ISSN: 2508-7894 © 2022 KODISA & KAIA.
KJAI website: http://acoms.kisti.re.kr/kjai
Doi: http://dx.doi.org/10.24225/kjai.2023.11.2.39

Market in Medical Devices of Blockchain-Based IoT and Recent Cyberattacks

Shih-Shuan WANG [1], Hung-Pu (Hong-fu) CHOU [2], Aleksander IŻEMSKI [3], Alexandru DINU [4], Eugen-Silviu VRĂJITORU [5], Zsolt TOTH [6], Mircea BOŞCOIANU [7]

Received: May 15, 2023. Revised: June 08, 2023. Accepted: June 14, 2023.

Abstract

The creativity of thesis is that the significance of cyber security challenges in blockchain. The variety of enterprises, including those in the medical market, are the targets of cyberattacks. Hospitals and clinics are only two examples of medical facilities that are easy targets for cybercriminals, along with IoT-based medical devices like pacemakers. Cyberattacks in the medical field not only put patients' lives in danger but also have the potential to expose private and sensitive information. Reviewing and looking at the present and historical flaws and vulnerabilities in the blockchain-based IoT and medical institutions' equipment is crucial as they are sensitive, relevant, and of a medical character. This study aims to investigate recent and current weaknesses in medical equipment, of blockchain-based IoT, and institutions. Medical security systems are becoming increasingly crucial in blockchain-based IoT medical devices and digital adoption more broadly. It is gaining importance as a standalone medical device. Currently the use of software in medical market is growing exponentially and many countries have already set guidelines for quality control. The achievements of the thesis are medical equipment of blockchain-based IoT no longer exist in a vacuum, thanks to technical improvements and the emergence of electronic health records (EHRs). Increased EHR use among providers, as well as the demand for integration and connection technologies to improve clinical workflow, patient care solutions, and overall hospital operations, will fuel significant growth in the blockchain-based IoT market for linked medical devices. The need for blockchain technology and IoT-based medical device to enhance their health IT infrastructure and design and development techniques will only get louder in the future. Blockchain technology will be essential in the future of cybersecurity, because blockchain technology can be significantly improved with the cybersecurity adoption of IoT devices, i.e., via remote monitoring, reducing waiting time for emergency rooms, track assets, etc. This paper sheds the light on the benefits of the blockchain-based IoT market.

Keywords : Medical IoT, Cyber-attack, Cyber security, Medical devices of Blockchain-based IoT, Confidential data

Major Classification Code: Medical IoT, Cyber-attack, Cyber security, Medical devices of Blockchain-based IoT, Confidential data

1. Introduction

1 First Author. Ph.D. student, Faculty Electrical Engineering and Computer Science; Faculty Technological Engineering and Industrial Management, Transilvania University of Brasov, Romania. Email: jacquesdemolay03@gmail.com
2 Second Author. Ph.D. student, Interdisciplinary Centre for Security, University of Luxembourg, Luxembourg. Email: hungpu.chou@uni.lu
3 Third Author. Ph.D. student, Faculty of Computer Science and Telecommunications. Poznan Univeristy of Technology, Poland Email: AleksanderIzemski@gmail.com
4 Fourth Author. Ph.D. student, Electronics and Computers Department, Transilvania University of Brasov, Romania, Email:alexandru.dinu@unitbv.ro
5 Fifth Author. Faculty of Technological Enginnering and Industrial Management, Transilvania University of Brasov, Email: eugen.vrajitoru@unitbv.ro
6 Sixth Author. Ph.D. student, Faculty of Technological Enginnering and Industrial Management, Transilvania University of Brasov, Email: zsolt.toth@unitbv.ro
7 Corresponding Author. Professor, Faculty Technological Engineering and Industrial Management, Transilvania University of Brașov, Romania. INCAS - National Institute for Aerospace Research "Elie Carafoli; AFAHC Brasov, Romania. Email: boscoianu.mircea@yahoo.com

Cyber security related to previous incidents sufficient, to employ a lot of specialists in preventing cyberattacks, with experience in other medical institutions. This section was abused because medical gadgets used in medical institutes are connected to the intranet, making external access impossible. My advanced technology of healthcare systems employing a blockchain smart contract will stop any duplication of copies in the parent centralized system. One way that researchers might benefit from blockchain technology is by being able to distribute authorized and timestamped copies of academic articles. There can be different medical cyber-security systems between institutions. Traditional medical devices are centralized system, the state of the art and novelty of my research field is medical devices of blockchain-based IoT, as known as the ledger system.

Even if computers have made life easier, they have also made individuals more vulnerable to and desired as targets for online thieves. All facets of everyday life are now regularly at risk from cyberattacks, which can create varying degrees of disruption depending on their aim, nature of the threat, impact, etc. In addition to having a significant detrimental impact on their targets, cyberattacks can also result in non-technological damage.

Medical mistakes can be done because of distortion of medical information between patients. the lack of security infrastructure could compromise the entire national medical system; the lack of infrastructure, or incompatible infrastructure or the lack of modern infrastructure may cause vulnerabilities in the medical security systems.

Authorities and managers are always looking for effective strategies to prepare for and protect against existing and upcoming cyber-attacks. Implementing security guidelines and requirements, such as cyber security awareness campaigns, is one of the frequent techniques. One of the biggest challenges facing security professionals is "how to enhance cyber security knowledge," thus they always strive to comprehend both recent and historical trends in the field. There are two main degrees of understanding cyber security trends (Sina Pournouri and Matthew Craven, 2014)

1.1. Recognizing and countering cyberattacks

The preceding step is finished at this level, and it helps security administrators be informed of current cyberattack techniques. In this stage, it shall be emphasized that "cyber-attack analysis" is a concept. In other words, by examining past cyberattacks on cyberfirms and figuring out how the different contributing elements relate to one another, a clearer picture will be produced that will allow management to act effectively in light of current cyberthreats (Sina Pournouri and Matthew Craven, 2014).

As medical devices used by blockchain-based IoT and healthcare institutes become a constant target for cyber attackers, the goal of this chapter is to evaluate potential vulnerabilities to those devices. Cyber specialists are reportedly noticing security flaws in healthcare organizations' IoT-based on blockchain medical equipment, which might hurt patients in a variety of ways (Kevin Fu, James Blum, 2013). Patients may be at risk from cyberattacks on medical equipment that are part of the blockchain-based Internet of Things, but tragedy may result from cyberattacks on healthcare institutions that contain critical patient data. For example, in 2015 theft of 1.5 million documents was allegedly committed by a cybercriminal group from Planned Parenthood's database and threatened to reveal the personnel records of this abortion clinic as well as the identity of its clients (Inae Oh ,2015).

The originality of research is the security of the medical system is very important to keep the confidentiality of the patient’s information. Because of the population aging the need of the medical services will increase and everybody will have more and more individual medical information stored on medical platforms. The medical criminals should not have access these databases because they can change the personalized treatment of each and every patient. Furthermore, the medical information can be stolen between private medical companies, the research results of one company can be illegally used by another one and so the fair competition can be destroyed.

2. Cybersecurity-related issues

Investment in research and development of medical security systems, to prevent the cyberattacks of medical devices. The medical security systems can be divided in multiple domains such as: information security, infrastructure security, hospital security systems, pharmacy security systems, stomatology security systems etc.

IoMT stands for "Internet of Medical Things," which is a key idea in the Internet of Things, and one has to be knowledgeable about the development of medical technology as well as security principles in order to fully understand and grasp its complexity. In order to comprehend the security concerns these devices confront with blockchain-based IoT, it is crucial to review some of the prior information as RF (Radio Frequency) modules are still often employed as the means of transferring data in medical implants. The next section provides an explanation of the fundamental information required to understand RF on a technical level, along with the problems it encounters.

2.1. Radio-frequency technology (RF)

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

Radio amplitudes, which may alternatively be described as 104–1012 Hz, are electromagnetic wave frequencies that operate in the 20–300 GHz range. Pacemakers and ICDs use the Medical Implant Communication System (MICS), a low-power, short-range frequency that operates between 402-405 MHz (Yuce MR, Islam MN, 2016). All medical implants use this frequency range since it is universally designated for use by medical implant devices of the blockchain-based Internet of Things. The fact that all medical implants work on the same band frequency has been widely publicized, which may be harmful. It could have been wiser to keep this information confidential and only share it with those who truly needed to know.

Numerous problems and weaknesses with RF technology exist; they are typically inevitable and represent a shortcoming of the technology. The Office of Communication, sometimes known as of Com, is responsible for overseeing radio frequency technologies and broadcasting in the UK.

Without a license, broadcasting on RF is illegal. This may discourage some people, but "radio pirates" remain unaffected. Some people like listening to pirate radio stations, and those who engage in this activity must become professionals to prevent detection. Therefore, it is logical to imagine that some of these professionals may have learnt about the MICS band range and may have even gone so far as to conduct their own home studies.

2.2. Interference with magnets (EMI)

There are typically signs against interference with medical implants posted in airports, hospitals, and other public places where electronic blockchain-based IoT devices are sending out signals. Users of ICDs are advised by the American Heart Association to avoid being in close contact to electrical equipment of blockchain-based IoT (Dick Cheney, 2013). There is a chance that several blockchain-based IoT devices, mobile devices, heart rate monitors, and airport scanners are just a few examples of devices that might affect an implanted medical device.

The fact that pacemakers, ICDs, and other implants have been protected against EMI creates conflicting information on this for at least the last 20 years. For instance, the design of pacemakers was changed to include a protected, airtight, sealed container that is normally composed of steel or titanium and coated with an insulated covering. Additionally, the EMI vulnerability of pacing systems was reduced by the introduction of bipolar leads (Okan Erdogan ,2002).

There are filtering techniques like the Bandpass filter (BPF), which, when specifically included into a pacemaker, may filter out non-cardiac impulses reducing external disturbance. Although it's unclear if BPF filtering is required or merely a standard best practice It is frequently employed by RF modules in medical implants.

2.3. Radio frequency-based identifiers (RFID)

A use of RF technology is radio frequency identification (RFID), which, in contrast to RF, differs in that it has a shorter range but can carry more data. Due of this, RFID technology makes use of tags, a tiny, data-containment IoT gadget built on blockchain technology.

Passive and active RFID are the two different kinds. Active tags are bigger and more expensive since they are more complex and require a power supply, passive RIFD tags are simpler and have a lesser range than active tags.

When it comes to RFID, there are three frequency bands:

• Low frequency (LF) reading range of up to 10 cm: 30-300 KHz

• High frequency (HF) reading range of up to 1 m, 3-30 MHz

• Up to 12 meters may be read using ultra-high frequency (UHF) signals between 300 MHz and 3 GHz.

When deciding which band to utilize, there are three key benefits to consider: Firstly, although carrying more data, higher frequencies are also more expensive to produce; First, interference is a problem with higher frequencies since they may carry more data but cost more to produce is worse with higher frequencies; and third, when it comes to security, a shorter range is safer since it reduces the attack surface area.

Second, interference gets worse as frequency increases, and third, it's better to have a shorter range to reduce the assault surface area.

Lower RFID frequencies are not, however, secure because of this. For instance, recent hacks have affected banking cards, which have an RFID chip inside. Contactless debit and credit cards include short-range RFID chips, therefore in order to use them to make purchases, a point of sale (POS) terminal needs to be in close proximity to the card. As a person knocking into you on a packed train might be excused as an accident, intelligent fraudsters started utilizing POS terminals on public transportation systems to steal money by billing the victim's card (Helena Horton, 2016). It is not improbable to assume that swiping a reader might result in a close-range attack on a pacemaker or ICD

given that a POS device of blockchain-based IoT is simply a pre-programmed RFID reader.

A study that was published in a medical journal in 2010 showed that pacemakers might be hampered by passive RFID tags provides more evidence in favor of this assertion (O'Connor 2010). Thirty units total—15 pacemakers and 15 ICDs—were subjected to FDA testing. There were thirteen distinct RFID readers tested, each of which could operate at a low, high, or ultra-high frequency. According to the findings, LF RFID interference was seen in 67%, or around 20 out of the thirsty units examined. Although they do not provide an immediate concern, as mentioned in the report, the rate at which technology is developing raises the possibility that they may.

3. Background Information on Pacemakers and ICDs

3.1. The Pacemaker's Operational Purposes

The sinus node is referred to be the "natural" pacemaker since it causes a heartbeat in a healthy heart by sending an electrical impulse (pacemakers n.d.). When a patient has an atypical heart and the sinus node does not operate as it should, an artificial pacemaker must be implanted. It is now estimated that at least 25,000 pacemakers are implanted annually, or around 500 each week. In accordance with the UK national assessment of cardiac rhythm management devices of blockchain-based IoT 2015-2016, this number will increase in the future, and pacemakers aren't the only devices that are contributing to this trend. All blockchain-based IoT-based medical device implant rates have clearly increased (David Cunningham, Morag Cunningham, Akosua Donkor, Nick Linker and Francis Murgatroyd, 2016).

Depending on the kind of cardiac disease present, a pacemaker may operate using one of two methods:

• On-demand: When required, the pacemaker will start an impulse on demand.

• Fixed rate: The pacemaker always causes all of the impulses.

A pacemaker's internal components include a pulse generator, a battery-operated circuit additionally three leads for bipolar electrodes. Directly implanted in the heart through a vein, these leads serve as the electrical impulse carriers. The name of the blockchain-based IoT device indicates how many leads it has, and there are several sorts of pacemakers (Damien Giry, Keylength, 2020).

3.2. A defibrillator that is implanted in the body (ICD)

In the case of an aberrant cardiac rhythm, a small implantable device known as an Implantable Cardioverter Defibrillator, or ICD, is intended to cause fibrillation through an electrical shock (Implantable cardioverter defibrillator n.d.). Since they also have the ability to shock the heart electrically, these blockchain-based IoT devices set themselves apart from pacemakers. The following treatments may be started by the ICD If cardiac arrest or an abnormal heart rhythm are found:

• Pacing: a sequence of low voltage electrical impulses delivered repeatedly in an effort to fix an irregular rhythm.

• Cardioversion: the process of using many more powerful electrical shocks in an effort to get the rhythm back to normal than pacing.

• Defibrillation: this procedure involves giving the heart a series of intense electrical shocks are administered to the heart during this operation in an effort to get it back to its regular beat.

Patients with dangerously irregular cardiac beats utilize an ICD. They may be fitted in advance to people who are at risk of receiving one in the future. The frequency of these depends on the patient's health and the kind of ICD that was implanted. Regular check-ups are necessary. The sufferer must alter their way of life, just as they would with any ailment. One piece of advise is to be cautious of the possibility of interference from electrical devices used in blockchain-based IoTs.

3.3. Residence Monitoring Devices

A blockchain-based IoT gadget called the home monitoring unit transmits data from the pacemaker over the user's home internet connection to a predetermined source (What exactly is remote monitoring? n.d. Patients who utilize the NHS have their information sent directly to a server that is remotely supervised by NHS staff.

Since patients may be informed by their doctors if it seems as though they are about to suffer a heart attack, this idea enters the realms of pre-emptive medicine. This gives patients the opportunity to fix the issue before it happens. Additionally, fewer hospital visits are required because a medical implant may now be examined without the use of specialist hospital equipment. The fact that the device is linked to a user's home network raises suspicions. It is feasible that these devices might serve if they are not adequately secure or if the user's home network is not, they might be used as a point of attack by malicious third parties.

In order to prevent a fake report from being sent that makes the user appear healthier or worse than they actually are, data must be protected using encryption and only be seen to those with the proper permissions. If medical data was not encrypted and only those with the proper authorization could access it, then it could be taken advantage of or altered. Legally speaking protecting all sensitive information is necessary, thus it is obvious that the home monitoring system must be subject to data protection rules.

Prior research revealed that the Merlin@Home version of St Judes monitoring devices was susceptible to man-in-the-middle assault (Damien Giry, Keylength, 2020). When information is transferred between homes monitors and implants, this vulnerability allows for its exploitation during transmission, making it possible to intercept the data. This data may include, among other things, orders to the implants, including a patient's individual medical information and statistics from the implants, as was already described.

3.4. RF Implants

Medical professionals used magnetic switches to access implants like pacemakers in the past. These switches activated wireless functionality by applying a modest magnetic field to the blockchain-based IoT device they were using. A magnetic switch was replaced with an RF broadcasting module in an IoT gadget by blockchain-based manufacturers in order to update the devices and open the door for more complex configurations like home monitoring capabilities.

Given the existence of more effective and efficient wireless communication methods, RF technology might be viewed as being obsolete nowadays.

3.5. Bluetooth Implants

The RF components will be replaced with wireless Bluetooth transceivers in the upcoming implant generation. With this modification, the data bandwidth will be increased, enabling the transmission of more data while also improving device compatibility for blockchain-based IoTs. Fundamentally, the home surveillance gadget was a ground-breaking idea, but its fundamental flaw is that it cannot be moved about. Because of the latest Bluetooth device generation of blockchain-based IoTs, this drawback may be eliminated by using a mobile device of blockchain-based IoT.

With the gradual but steady emergence of Bluetooth devices for blockchain-based IoTs, RF modules may eventually be completely replaced. It might be claimed that while Bluetooth has its own problems, RF is more difficult to hack. The majority of smartphones and other portable blockchain-based IoTs now use Bluetooth, which can transmit more data than traditional RF. The hacker community places a greater emphasis on any widely used technology since simple access is a prerequisite for any effort to hack something. Unauthorized parties may now install malware, intercept data, and even completely take control of an IoT device powered by blockchain thanks to a vulnerability called Blueborne (Tom Spring, 2017). Classified medical data may be altered If a pacemaker or ICD is linked to a shoddy blockchain-based Internet of Things device, and in the worst scenario, some amount of control over the linked medical implant may be attained.

4. Market and Cybersecurity

This report is aimed for a market overview and a trend in cyber security. Medical equipment of blockchain-based IoT no longer live in a vacuum, thanks to technological improvements and the introduction of electronic health records (EHRs).

There is a demand for integration and connection technologies to improve clinical workflow and patient care solutions, the overall hospital operations will continue to fuel the connected medical device market's fast expansion.

The push for blockchain technology and IoT-based medical device to enhance their health IT infrastructure and improve their design and development procedures will only get louder in the future. In this cybersecurity future, blockchain technology will be important. According to a recent article in Healthcare Informatics, a U.S.-based publication, the healthcare business is gradually investing more money in outsourcing of information systems and information technology (IS&T) solutions, primarily in the areas of information system implementation, processing services, and other information system and information technology (IS&T) related activities. Global corporate outsourcing of information systems and information technology (IS&T) solutions spending reached $86 billion in 1996 and is predicted to exceed $136 billion by 2001.

5. Conclusions and Future Scope

The fundamental principles of information systems and information technology (IS&T) implementation are discussed from the perspective of the market in medical devices of blockchain-based IoT, followed by a comprehensive review of information systems and information technology solutions, including project management, market, and cybersecurity considerations. In the future, the need of further investment in this medical

services security should force governments to include 1% of GDP to this sector. to obligate the companies and institutions to invest more in cybersecurity by changing the legislation.

In conclusion, the current state of the art and and novelty in medical devices of blockchain-based IoT, as well as the characteristics of health services information networks, concerns surrounding the organization of the information chain, computer-based patient records, and information project management and implementation factors of relevance to medical devices of blockchain-based IoT experts participating in information systems project development.

The most pressing requirement remains the construction of continuous information systems that allow the recovery of patient-oriented, problem-oriented, and procedure-oriented data at all levels of healthcare institutes. Only in the last twenty-five years have healthcare institutes recognized that information is a very valuable asset —The quality of management decision making, which is dependent on their performance in a highly competitive global market, is strongly tied to the quality of information accessible to their managers.

Furthermore, having a clear set of standards helps users to construct the necessary modules more rapidly and capitalize on market possibilities as they arise.

References

Damien Giry, Keylength (2020 May). Cryptographic key length recommendation. Retrieved June 08, 2023, from https://www.keylength.com/en/4/

Dick Cheney (2013 October). Heart implant attack was credible. Retrieved June 08, 2023, from http://www.bbc.co.uk/news/technology-24608435

David Cunningham, Morag Cunningham, Akosua Donkor, Nick Linker and Francis Murgatroyd (2016 March). National audit of cardiac rhythm management devices. Retrieved June 08, 2023, from http://www.ucl.ac.uk/nicor/audits/

Erdogan, O. (2002). Electromagnetic interference on pacemakers. *Indian Pacing and Electrophysiology Journal*, *2*(3), 74. PMID: 17006562; PMCID: PMC1564060.

Fu, K., & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, *56*(10), 35-37

Helena Horton (2016 February). Contactless card owners warned against public transport scanner hack. Retrieved June 08, 2023, from https://www.telegraph.co.uk/technology/2016/02/17/if-you-have-a-contactless-card-watch-out-for-this-scam/

Inae Oh (2015 July). Anti-Abortion hackers claim to have stolen data that could take down planned parenthood. Retrieved June 08, 2023, from https://thehill.com/policy/cybersecurity/249246-anti-abortion-hackers-claim-to-have-hit-planned-parenthood/

Islam, M. N., & Yuce, M. R. (2016). Review of medical implant communication system (MICS) band and network. *Ict Express*, *2*(4), 188-194.

Pournouri, S., & Craven, M. (2014). E-business, recent threats and security countermeasures. *International Journal of Electronic Security and Digital Forensics*, *6*(3), 169-184

Tom Spring (2017 September). Wireless 'BlueBorne' attacks target billions of bluetooth devices. Retrieved June 08, 2023, from https://threatpost.com/wireless-blueborne-attacks-target-billions-of-bluetooth-devices/127921/