South African Journal of Business Management
ISSN: (Online) 2078-5976, (Print) 2078-5585

IoT medical device risks: Data security, privacy, confidentiality and compliance with *HIPAA* and COBIT 2019

Authors:
Na-ella Khan[1]
Riaan J. Rudman[1]

Affiliations:
[1]School of Accountancy, Faculty of Economic Management Sciences, Stellenbosch University, Cape Town, South Africa

Corresponding author:
Na-ella Khan,
nvkhan@sun.ac.za

Dates:
Received: 15 July 2024
Accepted: 06 Dec. 2024
Published: 19 Feb. 2025

How to cite this article:
Khan, N., & Rudman, R.J. (2025). IoT medical device risks: Data security, privacy, confidentiality and compliance with *HIPAA* and COBIT 2019. *South African Journal of Business Management, 56*(1), a4796. https://doi.org/10.4102/sajbm.v56i1.4796

Purpose: This study aimed to develop a comprehensive framework to enable the identification of risks pertaining to data security, privacy and confidentiality when using medical Internet of Things (IoT) devices.

Design/methodology/approach: A qualitative, non-empirical study was undertaken to identify data-related risks when using medical IoT devices using a systematic literature review and two governance frameworks.

Findings/results: Within the medical field, risks of using IoT are concentrated around data security, privacy and confidentiality throughout the data lifecycle prevalent within each layer of the IoT architecture. A comprehensive framework was developed to identify these risks at each layer within the architecture in order to facilitate sound information technology (IT) and data governance.

Practical implications: This research documents evidence of the risks posed by IoT devices within the medical field particularly pertaining to IoT data. It provides those charged with governance with a tool to identify all significant risks in this field that is compliant with *Health Insurance Portability and Accountability Act* and Control Objectives for Information and related Technology 2019.

Originality/value: This research provides a comprehensive framework that can be used by those in charge of governance including IT specialist for risk identification during implementation for sound IT and data governance of medical IoT devices using recognised benchmarks. The use of the benchmarks ensures that all significant risks are identified, compared to previous research that identified risks in an *ad hoc* manner.

Keywords: IoT; data governance; health-care; HIPAA; COBIT 2019.

Introduction

The healthcare profession can be seen as an essential service to maintain the health of a nation encompassing specialities such as oncology, paediatrics and cardiology. Historically healthcare was hospital bound because of the need for a physical examination – making patients' care more hospital focussed and costly (Pradhan et al., 2021). The rising cost of care and resource limitations within the medical industry led to the embracement of technological advancements, the most notable of which is the use of Internet of Things (IoT) devices. The IoT devices in healthcare enable real-time data collection, analysis and sharing of data with other devices and the cloud aiding in remote patient monitoring and emergency response services (Jha et al., 2022; Karunarathne et al., 2021). These devices transmit data via wireless networks such as Wi-Fi, LoRa and Bluetooth within a hospital network facilitating data integration to provide better treatment (Morar et al., 2021). Internet of Things creates new opportunities within healthcare by integrating relevant diverse data to improve health service quality (Kelly et al., 2020). Information technology (IT) specialists and those in charge of governance may be eager to adopt IoT into their operations because of its proposed benefits in respect of, for example, cost reduction and personalised medication management (Karunarathne et al., 2021). Furthermore, the interconnected nature of IoT also creates opportunities for further analysis of integrated data to gain insights into better decision-making within any industry (Middleton et al., 2013).

Note: The manuscript is a contribution to the themed collection titled 'Corporate Governance and Sustainable Business Practices in the Fourth Industrial Revolution', under the expert guidance of guest editors Prof. Nicolene Wesson and Dr. George Frederick Nel.

Healthcare organisations can generate value by using integrated medical data; therefore data is an asset that needs to be managed and protected (Atlam et al., 2021). However, the use of IoT leads to mass data generation that because of its sensitive nature needs to be safeguarded (Institute of Directors Southern Africa [IODSA], 2016). Furthermore, the interconnected nature of IoT poses risks to patient data security, privacy and confidentiality, subjected to regulatory requirements outlined in the *Health Insurance Portability and Accountability Act (HIPAA) of 1996* (United States, 1996). *Health Insurance Portability and Accountability Act* represents a healthcare legislation drafted by the United States (US) that sets global standards for regulation with respect to patient data including personal data throughout its life cycle. When implementing IoT, the healthcare industry must be prepared by gaining knowledge about the impact that IoT devices will have on business operations and about the ways to identify risks arising from the use of these devices.

According to IODSA (2016), corporate governance should be a mindful act of compliance that considers an organisation's unique circumstances. In a hospital environment, the use of IoT and the sensitive nature of patient data transmitted is unique and needs to be governed with this in mind. As corporate governance includes IT governance and data governance as core components (Abraham et al., 2019b; Pearce, 2017; Smallwood, 2020), these components need to be considered in order to address the risks associated with IoT in this field to ensure compliance with corporate governance principles. Furthermore, many studies may make implicit references to corporate governance but few address how corporate governance principles should be applied as is true for many industries (Myeza et al., 2023).

Within an IoT environment, the risks may be pervasive as IoT infrastructure is permeating in nature. Adequate mitigation of risks is required to meet corporate governance requirements, which are best addressed through the use of a comprehensive framework such as Control Objectives for Information and Related Technology (COBIT) 2019 that addresses risk mitigation through corporate governance principles, IT governance principles and data governance principles (Information Systems Audit and Control Association, 2019). Governance over IoT devices in the medical field will contribute to responsible use thereof in a sustainable manner that will protect the patient and contribute to better healthcare resulting in enhanced management of these devices in a hospital environment. Therefore, those in charge of governance including IT specialists must consider the risks associated with IoT and IoT data in order to protect patient data when using IoT to ensure corporate governance and contribute towards worlds sustainability and enhanced business management.

Methodology

Research objectives

The introduction of IoT has expanded healthcare systems beyond the hospital, integrating patient data from homes and communities into a wider platform extending across the healthcare domain (Li & Carayon, 2021). The interconnected nature of IoT allows for data sharing across different stakeholder levels, for example patients, doctors and clinicians, shifting the focus onto the patient (Li & Carayon, 2021). However, this accessibility raises concerns regarding security breaches and data leaks hampering patient's data privacy and security (Li & Carayon, 2021). Despite embracing IoT, the industry often lacks awareness regarding associated risks and lacks the skills to identify them. This research aimed to *identify data security, privacy and confidentiality risks associated with IoT in the medical field in order to create a comprehensive framework to identify these risks*, which can be utilised by those in charge of governance (including IT specialists and auditors) to ensure that sound corporate governance practices are established while achieving enhanced business management and furthering sustainability efforts. The study focussed on wearable and implantable IoT devices and outlined the IoT data lifecycle including its transmission over networks using Internet protocols rather than delving into the technical design and programming of IoT and its enabling technologies.

Research methodology

A positivism philosophy with the purpose of gaining an understanding and obtaining theoretical insights into the nature of IoT and IoT data within the medical field in order to produce a comprehensive framework for identifying risks related to the use of IoT devices and IoT data in the medical field was used coupled with a deductive reasoning approach to gain specific insights from existing literature and theories within this field of study. A qualitative, non-empirical study was conducted to gain an understanding of the industry and technology that provided a foundation for the identification of appropriate frameworks that were used in identifying the risks associated with IoT and its impact on IoT data, commencing with a systematic review of relevant literature on the subject matter from 2002 to 2023 including relevant journal articles from accredited local and international journals, white papers, theses, electronic sources and books to obtain an understanding of the industry, underlying technology and applicable governance frameworks.

In order to add scientific rigour to the literature review and obtain a strong theoretical basis for the research, the three-stage process suggested by Levy and Ellis (2006) was employed, resulting in the 390,995 articles initially identified being narrowed down to 167 relevant articles. During the *input stage,* a wide selection of articles were selected to gain an understanding of the underlying literature to get an indication of the scope of knowledge on the subject; thus the quality, academic value and reputation of the literature were not considered. The search was wide and generic whereby suitable data were gathered from quality literature databases such as Elsevier®/ScienceDirect®, IEEE, Google Scholar and Scopus using the following keywords: 'IoT', 'IoT devices', 'health-care', 'data governance', 'IoT architecture', 'governance frameworks', 'data governance frameworks', 'data governance

principles', 'data governance components', 'IoT data' and 'risks of IoT'. The initial search was narrowed down to focus on sources that were fully accessible in English and that had a strong academic foundation often originating from peer-reviewed sources. In the *processing stage*, the literature was refined down to develop an understanding of *inter alia*, *'COBIT 2019'*, *'IoT risks in medicine'*, *'patient data'*, *'data governance for IoT'*, *'IoT architecture'*, *'electronic health records'*, *'corporate governance' and 'information technology governance'*. This was achieved by selecting readings that contained similar themes with respect to the use of IoT in the medical field, sensitive patient data, risks of using IoT, data governance, IT governance and IoT architecture after examining titles, abstracts and keywords. In some cases, articles may claim to define IoT but do not explore its uses and consequences in detail. As a result, 293 articles were identified to be relevant. The focus of this research was to identify and outline the enabling technologies of IoT in order to understand the architecture behind it, as such readings that provided an in-depth technical study of the design, development or programming of IoT, and any enabling technologies associated with it were not considered. Furthermore, only readings that considered the risks associated with IoT data were considered for further analysis; readings that considered IoT solely without a link to IoT data were not considered. Thereafter, an in-depth review was conducted of articles, websites, introductions and conclusions. The purpose was to identify applicable information that enabled the authors to gain a clear understanding of IoT in the medical field, the types of data and data flow in relation to IoT devices, risks associated with the data life cycle of patient data and governance frameworks to mitigate these risks. This assisted in developing a clear understanding of the extent of each theme and of how much should be discussed about each theme. In this stage, readings pertaining to the above-stated criteria were restricted to those published from 2009 onwards as prior may have outdated information pertaining to the technology. This yielded 167 articles. These articles were synthesised into a logical structured argument known as the *output stage* that could provide a reader with the details of what the researcher researched during the input stage and what insights were gained from the processing stage.

The systematic literature review conducted in the abovementioned stages formed a solid theoretical knowledge base for the understanding of the medical industry, IoT data, IoT architecture, IoT devices, IoT data life cycle, IT governance, corporate governance and data governance.

The literature formed the basis of the initial findings of this research. Using this basis, the following structured steps used by Sahd (2015), Van Wyk and Rudman (2019) and Van Niekerk and Rudman (2019) were used to meet the following research objectives:

- *Obtain a general understanding of the medical field and its relationship with IoT:* The recorded concepts found in the previous processes were arranged by the researchers to establish an integrated set of information in an elaborative and supportive document that contains a general understanding of the health industry and the impact of technology, including the impact of IoT, by describing the technological evolution in this field, its benefits and consequences.
- *Define IoT and its enabling technologies:* This foundation of understanding is used to form a definition of IoT and its enabling technologies. This assisted in understanding the architectural layers of IoT devices, which included an understanding of the different types of IoT devices. The aim was to gain an understanding of the technology and its architecture and a general understanding of the types of devices available as described in generally accepted literature.
- *Perform an analysis of data governance:* An investigation was conducted into the different types of data collected by IoT devices in relation to the data life cycle within IoT architecture. Furthermore, the key data-related challenges faced by the healthcare industry in relation to the use of IoT devices were analysed and considered when developing an understanding of effective data governance and applicable laws and regulations relating to patient data in order to understand its importance in this field and assists users when managing patient data. This further led to the identification of a suitable framework that was applied as a basis when identifying risks in relation to IoT data (*HIPAA*).
- *Perform an in-depth analysis of the COBIT 2019 governance framework and its processes and section 164 of HIPAA for data privacy and security:* By taking the knowledge and insights gained regarding IoT and IoT data into account, the COBIT 2019 governance framework as detailed by the Information Systems Audit and Control Association (2019) and section 164 of *HIPAA* were evaluated in detail. Through this evaluation, the relevant processes that were necessary to govern IoT and IoT data were identified. The applicable processes and detailed mapping of risks are available from the authors on request.
- *Identify risks associated with the use of IoT:* The relevant processes presented in the COBIT 2019 framework and section 164 of *HIPAA* were used to identify risks with respect to each COBIT process, the privacy and security rules outlined in section 164 of *HIPAA* and IoT data including related IoT enabling technologies used in the medical field. A risk-technology matrix was prepared, associating the enabling technologies with their risks (Appendix 2).

Notably, through the review of the literature, some articles highlighted IoT risks but few addressed IoT data risks with respect to data security, privacy and confidentiality in a comprehensive manner. The biggest weakness in prior research was in the *ad hoc* nature in which risks were identified. In order to address this, COBIT 2019 and *HIPAA*'s section 164 were selected as an appropriate framework. These are widely accepted and internationally recognised by

various organisations. It covers a wide range of IT processes that ensures easy alignment with other international frameworks and standards, thereby ensuring sound controls and regulatory compliance. COBIT 2019's 37 processes and *HIPAA*'s legislative guidance regarding privacy and security were used as a benchmark to identify areas that need to be governed. Should these areas not be properly governed, it would give rise to risks in the medical field. Therefore, the understanding of the IoT technologies was mapped to these two frameworks to identify significant risks that relate to IoT and IoT data. A risk and technology matrix was developed, linking significant risks to its origin within IoT architecture. Once the risks were identified, a further review of the literature was performed in order to expand the detail of the risks. The methodology employed is same as that employed by Van Wyk and Rudman (2019).

Literature review

The global healthcare industry has experienced significant growth in the level and quality of healthcare delivery because of technological advancements (Hajizada, 2023). Modern medical equipment such as magnetic resonance imaging (MRI) scanners, ultrasound machines and computed tomography (CT) scanners have enhanced patient care allowing for better healthcare plans resulting in better patients' care and faster diagnosis and treatment. Furthermore, the transition from paper-based documentation into electronic health records has streamlined patient care management and resources management across hospital departments as these records are available in real time and can be shared and accessed at any point in time (Rezaeibagha et al., 2015). Because of the evolution of healthcare, the medical industry has sought to use technologies that can assist it to further its goals and provide better medical care to all (O'Reilly et al., n.d.). Of these technologies, IoT is at the forefront. While the healthcare industry is quick to implement and encourage the use of IoT devices, it is often unaware of the exact nature of the risks these devices pose, and it often lacks the skills to identify these risks. The gap between IT and its implementation in business goes hand in hand, one not being able to succeed without the other.

Having said this, there is often a difference in understanding and assessing the needs of business and the needs from an IT perspective, thus giving rise to a skewed view of the role each plays in the success of a business, which can lead to challenges when determining technological solutions. A skewed view is considered to be one of the key challenges when assessing new technology to solve business issues that hinder proper corporate and IT governance. This brings to light the need for proper research guidance that can assist stakeholders in managing a new technology deployed to solve business problems and comply with best practices to ensure sound data and IT governance and by extension corporate governance allowing businesses to remain successful. This should in turn promote sustainability when using IoT in this field and contribute towards better business management.

Evolution of Internet of Things and the medical field

Technological advancement in health-care such as IoT are essential in addressing challenges such as rising cost of care, resource constraints and staff shortage that cause disparity in patient care (Pradhan et al., 2021).

In 1999, Kevin Ashton, initially defined 'IoT' as the idea of connecting radio frequency identification (RFID) technology with the Internet, for autonomous data collection (Ashton, 2009). Internet of Things has evolved into integrated enabling technologies forming a community of heterogeneous devices, including sensors and software components, that effortlessly work together and interact with users to provide specific state-of-the-art cyber-physical services (Birkel & Hartmann, 2019; Fortino et al., 2022). Internet of Things in medicine facilitates real-time monitoring of patients through wearable or implantable devices ranging from non-invasive wearable glucose monitors to implantable smart pacemaker for electrocardiogram (ECG) monitoring (Pradhan et al., 2021, Verma et al., 2022). A significant amount of available existing research has focussed on assessing the level of security of IoT devices used (Ahlmeyer & Chircu, 2016). Hajizada (2023) further identified safety and privacy concerns when using IoT devices in the medical field and investigated current safety safeguards and identified some risks pertaining to safety and privacy but does not consider confidentiality of patient data while focussing on establishing safeguards focussed only on the transmission of data through IoT, leaving out other architectural layers where risks might lie. Furthermore, apart from providing an overview of IoT architecture, Bandyopadhyay and Sen (2011) pointed out that IoT has challenges around interoperability as different devices use different operating systems and communicate using different languages that may pose as a risk to overall IoT security. Several studies have showed that security risks are often overlooked especially in healthcare as legacy healthcare systems lack security features (Birkel & Hartmann, 2019; Lee, 2020; Radoglou-Grammatikis et al., 2022; Raghuvanshi et al., 2022; Sivaparthipan et al., 2023). Furthermore, security vulnerabilities such as transmission layer weaknesses expose devices to privacy and confidentiality breaches and attacks such as eavesdropping and denial-of-service (DoS) attacks (Birkel & Hartmann, 2019; Sivaparthipan et al., 2023). In addition, privacy and confidentiality of IoT medical data is another challenge (Sivaparthipan et al., 2023).

While some research suggests that there needs to be a wider focus on data because of the emergence of big data and machine learning techniques that can assist in offering insights for the improved patient care (Subrahmanya et al., 2022), the importance of sound data governance within the IoT environment is frequently overlooked and should be addressed. Currently a lack of comprehensive frameworks for risk identification and governance arising from the use of IoT results in a general lack of confidence with regard to privacy, confidentiality and security of data that hampers implementation of IoT (Morar et al., 2021).

Definition of Internet of Things within the medical field

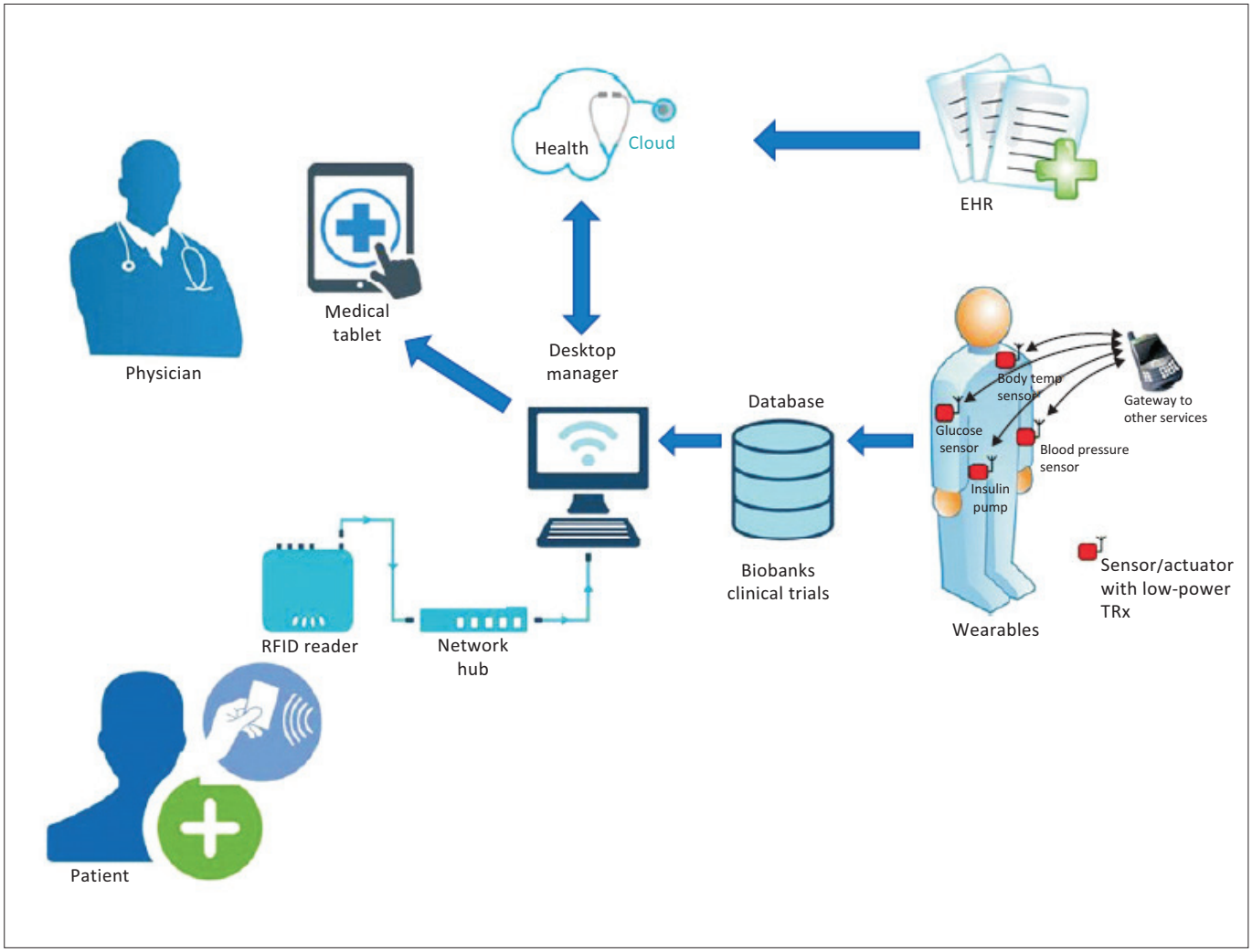
Internet of Things devices in healthcare are sensory devices that are connected to the Internet with the capability to record data about their surroundings, including capturing data streams regarding physical environments and biological environments of its host and exchanging data with other devices (Mishu, 2018; Trautman et al., 2020). Sensors can monitor bodily functions and biometric data, such as heart rate or glucose levels, by making use of vital sign patches (Kelly et al., 2020). Embedded sensors, known as wearable devices, gather data about its environment and its host and exchange it with others such as medical professionals (Dasgupta et al., 2019; Pradhan et al., 2021; Van Niekerk & Rudman, 2019). Another type of IoT device is implantable devices, which can be inserted into a patient's body or ingested and are often used for smart medication monitoring (Kelly et al., 2020). In addition, according to Thamilarasu et al. (2020), IoT in a medical context consists of a biome of connected devices and sensors that can enable healthcare applications such as elderly care, remote health monitoring and chronic disease management. The smartness of 'things' within IoT allows for these devices to have the ability to gather and communicate data across different stakeholder levels – for instance, data can be shared with patients, doctors and clinicians, thus shifting the focus onto the patient (Li & Carayon, 2021).

This process is displayed graphically in Figure 1.

Considering the preceding discussion, IoT is a worldwide communication network that contains various sensors embedded in virtual and physical objects that can be worn or implanted with the ability to be uniquely identifiable. These devices gather data in real time from its host (patient) and the host's surrounding environment that can be further integrated and analysed for better informed medical decisions.

Internet of Things architecture

Internet of Things architecture must be able to support the constant monitoring of patients' health through the collection, usage, storage, management and exchange of data. To do this, a six-layer IoT architecture is proposed starting with a basic three-layered architecture described by Calihman (2019) and Kelly et al. (2020), expanding on to include an additional



Source: Dimitrov, D.V. (2016). Medical internet of things and big data in healthcare. *Healthcare Informatics Research, 22*(3), 156–163. https://doi.org/10.4258/hir.2016.22.3.156
RFID, Radio Frequency Identification; Temp., temperature; EHR, electronic health records; TRx, transceiver.

FIGURE 1: Visual representation of Internet of Things devices in healthcare.

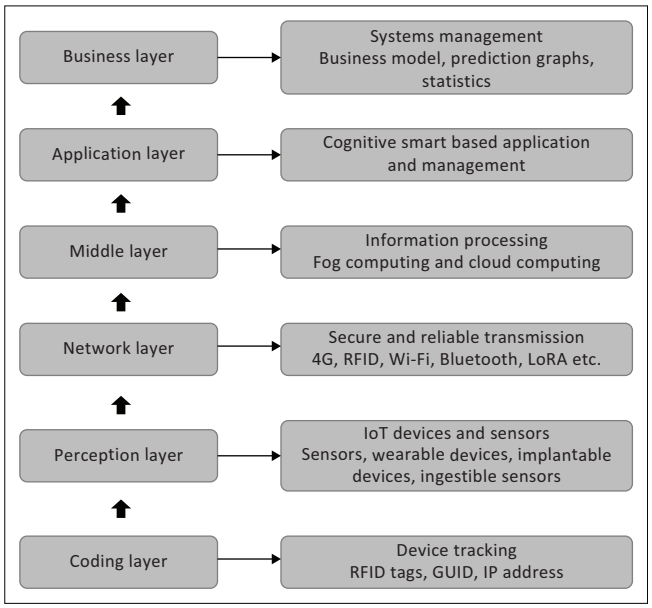
three layers adapted by the author after consideration of research conducted by Rahman and Hussain (2019) and Van Niekerk and Rudman (2019) as displayed in Figure 2.

The six-layer architecture with enabling technologies of IoT are described as:

- *Coding layer:* At this layer, devices are uniquely identifiable by means of number RFID tags enabling tracking of preventing unauthorised access to an organisation's network (Van Niekerk & Rudman, 2019).
- *Perception layer:* At this layer, data is collected by sensors that detect changes within their environment such as location, temperature, weather patterns or even changes in heart rate (Calihman, 2019; Kelly et al., 2020).
- *Network layer:* The virtual network layer facilitates communication through wireless technologies such as Wi-Fi, Bluetooth, 4G, LoRa and radio frequency, employing communication protocols to transmit data of which there are three categories. The main protocols used can be split into the following categories (Van Niekerk & Rudman, 2019):
  - *Application protocols* (e.g. data distribution service [DDS]) for real-time machine-to-machine communication to transfer data accurately.
  - *Search and resource discovery protocols* such as domain name system protocol (DNS) for device identification via an internet protocol (IP) address.
  - *Infrastructure protocols* that assist in identifying IoT devices within the network for example Internet Protocol version 4 (IPv4) and routing protocols for efficient data packet delivery.

- *Middle layer:* This layer uses technology to consolidate and standardise IoT data while providing screening, processing, an element of security management, resource location and error resolution (Abbasi et al., 2017, Fan & Chen, 2010). All of this is made possible by the deployment of fog computing and cloud computing (Morar et al., 2021):
  - *Cloud computing* is centralised data processing, filtering and modelling of data in a cloud server (Rahman & Hussain, 2019).
  - *Fog computing*: Supports heterogeneity, interoperability and mobility of data by offering computational, network and storage services between the cloud server and IoT devices made possible by the use of fog nodes that manage resources and services independently (Saqlain et al., 2019). Fog computing acts as a supplement to cloud computing, together they make up the middle layer.

- *Application layer:* This layer analyses and interprets results of the data collected by the device to make business decisions by integrating emerging technologies such as AI for prediction and imagery diagnosis for assisting with disease diagnosis (Kelly et al., 2020).
- *Business layer:* This layer manages IoT systems to ensure alignment between the IoT systems implemented and the entity's business goals (Van Niekerk & Rudman, 2019).



Source: Adapted from Babovic, Z., & Milutinovic, V. (2013). Novel system architectures for semantic-based integration of sensor networks. In *Advances in computers* (pp. 91–183). Academic Press

RFID, radio frequency identification; IoT, Internet of Things; GUID, globally unique identifier; IP, internet protocol.

FIGURE 2: A six-layer Internet of Things architecture.

A six-layer IoT architecture provides an outline of how IoT and its enabling technologies function. To put this into perspective, an understanding of the manner in which medical IoT data are processed within an IoT environment should be explored in order to understand its data life cycle.

Data life cycle of Internet of Things data in the healthcare environment and data governance

A data life cycle consists of a series of phases over the useful life of the data. The data lifecycle of IoT data in healthcare consists of the data generation phase through to data disposal and storage (Wing, 2019). Saqlain et al. (2019) fittingly divided the life cycle of IoT data into two domains: the real-world domain and the virtual domain. In the real-world domain, data are generated and collected by wearable or implantable devices whereby device identification using unique identifiers is made possible, representing the coding layer (Pradhan et al., 2021). The perception layer collects different types of data in different formats from the real world such as facial expressions, blood glucose level, heart rate, temperature, weather conditions and location (Alarcón-Paredes et al., 2019; Kelly et al., 2020; Pradhan et al., 2021) and is transmitted via wireless network connections and communication protocols found in the network layer (e.g. Wi-Fi). Transmitted data undergoes data cleaning and indexing, among others, allowing for interoperability within the middle layer that is located in the virtual domain.

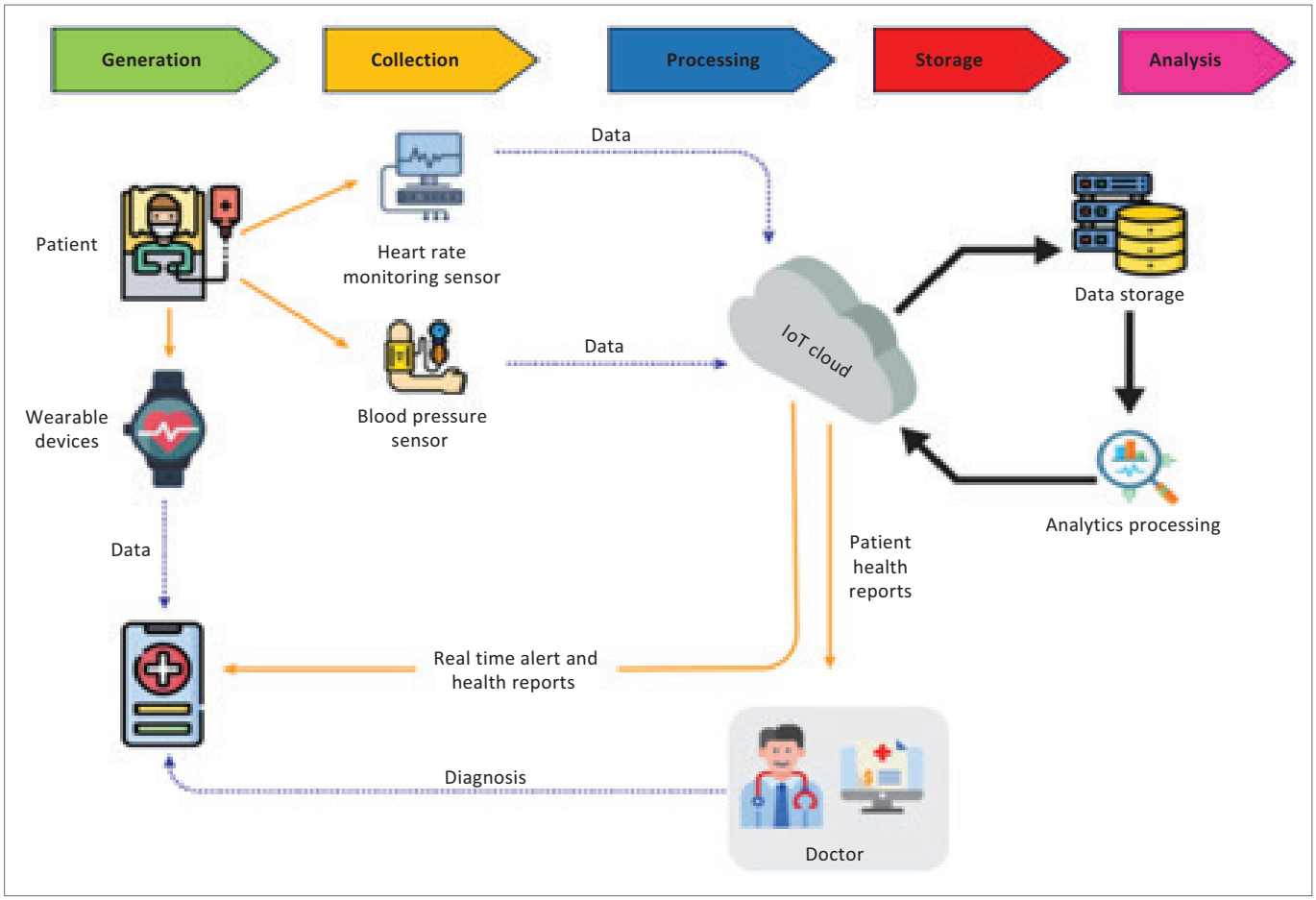
From the middle layer, the data can be sent to the application layer for further analysis and processing where data can also be visually presented and used to gain further insights for decision-making or for further medical research (Subrahmanya et al., 2022; Trautman et al., 2020). Otherwise, data are kept in cloud storage situated within the middle layer and remains in cloud storage until disposal. Figure 3 provides a visual representation of the data life cycle within an IoT environment.

Data gathered by IoT devices can be structured (e.g. patient details, heart and pulse rate) and unstructured (e.g. X-ray images, genomic and biometric data) (Dimitrov, 2016; Hendawi et al., 2019; Manogaran et al., 2018; Pradhan et al., 2021; Subrahmanya et al., 2022). Both categories of data have different characteristics that all need to be adequately safeguarded throughout the data lifecycle. Furthermore, sensitive health data pose a risk for the hospital and the patient involved if not properly secured and protected. As many IoT devices are not designed with security in mind, they are vulnerable to security breaches and data tampering (Trautman et al., 2020; Van Niekerk & Rudman, 2019). This can jeopardise patient privacy and confidentiality violating regulations such as HIPAA (Henriques et al., 2020; United States, 1996). In light of the foregoing and considering the sensitive nature of patient data governance within healthcare in respect of IoT is essential in addressing data security, privacy and confidentiality and is a crucial element when using IoT devices within this field to ensure regulatory compliance and compliance with corporate governance policies and practices.

Data governance

Internet of Things devices come with their own standards and protocols and handle sensitive personal and medical data, highlighting the need for robust data governance to ensure the privacy, confidentiality and security of the data (Islam et al., 2015; Karunarathne et al., 2021; Kelly et al., 2020; Morar et al., 2021; Van Niekerk & Rudman, 2019). Governance is seen as the bridge between technology and data that take shape in the form of decision rights and accountabilities built into a framework that encourages desirable behaviour to foster high-quality data for effective decision-making (Gao et al., 2022; Panian, 2010). While IT governance manages IT assets, data governance focusses on data as the asset to be governed (Dasgupta et al., 2019). As such, data governance can be seen as a component of IT governance. Both IT governance and data governance are components of corporate governance (IODSA, 2016) and need to be considered to adequately and comprehensively identify risks in this field, contributing to the establishment of sound corporate governance practices. Given the complexities of IoT and its susceptibility to privacy and security risks, a specific framework for governance is needed (Morar et al., 2021).

Instilling sound data governance in healthcare requires addressing IoT data architecture from the perspective of data management (Zakaria et al., 2019). Data governance is high-level planning that complements data management and includes a level of control over data management. This



Source: Adapted from Shrimali, R. (2020). *How IoT is transforming the healthcare industry*. Retrieved from https://embeddedcomputing.com/application/healthcare/telehealth-healthcare-iot/how-iot-is-transforming-the-healthcare-industry

IoT, Internet of Things.

FIGURE 3: The data life cycle within an Internet of Things environment.

encompasses planning, control and security of data throughout its lifecycle (Al-Ruithe et al., 2018; Marco, n.d.; Zakaria et al., 2019). Control over data management ensures data quality, achievable through adequate reference and master data management and the establishment of the appropriate data architecture while further addressing data security requirements to protect data throughout its life cycle. Data governance within IoT must provide security measures to protect data throughout the architectural layers, from application to network layer and within the device itself (Henriques et al., 2020). Therefore, it is essential to consider data governance when using IoT devices and IT governance over the devices to ensure that data will be safeguarded and should occur throughout each layer of the IoT architecture for a comprehensive risk assessment as risks pertaining to IoT may present themselves differently at different layers within the architecture.

Ethical considerations

Ethical approval to conduct this study was obtained from the Stellenbosch University Research Ethics Committee: Social, Behavioural and Education Research (REC: SBE) (No. ACC-2023-27501).

Results and discussions

Data risks associated with Internet of Things in the healthcare industry

Internet of Things has many benefits in the healthcare industry but can pose some challenges particularly in respect of data security, privacy and confidentiality (Chang et al., 2009; De Muylder et al., 2019; Van Niekerk & Rudman, 2019; Zakaria et al., 2019). This could be attributed to a lack of security in design and a lack of organisational knowledge to fully understand the depth and types of risks and challenges before implementation (Trautman et al., 2020; Van Niekerk & Rudman, 2019). After consideration of available research, it was noted that the most relevant challenges surrounding IoT are with respect to physical device vulnerability, insecure communication channels, an increased vulnerability surface area and limited computing power of devices (Ko et al., 2018; Van Niekerk & Rudman, 2019). These challenges are specific to IoT and highlight significant challenges within the healthcare sector and must be addressed to ensure sound data governance; and in doing so, it will contribute towards sound corporate governance. Many of the risks identified already exist in the Internet but when combined with enabling technologies in an IoT environment, new risks emerge. These risks are discussed in the following subsections.

Data security

Health Insurance Portability and Accountability Act defines data security as the protection against unauthorised use, disclosure, access, alteration, disruption and destruction of data, information and information systems using administrative, technical and physical controls (United States, 1996). Data security is thus implemented to provide privacy, confidentiality and availability of data and information (Kahn & Sheshadri, 2008). Threats to data security are discussed as follows:

Authenticity

Authenticity ensures the validity of data being transferred and presented by IoT devices to ensure that it is a true presentation of an actual live event and ensures that the data are collected in real time (Matin & Islam, 2012). The authenticity of IoT devices and the data they collect are exposed to impersonation, which are techniques used to gain access to an IoT device, a network and IoT data by fabricating authenticated identities. These types of attacks are highly effective in an IoT environment and can result in insecure data transmissions and unauthorised access which can compromise data security (Wan et al., 2021). Appendix 1 provides detailed examples of various impersonation attacks perpetrated within an IoT environment.

Furthermore, architectural deficiencies within IoT that impact authenticity are a *lack of policies and user guidelines.* Inadequate policies and guidelines available for the use of IoT devices to ensure protection and security over data can lead to unauthorised access to devices (Brous et al., 2020). Moreover, *weak authentication* can lead to IoT devices that often lack the ability to support password concealment, user authentication systems and logical access controls (including least-privileged principles) leaving devices unprotected against unauthorised access to sensitive data (Boeckl et al., 2019). The abovementioned threats not only compromise authentication but also pose a threat to access controls, further emphasising the need for authentication mechanisms within IoT environments in healthcare.

Unauthorised access

Unauthorised access refers to the viewing of and accessibility to data, information and resources by those who do not have permission from the owner to view or access the data and information. According to Rezaeibagha et al. (2015), the most common weaknesses are in relation to network connectivity, authentication methods and access controls. These weaknesses are concentrated around the device, device software and the network layer, middle layer and application layer within IoT architecture. Some threats such as data loss occur throughout the architectural layers.

Threats that impact the device such as *user compromise* occur because of the theft of cryptographic keys or passwords resulting in unauthorised access to the device or network leading to data transmission interruptions and alterations (Blanke & McGrady, 2016; Islam et al., 2015). Internet of Things devices may fail to shut down after unsuccessful login attempts resulting in unauthorised access (Boeckl et al., 2019), while reverse engineering can exploit device vulnerabilities to gain unauthorised access (Liang & Kim, 2021). In addition, attackers may target device software; for example during a user to *root (U2R) attack*, access is gained to the system as a normal account and allows for data manipulation, spying and

system disruptions impacting data transmissions (Abdullahi et al., 2022). Moreover, illegal packets sent to the system to exploit system privileges to gain access can be perpetrated through *remote to local user (R2L) attacks* including worm attacks (Abdullahi et al., 2022). Lastly, exploitation of medical imaging techniques by injection or removal of false data and medical imagery known as a computed tomography-generative adversarial network *(CT-GAN) technique* may lead to incorrect diagnostics (Affia et al., 2023).

Threats situated within the network layer of IoT architecture range from exploitation of weaknesses within IoT, node collusion and cloning, traffic classification errors and various malicious injections into the database known as SPARQL Protocol and RDF Query Language (SPARQL) and code and database injections including account hacking threats and message tampering that may lead to unauthorised access. These risks are explained in detail in Appendix 1.

Threats within the middle layer of the IoT architecture (including both fog and cloud computing) occur through *incorrect bootstrapping* when nodes are incorrectly authenticated, leaving the network open to unauthorised access via these nodes (Nebbione & Calzarossa, 2020). And more commonly, *cloud server breaches* that usually occur when cloud service providers do not hold security in as high a regard as the medical organisation making use of their services resulting in a gap in security that can result in data breaches (Abraham et al., 2019a; Vilakazi & Adebesin, 2023).

Another risk is a *poorly skilled service provider*. Cloud service providers may hire insufficiently skilled employees who lack the required knowledge regarding the identification and mitigation of risks associated with IoT (Ashktorab & Taghizadeh, 2012). Lastly, an *untrusted cloud server* may result in insecurity and privacy risks that can occur as data may not be stored correctly in the cloud server and can be deleted or altered (Sang et al., 2023).

Within the application layer, threats such as *insecure Application Programming Interfaces (APIs)* occur creating an opportunity for unauthorised access to sensitive data resulting in data destruction or unauthorised modification as APIs are used for users to interact with cloud services (e.g. data retrieval) (Ashktorab & Taghizadeh, 2012).

Furthermore, *Wi-Fi-based attacks* can occur when a ciphering stream is compromised, allowing for the recovery of keys to gain access to data (Khan et al., 2023). Another risk at this layer is a *cross-site scripting (XSS) attacks* that occur when malicious scripts are injected into the Web whereby malicious code is stored into the resource managed by a web application on a permanent basis or where attack scripts are immediately reflected back to the user without permanent storage. This can result in data alteration and unauthorised access (Ashktorab & Taghizadeh, 2012). Finally, at this layer, a *web attack* can also take place when intruders use generally trusted websites and web applications infused with malicious content to gain access to sensitive information, for example brute force attack (Manimurugan et al., 2020; Wheelus & Zhu, 2020).

On the other hand, data loss occurs that can occur at any layer of the IoT architecture when data are altered, deleted or destroyed (thus making it unrecoverable) before a back-up copy can be made posing as a risk to data and by extension data privacy and confidentiality (Ashktorab & Taghizadeh, 2012). Examples of these types of risk that arise from data loss are discussed in detail in Appendix 1.

Network availability

According to *HIPAA*, availability refers to data and information being accessible and usable on demand by authorised individuals (United States, 1996). Network availability is under threat from attacks that aim to compromise or disable the network leading to unauthorised access that can result in alteration, destruction and unauthorised disclosure of sensitive information. Several attacks that impact network availability are discussed in more detail as follows:

- *Jamming attacks:* Occurs when there is interference with the frequency that the sensor nodes use and can disrupt the entire network or parts thereof leading to incomplete data transmissions (Van Niekerk & Rudman, 2019; Vilakazi & Adebesin, 2023; Wang & Wyglinski, 2011).
- *Selective forwarding:* Using malicious nodes placed in the network that selectively only forward and drop certain data, compromising security of data (Thamilarasu et al., 2020; Van Niekerk & Rudman, 2019; Vilakazi & Adebesin, 2023).
- *Probe attack:* Data are obtained based on target external network sources (e.g. IPsweep or Portsweep), facilitating attacks within a peer network (Abdullahi et al., 2022).
- *Network properties attack:* This is conducted through a standard protocol compromise where the attacker deviates from standard network or application protocols behaving maliciously or via a network protocol attack where the attacker exploits vulnerabilities in protocol stack layers committing malicious acts (Islam et al., 2015).
- *Flooding:* A reactive approach where a node that received data or control packets sends data to all other nodes in the network, replicating packets, causing network overload for example, Hello flood attack (Matin & Islam, 2012; Vilakazi & Adebesin, 2023).
- *Routing loop attack:* This results in false error messages that are generated when the attacker modifies and replays routing information, attracting and repelling network traffic and increasing node latency (Matin & Islam, 2012).
- *Botnet attacks:* By the use of malware, embedded sensors are overtaken by an external botnet master that takes control of the device, posing a threat to network security (Ko et al., 2018; Liang & Kim, 2021; Vilakazi & Adebesin, 2023; Yin et al., 2019).
- *Remote code execution*: Using injections, malicious input is designed to look like a command in the form of an arbitrary code, creating a pathway for unauthorised

access to internal networks, thereby accessing data while the device is in operation (Agarwal et al., 2019).

- *Portscan attack:* IoT device data (e.g. the type of operating system and the services running) are collected by forwarding packets that have different destination points that can lead to device exploitation (Manimurugan et al., 2020).
- *Relay attack:* A connection is established between a legitimate reader and the target's legitimate tag making communication look like the legitimate tag and reader are in close proximity when in reality they are communicating through a wireless communication channel created by the attacker (Rotter, 2008).
- Interference within the network can impact data communication between IoT layers and affect network availability. In many instances, this interference is used to gain unauthorised access to the network where several attacks can be launched that pose as a risk to data security and will result in weaknesses in internal controls. Types of threats that create interference in the network are discussed in Appendix 1.

Data security planning

Data security planning is essential for safeguarding medical IoT data and involves identifying threats and creating, maintaining and supporting an active security culture (Abraham et al., 2019a). A lack of sufficient data security planning results in a *lack of organisational security strategy* when there is no well-thought-out security strategy, resulting in unmaintained operating systems leading to unauthorised access. Added to this, medical organisations often *do not develop adequate policies and regulations* resulting in no policies and guidelines to direct protection of healthcare data extending from data collection to destruction (Brous et al., 2020). This includes inadequate policies and guidelines for decommissioned IoT devices leaving old devices with sensitive data vulnerable to exploitation (Yousefnezhad et al., 2020).

In addition, *deficiencies in organisational security management strategy* result in a lack of risk assessment in IoT device design leading to security vulnerabilities that can be exploited (Chacko & Hayajneh, 2018). Lastly, there seems to be a lack of an *appointed security official* required by *HIPAA* resulting in non-compliance with *HIPAA* and results in control weaknesses as there is not an individual designated to oversee data security (United States, 1996).

Architecturally, IoT may lack certain features and functions for the implementation of data security planning. Key missing features and functions are *a lack of security audit ability* within devices resulting in the inability to record all security events of the organisations (Boeckl et al., 2019; Kamal et al., 2023). Internet of Things devices often have a *black box effect* where little or no information regarding the device's hardware or software can be established making device management challenging and hinder data protection capabilities (Boeckl et al., 2019). Moreover, devices often have *limited upgradability* because IoT device manufacturers may not release any upgrades for the IoT devices making it harder for an organisation to implement device security to protect patient data (Boeckl et al., 2019). Lastly, *incompatibility* with existing vulnerability scan systems used to monitor and identify malicious incidents resulting in unidentified malicious activity (Boeckl et al., 2019).

When unauthorised parties gain access to data because of, for example, a lack of data security, it can bring about attacks such as man-in-the-middle attacks. As discussed earlier, unauthorised access also impacts authenticity negatively; all of which can be seen as a symptom of a lack in data security planning. Furthermore, a lack in data security can result in unwanted attacks that can compromise data privacy and confidentiality; thus data security is a fundamental aspect in achieving data privacy and confidentiality.

Data privacy and confidentiality

Privacy can be considered to be the limitation of access to the personal information of the individual to whom the information pertains (United States, 1996). Privacy limits access to personal information, whereas confidentiality ensures data remain unaltered and inaccessible to unauthorised parties (United States, 1996; Liu et al., 2012). Unauthorised access can be gained through monitoring data over the network and monitoring network performance that can compromise the privacy and confidentiality of medical data. This can be a hinderance to data governance and by extension corporate governance that may leave the entity exposed to risk. Unauthorised access can be facilitated through *eavesdropping* that allows for the monitoring of network data with no signal emission (Islam et al., 2015; Selvan & Singh, 2022; Thamilarasu et al., 2020; Van Niekerk & Rudman, 2019). And *data sniffing* that allows for the capturing and interpretation of data transmissions using flaws in network security protocols (Liang & Kim, 2021; Sicari et al., 2018; Van Niekerk & Rudman, 2019). Furthermore, the IoT architecture may lack certain features that promote privacy and confidentiality. These several features are briefly discussed in Appendix 1.

Threats such as internal attacks, social engineering, phishing, man-in-the-middle attacks, data alteration, U2R attacks, RFID cloning and sleep deprivation attacks can occur including threats pertaining to authentication, unauthorised access and network availability such as the lack of policies and user guidelines for IoT, collusion attacks, incorrect bootstrapping, crypt analysis attack, cloud server breaches, untrusted cloud servers and remote code execution that impact data security will also pose a threat to data privacy and confidentiality.

Conclusion

Using IoT in the healthcare environment presents challenges because of its continuous connectivity requirements and

multiple entry points. Limited security awareness and knowledge of emerging technologies within healthcare increases these challenges (Ngqondi & Pottas, 2009; Samy et al., 2009). While general IoT-related risks have been identified in existing research, there was a weakness in studies that link risks relating to IoT and IoT data to an IT and data governance framework tailored for the healthcare sector. Organisations often follow a disjointed approach to the governance and management of the technology and data, by extension resulting in a haphazard attempt at corporate governance. The use of a framework to identify the risks ensures a comprehensive risk identification framework is developed to address data and IT governance concerns while also addressing corporate governance concerns in the process.

This research aimed to *develop a risk-technology-based matrix* using COBIT 2019 and Section 164 of *HIPAA* to identify IoT-related risks with respect to medical IoT devices. The risk-technology matrix produced in this research, represented in Appendix 2, can assist enterprises in implementing detailed controls that focus on their unique risk exposure and could also be used as a starting point to mitigate these risks to an acceptable level. The framework was developed to identify risk areas relating to *risks to data security* that consisted of risks that affected authenticity, secure access, network availability and security planning related to IoT data, which were compromised by threats involving fabricated identification of devices perpetrated by Sybil attacks, spoofing, data combination, cookie poisoning, global positioning system (GPS) deception and poisoning mainly aiming at compromising the network or gaining unauthorised access to the network or data by various means A lack of policies and user guidelines pertaining to IoT including a lack of authentication mechanisms within IoT leading to architectural deficiencies also created a further platform for the above risks to exist within this technology.

The risk of unauthorised access gained through a barrage of attacks throughout the architectural layers ranging from crypt analysis attacks to man-in-the-middle attacks, data alteration, U2R and R2L, among others, further contributed to areas of weakness when considering IoT in this field while network availability was compromised by threats withing the network layer of the architecture such as jamming, network properties attack, desynchronisation, probe attacks, storage attacks, on-off attack, flooding, routing loop attack, sleep deprivation, botnet attacks, remote code execution, portscan, radio frequency interference, relay attack and RFID tag limitations. Lastly, data security planning was impacted by a lack of organisational security strategy, risk assessment and sufficient user policies that contributed towards creating a space for the abovementioned threats to take hold, which hinders data and IT governance. These risks to data security created a platform for further risks towards *data privacy and confidentiality*.

Privacy and confidentiality breaches occurred because of unauthorised access gained by way of eavesdropping and data sniffing attacks while the IoT architecture lacked several features contributing to risks to privacy and confidentiality such as physical device tampering, a lack of privacy mechanisms and a lack of digital footprint privacy, a lack of encryption, a lack of device verification, data ownership ambiguity amplified by cross-border data transfers. Many of these risks result in deficiencies in technical design of IoT while others are because of the changing landscape of data transmission on account of the Fourth Industrial Revolution. Furthermore, other risks affecting data security also created a risk for privacy and confidentiality such as remote code executions, untrusted cloud server, incorrect bootstrapping, U2R, data combination, wireless probing, internal attacks and other attacks such as social engineering and phishing, which extend across the architectural layers of IoT.

Governance stakeholders (including IT specialists) must understand IoT architecture and access paths including the IoT data life cycle to timeously identify and mitigate risks. As healthcare is still in its early stages, a proactive approach to risk management is essential for successful deployment and may contribute towards promoting sustainability when implementing IoT and lead to successful business management within medical organisations.

While this research did not discuss the technical study of the design, development or programming of IoT, it would be beneficial to conduct further studies looking into the technicalities of IoT development, design and programming to assess whether any governance elements are considered upon the design of the technology. Future research could focus on developing controls to mitigate identified risks and address the ownership and control over IoT data.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

N.K. and R.J.R. equally contributed to the research and writing of this article.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The data that support the findings of this study are available from the corresponding author, N.K. upon reasonable request.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research.

The article does not necessarily reflect the official policy or position of any affiliated institution, funder, agency or that of the publisher. The authors are responsible for this article's results, findings and content.

References

Abbasi, M.A., Memon, Z.A., Syed, T.Q., Memon, J., & Alshboul, R. (2017). Addressing the future data management challenges in IoT: A proposed framework. *International Journal of Advanced Computer Science and Applications, 8*(5), 197–207. https://doi.org/10.14569/IJACSA.2017.080525

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L.F., & Abdulkadir, S.J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics (Switzerland), 11*(2), 198. https://doi.org/10.3390/electronics11020198

Abraham, C., Chatterjee, D., & Sims, R.R. (2019a). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons, 62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Abraham, R., Schneider, J., & Vom Brocke, J. (2019b). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49*, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Affia, A.O., Finch, H., Jung, W., Samori, I.A., Potter, L., & Palmer, X.L. (2023). IoT health devices: Exploring security risks in the connected landscape. *IoT, 4*(2), 150–182. https://doi.org/10.3390/iot4020009

Agarwal, S., Oser, P., & Lueders, S. (2019). Detecting IoT devices and how they put large heterogeneous networks at security risk. *Sensors, 19*(19), 4107. https://doi.org/10.3390/s19194107

Ahlmeyer, M., & Chircu, A.M. (2016). Securing the internet of things: A review. *Issues in Information Systems, 17*, 21–28. https://doi.org/10.48009/4_iis_2016_21-28

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018). Data governance taxonomy: Cloud versus non-cloud. *Sustainability (Switzerland), 10*(1), 95. https://doi.org/10.3390/su10010095

Alarcón-Paredes, A., Francisco-García, V., Guzmán-Guzmán, I.P., Cantillo-Negrete, J., Cuevas-Valencia, R.E., & Alonso-Silverio, G.A. (2019). An IoT-based non-invasive glucose level monitoring system using Raspberry Pi. *Applied Sciences (Switzerland), 9*(15), 3046. https://doi.org/10.3390/app9153046

Ashktorab, V., & Taghizadeh, S.R. (2012). Security threats and countermeasures in cloud computing. *International Journal of Application or Innovation in Engineering & Management, 1*(2), 234–245. Retrieved from https://www.citefactor.org/journal/index/3708/international-journal-of-application-or-innovation-in-engineering-management

Ashton, K. (2009). That 'internet of things' thing. *RFID Journal, 22*(7), 97–114. Retrieved from https://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

Atlam, H.F., Walters, R.J., Wills, G.B., & Daniel, J. (2021). Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT. *Mobile Networks and Applications, 26*, 2545–2557. https://doi.org/10.1007/s11036-019-01214-w

Aydos, M., Vural, Y., & Tekerek, A. (2019). Assessing risks and threats with layered approach to internet of things security. *Measurement and Control, 52*(5–6), 338–353. https://doi.org/10.1177/0020294019837991

Babovic, Z., & Milutinovic, V. (2013). Novel system architectures for semantic-based integration of sensor networks. In A. Hurson (Ed.), *Advances in computers* (pp. 91–183). Elsevier.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69. https://doi.org/10.1007/s11277-011-0288-5

Birkel, H.S., & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. *Supply Chain Management: An International Journal, 24*(1), 39–61. https://doi.org/10.1108/SCM-03-2018-0142

Blanke, S.J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of Healthcare Risk Management, 36*(1), 14–24. https://doi.org/10.1002/jhrm.21230

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K.N., Nadeau, E., O'Rourke, D.G., Piccarreta, B., & Scarfone, L. (2019). *Considerations for managing internet of things (IoT) cybersecurity and privacy risks*. National Institute of Standards and Technology.

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the internet of things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management, 51*, 101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008

Calihman, A. (2019). *Architectures in the IoT civilization*. Retrieved from https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/

Chacko, A., & Hayajneh, T. (2018). Security and privacy issues with IoT in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology, 4*(14), 155079. https://doi.org/10.4108/eai.13-7-2018.155079

Chang, C.C., Sun, P.R., Cheng, S.L., Chen, R.S., & Liao, K.H. (2009). Developing a risk analysis framework for hospital information security management. In *NCM 2009 5th International Joint Conference on INC, IMS, and IDC, 25–27 August* (pp. 104–1052). IEEE.

Dasgupta, A., Gill, A., & Hussain, F. (2019). A conceptual framework for data governance in IoT-enabled digital IS ecosystems. In *Proceedings of the 8th International Conference on Data Science, Technology and Applications, 01 August 2019* (pp. 209–216). SciTePress.

De Muylder, C.F., De Oliveira, J.G., Batista, C.L., & Marques, R.M. (2019). Information security in the health area: The convergence of two themes and the intensity of scientific publications. *Revista de Gestão em Sistemas de Saúde, 8*(2), 221–232. https://doi.org/10.5585/RGSS.v8i2.14139

Dimitrov, D.V. (2016). Medical internet of things and big data in healthcare. *Healthcare Informatics Research, 22*(3), 156–163. https://doi.org/10.4258/hir.2016.22.3.156

Fan, T., & Chen, Y. (2010). A scheme of data management in the internet of things. In *Proceedings of IC-NIDC*, 24–26 September, IEEE. Retrieved from https://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=A%20schema%20of%20Data%20management%20in%20the%20Internet%20of%20Things

Fortino, G., Guerrieri, A., Pace, P., Savaglio, C., & Spezzano, G. (2022). IoT platforms and security: An analysis of the leading industrial/commercial solutions. *Sensors, 22*(6), 2196. https://doi.org/10.3390/s22062196

Gao, J., Sun, Y., Rameezdeen, R., & Chow, C. (2022). Understanding data governance requirements in IoT adoption for smart ports – A gap analysis. *Maritime Policy and Management, 51*(4), 617–630. https://doi.org/10.1080/03088839.2022.2155318

Hady, A.A., Ghubaish, A., Salman, T., Unal, D., & Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access, 8*, 106576–106584. https://doi.org/10.1109/ACCESS.2020.3000421

Hendawi, A., Gupta, J., Liu, J., Teredesai, A., Ramakrishnan, N., Shah, M., El-Sappagh, S., Kwak, K.S., & Ali, M. (2019). Benchmarking large-scale data management for internet of things. *Journal of Supercomputing, 75*(12), 8207–8230. https://doi.org/10.1007/s11227-019-02984-6

Henriques, D., Pereira, R.F., Almeida, R., & Mira da Silva, M. (2020). IT governance enablers in relation to IoT implementation: A systematic literature review. *Digital Policy, Regulation and Governance, 22*(1), 32–49. https://doi.org/10.1108/DPRG-02-2019-0013

Hajizada, G. (2023). *Analysis of security and privacy in the communication of IoT medical devices*. Master's thesis. Universitat Politècnica de Catalunya.

Information Systems Audit and Control Association. (2019). *COBIT 2019 framework governance and management objectives*. COBIT.

Institute of Directors Southern Africa (IODSA). (2016). *King IV report: Corporate governance.* IODSA. Retrieved from http://www.iodsa.co.za/?page=KingIVEndorsers

Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., & Kwak, K.S. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access, 3*, 678–708. https://doi.org/10.1109/ACCESS.2015.2437951

Jha, A., Athanerey, A., & Kumar, A. (2022). Role and challenges of internet of things and informatics in healthcare research. *Health and Technology, 12*(4), 701–712. https://doi.org/10.1007/s12553-022-00661-y

Kahn, S., & Sheshadri, V. (2008). Medical record privacy and security in a digital environment. *IT Professional, 10*(2), 46–52. https://doi.org/10.1109/MITP.2008.34

Kamal, M., Rashid, I., Iqbal, W., Siddiqui, M.H., Khan, S., & Ahmad, I. (2023). Privacy and security federated reference architecture for internet of things. *Frontiers of Information Technology and Electronic Engineering, 24*(4), 481–508. https://doi.org/10.1631/FITEE.2200368

Karunarathne, S.M., Saxena, N., & Khan, M.K. (2021). Security and privacy in IoT smart healthcare. *IEEE Internet Computing, 25*(4), 37–48. https://doi.org/10.1109/MIC.2021.3051675

Kelly, J.T., Campbell, K.L., Gong, E., & Scuffham, P. (2020). The internet of things: Impact and implications for health care delivery. *Journal of Medical Internet Research, 22*(11), e20135. https://doi.org/10.2196/20135

Khan, Y., Su'ud, M.B.M., Alam, M.M., Ahmad, S.F., Salim, N.A., & Khan, N. (2023). Architectural threats to security and privacy: A challenge for internet of things (IoT) applications. *Electronics, 12*(1), 88. https://doi.org/10.3390/electronics12010088

Khera, M. (2017). Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications. *Journal of Diabetes Science and Technology, 11*(2), 207–212. https://doi.org/10.1177/1932296816677576

Ko, E., Kim, T., & Kim, H. (2018). Management platform of threats information in IoT environment. *Journal of Ambient Intelligence and Humanized Computing, 9*(4), 1167–1176. https://doi.org/10.1007/s12652-017-0581-6

Lee, I. (2020). Internet of things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet, 12*(9), 157. https://doi.org/10.3390/fi12090157

Levy, Y., & Ellis, T.J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: International Journal of an Emerging Transdiscipline, 9*(1), 181–212. https://doi.org/10.28945/479

Li, J., & Carayon, P. (2021). Health care 4.0: A vision for smart and connected health care. *IISE Transactions on Healthcare Systems Engineering, 11*(3), 171–180. https://doi.org/10.1080/24725579.2021.1884627

Liang, X., & Kim, Y. (2021). A survey on security attacks and solutions in the IoT network. In *IEEE 11th Annual Computing and Communication Workshop and Conference*, *27–30 January* (pp. 853–859). Institute of Electrical and Electronics Engineers.

Liu, C.H., Chung, Y.F., Chen, T.S., & Wang, S.D. (2012). The enhancement of security in healthcare information systems. *Journal of Medical Systems, 36*(3), 1673–1688. https://doi.org/10.1007/s10916-010-9628-3

Malhotra, P., Singh, Y., Anand, P., Bangotra, D.K., Singh, P.K., & Hong, W.C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors, 21*(5), 1809. https://doi.org/10.3390/s21051809

Manimurugan, S., Al-Mutairi, S., Aborokbah, M.M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access, 8*, 77396–77404. https://doi.org/10.1109/ACCESS.2020.2986013

Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P.M., Sundarasekar, R., & Thota, C. (2018). A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Generation Computer Systems, 82*, 375–387. https://doi.org/10.1016/j.future.2017.10.045

Marco, D. (n.d.). *Foundations of enterprise data management*. Retrieved from https://www.ewsolutions.com/foundations-enterprise-data-management/

Matin, M.A., & Islam, M.M. (2012). Overview of wireless sensor network. In M.A. Matin (Ed.), *Wireless sensor networks, technology and protocols* (Vol. III, pp. 18–389). INTECH.

Middleton, P., Kjeldsen, P., & Tully, J. (2013). *Forecast: The internet of things, worldwide*. Retrieved from https://www.gartner.com/en/documents/2625419

Mishu, A. (2018). *Developing sustainable information governance strategy for smart healthcare*. Retrieved from https://www.researchgate.net/publication/329156392

Morar, B., Barkawie, Y., Balakrishnan, R., Khasawneh, M., Bangara, J., & Abu Baker, H. (2021). *IoT governance.* Deliotte. Retrieved from https://www2.deloitte.com/xe/en/pages/technology/articles/iot-governance.html

Myeza, L., Ecim, D., & Maroun, W. (2023). The role of integrated thinking in corporate governance during the COVID-19 crisis: Perspectives from South Africa. *Journal of Public Budgeting, Accounting & Financial Management, 35*(6), 52–77. https://doi.org/10.1108/JPBAFM-08-2022-0133

Nebbione, G., & Calzarossa, M.C. (2020). Security of IoT application layer protocols: Challenges and findings. *Future Internet, 12*(3), 55. https://doi.org/10.3390/fi12030055

Ngqondi, T., & Pottas, D. (2009). *The ISO/IEC 27002 and ISO/IEC 27799 information security management standards: A comparative analysis from a healthcare perspective.* Unpublished doctoral dissertation, Nelson Mandela Metropolitan University.

O'Reilly, N., Mclene, C., Van der Stockt, T., Jackson, K., Sillo, O., & Hampt, L. (n.d.). *Levels of healthcare*. Retrieved from https://www.physio-pedia.com/Levels_of_Healthcare

Panian, Z. (2010). Some practical experiences in data governance. *World Academy of Science, Engineering and Technology, 62*, 939–946.

Pearce, G. (2017). *Align data governance with board governance imperatives*. Retrieved from https://tdan.com/align-data-governance-with-board-governance-imperatives/21355#

Polyzos, G.C., Marias, G.F., Fotiou, N., Fiedler, M., Herkenhoner, R., & De Meer, H. (n.d.). Privacy and governance considerations for the internet of things. In *2010 Proceedings of the 3rd Euro-NF IA. 7.5. Workshop on Socio-Economic Aspects of Networks of the Future*. Retrieved from http://www.net.fim.uni-passau.de/papers/Polyzos2010a

Pradhan, B., Bhattacharyya, S., & Pal, K. (2021). IoT-based applications in healthcare devices. *Journal of Healthcare Engineering, 2021*, 6632599. https://doi.org/10.1155/2021/6632599

Radoglou-Grammatikis, P., Rompolos, K., Sarigiannidis, P., Argyriou, V., Lagkas, T., Sarigiannidis, A., Goudos, S., & Wan, S. (2022). Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach. *IEEE Transactions on Industrial Informatics, 18*(3), 2041–2052. https://doi.org/10.1109/TII.2021.3093905

Raghuvanshi, A., Singh, U.K., Sajja, G.S., Pallathadka, H., Asenso, E., Kamal, M., Singh, A., & Phasinam, K. (2022). Intrusion detection using machine learning for risk mitigation in IoT-enabled smart irrigation in smart farming. *Journal of Food Quality, 2022*(3955514), 8. https://doi.org/10.1155/2022/3955514

Rahman, H., & Hussain, M.I. (2019). Fog-based semantic model for supporting interoperability in IoT. *IET Communications, 13*(11), 1651–1661. https://doi.org/10.1049/iet-com.2018.6200

Rezaeibagha, F., Win, K., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management Journal, 44*(3), 23–88. https://doi.org/10.12826/18333575.2015.0001.Rezaeibagha

Rotter, P. (2008). A framework for assessing RFID system security and privacy risks. *IEEE Pervasive Computing, 7*(2), 70–77. https://doi.org/10.1109/MPRV.2008.22

Sahd, L.M. (2015). *A structured approach to the identification of the significant risks related to enterprise mobile solutions at a mobile technology component level*. Unpublished masters dissertation, Stellenbosch University.

Saleh, M.M., AlSlaiman, M., Salman, M.I., & Wang, B. (2023). Combining raw data and engineered features for optimizing encrypted and compressed internet of things traffic classification. *Computers & Security, 130*, 103287. https://doi.org/10.1016/j.cose.2023.103287

Salimitari, M., Bhattacharjee, S., Chatterjee, M., & Fallah, Y. (2020). A prospect theoretic approach for trust management in IoT networks under manipulation attacks. *ACM Transactions on Sensor Networks, 16*(3), 1–26. https://doi.org/10.1145/3392058

Samy, N.G., Ahmad, R., & Ismail, Z. (2009). Threats to health information security. In *5th International Conference on Information Assurance and Security, IAS 2009, 18–20 August* (pp. 2540–2543). IEEE.

Sang, T., Zeng, P., & Choo, K.K.R. (2023). Provable multiple-copy integrity auditing scheme for cloud-based IoT. *IEEE Systems Journal, 17*(1), 224–233. https://doi.org/10.1109/JSYST.2022.3198098

Saqlain, M., Piao, M., Shim, Y., & Lee, J.Y. (2019). Framework of an IoT-based industrial data management for smart manufacturing. *Journal of Sensor and Actuator Networks, 8*(2), 25. https://doi.org/10.3390/jsan8020025

Selvan, S., & Singh, M.M. (2022). Adaptive contextual risk-based model to tackle confidentiality-based attacks in fog-IoT paradigm. *Computers, 11*(2), 16. https://doi.org/10.3390/computers11020016

Shrimali, R. (2020). *How IoT is transforming the healthcare industry*. Retrieved from https://embeddedcomputing.com/application/healthcare/telehealth-healthcare-iot/how-iot-is-transforming-the-healthcare-industry

Sicari, S., Rizzardi, A., Cappiello, C., Miorandi, D., & Coen-Porisini, A. (2018). *Toward data governance in the internet of things*. Studies in Computational Intelligence (pp. 59–74). Springer.

Sivaparthipan, C.B., Gnanasigamani, L.J., Agrawal, R., Awaji, B.H., Sathyaprakash, P., Jaber, M.M., & Khan Jumani, A. (2023). Internet of things enabled privacy-conserving health record virtual sharing using jungle computing. *Journal of Combinatorial Optimization, 45*(5), 111. https://doi.org/10.1007/s10878-023-01048-z

Smallwood, R. (2020). *Information governance, IT governance, data governance – What's the difference?* Retrieved from https://tdan.com/information-governance-it-governance-data-governance-whats-the-difference/26797

Subrahmanya, S.V.G., Shetty, D.K., Patil, V., Hameed, B.M.Z., Paul, R., Smriti, K., Naik, N., & Somani, B.K. (2022). The role of data science in healthcare advancements: Applications, benefits, and future prospects. *Irish Journal of Medical Science, 191*(4), 1473–1483. https://doi.org/10.1007/s11845-021-02730-z

Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., Xu, J., & Xiong, Y. (2016). Security and privacy in the internet of vehicles. In *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things*, 22–23 October (pp. 116–121). Institute of Electrical and Electronics Engineers.

Thamilarasu, G., Odesile, A., & Hoang, A. (2020). An intrusion detection system for internet of medical things. *IEEE Access, 8*, 181560–181576. https://doi.org/10.1109/ACCESS.2020.3026260

Trautman, L.J., Hussein, M., Molesky, M., & Ngamassi, L. (2020). Governance of the internet of things (IoT). *Jurimetrics, 60*(3), 315–352. https://doi.org/10.2139/ssrn.3443973

United States of America. (1996). *Health Insurance Portability and Accountability Act of 1996*. Retrieved from https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient%E2%80%99s%20consent%20or%20knowledge

Van Niekerk, A., & Rudman, R. (2019). Risks, controls and governance associated with internet of things technologies on accounting information. *Southern African Journal of Accountability and Auditing Research, 21*(1), 15–30. https://doi.org/10.10520/EJC-197ebe792e

Van Wyk, J., & Rudman, R. (2019). COBIT 5 compliance: Best practices cognitive computing risk assessment and control checklist. *Meditari Accountancy Research, 27*(5), 761–788. https://doi.org/10.1108/MEDAR-04-2018-0325

Verma, D., Singh, K.R.B., Yadav, A.K., Nayak, V., Singh, J., Solanki, P.R., & Pratap Singh, R. (2022). Internet of things (IoT) in nano-integrated wearable biosensor devices for healthcare applications. *Biosensors and Bioelectronics: X, 11*, 100153. https://do.org/10.1016/j.biosx.2022.100153

Vilakazi, K., & Adebesin, F. (2023). A systematic literature review on cybersecurity threats to healthcare data and mitigation strategies. In *Proceedings of Society 5.0 Conference 2023* (pp. 240–251). EPiC Series in Computing. Retrieved from https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=.+A+Systematic+Literature+Review+on+Cybersecurity+Threats+to+Healthcare+Data+and+Mitigation+Strategies&btnG=

Vongsingthong, S., & Smanchat, S. (2015). A review of data management in internet of things. *KKU Research Journal, 20*(2), 215–240. https://doi.org/10.14456/kkurj.2015.18

Wan, J., Waqas, M., Tu, S., Hussain, S.M., Shah, A., Rehman, S.U., & Hanif, M. (2021). An efficient impersonation attack detection method in fog computing. *CMC-Computers, Materials & Continua, 68*(1), 267–281. https://doi.org/10.32604/cmc.2021.016260

Wang, L., & Wyglinski, A.M. (2011). A combined approach for distinguishing different types of jamming attacks against wireless networks. In *Proceedings of the IEE Pacific Rim Conference on Communications, Computers and Signal Processing (*pp. 809–814). IEEE.

Wang, X., Huang, J., Qi, C., Peng, Y., & Zhang, S. (2023). An anti-collusion attack defense method for physical layer key generation scheme based on transmission delay. *PeerJ Computer Science, 9*, e1349. https://doi.org/10.7717/PEERJ-CS.1349

Wazid, M., Das, A.K., Rodrigues, J.J.P.C., Shetty, S., & Park, Y. (2019). IoMT malware detection approaches: Analysis and research challenges. *IEEE Access, 7*, 182459–182476. https://doi.org/10.1109/ACCESS.2019.2960412

Wheelus, C., & Zhu, X. (2020). IoT network security: Threats, risks, and a data-driven defense framework. *IoT, 1*(2), 259–285. https://doi.org/10.3390/iot1020016

Wing, J.M. (2019). The data life cycle. *Harvard Data Science Review, 1*(1), e26845b4. https://doi.org/10.1162/99608f92.e26845b4

Yin, M., Chen, X., Wang, Q., Wang, W., & Wang, Y. (2019). Dynamics on hybrid complex network: Botnet modeling and analysis of medical IoT. *Security and Communication Networks, 2019*(5), 1–14. https://doi.org/10.1155/2019/6803801

Yousefnezhad, N., Malhi, A., & Främling, K. (2020). Security in product lifecycle of IoT devices: A survey. *Journal of Network and Computer Applications, 171*, 102779. https://doi.org/10.1016/j.jnca.2020.102779

Zakaria, H., Abu Bakar, N.A., Hassan, N.H., & Yaacob, S. (2019). IoT security risk management model for secured practice in healthcare environment. *Procedia Computer Science, 161*, 1241–1248. https://doi.org/10.1016/j.procs.2019.11.238

Appendix 1

TABLE 1-A1: Detailed risks found within the Internet of Things architecture.

Risk category	Detailed risk
Unauthorised access: Impersonation	The following risks are the types of impersonation attacks that can take place in an IoT environment: **Sybil attacks** may occur where nodes presents several identities within a network by theft or fabrication of the identity of a legitimate node. An example of this is when an object appears to be in multiple locations which can hinder patient location (Selvan & Singh, 2022; Thamilarasu et al., 2020; Van Niekerk & Rudman, 2019). Similarly, attackers may modify IP addresses to impersonate an authorised node (Liang & Kim, 2021; Selvan & Singh, 2022). Unauthorised alteration of cookie content to gain unauthorised access to applications and web pages can occur more commonly known as **cookie poisoning** (Ashktorab & Taghizadeh, 2012). Furthermore, **poisoning attacks** that exploit the lack of security within mDNS can promote fake services directed at unaware nodes compromising data security (Nebbione & Calzarossa, 2020). Given the mobile nature of IoT, **GPS deception** can occur when a node provides false information about its location that can disrupt patient location tracking and may also impact ambulance tracking (Sun et al., 2016). Lastly, since IoT architecture uses cloud computing that requires data merging from multiple cloud clients resulting in data combination, the surface area of attacks by both organisations by association expands; putting both organisations at risk for data breaches (Ashktorab & Taghizadeh, 2012).
Unauthorised access: Network threats	The following risks impact authorisation and are situated within the network layer of IoT architecture: **A Crypt analysis attack** results in exploitation of weaknesses in cryptographic algorithms used to launch attacks by making use of weak points to decipher secret codes (Selvan & Singh, 2022). **Collusion** occurs when multiple malicious nodes work together to destroy the security of the system, by conspiring to steal keys used to encrypt the data resulting in unauthorised access and data tampering (Wang et al., 2023). **Data traffic classification errors** can occur when data traffic classification systems incorrectly classify unencrypted compressed data as encrypted and vice versa, thus compromising the security of all data being received (Saleh et al., 2023). Moreover, various injections may create opportunities for unauthorised access such as **SPARQL injections** that allow attackers to access the back end of the database by the transmission of SPARQL commands that have not been validated (Van Niekerk & Rudman, 2019). In addition, **code and database injections** occur when attackers pinpoint vulnerable entry points and inject malicious scripts that can overtake the entire network (Liang & Kim, 2021; Selvan & Singh, 2022). On the other hand, an account hacking threat known as a **Man-in-the-middle** attack allows for the interception and alteration of data and is highly successfully when impersonating other things or resources (Hady et al., 2020; Liang & Kim, 2021; Selvan & Singh, 2022; Sicari et al., 2018; Van Niekerk & Rudman, 2019; Vilakazi & Adebesin, 2023). For example, data alteration that allows an attacker to make changes to parts of the data collected by an IoT device that were redirected to the attacker from the device (Hady et al., 2020). **Message tampering** often occurs when RFID tag content is altered by deleting and modifying tag data allowing for unauthorised access (Islam et al., 2015; Selvan & Singh, 2022; Van Niekerk & Rudman, 2019). **RFID cloning** of an original RFID tag allows for unauthorised access to the network and restricted areas whereby private and confidential data can be abused (Selvan & Singh, 2022; Van Niekerk & Rudman, 2019). Similarly, **Masquerading –** often closely linked to RFID cloning – can compromise authorisation when multiple nodes have identical identification creating a platform for data alteration, destruction and network compromise among others (Sun et al., 2016).
Unauthorised access: Data loss	Data loss can occur at any point within the IoT architecture and poses a pervasive threat. The most common threats found in this research are: **Data loss by intentional action** occurs when data is altered or deleted by malicious attackers who can gain unauthorised access to data or by authorised users who alter or delete data from within an organisation for example, internal attack from within the organisation (Brous et al., 2020). While data loss by **unintentional action** occurs when alteration or deletion of data occurs by authorised individuals within an organisation or database administration accidentally, it can also occur because of **insufficient user training**, a lack of training and education on IoT as well as a lack of appropriately skilled individuals who can properly implement and manage IoT device usage within an organisation (Brous et al., 2020). Where there is a lack of training and education, it creates opportunity for **social engineering** whereby attackers can trick end users, allowing the tricksters to obtain and use sensitive data to control or manipulate the device for example, phishing (Liang & Kim, 2021; Malhotra et al., 2021; Vilakazi & Adebesin, 2023). **Device failure** results in in memory interruptions, hardware failure, software failure or cloud server failure which can also be caused by data recovery failure (Islam et al., 2015; Vongsingthong & Smanchat, 2015). While **sleep deprivation attacks** can lead to data loss through device exhaustion when malicious nodes make requests to other nodes multiple times to keep all the nodes active (Selvan & Singh, 2022). Consequently, the risk device failure or sleep deprivation are amplified where there is a **lack of secure backup and restore mechanisms** that render the device unable to recover data in cases of disaster (Boeckl et al., 2019). Other external factors such as **environmental elements** may harm the device for example, extreme heat. This can disrupt sensors and leave them unstable and unreliable when gathering data, resulting in inaccurate readings (Khan et al., 2023). **Theft** on the other hand can result in control or tampering of the devices. This includes hacking or attempting to gain unauthorised access to data on the device, network or database conducted via a wormhole attack using malicious links which creates network isolation by establishing a direct tunnel whereby attackers can send packets between two malicious nodes, bypassing all other nodes in the network (Aydos et al., 2019). Or via **rootkit attack** that uses malicious malware to remotely control the IoT device without being detected (Khera, 2017; Wazid et al., 2019; Yin et al., 2019). Or via a **trojan virus**, a form of software attack, which allows an attacker to steal data by parading as a legitimate programme (Kamal et al., 2023; Khera, 2017; Yin et al., 2019).
Network availability: Interference	Network interference can be perpetrated through a number of attacks aiming to disrupt the network in five unique ways: Firstly, using **desynchronisation attacks** causing interference between smart object parameters that communicate synchronously. This attack can cause the network to stop functioning properly resulting in transmission errors and delays (Aydos et al., 2019). Secondly, a **storage attack** can create unnecessary noise within the network or high frequency pulses interrupting packet transmission thus creating packet loss on the end of the receiver (Khan et al., 2023). Thirdly, **radio frequency interference** allows the attacker to use a device to hamper the connectivity of an IoT device by interfering with the frequency used for wireless communication (Liang & Kim, 2021). Fourthly, **RFID tag limitations** in range can cause the signal to drop at any point or be affected by dead spots, resulting in errors in data transmission (Vongsingthong & Smanchat, 2015). Lastly, **On-off attacks** can occur when an attacker behaves erratically disguising itself as temporary unintentional noise, masking its intrusion into the network (Salimitari et al., 2020).
Data privacy and confidentiality: Architectural deficits	Within IoT architecture, there are several deficiencies that can hinder the protection of patient data privacy and confidentiality. These include: A **lack of privacy mitigation mechanisms** within IoT architecture that fails to support privacy configurations and support mechanisms for example remote activation prevention results in data breaches (Boeckl et al., 2019). Building on this, a **lack of digital footprint privacy** leaves the digital footprint of IoT devices exposed and open to exploitation since these devices are always connected to the Internet for data transmission (Kamal et al., 2023). Often IoT architecture also does not support encryption by design throughout the IoT architecture (Kamal et al., 2023). There are also **verification challenges** as there is no way of verifying a device; IoT devices are unable to identify one another before the transmission of sensitive data, resulting in sensitive medical data being sent to unauthorised parties (Boeckl et al., 2019). When considering masquerading attacks, verification challenges could also be a contributing factor to data security risks. **Device tampering** also poses as a threat since physical access to the device can be obtained resulting in total control of the device by altering the device or replacing it with one embedded with malicious code (Islam et al., 2015; Jha et al., 2022; Liang & Kim, 2021; Van Niekerk & Rudman, 2019). Another risk pertaining to device location is **wireless probing** that causes a breach of users' privacy as their location can be tracked via the tracking of electronic product codes and RFID chips (Polyzos et al., n.d.). Pertaining to data, **data ownership ambiguity** arises from data amalgamation and decentralised data processing within IoT that can result in non-compliance with regulations for example HIPAA (Boeckl et al., 2019). At same time, **cross border data transfers** may result in the non-compliance with laws and regulations; and can expose private data to attacks as different privacy requirements are implemented by different regulatory bodies in different regions (Ashktorab & Taghizadeh, 2012). Lastly, a lack of appointment of a qualified privacy official to develop and implement privacy policies and procedures ensuring the privacy and confidentiality of PHI as required by HIPAA leads to gaps in privacy initiatives to protect data (HIPAA United States of America, 1996).

IP, internet protocol; IoT, Internet of Things; GPS, Global Positioning System; mDNS, Multicast Domain Name System; RFID, radio frequency identification; HIPAA, Health Insurance Portability and Accountability Act; PH, protected health information.

Appendix 2

TABLE 1-A2: A risk-technology-based matrix: Linking the architectural layers of Internet of Things to the relevant associated risks.

Risk category and section in text	Risk	Architectural layers of IoT								
		Coding layer	Perception layer		Network layer		Middle layer		Application layer	
		RFID	Sensors	IoT device	Transmission mediums	Communication protocols	Cloud server	Fog nodes	APIs	Application software
Data security: authenticity	Sybil	X			X					
	Spoofing			X	X	X	X			
	Data combination						X			
	Lack of policies and user guidelines	X	X	X	X	X	X	X	X	X
	Cookie poisoning						X	X	X	X
	GPS deception		X							
	Poisoning							X	X	X
	Weak authentication	X	X	X	X	X	X	X	X	X
Data security: unauthorised access	Crypt analysis				X		X			
	Collusion	X	X	X	X	X	X	X	X	X
	Cloud server breach						X	X		
	Poorly skilled service provider						X			
	Untrusted cloud server						X	X		
	Insecure APIs								X	X
	Incorrect bootstrapping				X	X			X	
	User compromise			X	X					
	Wi-Fi-based attack				X				X	
	XSS attack								X	X
	Code and database injection						X	X		
	SPARQL injection					X	X			
	CT-GAN					X				
	Data traffic classification errors				X	X	X	X	X	X
	Web attack								X	X
	Masquerading			X		X				
	Man-in-the-middle				X		X			
	Device failure			X						
	Data alteration				X					
	Rootkit			X						
	Reverse engineering	X	X	X						
	Intentional action	X	X	X	X	X	X	X	X	X
	Unintentional action	X	X	X	X	X	X	X	X	X
	Social engineering	X	X	X	X	X	X	X	X	X
	Sleep deprivation attack		X	X	X					
	Wormhole attack			X	X	X	X			
	Trojan virus			X						
	Environmental elements	X								
	Lack of secure back-up and restore mechanisms	X	X	X	X	X	X	X	X	X

Table 1–A2 continues on the next page →

TABLE 1-A2 (Continues...): A risk-technology-based matrix: Linking the architectural layers of Internet of Things to the relevant associated risks.

Risk category and section in text	Risk	Architectural layers of IoT								
		Coding layer	Perception layer		Network layer		Middle layer		Application layer	
		RFID	Sensors	IoT device	Transmission mediums	Communication protocols	Cloud server	Fog nodes	APIs	Application software
	Message tampering			X	X					
	RFID cloning		X							
	U2R				X	X				
	R2L				X					
Data security: Network availability	Jamming				X					
	Selective forwarding			X	X					
	Network properties attack					X				
	Probe attack				X					
	Desynchronisation				X					
	Storage attack				X					
	On-off attack				X					
	Flooding				X					
	Hello flood attack				X					
	Routing loop attack				X	X				
	Botnet attack		X		X		X			
	Remote code execution				X					
	Portscan			X						
	Radio frequency interference			X	X					
	Relay attack	X			X					
	RFID tag limitation	X								
Data security: Data security planning	Lack of organisational security strategy	X	X	X	X	X	X	X	X	X
	Deficient organisational security management strategy	X	X	X	X	X	X	X	X	X
	Lack of decommissioning policies	X	X	X	X	X	X	X	X	X
	Lack of security auditability	X	X	X	X	X	X	X	X	X
	Black box effect	X	X	X	X	X	X	X	X	X
	Limited upgradability	X	X	X	X	X	X	X	X	X
	Incompatible systems	X	X	X	X	X	X	X	X	X
	Lack of adequate policies and user guidelines	X	X	X	X	X	X	X	X	X
	No appointed security official	X	X	X	X	X	X	X	X	X
Data privacy and confidentiality	RFID tag cloning		X							
	Eavesdropping				X					
	Data sniffing				X		X			X
	Device tampering			X						
	Man-in-the-middle				X		X			
	Data alteration				X					
	Lack of privacy mitigation mechanism		X	X	X	X	X	X	X	X
	Lack of digital footprint privacy	X		X						
	Remote code execution				X					
	Untrusted cloud server						X	X		
	Incorrect bootstrapping				X	X			X	
	Lack of encryption				X					

Table 1–A2 continues on the next page →

TABLE 1-A2 (Continues...): A risk-technology-based matrix: Linking the architectural layers of Internet of Things to the relevant associated risks.

Risk category and section in text	Risk	Architectural layers of IoT								
		Coding layer	Perception layer		Network layer		Middle layer		Application layer	
		RFID	Sensors	IoT device	Transmission mediums	Communication protocols	Cloud server	Fog nodes	APIs	Application software
	Verification challenges	X	X	X	X	X	X	X	X	X
	U2R				X	X				
	Data ownership ambiguity	X	X	X	X	X	X	X	X	X
	Cross-border data transfer	X	X	X	X	X	X	X	X	X
	Data combination						X			
	Wireless probing	X								
	Internal attack	X	X	X	X	X	X	X	X	X
	Social engineering	X	X	X	X	X	X	X	X	X
	Phishing	X	X	X	X	X	X	X	X	X
	Collusion	X	X	X	X	X	X	X	X	X
	Crypt analysis				X		X			
	Lack of policies and user guidelines	X	X	X	X	X	X	X	X	X
	No privacy official	X	X	X	X	X	X	X	X	X
	Cloud server breach						X			
	Sleep deprivation attack		X	X	X					

IoT, Internet of Things; RFID, radio frequency identification; APIs, Application Programming Interfaces; GPS, Global Positioning System; XSS, cross-site scripting; CT-GAN, computed tomography-generative adversarial network; U2R, user to root; R2L, remote to local.