't often make sound decisions for themselves. Medical histories and existing conditions can also be detrimental to patients if stolen, reducing their quality of life and taking away their right to privacy. Monitoring and sensory IoMT devices can also be hacked to track and study location and behavior data. Research data can also be a valuable target for attackers, as they collect data on large quantities of patients at a time to study and share within their respective industries in the name of progress. This can be alleviated with proper training and hiding the data behind a firewall and encrypted VPN. All these risks can cause great harm to the lives of Alzheimer's patients because they are open to numerous types of attacks.

3.4.3. Emerging Threats and Attack Vectors

From phishing to ransomware, Alzheimer's patients, caregivers, and researchers are all targets of cyberattacks. Untrained caregivers or outdated infrastructure can enable breaches that compromise personal health data, research repositories, and prescription records. With the vast amounts and types of data associated with digital healthcare, there are several ways attackers will try to gain access to it. Phishing attempts can be directed toward patients, nonprofessional caregivers, and even health providers. Once the necessary credentials have been gained through these attempts, attackers have digital access to all the sensitive data. If family caregivers and health providers are not trained to recognize these phishing attempts, the stolen credentials and data may go unnoticed and unreported for a long time. Another area of attack is the research institutions gathering large swaths of data from Alzheimer's patients to study the disease. Attackers want this sensitive data for a number of schemes. They could steal large amounts of data to blackmail the large corporation they stole it from. They could use personal identification data to open or access financial accounts in the victims' names. Prescription information can be used to illegally acquire drugs from pharmacies. All these attacks adversely affect patient lives and diminish the image of trust in the companies and institutions involved. With so many angles of attack, the security solutions must be quite complex. Each type of attack must be mitigated. Each potential target, from patient to caregiver to health provider, needs proper training to recognize attacks, and the proper responses to take when an attack is discovered. With the unique mental state of Alzheimer's patients, these solutions require even more detailed protocols for support from the greater health community around them.

3.4.4. Real-World Consequences of Data Breaches

Breaches not only expose patients to fraud but can disrupt care continuity and erode trust in healthcare providers. Legal and recovery processes can be especially challenging for individuals with cognitive impairments, compounding the long-term effects of a data loss. Given their proclivity to require increased support from IoMT devices in their daily lives, Alzheimer's patients are surrounded by an abundance of security threats to their privacy as more and more data is collected by these devices to assist them. Their mental state also leaves them more susceptible to social engineering schemes like phishing fraud, another big risk to the security of their sensitive information. Caregivers focused on the physical and mental care of the patient can easily forget to follow stringent protocols safeguarding data from unseen, unknown adversaries. All this paints a picture showing that Alzheimer's patients can be a primary target for identity theft and data loss. Even more troubling is that their diminished cognition also makes them more vulnerable after the loss has occurred. In the recovery process, these patients have a much more difficult time dealing with the legal red tape of trying to prove who they are when they may not always know themselves. This is why one of the most important steps in Alzheimer's private data security is developing a strong and informed support network among family, caregivers, and healthcare providers. The challenges of dealing with day-to-day activities can make it tough to spot identity theft early on, and it would certainly be difficult to go through the process of recovery without the right kind of specialized help. Continuously tracking patients for safety reasons using location services could backfire if there are any lapses in controlling access to databases that hold their travel history. If this data falls into the wrong hands it could be used for social engineering attacks designed to exploit a patient's communication style, their personal memories, and relationships. Managing Alzheimer's currently requires human-focused support to navigate the world of data security. Relying solely on policy is not enough to address all the vulnerabilities associated with dementia across areas like healthcare, finance, self-perception, and community connection. Educating patient advocates, providing tools to take charge, and empowering them to maintain their sense of self as cognitive changes occur. Therefore, creating caring communities centered around each patient is crucial in providing a defense against the damaging effects confronted by this vulnerable group.

7. Conclusion

This systematic literature review has revealed the relationships among progress in artificial intelligence, serious risks to privacy, and the careful equilibrium between data protection and enhancing healthcare for older adults using IoMT technologies. Our thorough examination sheds light on key findings, addresses research gaps, and introduces new viewpoints to the field. Initially, we outlined how applied AI and machine learning methods hold promise in the diagnosis, care, and treatments for older adult patients using information gathered from emerging IoMT technology. However, through our

research, we discovered the need to address the increased privacy and security risks faced by the vulnerable group of older adults with Alzheimer's. By identifying vulnerabilities in the IoMT system and suggesting. regulatory measures to address them, this study provides effective ways to safeguard the privacy of older adults. Additionally, our examination of how to balance these security measures with the need for sharing health data highlights the importance of building trust among users of aging-related solutions. We believe that focusing on user design and educational initiatives can help overcome the obstacles to acceptance by enhancing accessibility and eliminating health literacy concerns. Considering the vulnerabilities faced by individuals dealing with Alzheimer's disease, our analysis of the challenges in data security and privacy that they might encounter aims to encourage compassionate policymaking. By looking at issues from a problem-solving perspective, we aim to inspire approaches driven by fairness and empathy. Ultimately, this literature review has forged an interdisciplinary framework integrating the technical dimensions of medical cybersecurity with user-focused perspectives on practical adoption. Through highlighting critical gaps ripe for future exploration by researchers and healthcare practitioners alike, we endeavored to pave inroads to access and agency for aging populations as the technological landscapes surrounding health and medicine evolve. Our insights are meant to spur progress rooted in empathy, wisdom, and an improved shared vision for humanity.

Despite the promising potential of IoT technologies in enhancing care for individuals with Alzheimer's disease and related dementias, several key limitations must be acknowledged. Methodological constraints, such as small sample sizes, limited longitudinal data, and variability in device accuracy, restrict the generalizability and robustness of findings. Additionally, challenges in ensuring secure interoperability across diverse IoT platforms introduce risks that are difficult to quantify within current research frameworks. Contextual factors—including disparities in digital literacy among older adults, socio-economic barriers, and ethical complexities surrounding informed consent—further complicate the deployment and acceptance of these technologies.

Theoretically, these limitations highlight the need for more comprehensive models that integrate technological, cognitive, and ethical dimensions of IoT use in dementia care. From a policy perspective, there is an urgent requirement for clear regulatory frameworks that address data privacy, security standards, and equitable access to technological solutions for vulnerable populations. Practically, healthcare providers and technology developers must prioritize user-centered design, tailored education, and robust security protocols to mitigate risks and enhance usability. Addressing these multifaceted challenges is critical to realizing the full benefits of IoT innovations in improving quality of life for patients and caregivers alike.

References

[1] Dementia n.d. https://www.who.int/news-room/fact-sheets/detail/dementia (accessed June 26, 2025).

[2] Rhea EM, Leclerc M, Yassine HN, Capuano AW, Tong H, Petyuk VA, et al. State of the Science on Brain Insulin Resistance and Cognitive Decline Due to Alzheimer's Disease. Aging Dis 2024;15:1688. https://doi.org/10.14336/AD.2023.0814.

[3] Botto R, Callai N, Cermelli A, Causarano L, Rainero I. Anxiety and depression in Alzheimer's disease: a systematic review of pathogenetic mechanisms and relation to cognitive decline. Neurological Sciences 2022;43:4107–24. https://doi.org/10.1007/S10072-022-06068-X/METRICS.

[4] Shen LX, Yang YX, Kuo K, Li HQ, Chen SD, Chen KL, et al. Social Isolation, Social Interaction, and Alzheimer's Disease: A Mendelian Randomization Study. Journal of Alzheimer's Disease 2021;80:665–72. https://doi.org/10.3233/JAD-201442/SUPPL_FILE/SJ-PDF-1-ALZ-10.3233_JAD-201442.PDF.

[5] Ienca M, Fabrice J, Elger B, Caon M, Pappagallo AS, Kressig RW, et al. Intelligent Assistive Technology for Alzheimer's Disease and Other Dementias: A Systematic Review. Journal of Alzheimer's Disease 2017;56:1301–40. https://doi.org/10.3233/JAD-161037;SUBPAGE:STRING:ABSTRACT;JOURNAL:JOURNAL:ALZA;WEBSITE:WEBSITE:SAGE;WGROUP:STRING:PUBLICATION.

[6] Syed L, Jabeen S, S. M, Alsaeedi A. Smart healthcare framework for ambient assisted living using IoMT and big data analytics techniques. Future Generation Computer Systems 2019;101:136–51. https://doi.org/10.1016/J.FUTURE.2019.06.004.

[7] Khan MF, Ghazal TM, Said RA, Fatima A, Abbas S, Khan MA, et al. An IoMT-Enabled Smart Healthcare Model to Monitor Elderly People Using Machine Learning Technique. Comput Intell Neurosci 2021;2021:2487759. https://doi.org/10.1155/2021/2487759.

[8] Awotunde JB, Ogundokun RO, Adeniyi AE, Abiodun MK, Ayo FE, Ajamu GJ, et al. Cloud-IoMT-based wearable body sensors network for monitoring elderly patients during the COVID-19 pandemic. Biomedical Engineering Applications for People with Disabilities and the Elderly in the COVID-19 Pandemic and Beyond 2022:33–48. https://doi.org/10.1016/B978-0-323-85174-9.00028-5.

[9] Jones D, Ghasemi S, Gračanin D, Azab M. Privacy, Safety, and Security in Extended Reality: User Experience Challenges for Neurodiverse Users. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2023;14045 LNCS:511–28. https://doi.org/10.1007/978-3-031-35822-7_33.

[10] Berridge C, Demiris G, Kaye J. Domain Experts on Dementia-Care Technologies: Mitigating Risk in Design and Implementation. Sci Eng Ethics 2021;27:1–24. https://doi.org/10.1007/S11948-021-00286-W/TABLES/5.

[11] Mishra PK, Iaboni A, Ye B, Newman K, Mihailidis A, Khan SS. Privacy-protecting behaviours of risk detection in people with dementia using videos. Biomed Eng Online 2023;22:1–17. https://doi.org/10.1186/S12938-023-01065-3/FIGURES/5.

[12] Rosenfeld L, Torous J, Vahia I V. Data Security and Privacy in Apps for Dementia: An Analysis of Existing Privacy Policies. The American Journal of Geriatric Psychiatry 2017;25:873–7. https://doi.org/10.1016/J.JAGP.2017.04.009.

[13] Gupta S, Kapoor M, Debnath SK. Cybersecurity Risks and Threats in Healthcare. Artificial Intelligence-Enabled Security for Healthcare Systems 2025:39–64. https://doi.org/10.1007/978-3-031-82810-2_3.

[14] Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: A systematic review. Technology and Health Care 2016;24:1–9. https://doi.org/10.3233/THC-151102.

[15] Khatun MA, Memon SF, Eising C, Dhirani LL. Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation. IEEE Access 2023;11:145869–96. https://doi.org/10.1109/ACCESS.2023.3346320.

[16] Madanian S, Chinbat T, Subasinghage M, Airehrour D, Hassandoust F, Yongchareon S. Health IoT Threats: Survey of Risks and Vulnerabilities. Future Internet 2024, Vol 16, Page 389 2024;16:389. https://doi.org/10.3390/FI16110389.

[17] Roobini S, Kavitha M, Sujaritha M, Rajesh Kumar D. Cyber-Security Threats to IoMT-Enabled Healthcare Systems. Cognitive Computing for Internet of Medical Things 2022:105–30. https://doi.org/10.1201/9781003256243-6.

[18] Chakraborty N, Iqbal S, Zulkernine M. Risk Assessment in Smart Aging Care Systems: An Elderly-Centered Perspective. Proceedings - 2023 IEEE International Conference on Digital Health, ICDH 2023 2023:1–12. https://doi.org/10.1109/ICDH60066.2023.00012.

[19] Shaik MA, Anik FI, Hasan MM, Chakravarty S, Ramos MD, Rahman MA, et al. Advancing Remote Monitoring for Patients With Alzheimer Disease and Related Dementias: Systematic Review. JMIR Aging 2025;8:e69175. https://doi.org/10.2196/69175.

[20] Sun F, Jiang L, Chen XS, Feng Y. Interactive AI Technology for Dementia Caregivers: Needs and Implementation Evidence. J Technol Hum Serv 2025. https://doi.org/10.1080/15228835.2025.2460156;JOURNAL:JOURNAL:WZCH20;CSUBTYPE:STRING:SPECIAL;PAGE:STRING:ARTICLE/CHAPTER.

[21] Arthanat S, Wilcox J, LaRoche D. Smart home automation technology to support caring of individuals with Alzheimer's disease and related dementia: an early intervention framework. Disabil Rehabil Assist Technol 2024;19:779–89. https://doi.org/10.1080/17483107.2022.2125088;PAGE:STRING:ARTICLE/CHAPTER.

[22] Addae S, Kim J, Smith A, Rajana P, Kang M. Smart Solutions for Detecting, Predicting, Monitoring, and Managing Dementia in the Elderly: A Survey. IEEE Access 2024;12:100026–56. https://doi.org/10.1109/ACCESS.2024.3421966.

[23] Bajpayi P, Sharma S, Gaur MS. AI Driven IoT Healthcare Devices Security Vulnerability Management. 2024 2nd International Conference on Disruptive Technologies, ICDT 2024 2024:366–73. https://doi.org/10.1109/ICDT61202.2024.10488939.

[24] Mejía-Granda CM, Fernández-Alemán JL, Carrillo-de-Gea JM, García-Berná JA. Security vulnerabilities in healthcare: an analysis of medical devices and software. Med Biol Eng Comput 2024;62:257–73. https://doi.org/10.1007/S11517-023-02912-0/TABLES/9.

[25] Tsantikidou K, Sklavos N. Vulnerabilities of Internet of Things, for Healthcare Devices and Applications. Proceedings - 2021 8th NAFOSTED Conference on Information and Computer Science, NICS 2021 2021:498–503. https://doi.org/10.1109/NICS54270.2021.9701497.

[26] Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal 2021;22:177–83. https://doi.org/10.1016/J.EIJ.2020.07.003.

[27] Ilori O, Nwosu NT, Nwapali H, Naiho N. Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. Https://WjarrCo.in/Sites/Default/Files/WJARR-2024-1727Pdf 2024;22:213–24. https://doi.org/10.30574/WJARR.2024.22.3.1727.

[28] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. The BMJ 2021;372. https://doi.org/10.1136/BMJ.N71.

[29] Dwivedi R, Mehrotra D, Chandra S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. J Oral Biol Craniofac Res 2022;12:302–18. https://doi.org/https://doi.org/10.1016/j.jobcr.2021.11.010.

[30] Litmaps | Your Literature Review Assistant n.d. https://www.litmaps.com/ (accessed June 26, 2025).

[31] Jaigirdar FT, Rudolph C, Bain C. Risk and Compliance in IoT- Health Data Propagation: A Security-Aware Provenance based Approach. Proceedings - 2021 IEEE International Conference on Digital Health, ICDH 2021 2021:27–37. https://doi.org/10.1109/ICDH52753.2021.00015.

[32] Chatzisofroniou G, Markellos C, Kotzanikolaou P. Assessing the Security Risks of Medical Mobile Applications. Proc IEEE Symp Comput Commun 2023;2023-July. https://doi.org/10.1109/ISCC58397.2023.10217984.

[33] Martinez CJ, Galmes S. Analysis of the primary attacks on IoMT Internet of Medical Things communications protocols. 2022 IEEE World AI IoT Congress (AIIoT) 2022:708–14. https://doi.org/10.1109/AIIOT54504.2022.9817252.

[34] Soundari D V., Kavya R, Monika P, Pooja S. IOT Based Surveillance and Health Monitoring System for Elderly and Physically Challenged People. Proceedings of the 6th International Conference on Communication and Electronics Systems, ICCES 2021 2021:702–6. https://doi.org/10.1109/ICCES51350.2021.9489185.

[35] Hassan MM, Gumaei A, Huda S, Almogren A. Increasing the Trustworthiness in the Industrial IoT Networks through a Reliable Cyberattack Detection Model. IEEE Trans Industr Inform 2020;16:6154–62. https://doi.org/10.1109/TII.2020.2970074.

[36] Frank F, Bjerregaard F, Bengel J, Bitzer EM, Heimbach B, Kaier K, et al. Local, collaborative, stepped and personalised care management for older people with chronic diseases (LoChro): study protocol of a

randomised comparative effectiveness trial. BMC Geriatr 2019;19:64. https://doi.org/10.1186/s12877-019-1088-0.

[37] Karssemeijer EGA, Aaronson JA, Bossers WJR, Donders R, Olde Rikkert MGM, Kessels RPC. The quest for synergy between physical exercise and cognitive stimulation via exergaming in people with dementia: a randomized controlled trial. Alzheimers Res Ther 2019;11:3. https://doi.org/10.1186/s13195-018-0454-z.

[38] Lee RZY, Yu J, Rawtaer I, Allen PF, Bao Z, Feng L, et al. CHI study: protocol for an observational cohort study on ageing and mental health in community-dwelling older adults. BMJ Open 2020;10:e035003. https://doi.org/10.1136/bmjopen-2019-035003.

[39] Bertini F, Beltrami D, Barakati P, Calza L, Ghidoni E, Montesi D. A Web-Based Application for Screening Alzheimer's Disease in the Preclinical Phase. Proc IEEE Symp Comput Commun 2023;2023-July. https://doi.org/10.1109/ISCC58397.2023.10218229.

[40] Ali HY, El-Medany W. IoT security: A review of cybersecurity architecture and layers. 2nd Smart Cities Symposium (SCS 2019), 2019, p. 1–7. https://doi.org/10.1049/cp.2019.0191.

[41] Hatzivasilis G, Soultatos O, Ioannidis S, Verikoukis C, Demetriou G, Tsatsoulis C. Review of security and privacy for the internet of medical things (IoMT): Resolving the protection concerns for the novel circular economy bioinformatics. Proceedings - 15th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2019 2019:457–64. https://doi.org/10.1109/DCOSS.2019.00091.

[42] Kaur A, Isha, Rai G, Malik A. Authentication and Context Awareness Access Control in Internet of Things: A Review. Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data Science and Engineering, Confluence 2018 2018:630–5. https://doi.org/10.1109/CONFLUENCE.2018.8443067.

[43] Gettel CJ, Chen K, Goldberg EM. Dementia Care, Fall Detection, and Ambient-Assisted Living Technologies Help Older Adults Age in Place: A Scoping Review. Journal of Applied Gerontology 2021;40:1893–902. https://doi.org/10.1177/07334648211005868.

[44] Sunny JS, Patro CPK, Karnani K, Pingle SC, Lin F, Anekoji M, et al. Anomaly Detection Framework for Wearables Data: A Perspective Review on Data Concepts, Data Analysis Algorithms and Prospects. Sensors 2022;22:756. https://doi.org/10.3390/s22030756.

[45] Capiau A, Foubert K, Van der Linden L, Walgraeve K, Hias J, Spinewine A, et al. Medication Counselling in Older Patients Prior to Hospital Discharge: A Systematic Review. Drugs Aging 2020;37:635–55. https://doi.org/10.1007/s40266-020-00780-z.

[46] Lovell J, Pham T, Noaman SQ, Davis M-C, Johnson M, Ibrahim JE. Self-management of heart failure in dementia and cognitive impairment: a systematic review. BMC Cardiovasc Disord 2019;19:99. https://doi.org/10.1186/s12872-019-1077-4.

[47] Malamas V, Chantzis F, Dasaklis TK, Stergiopoulos G, Kotzanikolaou P, Douligeris C. Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal. IEEE Access 2021;9:40049–75. https://doi.org/10.1109/ACCESS.2021.3064682.