IEEE
Advancing Technology for Humanity

IEEE ComSoc
IEEE Communications Society

Internet of Things, Ad Hoc and Sensor Networks Technical Committee Newsletter

(IoT-AHSN TCN)

Volume 1, No. 16

June, 2022

CONTENTS

PREFACE

The IEEE ComSoc Ad Hoc and Sensor Networks Technical Committee (IoT-AHSN TC) sponsors papers, discussions, and standards on all aspects of IoT, ad hoc and sensor networks. It provides a forum for members to exchange ideas, techniques, and applications, and share experience among researchers. Its areas of interest include systems and algorithmic aspects of sensor and ad hoc networks, networking protocols and architecture, embedded systems, middle-ware and information management, novel applications, flow control and admission control algorithms, network security, reliability, and management. In an attempt to make all the TC members as well as the IoT-AHSN worldwide community aware of what is going on within our main areas of concerns, this newsletter had been set up. The newsletter aims at inviting the authors of successful research projects and experts from all around the world with large vision about IoT-AHSN-related research activities to share their experience and knowledge by contributing in short news.

The sixteenth issue of the IoT-AHSN TC Newsletter focuses on the theme “Artificial Intelligence of Things”. Specifically, this issue includes 1 news article: Applications of Internet of Things in the Medical Field. We thank the contributors for their efforts to help make the IoT-AHSN TC Newsletter a success. We hope that the methods/approaches presented in this issue could significantly benefit researchers and application developers who are interested in IoT and ad hoc/sensor networks.

Newsletter Co-Editors
Qiang Ye (Dalhousie University, Canada)
Moez Esseghir (University of Technology of Troyes, France)
Lu Lv (Xidian University, China)

TC OFFICERS AND NEWSLETTER EDITORS

TC Officers

Name	Affiliation	Email
Jiajia Liu (Chair)	Xidian University, China	liujiajia@xidian.edu.cn
Sharief Oteafy (Vice Chair)	DePaul University, USA	soteafy@depaul.edu
Shuai Han (Secretary)	Harbin Institute of Technology, China	hanshuai@hit.edu.cn

Newsletter Editors

Name	Affiliation	Email
Qiang Ye (Editor in Chief)	Dalhousie University, Canada	qye@cs.dal.ca
Moez Esseghir (Technical Editor)	University of Technology of Troyes, France	moez.esseghir@utt.fr
Lu Lv (Technical Editor)	Xidian University, China	lulv@xidian.edu.cn

Applications of Internet of Things in the Medical Field

Cody Repass
TSYS School of Computer Science
Columbus State University
Columbus, GA 31907, USA
repass_cody@columbusstate.edu

Shamin Khan
TSYS School of Computer Science
Columbus State University
Columbus, GA 31907, USA
khan_shamim@columbusstate.edu

Lixin Wang
TSYS School of Computer Science
Columbus State University
Columbus, GA 31907, USA
wang_lixin@columbusstate.edu

Abstract—**The Internet of Things (IoT) allows for interconnectivity of smart objects to collect, send, and receive information. IoT has a wide range of applications, but one of its most beneficial uses is in the medical field. The Internet of Medical Things (IoMT) utilizes IoT technologies to provide more efficient and quality care for patients as well as less costly healthcare services. IoMT provides a mainstream method for healthcare professionals to analyze patient data in real-time and make informed decisions regarding patient care. However, the large attack surface and vulnerabilities of IoT systems needs to be secured. In this paper, we first introduce two IoMT devices as examples, then we propose efficient security solutions to better protect IoMT systems. These security solutions include the Artificial Intelligence (AI)-based and cloud-based security countermeasures. Finally, the paper introduces the role of AI in IoMT.**

Keywords—internet of things, healthcare, internet of medical things, security countermeasure, patient data

I. Introduction

IoT was introduced to make daily life easier and more efficient. This efficiency can be seen in many fields that utilize IoT [1]. Today, IoT is a part of almost everything. Modern vehicles for example, use computer and communication systems that provide essential functions like engine performance and safety sensors [2]. Modern buildings use connectivity to control functions like heating, venting, air conditioning, security, lighting, etc. [2].

One of the most impactful applications of IoT is in the field of healthcare [3]. IoT in healthcare is extremely important because it directly improves the quality of life of patients. The ways in which IoT can be applied in the medical field alone is growing exponentially. Smart pill boxes can detect how many pills are left and send reminders to their smart phone, a glucometer can detect glucose levels and send the information to an insulin pump to automatically dispense insulin, a monitor can be sent home with a patient to measure heart rate, blood pressure, oxygen levels, etc. Patient information can be collected and sent to healthcare provider who can review it remotely and make decisions from looking at the biometric data..

IoMT directly improves the quality of life of patients and eases the burden on healthcare providers. IoMT consists of IoT devices specifically developed to meet the needs of patients and healthcare facilities. IoMT is developed for remote patient monitoring, intensive care, and context awareness, which gathers information about a patient's environment. IoMT can also be utilized beyond direct patient treatment, such as medical equipment and medication management.

This paper introduces two IoMT devices, the Mobile Cardiac Telemetry 3 Lead (MCT3L) and the remote patient monitoring (RPM) kit from Vivify Health. The contributions of this paper include analysis of these two real IoMT devices, security solutions to protect them, and introduction to the role of Artificial Intelligence (AI) in IoMT. These security solutions consist of understanding the device manufacturer's role in security, implementing robust security policies and procedures organization wide, utilizing network hardening techniques and network segmentation, providing IoMT security training and education, using lightweight security protocols, and cloud computing technologies.

II. Two Real IoMT Devices

A. *MCT3L*

MCT3L is a device for continuous electrocardiogram (ECG) monitoring and arrythmia detection [4]. This device is issued to patients with symptoms of cardiac arrythmia for remote monitoring [4]. The device monitors patient ECG and automatically detects cardiac arrythmia based on an algorithm, which alerts the patient and records the data. Arrythmia events can also be recorded manually by the patient and transmits the ECG data to a monitoring center. The monitoring center then presents the data to the healthcare provider. The monitor, which is a handheld device, received the ECG data from the sensor via Bluetooth. The monitor can also store up to 30 days of data. The monitor runs on a proprietary application that translates the ECG data and sends it over cellular networks to the monitoring center. The sensor records and transmits ECG data to the monitor. The sensor is battery powered and uses four disposable electrodes that are placed on specific areas of the human body which connect to the sensor's lead wires [4].

B. *Vivify Health RPM System*

The Vivify Health RPM system includes a Samsung Galaxy Tab E 32GB tablet, and three BLE capable sensing devices: a sphygmomanometer, a pulse oximeter, and a weight scale. The sphygmomanometer is used to detect blood pressure, the pulse oximeter measures the amount of oxygen in the blood, and the weight scale detects weight by standing on it. The sphygmomanometer provides the patient with a blood pressure cuff and collects the reading. The pulse oximeter is a Bluetooth device that the patient places on their finger. Light beams from the pulse oximeter read the oxygen levels without having to draw blood. The weight scale records the weight after use. The sensing devices collect biometric data and send it via cellular network or WiFi to the telehealth provider, Vivify Health, who presents the data to the healthcare organization. The Samsung tablet houses the applications for the devices and acts as the gateway for communication.

III. Security Countermeasures for IoMT Systems

This section presents security solutions to protect IoMT systems. Understanding the device manufacturer's role in security, establishing security policies and procedures, and providing education and awareness of all users are countermeasures that can make IoMT a secure environment.

Creating guidelines for IoMT devices and information use is necessary. Having rules in place that dictate who can access what resources and for what purpose prevents unauthorized access and reduces the likelihood of the IoMT devices or information being compromised. Each covered entity in the healthcare sector that interacts with IoMT devices or information must follow the Health Insurance Portability and Accountability Act (HIPAA) rules. To reach and maintain compliance, policies and procedures are written to provide rules and guidelines.

Network segmentation is a useful security measure for the telehealth provider and the healthcare provider. Segmenting the Electronic health records (EHR) from the rest of the network provides additional security so that the protected health information (PHI) cannot be accessed from within the main hospital network. Network hardening refers to security countermeasures that bolster network security. Network hardening can mean that firewall rules are configured more strictly to prevent additional traffic. Closing certain ports and using demilitarized zones (DMZs) to protect the internal private network provides additional security. DMZs are used to separate the internal network from the public internet by housing the external-facing servers between firewalls. Disabling unused network services, implementing intrusion detection and prevention systems are all countermeasures to harden a network. Hardening and segmenting networks reduces the risk of common attacks like DoS attacks. An intrusion prevention system and advanced firewalls can prevent DoS and botnet attacks from disrupting services. If an attack like DoS does occur, a hardened network would be able to respond faster to these threats, reducing loss.

Healthcare professionals must have awareness of the risks involved with IoMT and understand that PHI is necessary to protect. A covered entity should have training and awareness for its employees to always keep security in the forefront.

Lightweight security countermeasures are currently being developed to further protect information on resource constrained IoT devices. 6LowPSec was proposed to provide end-to-end security that reliably delivers time sensitive data in resource constrained environments while reducing overhead and computational requirements [5]. The rule-based approaches, and deep machine learning algorithms (branches of AI) can also be employed as security countermeasures for IoMT systems. Furthermore, AI-based security countermeasures are essential to improve IoMT security performance.

In a private cloud, data can only be accessible by authorized users. A private cloud can provide secure data storage for IoMT systems. Mechanisms such as Amazon's Web Services simple storage service (S3) allows for scalable and secure storage of data [6]. The combination of AI and cloud computing results in an extensive network capable of holding massive volumes of IoMT data while continuously learning and improving. AI has significantly changed the cloud landscape with lower costs, intelligent automation, deeper insights, improved data management, and increased security.

IV. Role of artificial intelligence in IoMT

People are experiencing diseases frequently nowadays, many of which require a rapid treatment from health professionals or critical IoMT devices. Moreover, appropriate protection for healthcare professionals in close contact with patients is crucial as a lot of diseases are highly infectious. AI has made the remote diagnosis, treatment, and management possible [7]. There is a wide range application of AI in IoMT, and AI is getting more and more popular in medical diagnosis.

Offloading processing tasks to cloud services is a cost-effective solution to carry out AI heavy computations. Also, cloud-based platforms can potentially send critical samples to medical experts for better diagnosis and keep critical samples for future deep neural networks (DNNs) training. DNNs are currently used extensively in the AI community to carry out various tasks such as regression, segmentation, and classification. Furthermore, DNNs have gained popularity in the IoMT domain, and are widely used to predict analog parameters such as heart rate, blood sugar level, cholesterol level, etc.

V. Conclusion

The paper introduced the two real IoMT devices: MCT3L and the Vivify Health RPM system. Then we proposed security countermeasures to protect IoMT systems. Our proposed security solutions include understanding the device manufacturer's role in security, implementing robust security policies, network segmentation, network hardening, providing IoMT security training for healthcare professionals, using lightweight security protocols for data confidentiality, and cloud computing technologies. The role of Artificial Intelligence in IoMT was also discussed in this paper.

References

[1] Gokhale, et al. "Introduction to IoT", *International Advanced Research Journal in Science, Engineering and Technology*, ISO 3297:2007 Certified Vol. 5, Issue 1. January 2018.

[2] Evans, D. (2011) The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.

[3] Babu B., Srikanth K., Ramanjaneyulu T., Narayana I. "IoT for Healthcare", *International Journal of Science and Research*, volume 5 issue 2. February 2016.

[4] "Patient User Guide LifeWatch Mobile Cardiac Telemetry 3 Lead", on BioTel Heart, 2020.

[5] Glissa G., and Meddeb A. "6LowPSec: An end-to-end security protocol for 6LoWPAN", *Ad Hoc Networks*. Vol. 82.2, February 2018.

[6] https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#S3Features, 2022.

[7] Kakhi, Kourosh, et al. "The internet of medical things and artificial intelligence: trends, challenges, and opportunities." Biocybernetics and Biomedical Engineering (2022).