Chapter 5
Cyber Threat Intelligence for Lightweight Trust Architectures in Medical IoT Environments

Shreeja Chaki
Amity School of Engineering and Technology, Amity University, India

Saubhik Bandyopadhyay
Amity School of Engineering and Technology, Amity University, India

ABSTRACT

We explore the integration of cyber threat intelligence (CTI) in the internet of medical things (IoMT) with lightweight trust architectures. Addressing the unique vulnerabilities of IoMT devices, the authors survey for resource-efficient CTI architectures suitable for the constrained nature of medical IoT devices. The framework's core is the discussion of adaptive algorithms and models designed for real-time threat detection and response, essential in a landscape where cyber threats are increasingly sophisticated. The authors emphasize the synergy between CTI and lightweight cryptographic solutions, demonstrating their combined effectiveness in reinforcing IoMT security. The novelty aspect of the survey lies in the discussion of lightweight models in practical use-cases. The chapter outlines development roadmap for robust and trustworthy medical IoT ecosystems, highlighting the need for ongoing innovation in this critical area. This contribution aims to guide future efforts in securing IoMT environments, ensuring patient safety and data integrity in an increasingly digital healthcare landscape.

INTRODUCTION

The Internet of Medical Things (IoMT) is a large umbrella of innovative technologies that are used to store medical records over a wide network. The Healthcare Industry has started adopting the Internet of things for patient care and tracking the needs of the patients for remote monitoring of medical sensors, medical device integration, glucose monitoring, prescription dispensaries etc. Since IoMT is comprised of medical sensors that are strong enough to collect subtle data and send it to

DOI: 10.4018/979-8-3693-2109-6.ch005

the cloud storage but fail to detect whether the data has been tampered or not during transmission or storage while the patient is still consulting the doctors in the clinic. IOMT is linked to cloud platforms such as Amazon Web Service where the data can be stored and organized thus opening a rays of attacks. The cyber threat intelligence concept goes much beyond a list of IP addresses and different hashes with bad malware, etc. Cyber Threat Intelligence (CTI) is the evidence-based knowledge of an emerging or existing threat that helps us in making informed decisions and lets the intelligence team know how to respond in different situations when faced with various types of threats.In human history, for a prolonged time, every organization had to figure out its enemies for its existence, find out their capabilities, when they intend to accomplish something, where they are planning to achieve, why they want to accomplish it, and how they are planning to do it (Burger, Goodman, Kampanakis, & Zhu, 2014).

Cyber threat intelligence is a quite a new discipline that emerges cyber security and intelligence. So what basically is threat intelligence, it is a method of collecting data about threats that allows security teams to help or alleviate cyber attacks. The IoMT has become extremely susceptible to advanced cyber threat attacks which will hamper the confidentiality of patients medical records by purloining data unauthorisedly, disrupting the whole system of healthcare. The main aim of lightweight trust architecture is to foster trust without jeopardizing the security in an medical sectors or workplace with limited number of resources. This chapter will discuss the relationship between the data, information, threat and threat intelligence, the need for Cyber threat Intelligence for lightweight trust architecture in IOMT, the types of Threat Intelligence and its need in IOMT in section 3, tools used in cyber threat inteligence, how do organizations use artificial intelligence to counter cyber threats and lightweight digital section for CTI in section 4, solution to some challenges such as threat data quality, threat data overload, privacy and legal issues in section 5.

RELATED WORK

This section will discuss the work of various other authors. Ashok Kumar Reddy (Nadikattu, 2021) proposed how artificial intelligence improves cybersecurity and how that research will help in the United States. Md Sahrom Abu et.al (Abu, Selamat, Ariffin, & Yusof, 2018) discussed the various existing definition of CTI, the Source, and Standards of Threat Intelligence, tools, and challenges in CTI. They have used tools like CCE, CPE, and OTX but in this paper, we have mainly used Indicators of Attack (IOA), Indicators of Compromise (IOC), and Artificial Intelligence and provide solutions to their (Abu, Selamat, Ariffin, & Yusof, 2018) challenges. Anwar, A., & Hassan, S. I. (Anwar & Hassan, 2017) focused on the application of AI techniques in cyber attacks and future issues into consideration. Sauerwein Clemens et.al (Sauerwein, Pekaric, Felderer, & Breu, 2019) described that STIX is the facto standard for sharing CTI. Wagner C et.al (Wagner, Dulaunoy, Wagener, & Iklody, 2016) presented an overview of MISP in which they discussed data models, taxonomies, sharing levels, synchronization protocol, usage, and statistics of MISP. Y.Gao et.al (Yali Gao, Li, Peng, Fang, & Yu, 2020) proposed different approaches for threat identification like feature extraction, meta path, meta graph builder, heterogeneous GCN-based method, and analysis of the above-mentioned methods. S. Barnum (Standardizing cyber threat intelligence information with the structured threat information expression (stix), 2012)explained Structured Threat Information eXpression (STIX), language, and format for exchanging information about cyber threats. White TLP (WHITE, 2015) talks about the