JSST-RL

Journal of Sustainable Science and Transformative Research – Reviews & Letters, Vol 3 (1), 140-146 (2024)

Analysis of Privacy and Safety Concerns Regarding the Internet of Medical Things

ISSN: 2583-4118
doi:https://doi.org/10.56703/OKGY7002/Fibg8949/NNNH7652
www.jsst.uk

Md Afroz, Birendra Goswami, Satish Kumar Pandey[1]
[1] *Sai Nath University, Jharkhand, Ranchi, India*
Email id: afrozhasnain@gmail.com

Abstract: Microcomputing, mini-hardware manufacturing, and machine-to-machine (M2M) communications have advanced rapidly, enabling revolutionary Internet-of-Things (IoT) solutions to transform numerous networking applications. The Internet- of-Medical Things (IoMT) branch of IoT has transformed healthcare systems. IoMT systems allow chronic illness patients to be remotely monitored. As a result, it can rapidly identify patients to preserve their lives in emergencies. On their mobile devices, patients and healthcare professionals access, distribute, and analyze medical data. Ransomware and other assaults target IoMT devices because they store so much important data. As numerous actuators reuse these assets in CE, the problem is worsening. Medical consumers and producers underinvest in IoMT security because they are ignorant of the risks. However, knowing and relevant controls can greatly reduce vulnerability risk. This article discusses the key security and privacy controls needed in modern IoMT environments to protect users and stakeholders. The approach is a CE-based best-practices guide for safe IoMT system implementation.

Keywords: Internet of Medical Things (IoMT), IoMT security, e-health, healthcare infrastructure

1 Introduction

By 2025, the market for IoT-enabled devices will surpass $58 billion, predicts Gartner [1]. These large numbers of linked gadgets make them a more and more alluring target for attackers. Due to the discovery of numerous IoT flaws by academics and their successful exploitation by attackers, IoT security is now a top concern for the main Informatics companies (e.g., smart cars [2] and smart lighting [3]). According to Business Insider's IoT security study, the graphic below depicts predictions for the cybersecurity industry through 2030.

The security of IoMT devices and healthcare systems in general (thus, IoMT systems) remains a major hurdle. All stages of data gathering, transmission, and storage should be secure in IoMT systems that handle healthcare data. IoMT devices are potentially exploitable to some extent, according to the 2020 CyberMDX study. IoMT systems stand out from other systems because they have the ability to affect patients' lives and cause problems with respect to privacy if patients' names are made public. Additionally, the cost of healthcare data is 50 times higher on average than the cost of credit card data, rendering them very valuable on the black market

Security is therefore one of the essential requirements for the IoMT method to succeed. To provide data confidentiality, integrity, availability, nonrepudiation, and authentication, these systems must fulfill a total of 11 security criteria, known as CIANA [4]. These demands can be satisfied by even more traditional security choices. However, because of their power consumption and other system requirements, conventional techniques might not offer sufficient security guarantees. Instead, a number of approaches tailored especially for IoMT and IoT systems have been proposed by researchers. These techniques can be divided into three groups: Keyless noncryptographic encryption, symmetric cryptography, and asymmetric cryptography.

2 Literature Review

Most reviews of IoMT systems discuss their shortcomings, security issues, and remedies. In the case of wireless body area networks (WBANs) and IoMT systems, Hajar, M. S. [5] distinguished between cryptographic and noncryptographic security methods. They categorize the countermeasures into four groups: authorization, availability, and consciousness. Wang, Hongping, et al [6] investigated the remaining difficulties in these networks, such as adaptability, single points of failure, and managing emergencies.

IMDs, RFID tags, and wearable sensors are just a few examples of IoMT devices that have been reported to have various security issues. In various IMDs, including pacemakers, hormone pumps, defibrillators, and stomachal electrical stimulators, Yang et al. [7] highlight key security challenges (GES). The assessment found that IMDs' inadequate battery capacities were to blame for the facility denial attack that occurred. Halperin et al. looked at pacemakers and permanent internal organ defibrillators (ICDs). In order to lessen radio assaults and hacking efforts, the author adopted a zero-power security strategy. It was found that the suggested approach might take care of some of the security problems that frequently surfaced in ICDs. Radcliffe et al. created a completely machine-controlled closed-loop system to minimize human contact during communication between IMDs and external devices, increasing security.

According to Yu, Zhiyuan, et al. [8], a weak communication link between IMDs and external devices like smartphones, smartwatches, and sensible bands led to a hijacking attack. The author, however, suggested using a body-coupled communication route to lessen the impact of an IMD-hijacking attack. Internal organ machine-controlled external electronic device (CAED) remote control of the device through updated bespoke computer code is one of the serious security issues. Hanna et al. distributed formal code analysis of security evaluations of medical devices to thwart this attack. Electronic version accessible at: https://ssrn.com/abstract=3944800, which supported this analysis. He advised patients to confirm the accuracy of the code updates coming from etch sources. The suggested work also emphasises how using encrypted communication might increase the reliability of code changes.

To prevent device biological research difficulties, Daniluk et al. planned a non-public key encrypted knowledge utilisation in IMDs. The device biological research question brought up by device ID and computer file pattern prediction was examined by the author. Additionally, Xu et al. [8] developed a Physical Un-cloneable Operate (PUF) technique based on cryptography to address the problem of knowledge pattern prediction. The research on identifying security flaws in ICDs was distributed by Hosseini Khayat et al. The majority of devices lack cryptographic functionality. ICDs are experiencing

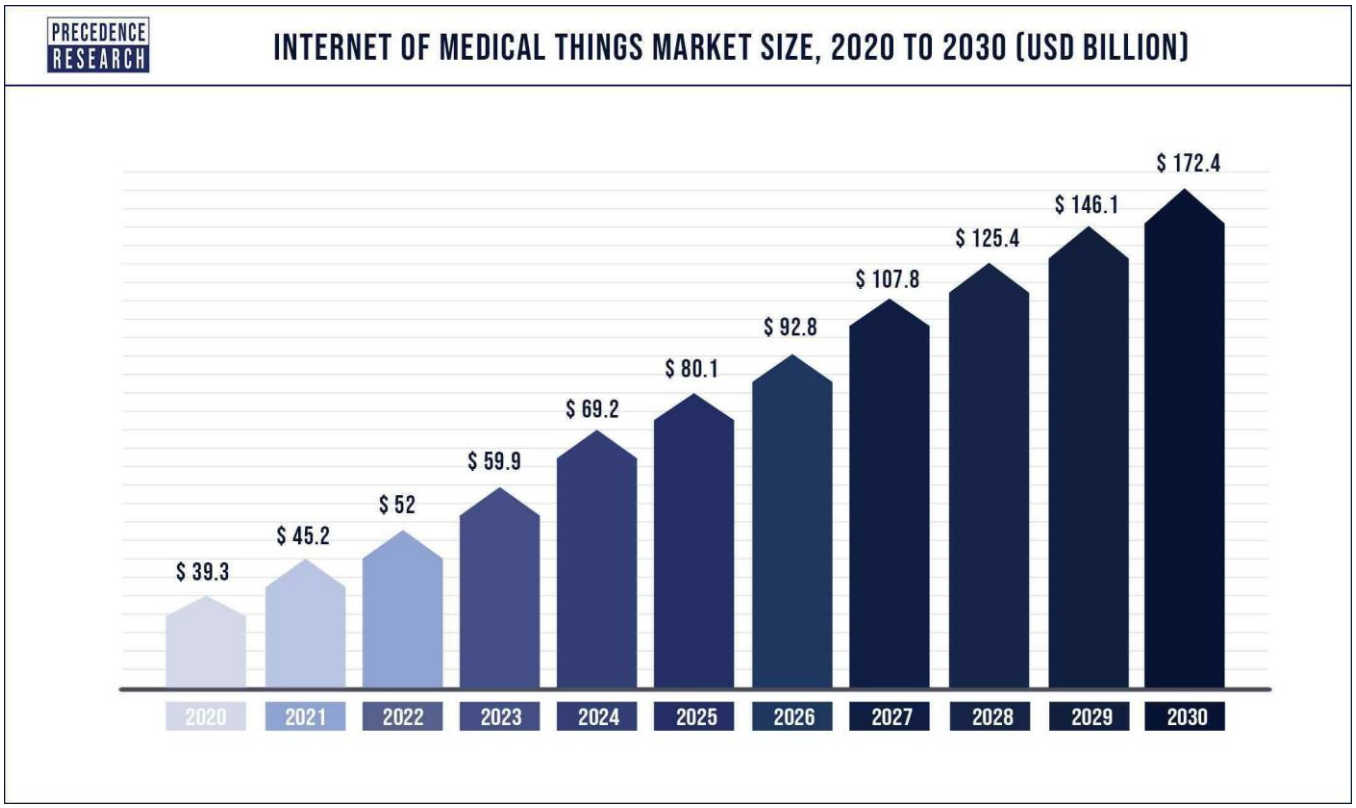

Fig. 1: IoMT -IoT Applications in Medical [21]

Fig. 2: Internet of Medical Things Market Size

issues with message change of state as a result. To improve IMD authentication, Xu et al. designed the wearable external guardian (IMDGuard) using the EKG-based key agreement technique. However, IMDGuard has the drawback of requiring changes to already installed devices.

To such questions, numerous researchers offered a solution, but the solution isn't quite clear. Cameras et al. [9] reviewed the security issue that is related to the most recent IMDs, and he planned a solution to strengthen the security mechanism in IMDs, which audits devices to find changes and strengthens security by utilising cryptologic solutions, enforcing access management, and biometric measures. Wang et al. were alert to the problem and provided a thorough analysis of the security concerns in wireless detector networks. The previous assaults in the various layers of IoT stated were backed by flaws and adjustments needed. RFID tags have been shown to interfere with ICD magnetism by Stachel et al.

He created a regular electromagnetic compatibility check structure to stop electromagnetic contamination inside the IMDs. a novel embedded IoT system that Sachin, a fictional character, and other people are developing. In IoT embedded devices, the framework seeks to handle security risks like physical, facet channel, software, network, and scientific field assault. It includes tamper-resistant, secure execution, a secure network environment, secure electronic contact, secure knowledge management, secure identity management, and secure storing. It also includes protective user authentication. Joshua, Salaki Reynaldo, Wasim Abbas, and Je-Hoon Lee. [10] developed a degree design for Assisted Living (AAL) applications that are connected to mobile health. He mentioned how RFID technology is being widely used for mobile health monitoring. The main advantage of RFID is the potential for information reading without direct interaction. It is still feasible to receive the data even if the RFID technology is embedded under the patient's skin. By utilizing historical knowledge management, visualisation, and information storing functions, Abinaya et al. created a degree eco-health observation system that provides a benefit in tracking the health of patients. However, history study, quantitative analysis, and qualitative analysis were all mixed.

Additionally, there are security concerns with the Eco-Health Observation System, security issues with ontology-based frameworks, reduced viability with SDN, implementation issues with closed-loop approaches, complexity with RFID technology, and security issues with lightweight protocols. The procedure of secured communication through IoMT is complicated by the challenges and security issues that have been identified.

Additionally, IoMT might broaden the attack surface of contemporary e-health. The computerised insulin pumps manufactured by Johnson and Johnson are susceptible to hacks, the company has declared. An impartial security professional identified the issue after studying the devices' communication interfaces and utilising it with patience for some time. Although there is a low likelihood that the weakness will be abused, related products represent a major and expanding tendency in modern healthcare technology (e.g. pacemakers and defibrillators). This novel type of danger is posed by such tools. In order to better understand the security and private features provided, risk analysis is essential for the healthcare system.

Thus, participation in and the success of the sociotechnical health environment are seriously threatened by security and privacy considerations. At this point, it is obvious that security must conform to all existing laws and regulations and be adaptable enough to meet new demands, technological hurdles, and legal responsibilities.

The most recent approaches to the problem are reviewed in this study.

It functions as a practical guide for developing cutting-edge IoT and IoMT applications while also taking into consideration CE's enduring contributions to the healthcare industry. The assessment includes the protective measures that must be obtained from the device to the cloud endpoints (E2E), and from the processing, transportation, and data retention to the reuse or destruction of the associated equipment.

3 The Internet of MEDICAL Things' ARCHITECTURE

3.1 Forms of IoMT

For a number of medical disorders, IoMT systems provide the necessary or better support. For some medical situations, implantable devices are necessary, such as pacemakers for cardiovascular problems. Fig. 1. shows examples of IMDs and where in the body they might be found.

For a better healthcare experience, helping gadgets are typically wearables, such smartwatches. These variations divide the IoMT systems into two groups:.

4 Implantable medical devices (IMDs :

An IMD is any implanted device that replaces, supports, or improves a biological structure. A pacemaker, for instance, is an IMD that aids in controlling aberrant heart rhythms by encouraging the heart to beat normally if it is beating too quickly or slowly [11].

The locations of numerous well-known IMDs in the human body are shown in Fig. 1. Infection and cable breakage problems with wired IMDs have lately been proposed as solutions by using wireless IMDs . IMDs frequently have very tiny cells with very long battery lives. Therefore, low power usage, limited storage space, and small batteries that last a long time are essential requirements for these devices to remain inside a human body for an extended period of time. As an illustration, pacemaker implants usually last 5 to 15 years [11].

5 Internet of Wearable Devices (IoWDs :

These are devices people wear to track their biometrics, such as their heart rate, and may help people have better general health. Examples include electrocardiogram (ECG) monitors, blood pressure monitors, fall detection bands, smartwatches, and more.

Smartwatches are currently one of the most well-known IoWDs for monitoring biometrics, such as heart rate and mobility. The tracking can be used to detect slow and fast heartbeats when the subject is not moving. The most recent wristwatches now have fall detection and ECG data for conditions like atrial fibrillation (irregular heartbeat). They are presently used a lot for non-critical patient monitoring.

However, these gadgets are unlikely to take the place of IMDs in emergency circumstances due to their poor sensor accuracy and short battery life.

6 Systems Architecture for IoMT

Most contemporary IoMT devices are usually divided into four layers. These layers encompass each data stage, from the stage of gathering a person's biometric data to the storage of the data and subsequent viewing by a doctor for analysis. The patient can also access their cloud-based general health condition. Given that IMDs can communicate with gateways, IMDs and IoWDs largely share the same design at this time.

1. Sensor Layer: Small implanted or wearable sensors capture patient biometrics. Wi-Fi, Bluetooth, or MedRadio frequency (RF) spectrum for IMDs send data to the second layer.

2. Gateway Layer: Data are sent to the gateway layer without processing because IoMT sensors have limited computational and storage capacity. In most cases, a patient's smartphone or a specific access point (AP) is more potent than monitors. They can validate, briefly store data, and run basic AI-based analysis. Additionally, they put sensor data live in the cloud.

3. Cloud Layer: Data from the gateway is stored in the cloud layer, where it is also analyzed and secured. Data processing may show

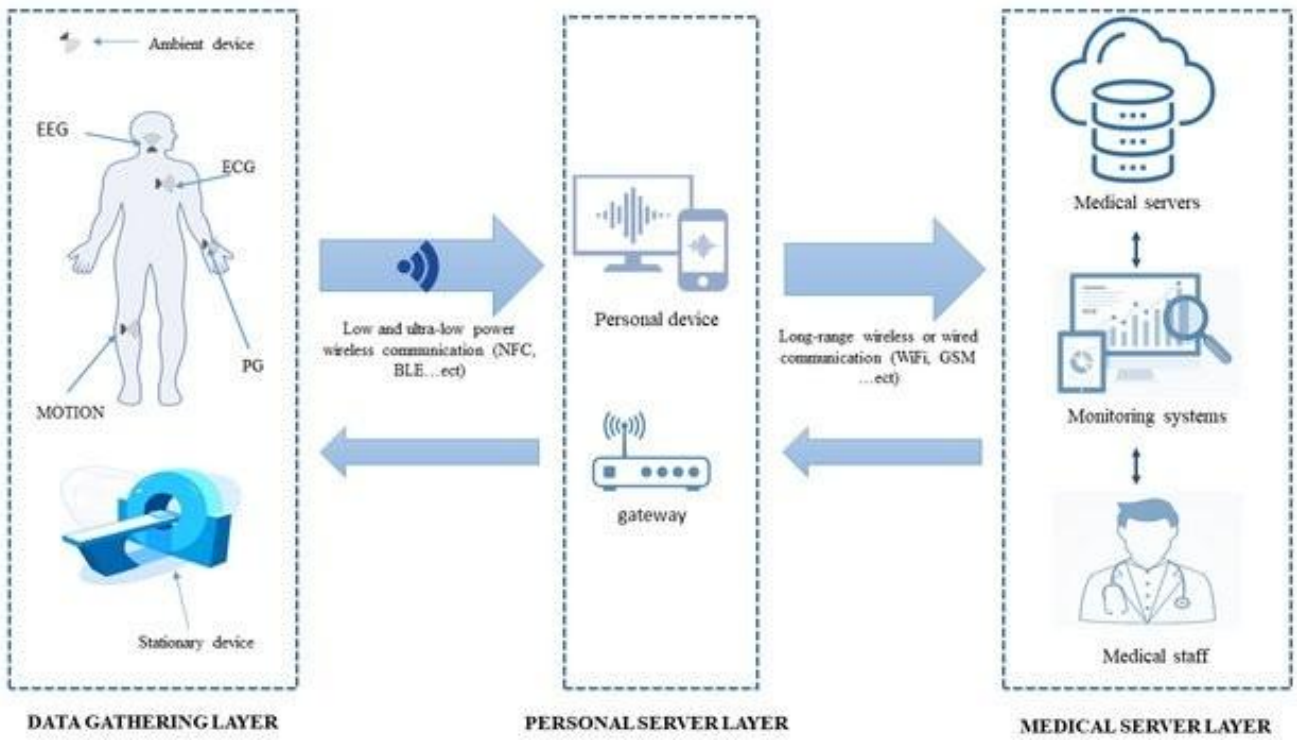

Fig. 3: IoMT Architecture

changes in health and educate patients and doctors. System components' IDs and keys are generated by KGS. This layer regulates distant sensor access..

4. Visualization/Action Layer: This layer shows doctors and patients health data. This layer comprises the doctor's health-related recommendations, Prescriptions and dose changes are examples.

7 IoMT Security Needs

Due to the sensitivity and safety of patient data, IoMT systems must meet all security criteria.

Microsoft, IBM, Siemens, Gemalto, and other significant computer and software providers recommend the following security areas for IoT development:

Security of the Device: The phrase "security of the device" describes the procedures and tactics used to safeguard the device once it has been placed in use.

Safety of Network Connections: It describes the procedures and techniques used to guarantee that the information transferred between Internet of Things devices and the Internet of Things Hub or Gateway is safe and unaltered.

Secure Cloud: Secure Cloud refers to the procedures and protocols that are used to protect data both while it is being uploaded to the cloud and while it is being stored there.

Following is a snapshot of the current state of the art regarding Internet of Things (IoT) security, organised according to the three primary topics outlined earlier.

7.1 Security of the Device

Device security is the implementation of the different components for device authentication in an Internet of Things application. Two essential components are required to achieve this goal: a unique security token or identity key for each individual device. The gadget uses this key to communicate with the IoT gateway and to authenticate its own identity to it. To connect the device to the IoT gateway, the device stores a local copy of its private key and X.509 certificate. The authentication system must make sure that this private key is never publicly disclosed and is never known to anyone other than the device at any time in order to achieve a higher degree of privacy. For every exchange that is made between the device and the IoT gateway when everything is working as it should, the device token is used to provide authentication. As a result, every operation is associated with the symmetric key. The X.509-based method makes it possible to conduct device authentication at the physical layer while the TLS connection is being established (connectivity security). [13]. The certificate includes data about the devices, which would include their ID and other details. It also includes details about the business. The security token can also be used independently, but doing so creates a less secure setting because it does not need X.509 authentication. The primary factors that influence the choice between the two methods are the availability of appropriate resources on the device end (for example, the ability to store the private key in a secure location) and the level of authentication security that is needed by the application.

8 Safety of Network Connections

Internet-connected IoT devices pose data security risks. Thus, all device-to-IoT gateway-to-cloud data must be secured.

The IoT gateway authenticates devices and services with security tokens. IoT platforms automate it. The security measures of essential protocols including AMQP, MQTT, and HTTP support seamless communication [12]. The proper use of security credentials should be verified in each situation because different underlying systems handle them in different ways. This technological problem entails mapping token-related data to the data format of each protocol. While HTTP uses the valid token in the authorization request header, MQTT uses the device ID as the username and the security token as the password. Users must generate and use security tokens in order to use certain program options. Examples include using AMQP, MQTT, or HTTP directly.

Device IDs and security keys are stored in an identity directory by the IoT gateway. Add devices or groups to a list of allowed or forbidden devices to completely control device access. High-level device provisioning entails: Associating a device identification

and/or X.509 certificate with the real device during manufacture or commissioning. Create an appropriate entry in the identification registry for the gateway. Register the fingerprint of the X.509 certificate in a secure manner. The device must authenticate the gateway. The details for the gateway are validated by a root certificate from the device software development kit SDK. Despite their durability, root credentials are subject to expiry or revocation. In order to prevent the IoT devices from being unable to connect to the IoT gateway or cloud services, a secure method must be designed for updating the root certificate on the device end. Last but not least, the gateway-device Internet link is secured by SSL/TLS 1.2 standards. Older protocols might be maintained for backwards compatibility (i.e., TLS1.1, TLS 1.0).

9 Secure Cloud

Cloud computing security vulnerabilities can have grave effects if ignored.

Shared technologies: An attacker can use shared memory technologies to steal encryption keys.

Data breach: Credit card data can be lost or disclosed.

Account/service hijacking: Access to critical services can be gained by attackers using leaked login information, jeopardizing secrecy, integrity, and accessibility.

Denial of Service (DoS): Cloud infrastructure defense mechanisms scale up their resources in response to DoS attacks, but this gives the intruder more resources to carry out his harmful objectives and may have financial consequences.

Malicious insiders: A firm employee may obtain data from hosted services..

Datacenters need high-level physical security to prevent physical access assaults. To prevent insider attacks, XACML can limit employee access. KAISER kernel space isolation can prevent side channel attacks. Intel trusted execution technology, which installs and runs the Virtual Machine Monitor (VMM) or Operating system kernel, has a serious flaw as described If an attacker has physical access to the servers, he can easily access it. Developers can employ abuse patterns as a repository for attack security. Intruders can be stopped by system called intrusion detection systems (IDS) that watch for and identify harmful behavior. A hybrid intrusion detection system can be used in the cloud due to its intricacy.

Sniffing and Spoofing Attacks can be prevented by using an encrypted network protocol that encrypts all traffic from source to destination. SSL and TLS encryption can protect sensitive data. CPs also employ IPsec, a protocol suite for IP packet authentication and encryption. VPN, SSH, and IPsec tunnels are used to protect cloud network traffic between servers. [14].

9.1 Other Security Modules

Modern IoT ecosystems may need other critical goods besides devices, networks, and platforms. These include security products and tamper-resistant solutions for SIM, TPM, and HSM devices (HSM).

Nowadays, a subscriber identification module (SIM) is a common component of mobile Internet of Things devices. This integrated circuit safely stores the international mobile subscriber identity (IMSI) number and key. Subscriptions are identified and verified using this data. There is no way to alter the SIM info because it is hardcoded into the chip. As a result, whenever the operator of a device moves, the SIM card needs to be replaced.

In the IoT, the embedded SIM (eSIM) card solution facilitates M2M device communication. Reprogrammable eSIM modules allow remote operator subscription provisioning. Thus, it is essential for M2M communications, enabling easy mobile connectivity of all communicating devices. Card sizes and shapes vary. When cards don't need to be switched, the chip is kept in a machine that shields it from extremes in temperature, humidity, and vibration. The user automatically updates the settings when the operator changes, enhancing usability and enhancing apparatus safety. This is necessary for commercial operations, intelligent transportation systems, and precision agriculture. Gemalto and GSMA are popular eSIM vendors. The interfaces mimic mobile operator SIM personalization procedures. Another class of M2M SIM cards protects device identities and uses secure authentication and ciphering on cellular network

10 PRIVACY

Controls on information security by themselves are not sufficient for today's environments. In recent years, there has been a significant increase in the amount of attention paid to the preservation of individuals' privacy, particularly in relation to electronic health applications.

10.1 Private Data

Numerous private information packets are sent through the underlying systems in IoMT apps. This raises significant privacy-related concerns, making it crucial for end users to put in place appropriate protection measures. In an attempt to address these issues, a number of laws and standards (such as the GDPR of the European Union - Regulation (EC) 2016/679) are being created. The ISO/IEC standards 27018 and 29100 are among them.

The term "Personal Identifiable Information" (PII) refers to the type of information that can be used to identify a specific individual. It is possible to classify the data as personal sensitive, sensitive, or scientific, with the first group needing the highest level of privacy protection. However, since statistical data is frequently made public through survey reports, it only needs a moderate level of security.

In addition, three different types of actuators are specified, which marshal the authority over private data and the related processing rights. The person to whom the data refers is known as the PII principle or owner, and they are required to have complete control as well as all legal rights to the data. The term "PII contracted processor" refers to an individual or organization that has been given permission by the PII principal to process his or her personally identifiable information (PII) for a specific reason. The organization is permitted to use the data for the intended purpose under this agreement. The processor is restricted and is not permitted to use the data in a way that would contravene their shared arrangement with the principal. Despite this, it might be necessary for the processor to disclose the PII to a third party in order for the processor to provide the required functionality. The processing terms and access privileges correspondingly restrict the use for the third party, and the processor is needed to obtain the principal's unqualified consent. In the case of a breach, the proprietor of the PII is responsible for holding the contractual processor and any other third parties accountable.

10.2 Mechanisms for providing protection

Privacy concerns include harmful or non-malicious occurrences that influence protected PII, such as smart home equipment connection vulnerabilities or wearable fitness monitoring device data leak. Transmission and storage must protect private data. The CIA principles are protected by the security methods in the previous subsections.

ISO/IEC standards 27018, 29100, and Regulation (EC) 2016/679 define the general privacy framework and attributes. The following table lists these efforts' major privacy attributes and particular protection techniques.

IoMT devices can be controlled. Minimize sampling rate, data amount, recording length, parameters, and application data volume. [15].

Limit data storage and retention. Thus, avoid storing data longer than necessary. In order to protect data sources and user-related information (such as location) from hackers, edge computing should be encouraged to process as much data as is feasible at the field layer. By removing PII, data should be anonymized to prevent unintentional exposure. Instead of giving out the exact address, use location-related information instead, and store data safely. Applications, services, or users should be prevented from repeatedly

requesting specific data if they don't plan to use it in this way. (For instance, "the majority of individuals that visited the examined area in this time interval were young students" is adequate knowledge for a neighboring shop's ad application without processing raw data from the personal IoT devices).

10.3 Anonymity and Identification

Every privacy strategy prioritises user identification. Integrating many data sources may allow an opponent to link trade data to a single person. The user may choose to remain anonymous to the service provider. Thus, user access to an application affects privacy. The requested functionality determines three user access types:

In e-government and social-media platforms, authenticated users must login and utilise the service using their own identity. The user's behavior may be tracked by the system, and the service supplier is aware of who they are. User is aware and gives permission. The provider and any unauthorized users or attackers who obtain access to this information may use it. In these cases, security and private constraints (such as storing encrypted data within a database and minimizing personal information) must be applied to limit the negative effects.

Pseudonyms hide users. This offers sufficient privacy for many purposes. Context can still reveal user information. Service requests from hospital users indicate that they are either personnel, patients, or their companions.

Faculty may use a hospital IoT application service daily If a user accesses the system frequently from a different location that is also frequently used, we may presume that this other location is the user's home, in which case we will attempt to determine the user's true identity and link all service activity to that particular person. Additional defenses are therefore required, especially for location-based services (LBS) offered by IoT devices.

Cloaking and k-anonymity are the key defences). When users move across cloaking areas, their mobile devices randomly switch pseudonyms. In an IoT ecosystem with smart automobiles, anonymization locations may be traffic lights or road crossings, where several cars slow down and facilitate identity change. Context information is still inferable. This solution's efficacy depends on anonymization area density and user volume over time. Density and bulk increase protection. Advanced countermeasures are suggested.Semantic obfuscation mixes semantically varied domain material to limit context knowledge [16]. Other protection techniques can give the LBS provider fake location data. The cloaking approach only works for mobile services like LBS. The name of at least k users is obscured by an intermediary between users and the service using k-anonymity. To get around masking area locale restrictions, users might have to sign up for this entity and use the function online. The user community must trust the entity. Peer-to-peer services on users' devices can also incorporate the capability. However, this solution requires people to actively participate and utilise their own resources for the community.

However, system design benefits from k-quantifiable anonymity's and configurable protection level. K factor increases privacy defence. Combinatorial ways of cloaking areas and k-anonymity schemes are also suggested, combining their benefits. Anonymity requires threshold signature schemes [17]. The threshold scheme processes crowdsourced credentials. Everyone knows the secret. n valid shares are needed to decrypt and authenticate credentials. Thus, users share their acquired data with the provider. The service authenticates the group's credentials using n shares and processes their data. The data collector knows only part of the group's credentials from the user.

While maintaining anonymity, the collector trusts and processes the data. Centralized, decentralised, or hybrid schemes exist. The threshold scheme's n parameter controls protection. Honest and trustworthy community signing key dealers are a security issue.

E-commerce and tailored marketing are however restricted by methods that preserve anonymity. As a result, attribute-based credentials (ABC) are advised to protect anonymity while providing service providers with sufficient data. Attribute-related information, such as X.509 credentials, are stored in ABC cryptographic containers. The owner of ABC receives a container and a hidden key from a reliable source. All that can be displayed are the user's attributes and permission signature. Users can share only a specific attribute subset, such as their purchase threshold for discounts or other advantages, using the selective disclosure feature. The user's secret key is shielded from the service provider by zeroknowledge proof. Multiple-show unlinkability is permitted by certain ABC schemes, which prevents the provider from connecting two user viewings.

10.4 Deleterious Effects on Data

Another significant issue, the deletion of data from any equipment that is recycled or thrown away, is something that, in most instances, is not dealt with in the appropriate manner. There will be issues with security and privacy if the information are not correctly wiped from the non-volatile memory. This is because the new owner of the equipment will be able to reveal valuable information about the prior user, including medical files, credit card details, and more. The issue is much more urgent than normal in CE situations where the digital assets are meant to be utilized and shared across the numerous actuators.

As a result, particular regulations are being recommended in order to delete the data from the device in a way that is irreversible prior to the device's disposal [18, 19].

However, it might not always be feasible to use the aforementioned solutions in situations involving distributed storage or the cloud. The implementation of self-destruction policies for the data that is kept, either on-select or after a predetermined amount of time, is therefore made possible by a number of state-of-the-art solutions that use cryptography (i.e. ABE schemes) [20]

11 Conclusions and future work

The integration of Circular Economy (CE) principles with the Internet of Medical Things (IoMT) has witnessed significant growth. This synergy has paved the way for innovative applications in remote sensing, elder care, and bioinformatics, harnessing the power of crowdsourcing and Big Data analytics. Within this context, this paper endeavors to delineate the central components of end-to-end security and privacy measures. Such a by-design strategy is paramount in ensuring the protection of users/patients and the integrity of the healthcare sector.

One of the fundamental objectives of IoMT is to curtail healthcare costs while simultaneously enhancing the quality of patient care. It is imperative to acknowledge that the security of IoMT devices stands as a linchpin in achieving these objectives. IoMT sensors, in particular, operate within constrained resource environments, with implanted devices necessitating external security mechanisms for their safeguarding. This article undertakes a comprehensive exploration of the security imperatives associated with IoMT, addressing modern security methodologies and the evolving landscape of potential threats.

The cornerstone of this article revolves around the articulation of primary end-to-end security and privacy defenses. By adhering to a proactive design approach, this strategy serves as a bulwark, shielding both end-users and patients, as well as the broader healthcare ecosystem. Within each stratum of IoMT infrastructure, this exposition delves into secure functionalities and cutting-edge solutions.

Moreover, this study, deeply embedded within the context of Circular Economy principles, extends its applicability beyond the realm of IoMT, serving as a template for best practices in the broader Internet of Things (IoT) domain. The symbiosis between CE and IoMT not only contributes to resource optimization but also ensures the responsible and sustainable deployment of technology in healthcare and other sectors. As such, this paper assumes the role of a comprehensive guide, offering valuable insights and recommendations for practitioners and stakeholders vested in the IoMT landscape.

In conclusion, the confluence of Circular Economy ideals with the Internet of Medical Things holds promise for reshaping healthcare

delivery and resource management. With security and privacy concerns at the forefront, the principles elucidated in this article lay the foundation for a resilient and sustainable future, not only for IoMT but also for the broader spectrum of IoT applications.

Received 20 October 2023
Revised 19 December 2023
Accepted 22 January 2024

12 References

1 IT Services for IoT., 2023, **18**, pp. 20–20. Worldwide, 2019-2025. Accessed: Janaury. 18, 2023. [Online]. Available:https://www.gartner.com/en/documents/4004741#:~:text=The%20IT%20Services%20for%20IoT,occur%20in%20the%20run%20phase.
2 Mahadevegowda. 'Spandan. Secure Communication Networks for Connected Vehicles',. Diss. Virginia Tech, 2023.
3 Stellios, I., Mokos, K., Kotzanikolaou, P. Assessing vulnerabilities and IoT-enabled attacks on smart lighting systems. In: European Symposium on Research in Computer Security., Springer International Publishing, 2021. pp. 199–217.
4 'United States Naval Acad',. Annapolis, MD; USA. Available, 2020. Available from: https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l21/lec.html.
5 Hajar, M. S., Al-Kadri, M. O., Kalutarage, H. K.: 'A survey on wireless body area networks: Architecture, security challenges and research opportunities', *Computers & Security*., 2021, **104**, pp. 102211–102211.
6 Wang, H., Abdin, A. F., Fang, Y. P., *et al.*: 'Resilience assessment of electrified road networks subject to charging station failures', *Computer-Aided Civil and Infrastructure Engineering*., 2022, **37** (3), pp. 300–316.
7 Alzubaidi, L., Zhang, J., Humaidi, A. J.: 'Review of deep learning: concepts, CNN architectures, challenges, applications, future directions', *Journal of Big Data*., 2021, **8** (1), pp. 53–53.
8 Yu, Z., Kaplan, Z., Yan, Q., *et al.*: 'Security and privacy in the emerging cyber-physical world: A survey', *IEEE Communications Surveys & Tutorials*., 2021, **23** (3), pp. 1879–1919.
9 Camara, P. A., Peris-Lopez, J. E., Tapiador: 'Security and privacy issues in implantable medical devices: A comprehensive survey', *Journal of Biomedical Informatics*., 2015, **55**, pp. 272–289.
10 Joshua, S. R., Abbas, W., Lee, J. H.: 'M-Healthcare Model: An Architecture for a Type 2', *Diabetes Mellitus Mobile Application. Applied Sciences*., 2022, **13** (1).
11 Pacemaker, Mayoclinic, Rochester, *et al.*, . Available from: https://www.mayoclinic.org/testsprocedures/pacemaker/.
12 Alzahrani, B. A., Irshad, A., Albeshri, A., *et al.*: 'A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks', *Wireless Pers. Commun*., 2020, pp. 1–1.
13 Bhatia, T., Verma, A. K., Sharma, G.: 'Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing', *Concurrency Comput. Pract. Exp*., 2020, **32** (5), pp. 1–16.
14 Kalyani, G., Chaudhari, S.: 'An efficient approach for enhancing security in Internet of Things using the optimum authentication key', *Int. J. Comput. Appl*., 2020, **42** (3), pp. 306–314.
15 Idrees, A. K., Khlief, M. S.: 'Efficient compression technique for reducing transmitted EEG data without loss in IoMT networks based on fog computing', *The Journal of Supercomputing*., 2023, **79** (8), pp. 9047–9072.
16 Hady, A. A., Ghubaish, A., Salman, T., *et al.*: 'Intrusion detection system for healthcare systems using medical and network data: A comparison study', *IEEE Access*., 2020, **8**, pp. 106576–106584.
17 Gupta, L., Salman, T., Zolanvari, M., *et al.*: 'Fault and performance management in multi-cloud virtual network services using AI: A tutorial and a case study', *Comput. Netw*., 2019, **165**.
18 Syed, F., Gupta, S. K., Alsamhi, S. H., *et al.*: 'A survey on recent optimal techniques for securing unmanned aerial vehicles applications', *Transactions on Emerging Telecommunications Technologies*., 2021, **32** (7), pp. 4133–4133.
19 Singh, R. K., Kumar, A., Hussain, M.: 'A Secure Key Agreement Mechanism for Smart Home Networks', *2022 International Conference on Connected Systems & Intelligence (CSI)*., 2022, pp. 1–6.
20 Almajali, S., Salameh, H. B., Ayyash, M., *et al.* A framework for efficient and secured mobility of IoT devices in mobile edge computing. In: Proc. 3rd Int. Conf. Fog Mobile Edge Comput. (FMEC), 2018. pp. 58–62.