DISCOVERY

*58(316), April, 2022*

# Techniques for Mitigating IoT Privacy and Security Issues in Healthcare: A Review

**Akaninyene U Ntuen[1], John E Efiong[2], Itoro S Okoroudoh[3], Ogbunude F Okechukwu[4]**

**To Cite:**
Ntuen AU, Efiong JE, Okoroudoh IS, Okechukwu OF. Techniques for Mitigating IoT Privacy and Security Issues in Healthcare: A Review. *Discovery*, 2022, 58(316), 340-348

**Author Affiliation:**
[1,4]Department of Computer Science, Akanu Ibiam Federal Polytechnic, Unwana, Nigeria
[2]Department of Computer Science, Wesley University, Ondo, Nigeria
[3]ICT Department, Akanu Ibiam Federal Polytechnic, Unwana, Nigeria

**Email:**
[1]auntuen@akanuibiampoly.edu.ng; [2]john.efiong@wesleyuni.edu.ng; [3]sitoro@akanuibiampoly.edu.ng; [4]festula@gmail.com

**Peer-Review History**
Received: 11 February 2022
Reviewed & Revised: 14/February/2022 to 21/March/2022
Accepted: 23 March 2022
Published: April 2022

**Peer-Review Model**
External peer-review was done through double-blind method.



## ABSTRACT

In the last few years, Internet of Things (IoT) devices are widely utilized in many industries such as healthcare. These IoT devices are connected to the Internet and interact with one another to collect data for systems to analyze and make appropriate decisions. As a result, cyberattacks target IoT systems to evade security and explore the system without being discovered. The goal is to steal important information from the organisation or to cause service disruptions. This invasion of privacy and security has been the most important impediment to the widespread adoption of the IoT in the healthcare industry. Therefore, this paper examines the privacy and security challenges in healthcare IoT and suggests measures to mitigate them.

**Keywords:** Cyberattack, Healthcare, IoT, Privacy, Security, Attack Mitigation.

## 1. INTRODUCTION

The Internet of Things (IoT) is a notion that encompasses a related set of anybody, anything, at any time, in any location, with any service, and on any network (Islam, 2015). The Internet connects specialists and patients all over the world, allowing for the monitoring of patients' medical status, the transfer of patient data, and the administration of therapies to patients (Elhayatmy, Dey, & Ashour, 2018). However, Internet access exposes infiltration ports, raising privacy and security issues, which has been the major significant barrier to the extensive adoption of the IoT owing to the unusual threats it offers to users and their surroundings (Chacko & Hayajneh, 2018). As a result, this study aims to investigate the privacy and security challenges in healthcare IoT and offer techniques to mitigate them. The outcome of this study is expected to satisfy the research aim. Hopefully, among other benefits, it would address the issues of privacy and security in healthcare thereby increasing productivity, inspiring stakeholders' (policymakers, health professionals, and patients) confidence, and giving clients hope of safety. It will also be of interest to researchers that require relevant information for either studies or projects.

`

## 2. LITERATURE REVIEW

In 1999, Kevin Ashton invented the term "Internet of Things" (Prasad & Rohokale, (2020). It entailed using the Internet to allow computers to sense the world for

themselves (Granell *et al*., 2020). According to Ahmadi *et al.* (2019), the Internet of Things (IoT) is an ecosystem that connects hardware, software, and physical objects. According to a recent forecast by International Data Corporation (IDC), 41.6 billion "things" will be connected to the internet by 2025, creating 79.4 zettabytes (ZB) of data (Lucivero, 2020). The benefit is that the connection will encourage the collection of data and will apply the knowledge gained from this data independently to handle and make intelligent decisions (Ahmadi *et al,* 2019; Purbey & Khandelwal, 2021). More importantly, rapid access to health data increases the value of healthcare, enhances patient satisfaction, and facilitates timely intervention (Korzun, Nikolaevskiy, & Gurtov, 2015). On the contrary, additional intrusion ports would be opened, raising the level of privacy and security concerns (Islam, 2015).

In analyzing user actions in healthcare, Gupta, Maharaj, & Malekian, (2017) suggested using a cloud of things approach. The authors highlighted privacy, trust, integrity, and authentication principles in access to health data for a cloud-based security solution. They suggest AES and RSA protocols for the public and private cloud environments, respectively, to investigate the security features of this architecture. This method ensures data security in the cloud. The two approaches were compared in their research by determining decryption and encryption times. The results reveal that the RSA method is much more secure and robust than the AES method. Most of the privacy and security vulnerabilities were identified by Kraijak, & Tuwanut, (2015) to include network security, equipment, and front-end sensors among the most pressing concerns. The authors outline how problems of privacy should be addressed throughout the data transfer process.

Monshizadeh *et al*., (2020) found most of the privacy and security issues in the healthcare sector, which is consistent with this study. The researchers discussed how to authenticate a user's identity using authentication approaches such as a smart card, password, signature, tokens, fingerprint scanning, and speech pattern. The authors went on to say that adequate guidelines and standards, such as the ISO/IEC 27,000 series, as well as information security protocols, should be met. In addition, socio-ethical factors such as consumer advocacy, information disclosure policies, and patient rights must be thoroughly considered.

Zahmatkesh & Al-Turjman (2020) discussed a medical sensor security strategy. The authors use software and hardware simulation and prototype to look at the model's key properties, such as energy efficiency and security. The proposed approach, called SEA, acts as a gateway in the fog layer, establishing authorization protocols. When compared to existing end-to-end security solutions, the researchers claim that this methodology reduces packet preparation, routing table, and routing procedure by 26%. Furthermore, the time it takes the remote computer to receive a data packet is lowered by 16 percent. Dwivedi *et al.* (2019) also recommended digital signatures and certificates based on symmetric and asymmetric algorithms as the best ways for addressing security problems in healthcare. Despite these current tactics, threats and attacks continue to be disturbing.

According to Chacko & Hayajneh (2018), two security researchers uncovered 68,000 medical systems exposed online in 2015, and one healthcare organization owned 12,000 of them. This demonstrates the amount of insecurity in healthcare IoT despite the efforts of experts to address the problems. Therefore, this research suggests technological and general techniques to tackle privacy and security problems in healthcare IoT. If these techniques are well harnessed, it is believed that these problems will be mitigated thereby encouraging an extensive adoption of IoT in healthcare.

## 3. RESEARCH METHOD

Following the criteria in Kitchenham (2009), the study adopts a systematic research technique to guide the literature search in several electronic databases on privacy and security risks in healthcare IoT. The electronic databases evaluated included Google Scholar, Scopus, Science Direct, Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library, Association for Computing Machinery (ACM) Digital Library, and Springer Link. The steps of this review, which included a search strategy, study selection (inclusion/exclusion criteria), research eligibility, and quality evaluation, were guided by Kitchenham (2009) methodology.

### A. Searching Strategy

The following search keyword was used to find previously published studies on privacy and security challenges in healthcare IoT: Internet of Things, privacy, security, healthcare, and cyber-attacks.

### B. Study Selection (inclusion and exclusion criteria)

Our research selection (inclusion and exclusion criteria) was based on peer-reviewed, English-language papers. These publications' titles and abstracts were then screened. Opinion pieces, non-peer-reviewed papers, incomplete articles, and studies in languages other than English that were not translated into English were also eliminated.



ISSN 2278–5469 EISSN 2278–5450 I OPEN ACCESS

**C. Eligibility and Assessment of Study Quality**

To ensure research eligibility and quality, all articles were double screened by all authors. Article names and abstracts were evaluated. There were no more duplicates. We verified that all articles giving information on IoT that is tied to privacy and security are included by completing citation chains for extra study for each retrieved article, and we published our findings in the next section.

## 4. PRIVACY AND SECURITY CHALLENGES IN HEALTHCARE IOT

**A. Privacy Challenges in Healthcare IoT**

IoT privacy refers to the process of protecting an individual's data from disclosure in an IoT context, as well as ensuring that people have control over what data is collected about them, who keeps it, who uses it, how it is used, and for what purpose it is used Maras (2015). Privacy, according to Atlam & Wills (2020), is a notion with four basic components: information, communications, body, and territory. Information privacy has to do with diverse data of individuals collected and managed by an organisation like financial or medical information; privacy of communication is concerned with the data protection exchanged among two nodes of communications through a communication channel of any kind; body privacy is connected with the physical safety of an individual as well as any potential outside harm; while territorial privacy is concerned with establishing boundaries around physical space like home, workplace, and public areas.

Individual privacy has become a difficult task to achieve in the healthcare IoT. The reason for this is that the data collection approach used is more passive, ubiquitous, and less intrusive, resulting in users being unaware that they are being tracked (Ziegeldorf, Morchon, & Wehrle, 2014). A privacy threat refers to the possibility of losing control over personal information. This threat is one of the most common concerns among users, and it has a direct impact on the amount of adoption of any new technology, according to Zhang *et al*. (2018). One of the key characteristics of the IoT is the ability of devices to perceive and feel their surroundings. However, this capability leads to the monitoring and tracking of movements of individuals and activities, which violates personal privacy and leads to additional problems that can lead to users' deaths (Kassirer, 2000).

The main privacy problems in healthcare IoT according to Sciforce (2019) include Risks of Patients' Privacy Exposure, Data Eavesdropping, Ownership of data, and Location privacy.

**1) Risks of Patient's Privacy Exposure**

The most important aspect of patient privacy is maintaining the confidentiality of their Personal Health Records (PHR). A PHR is simply "a collection of personal and confidential information regarding a patient's health," according to *Archer et al.* (2011), and can be either traditional paper records or computerized data. Electronic Protected Health Information (e-PHI) is also gathered and stored in PHRs by healthcare IoT devices. Vital signs such as the temperature of the body, pulse rate, and respiration rate are examples of e-PHI obtained via IoT devices. PHR must be kept secret by healthcare institutions and only primary caregivers should have access to this information. PHRs are appealing targets for hackers looking to steal customer data and information due to their confidential nature (Patel, 2020). Perpetrators may copy, modify, or damage this data because of an intrusion. Such harmful acts by attackers jeopardize patients' privacy.

**2) Data Eavesdropping and Confidentiality**

In general, patient health data is maintained in strict confidence and is only accessible to authorized caregivers. However, such information can be stolen from storage or eavesdropped on as it travels across wireless networks. Eavesdropping is the stealing of information from a smartphone, computer, or other connected devices while it is being transferred across a network (Lin *et al.*, 2018). To gain access to data as it is transmitted or received by the user, the attacker exploits unsecured network communications. Eavesdroppers can intercept a phone call, video chat, fax transfer, and instant messages to obtain sensitive or desirable information and data according to Forte & de Donno (2010). For example, a widely used IoT-based glucose monitoring and insulin administration system can save lives and improve greatly the quality of a patient's life but it makes use of wireless communication links, which are regularly exploited to launch privacy assaults, necessitating adequate data protection. The loss of a patient's privacy, particularly her identifying data, can cause serious physical, emotional, and financial harm to the patient.

**3) Data Ownership**

According to Rains *et al*. (2019), patients' data is protected by law in most countries, but laws vary by state. Furthermore, in other circumstances, such as with healthcare wearables, consumers assume that the data tracked and collected is protected by law,



ISSN 2278–5469 EISSN 2278–5450 I OPEN ACCESS

although this is not always the case. Although consumers may naturally think that the data, they obtain through consumer wearables belongs to them, ownership may be determined by country or state regulation. The same is true of user location data; most people desire to keep it private, but it is frequently shared with other parties (Brush, Krumm & Scott, 2010).

**4) Location Privacy**

Healthcare IoT faces numerous challenges when it comes to data privacy. The data location of the user, for instance, is regarded as personal information, and its privacy can be readily stolen and disclosed to third parties (Conger, Pratt & Loch, 2013). Duckham & Kulik (2006) inform that threats to location privacy and spying on a user's location are two major problems relating to location privacy.

**B. Security Challenges in Healthcare IoT**

Several serious healthcare IoT security problems surfaced at the time when hospitals began using the Internet of Things (IoT). The biggest security problems in healthcare IoT, according to Billingsley (2019) are hardware, network segmentation, legacy systems, ransomware, and Medjacking.

**1) IoT Hardware**

IoT hardware encompasses a wide range of devices, including sensors and wearables. According to Boyes *et al*. (2018), the following components make up each piece of IoT hardware: Things (the asset you desire to control); Data Acquisition Module (a set of hardware and software that enables the measurement or control of physical features of a thing in the real world); Data Processing Module (a group of machines, people, and processes that create a specific set of outputs in response to a specific set of inputs); and Communication Module (handles the exchange of messages between modules on different robots). Thierer (2015) informs that IoT security concerns in healthcare are growing by the day and it poses a danger to obsolete hardware. Because manufacturers' efforts are focused on mass manufacturing of new brands, safety is not considered. As a result, most gadgets are not upgraded to satisfy the latest IoT security regulations, and hackers may discover flaws that have not yet been fixed by new updates. Another possible IoT hardware danger to hospitals according to Elkanishy *et al*. (2021) is that a malicious circuit may be introduced into a microchip at any point during its construction, even after it has been successfully fabricated. In this instance, sensitive data might be exposed, and critical system mechanisms could fail.

**2) Segmentation of Network**

For the execution of a good security plan, segmentation is crucial. The study of Hayajneh, Bhuiyan, & McAndrew (2020) found that subnetting a network is a common technique for the organization to increase performance and medical IoT security. One may separate traffic into internal (internal users) and external (guests and external users) segments using network segmentation (authorized users). If this is lacking, a locally deployed device might end up causing harm to the entire organization while transporting critical medical data (Subashini & Kavitha, 2011). Without network segmentation, an attacker can easily take hold of misconfigurations within an organisation. To achieve network segmentation, one has to: Use Network Access Control to identify all incoming devices; distinguish the IoT segment from other networks; and provide an automated security architecture to safeguard the network (Bai *et al*., 2018).

**3) Legacy Systems**

The nature of hospital operations is the source of this problem. Patching and upgrading systems, according to Webster (2011), is frequently an expensive luxury for hospitals since it interferes with the care of a patient, which is required always. As such, hospitals are compelled to work with outdated Windows XP or MS-DOS systems, increasing the incidence of IoT security breaches and vulnerabilities. Hospitals will be deficient in security improvements and crucial cybersecurity precautions in this scenario, making attackers' tasks much easier.

**4) Ransomware**

Ransomware is a sort of software that locks the user out of their device and its contents, forcing them to pay a ransom to regain access (Aurangzeb *et al*., 2017). Ransomware, which was formerly the most common security issue in healthcare, has recently been eclipsed by emerging threats and errors made by humans. Despite this, security firms stress the significance of always accessing our protection level to avoid ransomware attacks. Endpoint security software, alongside frequent backups, antivirus, effective access



ISSN 2278–5469 EISSN 2278–5450 I OPEN ACCESS

control, and a disaster recovery strategy, is necessary for the effective protection of an organization (McIntosh *et al.,* 2021). If such an attack is not prevented promptly, the hospital will be taken offline for an extended period, and its operations will come to a halt.

**5) Medjacking**

Research by Meggitt (2018) has found Medjacking to be a form of security risk implemented in medical equipment to obtain access to its software. After a TrapX investigation demonstrated the susceptibility of all healthcare organizations to medical device hijacking, including the infusion pump, which injects medications straight into the blood of a patient (Chacko & Hayajneh, 2018), the medical sector began talking about the problem in 2015. Ayala (2016) informs that hackers might gain access to the device and murder victims manually. Devices may also be infected with malware through Medjacking to steal personal or confidential information (Meggitt, 2018). That same year, it was determined in the United States to stop using all vulnerable devices. Medical gadgets must still be carefully selected and verified by vendors today.

## 5. TECHNIQUES TO MITIGATE PRIVACY AND SECURITY CHALLENGES IN HEALTHCARE INTERNET OF THINGS

**1) Electronic Digital Signature and Monitoring Systems**

Malicious threats' entry into hardware can have a wide range of implications, from personal gadgets disablement to interfering with the transportation and defence systems operation, which can be devastating. To prevent the hacking of hardware, Das *et al*. (2021) say that the device's debug port must be difficult to access and can be further safeguarded by an electronic digital signature to encrypt the document; permanently embed the information in it; and invalidate if a user attempts to edit the document.

The process of testing and identifying viruses should encompass actions ranging from discovering random defects to thoroughly hidden and purposeful flaws as a preventative step. A shift in the design process that limits information and provides selective access to people involved in a particular developmental activity can have a favourable influence on hardware security. To mitigate the harmful effects of viruses, Kim, Smith, & Shin (2008) say that monitoring systems must be installed in the chips to detect suspicious behaviour and, if necessary, quick quarantine. Finally, for IoMT security, Jalali, & Kaiser (2018) say that compliance with HIPAA (Health Insurance Portability and Accountability Act), HITECH (Health Information Technology for Economic and Clinical Health Act), NHS (National Health Service), and FDA (Food and Drug Administration) should be ensured.

**2) Cryptography and Encryption**

On both the hardware and software stages, cryptography can be used to prevent data eavesdropping in the IoT context. However, in the latter situation, it will be even more difficult. Lightweight cryptography (LWCRYPT) has traditionally been utilized as a cryptography approach for IoT smart products. Dewanjee, Verma & Vjas (2016) named asymmetric and symmetric LWCRYPT techniques to choose from:

**(i) Asymmetric:** This approach encrypts with two keys. The public key is accessible to everyone, while the private key is only accessible by the owner. Asymmetric encryption is only used to launch a handshake, also known as the exchange of keys, in which the sender and recipient exchange public and private keys (Galla, Koganti & Nuthalapati, 2016). The main task is then taken over by symmetric encryption.

(ii) **Symmetric:** The simplest encryption scheme is symmetric according to Agrawal & Mishra (2012). The authors inform that it is after the handshake, during the session, that this kind of encryption is created, and it employs one secret key (either a character set, any number, word, or symbols that are not on the layout of a keyboard). To decode, the contents of this key must be known to the sender and receiver. Hardware solutions, like numerous sensors and devices, hold asymmetric keys to construct a connection that is secure between the sensor and the customer in the form of an HTTP (Hypertext Transfer Protocol) tunnel (Mrabet et al., 2020). The pattern of authentication for implantable devices used in healthcare has been designed to substitute regular passwords to deal with the challenges of the insecure encrypted IoT network (Camara, Peris-Lopez & Tapiador, 2015). In this manner, using ultraviolet light enables encrypted keys in the body of a patient to be sealed.

**3) Malware Detection and Prevention**

One can successfully employ several malware protection methods:

**(i) Signature-based Detection:** This is the most prevalent method that relies on the signature of an antivirus system. When no commonalities are observed between signatures in the database, malware is recognized (Tchakounté *et al*., 2021). This strategy is not appropriate for devices with limited memory.



ISSN 2278–5469 EISSN 2278–5450 I OPEN ACCESS

**(ii) Static Methods:** These are based on the device's static properties. The static analysis looks for malware without changing the code, and it uses a variety of methods to identify and gather simple signatures (Talukder, 2020). It is small and light on resources, but verification is restricted.

**(iii) Dynamic Methods:** Dynamic detection, as opposed to static detection, detects malware by examining unusual behaviour such as CPU load, network behaviour, virtual memory, calls, and SMS (Ferrante et al., 2017). Combining static and dynamic detections is the best method to defend oneself. Yaqoob, Abbas & Atiquzzaman (2019) inform that One can accomplish reliable security against viruses like Medjacking by isolating IoT health services from other apps in a secure environment. Another option according to Clark (2018) is to connect independent devices to healthcare service providers through a hub. The wristband gadget Amulet, for example, makes touch with a smartphone before a secured connection is established with a healthcare service provider.

**4) Shielding and Filtering**

Every year, as our lives become increasingly reliant on electronic gadgets, the issue of EMI (Electromagnetic Interference) becomes more important. EMI attacks transmit electromagnetic waves to electronics, causing them to malfunction (Kaur, Kakar & Mandal, 2011). Noto, Fenical, & Tong (2010) mentioned shielding and filtering as the most effective ways to cope with EMI. They can boost resistance before EMI. Shielding encircles an object with a metal plate to stop electromagnetic pulses, which scatter in diverse ways when they come into touch with it whereas, with filtering, the essential noise and interference are carried through the electric current in the conductors, while undesired noise is removed (Raj, Jayakumar & Thavasimuthu, 2002). Abnormal sensory signals can be detected using a combination of shielding and filtering.

**5) Complete Command over the Network**

According to Mykola and Oleksandr (2020), the major means of controlling the visibility of the network, that is, monitoring it for breaches to reduce risks, is to manage it. The network is equipped with intelligence, scanners, and a variety of technologies to provide the best possible Défense against cyber threats. The provision of network segmentation facilitates optimal network control. In essence, Yang *et al*., (2017) inform that it allows one to transfer data exclusively to authorized users for redistribution. The sensors send data to the server through Bluetooth, which subsequently sends it to the server via the HTTP channel. Thus, even if data is intercepted by intruders, they will be unable to decrypt it without a key (Shiu *et al*., 2011) Following that, the server transfers data to the database, which requires access from within the company. Thus, each piece of a network's IoT security must be safeguarded at its level to achieve high-quality IoT security.

**6) Security in the Context**

For a variety of reasons, one's platform should include contextual security. IoT solutions can be isolated in their network at any moment, thanks to this form of security, and policies can be configured to monitor suspicious behaviour (e.g., attempts to intercept data) or even traffic patterns (Rizvi *et al,* 2020). The implementation of additional thresholds and filters for greater security will benefit the IoT network. If a DDOS (distributed denial-of-service) attack is detected, it can be mitigated by closing the network in part or whole (Velliangiri, Karthikeyan & Kumar, 2021).

**7) Segmentation and Centralization of Connected Devices**

When working with connected devices, it is a good idea to set up a separate network to keep track of them. Device segmentation and centralization will provide for greater control flexibility, with the ability to switch between both ways depending on the danger (Borhani *et al*., 2020). For further device control, IoT aggregation hubs make sense. Keep in mind that one should always be aware of what the gadgets have access to. Their Internet of Medical Things (IoMT) security policy settings will be determined by the requirements for data storage and access to PHI/PII (Protected Health Information/Personally Identifiable Information).

**8) Maintenance of Visibility and Testing**

Because of the danger of hardware infection that we stated earlier, connecting new devices to the network will require one to be as nimble as possible. The wireless architecture will assist one in tracking and managing their growth. The number of devices connected to a network determines the level of monitoring complexity (Suh *et al*., 2006). It is vital not to lose sight of them and to establish a quality monitoring framework from the start.



ISSN 2278–5469 EISSN 2278–5450 I OPEN ACCESS

## 6. CONCLUSION

Recent advancements in the field of the Internet of Things (IoT) hold a lot of potential for healthcare solutions. IoT devices are thought to be here to stay because they make vital operations easier to accomplish. In IoT healthcare, however, there are numerous privacy and security concerns. As a result, it is necessary to ensure that networks perform automatic work cycles, provide speedy access to important data, and ensure the safety of everything. This is achievable by enforcing policies regarding security and putting in place remedies that is centering on configuration assessments, vulnerabilities, malware defenses, event, and activity monitoring. In this study, we investigated the privacy and security problems that have arisen in the healthcare IoT, with a focus on what has been done so far and what problems still need to be addressed. We discovered that patient privacy threats, data eavesdropping and confidentiality, data ownership, and location privacy are some of the privacy challenges encountered by the healthcare business, while security challenges include hardware, network segmentation, legacy systems, ransomware, and medjacking. We discussed strategies that can be followed to address these problems which include the use of electronic digital signatures and monitoring systems, cryptography and encryption, malware detection and prevention, shielding and filtering, complete network control, security in context, segmentation, and centralization of connected devices, and maintenance of visibility and testing. The problems of privacy and security in healthcare IoT are expected to be mitigated if the solutions offered in this article are properly harnessed. It will reduce threats to the healthcare industry and enable widespread IoT use in healthcare.

**Funding**

This study has not received any external funding.

**Conflicts of interests**

The authors declare that there are no conflicts of interests.

**Data and materials availability**

All data associated with this study are present in the paper.

## REFERENCES AND NOTES

1. Agrawal, M., & Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. *International Journal on Computer Science and Engineering*, *4*(5), 877.
2. Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M., & Alizadeh, M. (2019). The application of internet of things in healthcare: a systematic literature review and classification. Universal Access in the Information Society, 18(4), 837-869.
3. Al Hayajneh, A., Bhuiyan, M. Z. A., & McAndrew, I. (2020). Improving Internet of Things (IoT) security with software-defined networking (SDN). Computers, 9(1), 8.
4. Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. A., & Straus, S. E. (2011). Personal health records: a scoping review. Journal of the American Medical Informatics Association, 18(4), 515-522.
5. Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety, and ethics. In Digital twin technologies and smart cities (pp. 123-149). Springer, Cham.
6. Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: a survey and trends. Journal of Information Assurance & Security, 6(2), 48-58.
7. Ayala, L. (2016). Cybersecurity for hospitals and healthcare facilities. Berkeley, CA.
8. Bai, L., Yao, L., Kanhere, S. S., Wang, X., & Yang, Z. (2018, October). Automatic device classification from network traffic streams of the internet of things. In 2018 IEEE 43rd conference on local computer networks (LCN) (pp. 1-9). IEEE.
9. Billingsley, L. (2019). Cybersmart: Protect the patient, protect the data. Journal of Radiology Nursing, 38(4), 261-263.
10. Borhani, M., Liyanage, M., Sodhro, A. H., Kumar, P., Jurcut, A. D., & Gurtov, A. (2020). Secure and resilient communications in the industrial internet. In *Guide to Disaster-Resilient Communication Networks* (pp. 219-242). Springer, Cham.
11. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in industry, 101, 1-12.
12. Brush, A. B., Krumm, J., & Scott, J. (2010, September). Exploring end-user preferences for location obfuscation, location-based services, and the value of location. In Proceedings of the 12th ACM international conference on Ubiquitous computing (pp. 95-104).
13. Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices:



ISSN 2278–5469 EISSN 2278–5450 I OPEN ACCESS

A comprehensive survey. *Journal of biomedical informatics*, *55*, 272-289.

14. Chacko, A., & Hayajneh, T. (2018). Security and privacy issues with IoT in healthcare. EAI Endorsed Transactions on Pervasive Health and Technology, 4(14).
15. Clark, S. A. (2018). Secure Integration of Information Systems in Radiology.
16. Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. Information Systems Journal, 23(5), 401-417.
17. Das, S., Siroky, G. P., Lee, S., Mehta, D., & Suri, R. (2021). Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices. *Heart rhythm*, *18*(3), 473-481.
18. Dewanjee, R., Verma, P., & Vjas, R. (2016). Cryptography Techniques and Internet of Things. In *3rd International Conference on Electronics and Communication Systems (IEEE, ICECS'16)*.
19. Duckham, M., & Kulik, L. (2006). Location privacy and location-aware computing. In Dynamic and Mobile GIS (pp. 63-80). CRC press.
20. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326.
21. Elhayatmy, G., Dey, N., & Ashour, A. S. (2018). Internet of Things based wireless body area network in healthcare. In the Internet of things and big data analytics toward next-generation intelligence (pp. 3-20). Springer, Cham.
22. Elkanishy, A., Furth, P. M., Rivera, D. T., & Badawy, A. A. (2021). Low-overhead Hardware Supervision for Securing an IoT Bluetooth-enabled Device: Monitoring Radio Frequency and Supply Voltage. ACM Journal on Emerging Technologies in Computing Systems (JETC), 18(1), 1-28.
23. Ferrante, A., Malek, M., Martinelli, F., Mercaldo, F., & Milosevic, J. (2017, October). Extinguishing ransomware-a hybrid approach to android ransomware detection. In *International Symposium on Foundations and Practice of Security* (pp. 242-258). Springer, Cham.
24. Forte, D., & de Donno, A. (2010). Mobile network investigations. In Handbook of digital forensics and investigation (pp. 517-557). Academic Press.
25. Galla, L. K., Koganti, V. S., & Nuthalapati, N. (2016, December). Implementation of RSA. In *2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)* (pp. 81-87). IEEE.
26. Granell, C., Kamilaris, A., Kotsev, A., Ostermann, F. O., & Trilles, S. (2020). Internet of things. In Manual of digital earth (pp. 387-423). Springer, Singapore.
27. Gupta, P. K., Maharaj, B. T., & Malekian, R. (2017). A novel and secure IoT-based cloud-centric architecture to perform predictive analysis of user's activities in sustainable health centers. Multimedia Tools and Applications, 76(18), 18489-18512.
28. Islam, S. 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.
29. Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research*, *20*(5), e10059.
30. Kassirer, J. P. (2000). Patients, Physicians, And The Internet: Coming generations of doctors are ready to embrace new technology, but few incentives now exist to encourage their older peers to do likewise. Health Affairs, 19(6), 115-123.
31. Kaur, M., Kakar, S., & Mandal, D. (2011, April). Electromagnetic interference. In *2011 3rd International Conference on Electronics Computer Technology* (Vol. 4, pp. 1-5). IEEE.
32. Kim, H., Smith, J., & Shin, K. G. (2008, June). Detecting energy-greedy anomalies and mobile malware variants. In *Proceedings of the 6th international conference on Mobile systems, applications, and services* (pp. 239-252).
33. Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. Information and software technology, 51(1), 7-15.
34. Korzun, D. G., Nikolaevskiy, I., & Gurtov, A. (2015). Service intelligence support for medical sensor networks in personalized mobile health systems. In the Internet of things, smart spaces, and next-generation networks and systems (pp. 116-127). Springer, Cham.
35. Kraijak, S., & Tuwanut, P. (2015, October). A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation, and future trends. In 2015 IEEE 16th International Conference on Communication Technology (ICCT) (pp. 26-31). IEEE.
36. Liu, K., Shen, W., Cheng, Y., Cai, L. X., Li, Q., Zhou, S., & Niu, Z. (2018). Security analysis of mobile device-to-device network applications. IEEE Internet of Things Journal, 6(2), 2922-2932.
37. Lucivero, F. (2020). Big data, big waste? A reflection on the environmental sustainability of big data initiatives. Science and engineering ethics, 26(2), 1009-1030.
38. Maras, M. H. (2015). Internet of Things: Security and privacy implications. International Data Privacy Law, 5(2), 99.
39. McIntosh, T., Watters, P., Kayes, A. S. M., Ng, A., & Chen, Y. P. P. (2021). Enforcing situation-aware access control to build malware-resilient file systems. Future Generation Computer Systems, 115, 568-582.
40. Meggitt, S. (2018). MEDJACK Attacks: The Scariest Part of the Hospital.



ISSN 2278–5469 EISSN 2278–5450 I OPEN ACCESS

41. Monshizadeh, M., Khatri, V., Koskimies, O., & Honkanen, M. (2020). IoT Use Cases and Implementations: Healthcare. IoT Security: Advances in Authentication, 225-245.
42. Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors*, *20*(13), 3625.
43. Mykola and Oleksandr (2020, April 29). Healthcare IoT Security: Risks, Rules, Best Practices, and our advice. https://www.aimprosoft.com/blog/iot-security-in-healthcare-software-development/.
44. Noto, J., Fenical, G., & Tong, C. (2010). Automotive EMI shielding–controlling automotive electronic emissions and susceptibility with proper EMI suppression methods. *URL: https://www.lairdtech.com/sites/default/files/public/solutions/Laird-EMI-WP-Automotive-EMI-Shielding-040114.pdf*.
45. Patel, R. (2020). Internet of Things (IoT): Cybersecurity Risks in Healthcare.
46. Prasad, R., & Rohokale, V. (2020). Internet of Things (IoT) and Machine to Machine (M2M) Communication. In Cyber Security: The Lifeline of Information and Communication Technology (pp. 125-141). Springer, Cham.
47. Purbey S, Khandelwal B. (2021). Analyzing frameworks for IoT data storage, representation and analysis: A statistical perspective. *Indian Journal of Engineering*, 18(49), 151-163
48. Rains, L. S., Zenina, T., Dias, M. C., Jones, R., Jeffreys, S., Branthonne-Foster, S., ... & Johnson, S. (2019). Variations in patterns of involuntary hospitalization and legal frameworks: an international comparative study. The Lancet Psychiatry, 6(5), 403-417.
49. Raj, B., Jayakumar, T., & Thavasimuthu, M. (2002). *Practical non-destructive testing*. Woodhead Publishing.
50. Rizvi, S., Pipetti, R., McIntyre, N., Todd, J., & Williams, I. (2020). Threat model for securing the internet of things (IoT) network at the device level. *Internet of Things*, *11*, 100240.
51. Sciforce (2019, Mar 18). Ensuring privacy and security in the healthcare IoT. https://medium.com/sciforce/ensuring-privacy-and-security-in-the-healthcare-iot-7b97549d629c
52. Shiu, Y. S., Chang, S. Y., Wu, H. C., Huang, S. C. H., & Chen, H. H. (2011). Physical layer security in wireless networks: A tutorial. *IEEE Wireless Communications*, *18*(2), 66-74.
53. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
54. Suh, K., Guo, Y., Kurose, J., & Towsley, D. (2006). Locating network monitors: complexity, heuristics, and coverage. *Computer Communications*, *29*(10), 1564-1577.
55. Talukder, S. (2020). Tools and techniques for malware detection and analysis. *arXiv preprint arXiv:2002.06819*.
56. Tchakounté, F., Ngassi, R. C. N., Kamla, V. C., & Udagepola, K. P. (2021). LimonDroid: A system coupling three signature-based schemes for profiling Android malware. *Iran Journal of Computer Science*, *4*(2), 95-114.
57. Thierer, A. D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. Adam Thierer, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21.
58. Velliangiri, S., Karthikeyan, P., & Vinoth Kumar, V. (2021). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *Journal of Experimental & Theoretical Artificial Intelligence*, *33*(3), 405-424.
59. Webster, P. C. (2011). The rise of open-source electronic health records. The lancet, 377(9778), 1641-1642.
60. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250-1258.
61. Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Communications Surveys & Tutorials*, *21*(4), 3723-3768.
62. Zahmatkesh, H., & Al-Turjman, F. (2020). Fog computing for sustainable smart cities in the IoT era: Caching techniques and enabling technologies-an overview. Sustainable Cities and Society, 59, 102139.
63. Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. Information & Management, 55(4), 482-493.
64. Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728-2742.



ISSN 2278–5469 EISSN 2278–5450 I OPEN ACCESS