Security Considerations in the Internet of Medical Things: COVID-19 IoMT Gadgets

Charaf Eddine AIT ZAOUIAT[1], Mohamed BASLAM[2], Mohamed EDDABBAH[3], Mohamed ABDELBAKI[4] Mohamed EL GHAZOUANI[1] and Layla AZIZ[1]

[1]Information Science and Modeling Research Team, Polydisciplinary Faculty of Sidi Bennour, Chouaîb Doukkali University, Morocco
[2]Laboratoire Traitement de l'Information et Aide à la Décision, Sultan Moulay Slimane University, Beni Mellal, Morocco
[3]LABTIC. ENSA Tangier Abdelmalek Essaadi University, Tetouan, Morocco
[4]Information Science and Modeling Research Team, National School of Applied Sciences, Cadi Ayyad University, Marrakech, Morocco

E-mail: charafeddineaitzaouiat@gmail.com

Article history

Received Sep 11, 2023
Revised Oct 09, 2023
Accepted Oct 16, 2023
Published Oct 19, 2023

ABSTRACT

The COVID-19 pandemic has underscored the significance of the Internet of Medical Things (IoMT) in healthcare. During this crisis, IoMT devices played a crucial role in remotely monitoring patients, tracking virus transmission, and supporting healthcare professionals. However, the increased adoption of IoMT devices has also raised concerns regarding security and privacy vulnerabilities. This paper presents a comprehensive analysis of the vulnerabilities found in IoMT devices designed and rapidly deployed during the pandemic, such as remote patient monitoring devices and telemedicine platforms. The study identifies common hardware, software, and communication vulnerabilities that pose potential threats to patient safety and the integrity and confidentiality of healthcare data. Furthermore, the paper examines proposed security mechanisms, including blockchain-based frameworks and lightweight authentication schemes, all of which aim to address these challenges. By raising awareness of these vulnerabilities and risks, this research aims to encourage the development of more secure and resilient IoMT devices in the future.

Keywords: ***IoMT, Vulnerabilities, Security, Covid-19, Countermeasures.***

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized the way we live and work, connecting billions of devices to the internet and enabling them to communicate with each other. One of the most important applications of IoT is in the field of healthcare, known as the Internet of Medical Things (IoMT). IoMT devices, such as wearable sensors and remote monitoring systems, have the potential to improve patient outcomes, increase efficiency, and reduce healthcare costs.

The COVID-19 pandemic has highlighted the critical role that IoMT can play in healthcare. During the pandemic, IoMT devices were used to remotely monitor patients, track the spread of the virus, and ensure that healthcare workers had access to the resources they needed. However, the increased use of IoMT devices also raises concerns about security and privacy.

Several studies have shown that IoMT devices are vulnerable to various types of attacks, including hardware, software, and network-based attacks. For example, a recent study by Jeyavel et al. [1] found that many IoMT devices used during the pandemic were vulnerable to hardware attacks, such as power analysis and fault injection attacks. Another study by Sadhu et al. [2] found that many IoMT devices suffered from software vulnerabilities that could be exploited by attackers to gain unauthorized access or manipulate patient data.

To address these security concerns, several researchers have proposed various security mechanisms for IoMT devices. For instance, Dilawar et al. [3] proposed a blockchain-based security architecture for IoMT devices to ensure data integrity and confidentiality. Similarly, Amintoosi et al. [4] proposed Slight, a lightweight authentication and key management scheme for IoMT devices to protect against unauthorized access.

In this work, our main contribution is to demonstrate the vulnerabilities and potential security risks associated with some IoMT devices designed during the COVID-19 pandemic. We aim to provide a comprehensive analysis of these vulnerabilities and their potential impact on patient safety and healthcare systems. To achieve this, we conducted an extensive literature review of previous studies on the security of IoMT devices. Based on this review, we identified a number of vulnerabilities that are common in many IoMT devices, including hardware vulnerabilities, software vulnerabilities, and communication vulnerabilities. We then focused on IoMT devices that were designed or rapidly deployed during the COVID-19 pandemic, such as remote patient monitoring devices and telemedicine platforms. By analyzing the design and implementation of these devices, we were able to identify specific vulnerabilities that pose a potential threat to patient safety and the confidentiality, integrity, and availability of healthcare data.

Overall, our contribution highlights the importance of addressing these security challenges in IoMT devices, especially during times of crisis such as the COVID-19 pandemic. By raising awareness of these vulnerabilities and the potential risks they pose, we hope to encourage the development of more secure and resilient IoMT devices in the future and to do so in alignment with all the new emerging technologies such as machine learning and artificial intelligence models in general [5].

II. IoT Medical Applications

The Internet of Things (IoT) has revolutionized the healthcare industry, offering a wide range of medical applications that have the potential to transform the way healthcare services are delivered. IoT-enabled medical devices and systems can provide remote patient monitoring, real-time data collection, and analytics, resulting in better diagnosis, treatment, and patient outcomes. However, the development and deployment of IoT medical applications also present several challenges that need to be addressed, some of which were discussed in detail by Ajagbe et.al. [6].

One of the most significant benefits of IoT medical applications is remote patient monitoring. With the help of wearable devices and sensors, patients can be monitored continuously, and data can be collected and analyzed in real-time. This allows doctors to track patients' vital signs, medication adherence, and other health parameters, resulting in timely interventions and improved health outcomes. In their review on IoMT-based remote health monitoring for diabetic patients, Alshorman et al. [7] provided compelling evidence of precisely that.

Another important use case for IoT in healthcare is the development of smart medical devices that can perform diagnostics, track patient progress, and provide real-time feedback. For example, IoT-enabled inhalers can detect inhaler usage and provide feedback to patients to help them use their medication correctly [8]. Similarly, smart glucose meters can track blood glucose levels and provide real-time feedback to help patients manage their diabetes better [9].

However, IoT medical applications also present several challenges. One of the primary challenges is to ensure data privacy and security in all of its different aspects as shown in Figure 1. IoT medical devices collect sensitive personal health data, which must be protected from unauthorized access and cyberattacks. Ensuring the security and privacy of patient data is critical to building trust in IoT medical applications and ensuring widespread adoption [10].

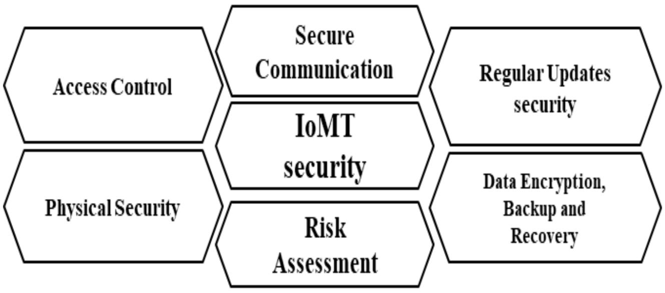


Figure 1. Facets of Internet of Medical Things Security

Another challenge is interoperability. IoT medical devices and systems must be able to communicate and exchange data seamlessly, regardless of the manufacturer or technology used. Achieving interoperability requires the development of common standards and protocols that allow different devices and systems to communicate with each other. In addition to data privacy and interoperability, AlShorman et al. [11] highlighted multiple other challenges faced by medical applications. These include usability, data acquisition, and power consumption.

III. Security of Medical IoT Systems

The security of Medical IoT systems can be divided into a collection of more specific concerns, such as vulnerabilities, attacks and countermeasures. In many medical IoT systems as cited by Chanal et. al [12], security objectives include:

Medical Information Privacy: The caregiver has the obligation to respect the confidentiality of the information of which he has knowledge in the exercise of his profession towards any person, so a medical IoT system must also be subject to this regulation and must stop unauthorized users from accessing sensitive patient information stored or communicated by the system.

Medical Information Integrity: The results of blood analyze, vital signals records as well as the functional explorations are the keys to a successful diagnosis leading to the appropriate care offer for a patient. Therefore, the integrity of these data must be guaranteed by the Medical IoT system, and under no circumstances should they be deleted or modified without permission, whether by error, malicious user or virus [13].

Availability: it refers to the IoT Medical system being accessible when needed by an authorized entity, and without undue delay. For example, uptime is to ensure that denials of service do not succeed. However, the accessibility of a system does not mean that it is available because the system must also perform its function correctly.

Thus, IoT Medical systems remain very vulnerable objective in the face of malicious actions from several sources, namely competitors, hackers, enemies, or even terrorists.

IV. Medical IoT Systems Vulnerabilities and Attacks Classification

In the realm of IoT security, vulnerabilities can be classified into two main categories: system vulnerabilities and human vulnerabilities. Djenna et al. delve into the comprehensive examination of system vulnerabilities, presenting us with an expanded classification of system vulnerabilities [14]. We also compiled into Figure 2 an overall categorization of the most known types of vulnerabilities and attacks that often target information systems.

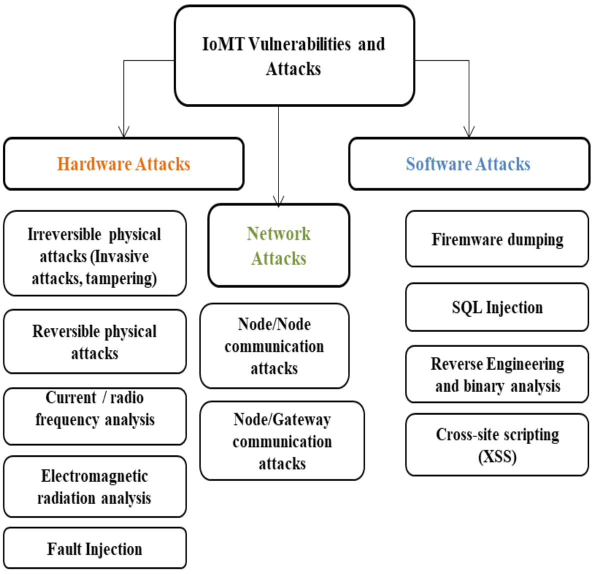

IoMT Vulnerabilities and Attacks
Hardware Attacks
Network Attacks
Software Attacks
Irreversible physical attacks (Invasive attacks, tampering)
Reversible physical attacks
Current / radio frequency analysis
Electromagnetic radiation analysis
Fault Injection
Node/Node communication attacks
Node/Gateway communication attacks
Firemware dumping
SQL Injection
Reverse Engineering and binary analysis
Cross-site scripting (XSS)

Figure 2. Classification of IoMT vulnerabilities and attacks

While those are important to address, we would like to focus here on the end-to-end vulnerabilities and specifically on the main factors that make them easy to exploit:

Social Environment: it is easy to design a safe IoT Medical system based on the natural physical security of the system (no one can open the system) or to assume that parts of the system cannot be accessed by malicious entities. However, these systems sometimes need to work in complex relationships, where a healthcare provider wishes to put a secure part in the hands of others. Ensuring that the second part cannot modify the internal parts of the device.

Complex design process and multi-vendors: due to a multi-vendor architecture, it may not be possible to pre-validate every component of the IoT medical system to ensure its security. In other words, even if each component of the system is insured on its own, it is possible that the composition of the parts exposes new vulnerabilities due to the backdoor of each manufacturer [15].

Development tool kits: in order to provide and enrich the functionality of medical IoT systems and personalized them for the end user, it is sometimes necessary to have the ability to download and run untrusted (approved) software, (with viruses, threesomes, etc ...) which can be the source of the vulnerabilities.

Practically, all these attacks can be classified based on two criteria: The functional objective and the methods used to execute these attacks. The first Criterion involves the issues of confidentiality, integrity and availability in the medical IoT systems. While the second criterion involves Hardware, tools and methods used for medical IoT systems security penetration.

Hence, according to the architecture explained above, we can deduce that the IoT or IoMT ecosystem in particular has four attack surfaces. A first surface, which is the “thing” itself, namely its hardware, and software, and then a second surface, which concerns the networking of that thing with the rest of the ecosystem. The third and the firth surfaces concern respectively the mobile and cloud surfaces. The investigation on the reminder of this paper will focus on the methods and tools used to attack medical IoT systems, based on a case study of COVID-19 IoT gadget.

V. Covid-19 IoT Gadget Security

A. *Covid-19 IoT Gadget for Home Healthcare Protocol (HHP) Benchmarking*

The Covid-19 pandemic has highlighted the importance of remote patient monitoring systems in healthcare [16]. With the advent of IoT technology, medical telemonitoring solutions have become increasingly popular in recent years. The Covid-19 IoT Gadget for Home Healthcare Protocol (HHP) is an example of such a solution. It allows patients diagnosed with Covid-19 to be remotely monitored from home, reducing the need for hospitalization and the risk of exposure to the virus. The HHP includes a range of IoT devices such as wearables, sensors, and mobile apps, which are used to collect patient data such as vital signs, oxygen levels, and temperature. The collected data is transmitted securely to healthcare providers, who can use it to monitor the patient's condition and adjust treatment as needed. The HHP can also be used in nursing homes to monitor the health of residents and prevent the spread of Covid-19.

IoMT devices have played a crucial role in the fight against Covid-19 [17]. Examples of these devices include contactless thermometers, pulse oximeters, smart masks, and remote monitoring systems. Contactless thermometers allow for remote temperature monitoring without physical contact, while pulse oximeters monitor the oxygen saturation levels in a patient's blood. Smart masks can monitor a person's respiratory rate, temperature, and air quality, and remote monitoring systems can track patients' vital signs.

Benchmarking these devices involves evaluating their effectiveness, usability, and security. For example, one benchmark might be the accuracy of a contactless thermometer compared to a traditional thermometer. Another benchmark might be the ease of use and comfort of an IoT-enabled mask. Security benchmarks might include evaluating the device's encryption protocols and vulnerability to hacking. While IoMT devices offer many benefits in the fight against Covid-19, they also pose several security challenges. The transmission of patient data over the internet raises concerns about data privacy and confidentiality, and IoT devices themselves may be vulnerable to cyber attacks. Addressing these security challenges is critical to realizing the full potential of IoMT devices in healthcare.

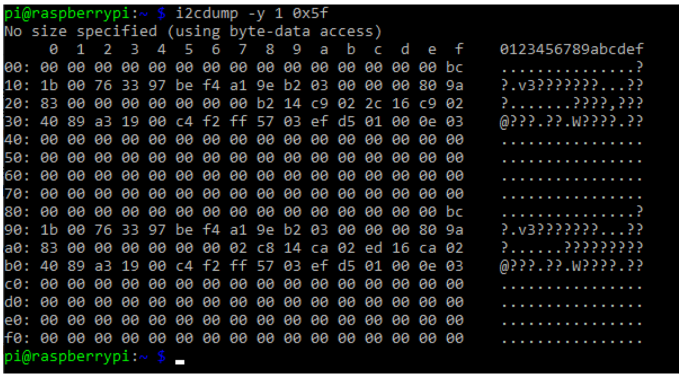
B. Pressure Sensor I2C Memory Dumping

Pressure sensors are electronic devices that convert gas or liquid pressure into an electrical signal. In medical applications, these sensors play a vital role in measuring physiological pressures, such as blood pressure, intracranial pressure, and pulmonary pressure, to provide accurate diagnosis, monitoring, and treatment of various medical conditions.

One example of an I2C pressure sensor is the NXP MPX5010DP, which is used in medical devices such as respiratory monitors, anesthesia machines, and blood pressure monitors. Other examples of I2C pressure sensors include the BMP280 from Bosch Sensortec, the MS5803 from Measurement Specialties, and the LPS22HB from STMicroelectronics.

Manufacturers such as Philips Respironics and GE Healthcare use I2C pressure sensors in their medical devices. Philips Respironics, for example, uses the NXP MPX5010DP in their Trilogy ventilators to monitor airway pressure and adjust the ventilator settings accordingly. GE Healthcare uses the MS5803 in their B40 patient monitor to measure invasive blood pressure.

While I2C pressure sensors have improved patient outcomes and advanced healthcare technology, they are also vulnerable to firmware dumping. Firmware dumping is a serious security concern for medical devices that use pressure sensors and other types of sensors. If an attacker gains access to the device's firmware, they can potentially modify the sensor's output values, compromising the device's integrity and the accuracy of the patient data it collects. This can lead to incorrect diagnoses, improper treatment, and potentially life-threatening situations for patients. Furthermore, attackers can extract sensitive patient data from the device's firmware, violating patient privacy and exposing them to identity theft or other forms of harm.



```
pi@raspberrypi:~ $ i2cdump -y 1 0x5f
No size specified (using byte-data access)
     0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f    0123456789abcdef
00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bc    ...............?
10: 1b 00 76 33 97 be f4 a1 9e b2 03 00 00 00 80 9a    ?.v3???????...??
20: 83 00 00 00 00 00 00 00 b2 14 c9 02 2c 16 c9 02    ?.......????,???
30: 40 89 a3 19 00 c4 f2 ff 57 03 ef d5 01 00 0e 03    @???.??.W????.??
40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bc    ...............?
90: 1b 00 76 33 97 be f4 a1 9e b2 03 00 00 00 80 9a    ?.v3???????...??
a0: 83 00 00 00 00 00 00 02 c8 14 ca 02 ed 16 ca 02    ?......?????????
b0: 40 89 a3 19 00 c4 f2 ff 57 03 ef d5 01 00 0e 03    @???.??.W????.??
c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
pi@raspberrypi:~ $
```

Figure 3. i2c dumping with Raspberry Pi

In very basic scheme, the Raspberry Pi can be employed to perform I2C dumping, enabling data acquisition from various sensors, including medical pressure sensors. To utilize the Raspberry Pi for I2C dumping, researchers must first ensure that the necessary hardware and software components are in place. This involves connecting the Raspberry Pi's GPIO pins to the appropriate pins on the pressure sensor using jumper wires. Additionally, researchers must enable the I2C interface on the Raspberry Pi by modifying the system's configuration. Once the physical connections and interface settings are established, researchers can utilize Python programming and the appropriate libraries, such as smbus, to initiate I2C communication with the pressure sensor. Through the I2C protocol, researchers can send commands and receive data from the pressure sensor as depicted in Figure 3. This data can then be logged, analyzed, and visualized for further scientific investigation. The Raspberry Pi's versatility, low cost, and ease of use make it a valuable tool in scientific research, providing researchers with the means to interface with medical sensors and perform I2C dumping for data acquisition and subsequent analysis.

C. Temperature Sensor UART Firmware Update

When it comes to UART temperature sensors, several manufacturers offer solutions tailored for diverse applications. Maxim Integrated is recognized for its range of UART-enabled temperature sensors suitable for healthcare and industrial monitoring. Texas Instruments produces temperature sensor ICs with UART interfaces, providing flexibility in temperature sensing applications. Sensirion, another prominent manufacturer, offers a wide array of sensors including temperature sensors with UART interfaces, commonly utilized in industrial and consumer settings. Silicon Labs specializes in UART-enabled temperature sensors, ensuring precise temperature measurement and monitoring across various environments. While these manufacturers provide UART temperature sensors, it is essential to explore their product catalogs to identify the most suitable option based on specific project requirements and compatibility.

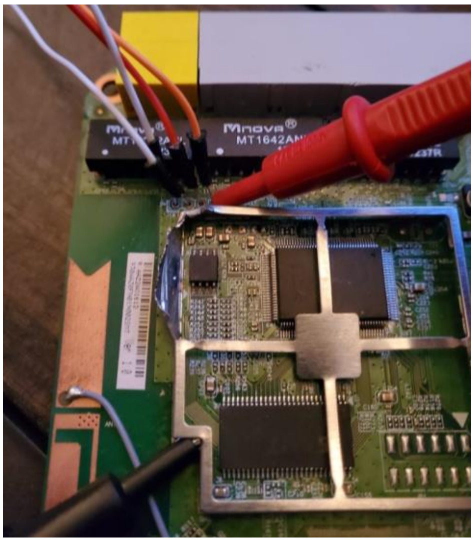


Figure 4. UART firmware dumping

UART temperature sensors, like any devices with UART interfaces, can potentially be vulnerable to UART firmware dumping if proper security measures are not implemented. The vulnerability arises due to factors such as insecure UART implementations, debugging or development features, or the absence of secure boot mechanisms and firmware encryption. If the UART interface on the temperature sensor's microcontroller or IoT device is not adequately secured, an attacker with physical access to the device could connect to the UART port and interact with the firmware. We can refer to Figure 4 where it can be seen how this can be done if an attacker could expose the internal circuit of a device. They could potentially dump or extract the firmware from the device, gaining access to sensitive information or the underlying code. Lack of secure boot mechanisms or firmware encryption further increases the risk, as it enables attackers to intercept communication over the UART interface and capture the firmware data being transmitted. To mitigate these vulnerabilities, it is crucial to secure the UART interface, implement secure boot mechanisms, enable firmware encryption, and ensure proper physical access restrictions to prevent unauthorized firmware dumping and protect the integrity and confidentiality of the temperature sensor's firmware.

D. Covid-19 IoT *Gadaget* HTTPS Data Interception

The COVID-19 pandemic has ushered in a digital transformation in healthcare, with the widespread adoption of online applications and services to facilitate COVID-19 testing, telehealth consultations, vaccine appointments, contact tracing, and access to information portals. While these applications utilize HTTPS (Hypertext Transfer Protocol Secure) to protect data transmission and ensure privacy, it is crucial to understand the potential vulnerabilities that can arise with HTTPS interception, particularly when it comes to the data privacy of patients.

COVID-19 Testing Portals have emerged as a critical component of testing infrastructure, enabling individuals to schedule appointments, receive test results, and manage their health information online. These portals rely on HTTPS encryption to secure the sensitive personal data exchanged between users and the healthcare providers. However, in situations where the network infrastructure or client devices are compromised, attackers can intercept the HTTPS traffic, potentially gaining unauthorized access to personal health data. This interception could expose sensitive information such as personal identification details, medical history, and test results, posing significant risks to patient privacy and confidentiality.

Telehealth Services have witnessed a tremendous surge during the pandemic, allowing patients to receive medical consultations remotely. While HTTPS ensures privacy during these online interactions, attackers could intercept the encrypted traffic and gain access to patient-doctor communications or manipulate medical data by decrypting it on their machines offline (Figure 5 provides a visual depiction of this process). The interception of HTTPS in telehealth services could compromise the confidentiality of sensitive medical discussions, diagnosis information, and treatment plans, undermining the trust and privacy expected in these virtual healthcare encounters.

Vaccine Appointment Systems have become pivotal in managing the vaccination campaigns against COVID-19. These systems rely on HTTPS encryption to secure the transmission of personal details during appointment bookings. However, interception of HTTPS traffic by malicious actors could expose sensitive information, including personal identification data, contact information, and medical history. Such interception not only jeopardizes the privacy of individuals but also opens avenues for potential identity theft or misuse of personal data.

Contact Tracing Applications have been widely employed to help identify potential exposure to COVID-19 by logging interactions between individuals. These apps utilize HTTPS to protect user privacy during data transmission. However, if the HTTPS connection is intercepted, adversaries may gain access to sensitive location data, personally identifiable information (PII), and potential exposure history. This interception not only compromises the privacy of individuals but could also result in stigmatization or targeted attacks based on individuals' COVID-19 status.

COVID-19 Information Portals have served as critical resources for individuals seeking up-to-date information, guidelines, and resources related to the pandemic. These portals typically employ HTTPS to ensure secure browsing and protect user data. However, interception of HTTPS traffic can enable attackers to inject malicious content into the website, leading to misinformation dissemination, phishing attacks, or the exploitation of individuals seeking reliable COVID-19 information. Such risks not only undermine data privacy but also compromise the trust and well-being of users relying on these platforms

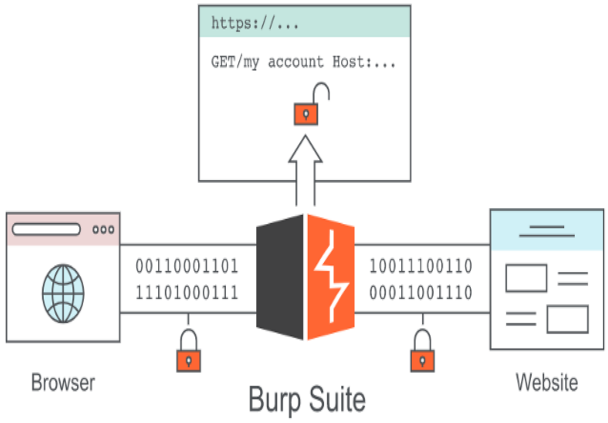


Figure 5. HTTPS interception with Burp Suite Tool

To mitigate these vulnerabilities and safeguard patient data privacy, organizations and individuals must take several precautions. These include ensuring the use of trusted HTTPS certificates, implementing strong encryption protocols, staying up to date with security patches, regularly monitoring network traffic for signs of interception or tampering, and educating users about the importance of verifying website authenticity and avoiding suspicious links or downloads. Additionally, regulatory compliance, data encryption at rest, robust access controls, and secure storage and transmission mechanisms should be prioritized by healthcare providers and application developers to protect patient privacy throughout the entire lifecycle of these applications.

E. Covid-19 IoT Gadget Attacks Countermeasures

The COVID-19 pandemic has highlighted the importance of countering the potential vulnerabilities in medical IoT devices and applications. Several countermeasures can be implemented to enhance the security and privacy of these systems.

Firstly, strong encryption protocols should be implemented to protect the data transmitted between IoT devices and healthcare providers. The use of robust encryption algorithms and secure key management practices can significantly enhance data security.

Secondly, secure boot mechanisms can be employed to ensure the integrity of the firmware running on IoT devices. Secure boot verifies the authenticity and integrity of the firmware during the device's startup, preventing unauthorized or malicious firmware from being loaded.

Thirdly, access controls should be implemented to restrict physical and remote access to IoT devices. By implementing proper authentication and authorization mechanisms, only authorized individuals should be able to access and interact with the devices.

Regular security updates and patch management are also crucial to address any identified vulnerabilities promptly. Manufacturers and developers should actively monitor and address security vulnerabilities by releasing timely patches and updates.

Furthermore, organizations should prioritize the implementation of secure development practices, including secure coding, vulnerability testing, and rigorous security audits. This ensures that IoT devices and applications are built with security in mind from the ground up.

User awareness and education play a vital role in mitigating security risks. Healthcare providers and IoT device manufacturers should educate users about best practices for data privacy and security. This includes advising users to keep their devices updated, use strong and unique passwords, and avoid connecting to unsecured networks.

Lastly, compliance with privacy regulations, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA), is crucial to safeguard patient data privacy. Organizations should implement appropriate measures to comply with these regulations and ensure that patient data is handled in a secure and compliant manner.

By implementing these countermeasures, the risks associated with IoT devices and applications in the context of COVID-19 can be significantly reduced. Protecting patient data privacy and maintaining the integrity of medical IoT systems are crucial to building trust and ensuring the effectiveness of these technologies in providing quality healthcare services.

VI. CONCLUSION

The COVID-19 pandemic has revealed both the potential and vulnerabilities of IoMT devices in healthcare. While IoMT has shown its value in remote patient monitoring and supporting healthcare delivery during crisis situations, it has also exposed security and privacy risks that must be addressed. This study conducted a thorough analysis of vulnerabilities in IoMT devices designed during the pandemic and identified common hardware, software, and communication vulnerabilities.

To mitigate these risks, researchers have proposed various security mechanisms, including blockchain-based frameworks and lightweight authentication schemes. These approaches aim to ensure data integrity, confidentiality, and secure access to IoMT devices. However, further research and collaboration between industry stakeholders, healthcare providers, and security experts are necessary to develop standardized security measures and best practices for IoMT devices.

Addressing the security challenges in IoMT devices is crucial to protect patient safety, maintain the trust of users, and encourage the wider adoption of these technologies. By raising awareness of the vulnerabilities and potential risks associated with IoMT devices, this research contributes to the ongoing efforts to develop more secure and resilient healthcare systems. Future advancements in IoMT security should prioritize the implementation of robust security measures, regular vulnerability assessments, and comprehensive testing to ensure the confidentiality, integrity, and availability of healthcare data in all scenarios, including times of crisis.

REFERENCES

[1] J. Jeyavel, T. Parameswaran, J. M. Mannan, and U. Hariharan, “Security Vulnerabilities and Intelligent Solutions for IoMT Systems,” in Internet of Medical Things: Remote Healthcare Systems and Applications, D. J. Hemanth, J. Anitha, and G. A. Tsihrintzis, Eds., in Internet of Things. Cham: Springer International Publishing, 2021, pp. 175–194. doi: 10.1007/978-3-030-63937-2_10.

[2] P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, “Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions,” Sensors (Basel), vol. 22, no. 15, p. 5517, Jul. 2022, doi: 10.3390/s22155517.

[3] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, “Blockchain: Securing Internet of Medical Things (IoMT),” ijacsa, vol. 10, no. 1, 2019, doi: 10.14569/IJACSA.2019.0100110.

[4] H. Amintoosi, M. Nikooghadam, M. Shojafar, S. Kumari, and M. Alazab, “Slight: A lightweight authentication scheme for smart healthcare services,” Computers and Electrical Engineering, vol. 99, p. 107803, Apr. 2022, doi: 10.1016/j.compeleceng.2022.107803.

[5] C. E. Aitzaouiat, A. Latif, A. Benslimane, and H.-H. Chin, “Machine Learning Based Prediction and Modeling in Healthcare Secured Internet of Things,” Mobile Netw Appl, vol. 27, no. 1, pp. 84–95, Feb. 2022, doi: 10.1007/s11036-020-01711-3.

[6] S. A. Ajagbe, J. B. Awotunde, A. O. Adesina, P. Achimugu, and T. A. Kumar, “Internet of Medical Things (IoMT): Applications, Challenges, and Prospects in a Data-Driven Technology,” in Intelligent Healthcare: Infrastructure, Algorithms and Management, C. Chakraborty and M. R. Khosravi, Eds., Singapore: Springer Nature, 2022, pp. 299–319. doi: 10.1007/978-981-16-8150-9_14.

[7] O. AlShorman, B. AlShorman, M. Al-khassaweneh, and F. Alkhatani, “A review of internet of medical things (IoMT) - based remote health monitoring through wearable sensors: a case study for diabetic patients,” IJEECS, vol. 20, no. 1, p. 414, Oct. 2020, doi: 10.11591/ijeecs.v20.i1.pp414-422.

[8] Q. Chen, Y. Zhao, and Y. Liu, “Current development in wearable glucose meters,” Chinese Chemical Letters, vol. 32, no. 12, pp. 3705–3717, Dec. 2021, doi: 10.1016/j.cclet.2021.05.043.

[9] R. Hireche, H. Mansouri, and A.-S. K. Pathan, “Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis,” Journal of Cybersecurity and Privacy, vol. 2, no. 3, Art. no. 3, Sep. 2022, doi: 10.3390/jcp2030033.

[10] O. AlShorman, B. Alshorman, M. Masadeh, F. Alkahtani, and B. Al-Absi, “A review of remote health monitoring based on internet of things,” IJEECS, vol. 22, no. 1, p. 297, Apr. 2021, doi: 10.11591/ijeecs.v22.i1.pp297-306.

[11] P. M. Chanal and M. S. Kakkasageri, “Security and Privacy in IoT: A Survey,” Wireless Pers Commun, vol. 115, no. 2, pp. 1667–1693, Nov. 2020, doi: 10.1007/s11277-020-07649-9.

[12] S. Bowman, “Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications,” Perspect Health Inf Manag, vol. 10, no. Fall, p. 1c, Oct. 2013.

[13] Djenna and D. Eddine Saidouni, “Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure,” in 2018 2nd Cyber Security in Networking Conference (CSNet), Paris: IEEE, Oct. 2018, pp. 1–4. doi: 10.1109/CSNET.2018.8602974.

[14] S. Weyer, M. Schmitt, M. Ohmer, and D. Gorecky, “Towards Industry 4.0 - Standardization as the crucial challenge for highly modular, multi-vendor production systems,” IFAC-PapersOnLine, vol. 48, no. 3, pp. 579–584, Jan. 2015, doi: 10.1016/j.ifacol.2015.06.143.

[15] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Examining smart-card security under the threat of power analysis attacks,” IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, May 2002, doi: 10.1109/TC.2002.1004593.

[16] H. Mohd Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, “IoMT amid COVID-19 pandemic: Application, architecture, technology, and security,” Journal of Network and Computer Applications, vol. 174, p. 102886, Jan. 2021, doi: 10.1016/j.jnca.2020.102886.

[17] B. Šehović and K. Govender, “Addressing COVID-19 vulnerabilities: How do we achieve global health security in an inequitable world,” Global Public Health, vol. 16, no. 8–9, pp. 1198–1208, Sep. 2021, doi: 10.1080/17441692.2021.1916056.