IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, October 2022

A Review of the New Remote Patient Monitoring Device Security Framework

Navneet Vishnoi, Assistant Professor,
Department of CCSIT, Teerthanker Mahaveer University Moradabad, Uttar Pradesh, India
Email Id- vishnoi_navneet@yahoo.co.in

ABSTRACT: ***Security has long been a source of contention in the healthcare business. Because of a lack of understanding and insufficient security implementation in healthcare, patients' data is vulnerable to attackers. The main problem is figuring out how to provide security in an RPM environment. There is little practical data on how to correctly install security, as per the findings in the literature. As a result, it's important to address cybersecurity risks in medical equipment. And, to use a Microsoft threat modelling approach and a review of the current literature on remote patient monitoring, discover and analyse existing vulnerabilities and hazards in IEEE 11073 standard devices in order to propose a new security architecture for remote patient monitoring devices. Furthermore, even though current RPM machines have a restriction on the total of people who can truly share a single device, individuals propose using NFC as an identification number in Remote Patients Monitoring devices for multi-user environments where multiple people share a single device to reduce errors associated with incorrect user identification. Finally, we show how the proposed framework was built utilising a number of techniques.***

KEYWORDS: ***Monitoring Security, Remote Patient, Telehealth Security, Telemedicine Security.***

1. INTRODUCTION

Remote patient monitoring (RPM) is the use of technology to monitor patients from the comfort of their own homes, with the goal of improving access to high-quality treatment while lowering healthcare expenditures. The FDA defines cybersecurity as "the process of preventing access, modification, misuse, as well as denial of use of information that is stored, accessed, or converted from a medical product to an external recipient, as well as the unapproved use of data that is stored, accessed, or transferred from a medical product to an external recipient." Cybercriminals have turned their attention to the healthcare industry. According to a recent study, 94 percent of healthcare organizations have been attacked by hackers, including medical device assaults[1], [2]. As a result, the FDA in the United States has been charged with ensuring the safety, efficacy, and security of medical products in the nation. A healthcare cyber threat report launched in February 2014 by Norse as well as SANS involving a one-month study of malicious traffic aimed at healthcare organizations in the US found 49,917 unique attacks across and over 700 devices, with 375 US-based healthcare organizations compromised.

Compromised devices included mail servers, firewalls, and radiology software. An attacker hacked a dialysis machine and attempted to buy items online using a fake credit card information, according to the Norse and SANS study. If the dialysis equipment malfunctions, an opportunistic assault may quickly put the patient who is using it in risk. These results indicated that RPM systems may be remotely hacked, putting patients' lives in jeopardy. Furthermore, it is quite probable that prospective attackers would monitor the actions and health information of RPM devices over time, highlighting the problem of patient privacy. Furthermore, there is evidence that thieves may steal medical data and impersonate patients, according to the research. To address the problem of cyberattacks, certain organizations, such as NHS trusts in England, must have appropriate training programs in place to guarantee that their employees are protected from cyber threats. As a consequence, failing to maintain

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, October 2022

cybersecurity and properly respond to cyber-attacks may result in not only medical equipment being compromised, but also data loss, integrity, and availability, posing a danger to patients' lives.

As a result, healthcare providers that utilize medical devices must not depend only on device makers to guarantee device security, but must also take measures to protect patient information inside their networks. Furthermore, healthcare providers must keep their antivirus software and firewalls up to date, disclose any medical device security vulnerabilities, and keep an eye on any unauthorised network activity[3], [4].

Encryption of Health Data Legislation There is a comprehensive set of laws in place to safeguard personal health data, including regional, national, and international legislation. For example, HIPAA in the United States and the Data Protection Act 1998 in the United Kingdom apply to both electronic and paper methods to health record administration. These laws address some of the problems while also protecting privacy and security by imposing penalties on those who break the law. The HIPAA, for example, stipulates up to ten years in jail for selling a patient's health data when sensitive information about just a person's health problems is revealed and societal harm is caused. However, there is no mechanism to revoke the information or return the individual. As a result, technical tools for enforcing privacy protection and preventing security and privacy breaches are crucial.

1.2.Problems with Current RPM Devices:

One of the major holes in RPM architectural research, according to telehealth research, is that the problem of security is not addressed since the researchers are unfamiliar with it. These results indicate that telehealth and Remote Patient Monitoring (RPM) devices may offer an ideal environment for opportunistic security assaults. Furthermore, the number of users who may use any RPM device at any one time is restricted, and only the person who is being monitored is permitted to use the device. As a result, if another individual uses the same device, an erroneous reading will be recorded in the patient's file. According to the results in the literature, there is little practical data on how security is implemented in RPM devices, or if there is, it is done badly. Furthermore, owing to a lack of standards that specify interoperability, none of the studies performed so far have addressed the question of how to effectively integrate security on RPM devices. The majority of research have assumed that medical device makers are responsible for security. The problem of verification of the person using the device was also a concern in the present design of RPM devices since the measurement is not monitored at home and the device lacks an identity and authentication mechanism. As a result, if the patient's ID is not validated, erroneous data may be entered into the patient's record, potentially leading to wrong diagnosis and treatment. As a result, a number of important issues in the RPM device architecture must be addressed.

If several people use the same equipment without identifying themselves, the erroneous measurement may be transmitted to the wrong user, resulting in the user receiving the incorrect intervention. To address these issues, a diagnosis is established technique built into RPM devices can be beneficial in settings such as nursing homes for the elderly and households with two or more persons suffering from the same chronic disease, as it will allow for a large number of users to be monitored while reducing the costs of having multiple devices. With the present design, however, this option is restricted[5].

1.3.Models of Security:

Other frameworks suggested by other writers provide the necessary analyses for safe health. Although these frameworks have some value, the authors believe that a new framework is needed that incorporates the features and functionality of these structures in contexts of major

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, October 2022

entities such as cloud infrastructure, applications, as well as the cognitive abilities of the elderly, who are the primary beneficiaries of RPM. As a result, these frameworks may be used as reference models. The United4health functional model examines how to integrate end-to-end security in an RPM architecture in great depth. The United4Health security paradigm and its description are discussed in the next section.

1.4.Telehealth Functional Model for United Health:

Security of RPM devices was examined in a research performed by for the United Health telehealth trial system for chronic obstructive pulmonary disease (COPD) patients project. Despite the fact that their functional model has not been implemented in RPM, it offers a comprehensive overview of the security needs for RPM. They recommended the use of PINs for patient identification in their functional model; however, because this technology is for the elderly who may have cognitive impairments, this approach would not be practical for them. The authors also state that if users forget their PINs, they must call the nurses supporting the service for assistance; this approach will not be practical for them. They also ignore the problem of multi-user environments, in which users must share a single device.

1.5.Authentication of devices:

When an unauthenticated device is brought into an RPM environment, this danger arises. Only authorized devices will be permitted on the network thanks to device authentication. In healthcare, diseases like diabetes rely on precise measurements for treatment; if a device is lost or replaced with a rogue device and then released into the ecosystem, there's a good chance it'll send the wrong reading, triggering the wrong treatment, potentially putting the patient's life at risk. Data availability refers to the steps taken to guarantee that data is available at the necessary level of performance in a variety of circumstances, from normal to catastrophe. It's quite probable that data will be rendered inaccessible or hacked if the telemonitoring server and management device don't have adequate security measures in place. The problem of data availability is not addressed in this approach [6], [7].

Take charge of device security. When managers are attacked with malware that has the capacity to alter data format, security problems may emerge. The authors of United4Health (United4Health project aiming at exploitation and further deployment of novel telemedicine services developed and trailed under the renewing health projects) neglected to include the management device's security criteria, which are critical[8].

Point of care: The patient collects their readings from the SpO2 sensor device, which sends the data to the management device through a wireless Bluetooth connection. The SpO2 data is saved locally on the management device in a database. The data is subsequently sent to the HIS infrastructure via the management device. The patient enters a PIN on the management device to verify their identity. The patient is identified via a login and PIN.

1.6.Service of Health Information:

The data is sent and stored in a PEHR from the management device. Clinicians and caregivers may get access to the information through a telehealth service that offers web-based information. End-to-end encryption communication between the management device and the PEHR is provided via HTTPS. For authentication and bidirectional session encryption, the management device's unique device identification and the associated symmetric key known to the PEHR are utilized [9].

1.7.Sources and health care:

Patients' data is accessible to a variety of organizations, doctors, and care providers. This may be accessed through a web-portal that contains information on the data being monitored by

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, October 2022

the HIS infrastructure. The system's users are granted access depending on their roles. The United4health functional model offers a comprehensive overview of the RPM system's security needs.

1.8.The New RPM Device Security Framework:

The researchers suggest a security model for RPM devices, which is currently the most complete security framework available. The suggested framework is built using guidelines from the literature as well as the threat model. As a result, the suggested paradigm provides a foundation for understanding and evaluating security in RPM. The suggested security paradigm for RPM devices is broken down into many components, which are detailed below.

Local Area Network (LAN) The sequence and prompts must be simple to follow since the suggested technology is for the elderly. From turning on the device to patients identifying themselves to the device with their NFC tags and transmitting the BP measurements, the process and instructions must be simple to follow. A few suggestions have also been suggested to improve usability and make it easier to understand and follow.

How It Will Operate A patient uses their NFC tag to identify themselves on the NFC reader, then takes their blood pressure. The system will next check to see whether the patient or caregiver has been given permission to transmit blood pressure measurements, and if so, the system will enable the sender to do so.

The IEEE 11073 PHD standards do not establish security requirements for the management device, while the present research suggests that security requirements for a manager device should be specified since the manager device is susceptible to security threats, as shown by the threat model. The threat model was utilized in the suggested framework to detect existing risks in RPM devices. The proposed architecture includes mitigation methods that may be utilized to protect current devices against attacks. The threat modelling tool aids in the detection of security risks and flaws. Malware on the management device has the ability to corrupt and alter the data format. Malware and viruses may be protected using an anti-virus program. Furthermore, the threat model highlighted the danger of spoofing and repudiation in agent manager communication. As a result, it's critical to verify the sender's identity, and digital signatures may be employed to avoid non-repudiation problems.

Infrastructure for Telemonitoring Servers The information gathered from patients utilizing PHDs is kept on a telemonitoring server at the clinic or hospital that is monitoring the patients. The telemonitoring server's security is critical because it guarantees the confidentiality, availability, and privacy of the patient's health data, and without the proper security measures in place, the telemonitoring server may be susceptible to security assaults. This research suggests storing data in the cloud to guarantee data availability in the event that the telemonitoring server is hacked. Asymmetric keys may be used to encrypt sessions using the Public Key Infrastructure (PKI) (PKI). In addition, a Certification Authority (CA) may issue and verify digital certificates for manager and telemonitoring server authentication.

Infrastructure for Cloud Servers The present research suggests using cloud infrastructure to ensure PHR/EHR availability and security. The suggested file system is a distributed file system with all data blocks encrypted. The data blocks will be duplicated and distributed among many cloud block storage servers at random. It is important to remember, however, that each country's data security standards will be different. The meta-data portion of the file will not be kept in the cloud to enhance security. The meta-data is secured such that even if an intruder decodes a block of data, reading the whole file would be very difficult. The data blocks are secured using AES 256-bit encryption, which is the NHS's approved encryption method in the United Kingdom [10].

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, October 2022

2. DISSCUSION

The use of technology to monitor patients from the comfort of their own homes with the aim of increasing access to high-quality treatment while reducing healthcare costs is known as remote patient monitoring. "The process of preventing unauthorized access, alteration, misuse, as well as denial of use of data that is stored, accessed, or transmitted from a medical product to an external recipient," according to the FDA, as well as "the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient." Security is becoming a major issue, and it must be prioritized in order for telehealth to thrive. NFC was proposed as a solution to the issue of multi-user device patient identification in this study. In an RPM ecosystem, the RPM security model will help to reduce security vulnerabilities and threats while also possibly enhancing security. As a result, addressing cybersecurity concerns in medical equipment is critical. Discover and evaluate existing vulnerabilities or hazards in IEEE 11073 standard devices using a Microsoft threat modeling tool and a study of the current literature on remote patient monitoring in order to propose a new security architecture for remote patient monitoring devices. Furthermore, even though current RPM devices have a limit on how many people can actually share a single device, humans recommend using NFC as an identifier in Remote Patients Monitoring equipment for multi-user climates where multiple people creates a common device to minimize errors caused by incorrect user identification.

3. CONCLUSION

Security is becoming a significant problem, and in order for telehealth to succeed, it must be a primary focus. In this research, NFC was suggested as a solution to the problem of multi-user device patient identification. The RPM security model will aid in reducing security vulnerabilities and threats in an RPM ecosystem, as well as potentially improving security. Because this technology is utilized by the elderly, concerns like as usability must be prioritized for telehealth to be generally accepted.

REFERENCES:

[1] S. D. Verifier and A. H. Drive, “Simulink ® Verification and Validation ™ Reference,” *ReVision*, 2015.

[2] I. Mergel, “OpenCollaboration in Public Sector: The case of social codign on Github,” *Gov. Inf. Q.*, 2012.

[3] Sandra V. B. Jardim*, “The Electronic Health Record and its Contribution to Healthcare Information Systems Interoperability,” *Procedia Technol.*, 2013.

[4] S. De Geest *et al.*, “Interventions for enhancing medication adherence (Review) Interventions for enhancing medication adherence,” *JMIR mHealth uHealth*, 2017.

[5] SAMA *et al.*, “Digital Transformation for a Sustainable Society in the 21st Century,” *Commun. Comput. Inf. Sci.*, 2017.

[6] S. Kumari, D. C. S. Lamba, and A. Kumar, “Performance Analysis of Adaptive Approach for Congestion Control In Wireless Sensor Networks,” *IOSR J. Comput. Eng.*, 2017, doi: 10.9790/0661-1903047178.

[7] P. Ravichandran, “Application of wireless sensor networks in real time patient health status monitoring system,” *J. Eng. Appl. Sci.*, 2017, doi: 10.3923/jeasci.2017.3933.3935.

[8] B. Ondiege, M. Clarke, and G. Mapp, “Exploring a new security framework for remote patient monitoring devices,” *Computers*, vol. 6, no. 1, 2017, doi: 10.3390/computers6010011.

[9] D. Vassis, P. Belsis, C. Skourlas, and G. Pantziou, “A pervasive architectural framework for providing remote medical treatment,” 2008, doi: 10.1145/1389586.1389614.

[10] E. Al Alkeem, C. Y. Yeun, and M. J. Zemerly, “Security and privacy framework for ubiquitous healthcare IoT devices,” 2016, doi: 10.1109/ICITST.2015.7412059.