Journal of Theoretical and Applied Information Technology
31st May 2022. Vol.100. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY ON SECURITY THREATS IN THE INTERNET OF MEDICAL THINGS (IoMT)

WAEL TOGHUJ[1], NIDAL TURAB[2]

[1]Dr., Department of Computer Science, Al-Ahliyya Amman University, Amman, Jordan

[2]Professor, Department of Networks and Information Security, Al- Ahliyya Amman University, Amman, Jordan

E-mail: [1]w.toghuj@ammanu.edu.jo, [2]n.turab@ammanu.edu.jo

ABSTRACT

Recent developments in the Internet of Things (IoT) have led to the development of the Internet of Medical Things (IoMT). Data collection, analysis, and transmission are key elements of IoMT tools that are revolutionizing healthcare delivery. Nevertheless, researchers and industry practitioners have several challenges with IoMT, particularly in the area of data security. Security breaches in the healthcare industry have downsides such as patient's personal information breach, possibly of death incidence. As a such, IoMT requires high standards of security. In this paper, we provide a review of IoMT security challenges and their possible mitigations. By surveying multiple scientific research papers, we aimed to guide researches on latest trends in medical device security provide mitigation of threats against various IoMT devices. In addition, the current weaknesses of various e-Health domains and demonstrates the results of recent works to overcome these obstacles is also explored.

Keywords: *Security, E-Health, IoMT, WBAN, IMD, EHR, EMR.*

1. INTRODUCTION

In last decades, the healthcare realm has experienced numerous developments in terms of emerging technologies and treatment methods. Advancements in the fields of the Internet, wireless technologies and communication links raised the healthcare delivered to patients either within the health care provider premises or remotely where patients are far from physicians; remote monitoring utilizes different sensors monitor vital signs that conveyed by smartwatches, smart phones laptops to remote physicians via the Internet. If they are connected to each other and to external devices via the Internet, they form what is known as the Internet of Things (IoT). The incorporation of medical devices and requests and connect them to health care providers via the Internet is the Internet of Medical Things (IoMT) [1]. A typical IoMT-based e-Health system is illustrated in figure 1 [2]. IoMT can reduce hospital visits and the by connecting patients and physicians and allowing the transfer of medical data over the Internet. Data collected from patients, known as Electronic Health Record (EHR), An EHR is a medical record presented in digital format rather than papers format. EHR might include demographics, patient progress medical notes, described medications, patient's vital signs, patient's medical history, inoculations, laboratory and radiology reports. EHRs need to be secured while being transmitted and after storage in the final destination [3].

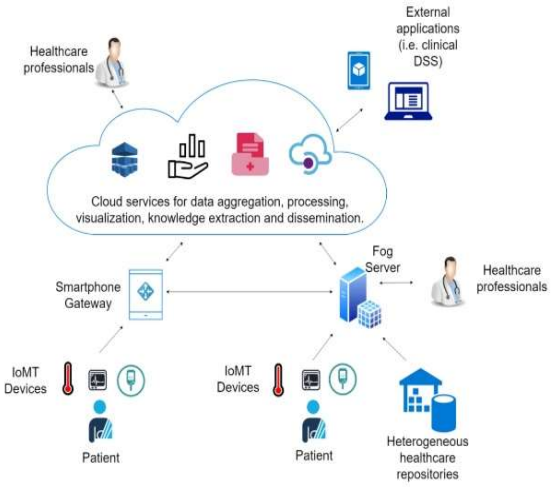

Figure 1: Typical IoMT-based e-Health system

Figure 2 illustrates the architecture of IoMT, where the perception layer contains of sensors, actuators and any entity that senses and monitors

patient vital signs, the network layer is the intermediate layer that transfers medical data to the application layer to be processed, analyzed and stored [4].

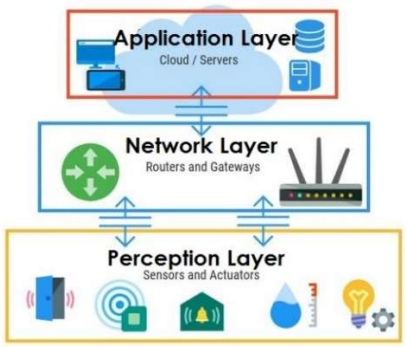

Figure 2: Architecture for Internet of Medical Things (IoMT)

Implantable Medical Device (IMD) that is implanted surgically inside human body during medical surgery, and is intended to stay for a while after the surgery. Examples of IMD include: coronary stents, implantable insulin pumps and cardiac pacemakers. IMDs suffers from the constrained power source [5, 6].

Wearable medical devices are a network electronic devices worn by patients record their health records. Wearable medical devices include skin patches, electrocardiogram (ECG) monitors, they are connected to the cloud for further collection and analysis [7].

In addition, the advancement of low-power and small size sensors and wearable medical devices leads to Wireless Body Area Network (WBAN). WBAN connects sensors and actuators all over the human body wirelessly to a physician's medical station or smart phone [8]. An example of a WBAN architecture for ECG monitoring is shown in figure 3.

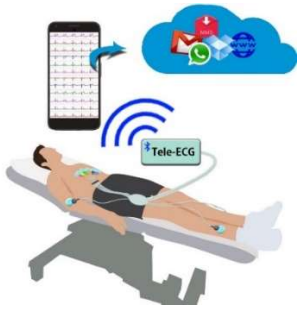

Figure 3: Architecture sample of Tele-ECG monitoring

As most of medical devices are remotely available through wireless technology such as Wi-Fi, Bluetooth Low Energy (BLE) and ZigBee. They can be eavesdropped by an outsider to exploit electronic transmitted data that can lead to terrible health consequences and violating patients' privacy and scarifying the whole healthcare providers' system. Unfortunately, there is no complete security solution available and standards that can lessen the emerging healthcare cyber-attacks.

Here are some security weaknesses that can compromise healthcare systems [6]:

- Data exploitation: the attacker can modify or even delete health records and can threaten patient health.
- Medical records can be accessed by medical staff at the health care providers and can be used for blackmail.
- Medical sensors, actuators and devices might not comply with security standards so they represent networks durability. In addition, they can be stolen or hijacked and used to access the patient and medical healthcare provider records.
- The adaptation of the Internet to provide healthcare is an evolving technological field where there is no adequate research has not been accompanied. Also, the manufacturers of medical health devices demand IoMT security solutions.
- Majority of the IoMT devices are integral with wireless communication capabilities, so they are imposed to the most wireless security problems.
- There is no interoperability between different IoMT applications from different manufacturers. There are consequences of lacking of standard application security.
- Security computations demand large computation power, many of IoMT devices are resource constrained devices. As a consequence, traditional strong encryption is not suitable for IoMT devcies.
- Denial and Distributed Denial of Service (DOS and DDoS) attacks: that happens when an attacker overwhelmed by huge volume of Internet traffic.

This study aims to provide a review of IoMT security challenges and their mitigation and cryptographic techniques, algorithms, and approaches proposed by recent researchers. Firstly, an introduction to the medical IoMT were presented, then the importance of securing IoMT data such as EHR, major IoMT flaws and weakness were calcified and finally the open research areas of IoMT security were presented. To attain the paper goals, more than 40 publications on IoMT and their security approaches were reviewed from 2019 to 2022; using keyword such as "IoMT", "WBAN", "IMD" among

different scientific databases such as Scopus and Google Scholar then the results of the surveyed paper were compared and summarized.

2. IoMT SECURITY AND PRIVACY: LITERATURE REVIEW

An architecture for long-distance communication for medical devices based on the Long RangeWide-Area Network (LoRaWAN) protocol was proposed in [10] that allows long distance (more than 10 km) data communications. The proposed stack of LongRange (LoRa) consisted of a device connected to the Internet by either Bluetooth, Wi-Fi or LoRa. LoRaWAN gateway is used to convey data to the Internet. The transmitted data is stored in the Cloud and can be used to monitor patients by their families and physicians.

The security during the software design of life-critical embedded systems was studied in [11]. The authors developed framework and software models for security risk assessment and management in medical embedded systems (any medical device that help identifying sicknesses and conduct different medical tests and deliver an accurate and reliable healthcare). They presented Software-based Architectural Framework for Ensuring Security (SAFES) as multi-modal software design with an extremely integrated risk model. They also presented and Finely Integrated Risk Evaluation Method (FIRE) methodology that integrates the software development lifecycle by integrating both stationary risk evaluation during design phase and adaptive dynamic risk evaluation for software deployment.

The authors of [12] suggested some security defense strategies against attacks aimed to harm the Healthcare Critical National Infrastructure (HCNI) that compromised medical diagnosis records. They established an Intelligent Medical Diagnosis System (IMDS) simulation platform. A cardiac diagnosis component was then added to the IMDS. The IMDS is fed with the ECG data launched systematic National Institute for Standards and Technology (NIST) ethical hacking to identify four vulnerabilities identified from the OpenEMR (is an open source electronic health records and medical practice management solution [13]). The attacks started by identifying the entry points of the medical websites and then penetrated to the medical records server to modify the heart disease diagnosis records.

An automated security assessment framework for wearable BLE enabled Health Monitoring Devices was proposed in [14]. The proposed framework based on Penetration Testing Execution Standard (PTES). It contains different stages: information gathering, threat modelling, vulnerability analysis and exploitation. They stated that the proposed framework can be used to recognize and realize existing and new vulnerabilities in Wearable Health Monitoring Devices (WHMD). They stated that the proposed framework could be used to evaluate wearable devices during the design and implementation of new devices or before adoption.

A wearable sensor system, integrated into a hospital network was proposed in [15], with intention of supporting high data rates generated by multiple wearable medical sensors while maintaining strong end-to-end communication security. The proposed system contains two units: the patch (a wireless wearable battery-powered device) and local Linux server. They studied the impact of using wireless network protocol and the security architecture on the amount of consumed energy. Their results showed that Wi-Fi combined with the Transport Layer Security (TLS) protocol is the most energy efficient and end-to-end security protocol.

The authors of [16] evaluated cyber threats targeted IMDs. They stated that use of IMD frequently ignore security warnings, especially if the security warnings are frequent or difficulty in the user interface. However, as the IMD users are considered the most vulnerable communication party, patients and health care providers should have a satisfactory level of cybersecurity awareness on IMD. Moreover, they stated that the attacker can neither capture intercept traffic (due to short range of IMD) nor capture the information from IMD operating system.

Efficient data access control protocol for IMD devices was proposed in [17], The protocol ensures anonymous Data Access Control (DAC) through a Signcryption Scheme with Proxy ReEncryption (DAC-PRE). Signcryption is a cryptographic primitive where digital signature and public-key encryption are done in a single stage. PRE systems proxies from third parties used to modify an encrypted text. They tested the randomness of the proposed scheme by the random oracle model. Lastly, they stated that their scheme

has very a low computation time, communication overhead and energy consumption.

The authors of proposed [18] the use of system identification and mitigations to assure system reliability by using medical information convergence in medical artificial intelligence. They checked the life cycle of medical information and traced the flow and location of information, they analyzed the security threats, derived security framework and proposed technical mitigations to overawe such threats. The proposed framework can be couturier to any hospital size.

A security system for protecting medical EHR from security challenges was proposed in [19]. The proposed system consists of two algorithms and discloses a mobile application system to validate a reliable IoT data communication system. A pair of algorithm were proposed: the first for generating the necessary encryption/decryption keys and the second is an encryption algorithm. Attribute-based encryption (ABE) approach was used to encrypt patient's health record. Their obtained experimental results showed the system had a real success which provides excellent security and privacy in IoMT.

Remote software-based verification for real-time constrained embedded devices was proposed in [20]. The authors proposed Remote Software-based Attestation (RealSWATT) software-based remote verification framework for real-time critical devices that works on service low-cost embedded devices. Their framework exploited separate processor core for verification to ensure the correct scheduling and timing of real-time actions. In addition, they proposed a continuous verification and a network architecture for the software-based verification of embedded devices to block the severe timing constraints and hardware requirements. They used 32-bit microcontrollers (ESP32) that used on real-world regular IoT devices.

The authors of [21] examined the security and privacy of the Healthcare IoT. They addressed the following areas of concerns to improve the Healthcare IoT model: (1) Generally, there is poor management of sensitive data, (2) Lack of unique standard naming and identity management, (3) Trust management and policy need further investigation with sharp vision, (4) The huge volume of data collected from Healthcare IoT devices in real-time and (5) However, resource constraint device preventing the utilization of intelligent machine learning algorithms.

A Four-layer architecture model for skin monitoring system was proposed in [22], the proposed system composed of four layers: (A) Perception layer the skin sensors that sense and transmit patient's skin information to its preceding transmits the data to its next network layer; (B)The network layer: transports it for further processing and analysis. Several networking technologies can used in this layer. (C) Operational layer: skin patient's niceties processed and classified at this layer using machine learning algorithms. (D) Requisition layer: provides interface for healthcare providers.

The authors of [23] proposed an architecture for ECG remote monitoring; the proposed architecture composed of four levels: The Things/Sensing level where a mobile tele-electrocardiograph device attains health signals from the patient and transmits them to the Edge/Fog Computing level (the second level) that contains software module and performs graphical interfacing, it process data from the mobile device. The third level is the Cloud level that used for long-term data storage; while the fourth level is Services/Applications that used by healthcare providers to track patient progress and to send the appropriate notifications or approvals.

An E-health care system with the two constrained protocols: Constrained Application Protocol (CoAP) and message query telemetry transports (MQTT) was proposed in [24]. In the proposed framework, CoAP and MQTT, were used to provide peer to peer security in E-Health constrained environment however RESTful HTTPs had been used to provide secure communication through the Internet. To ensure reliable and secure end-to-end communication, CoAP and RESTful HTTPs were cooperatively used. The Internet secure connectivity was important as clinical data comes from the health sensors transmitted on the cloud for further storage and future analysis.

Separate and networked IMDs and their security threats were discussed in [25]. Some of the attacks they explored are: attacks on implantable drug delivery system, attacks on implantable cardioverter defibrillator, attacks on Cardiac pacemakers and attacks on neurostimulator. They also explored other security risks related to IMDs

such as: Risks of wireless communication, Electromagnetic interference attacks, Battery leakage lack of software patches/updates and possible infections. They stated that, despite the fact there are no real-life instances of security breaches on IMDs, there are true security attacks and vulnerabilities targeted IMDs. They also conversed some security countermeasure to reduce the attacks on IMDs.

The privacy, security, and storage management in IoMT infrastructure were discussed in [26], they demonstrated the possibility of leveraging blockchain and Interplanetary File Systems (IPFS), the proposed framework was divided into two levels: initialization and authentication levels. Patients and their medical devices are registered into the initialization level while the authentication level includes the mapping of the following parameters: patient Id (PID), device Id (DID) and Device Public Address (DIP) and spread into the network of IoMT blockchain.

To authenticate the smart medical monitoring devices, the authors of [27] used unique addressing (IPv6) and identification methods. To secure communication and protect the network from attacks, they used session keys without increasing the packet size. And only one time during sessions the secret keys were used to protect the IoT network. In order to validate the proposed Secure Addressing and Mutual Authentication protocol scheme, Body Area Network (BAN) logic was applied.

The authors of [28] via literature review explored and classified the reasons that could have bad impact on security of IoT including healthcare sectors. Twenty-one challenges have been identified. Researchers performed an empirical study in order to gain insight into the identified challenge from industrial experts. Confidentiality, integrity, and availability were cited as the top three challenging factors for secure IoT. By using fuzzy-AHP approach the main challenges has been identified.

The authors of [29] focused on the significance of context-awareness in IoT to fulfill secure communication between IoT nodes. As a basis for developing the security ontology for healthcare environments, they used the Security Toolbox: Attacks & Countermeasures (STAC) ontology. As part of their study, they classified continuous context-awareness based on various definitions and provided context-aware data security based on patient context (for example, treatment history and diagnosis). By using the protégé tool, a graphical representation of healthcare ontology was created. Based on the results of the evaluation, the authors conclude that their concept offers annotated recommendations that require less human intervention and is reliable.

The authors of [30] focused on the security aspects of IEEE 802.15 TG6 standard by making some improvements to enhance the security of future Medical Body Area Network (MBAN) applications. They underscored the disadvantages of the security levels offered by the standard, such as the lack of privacy protection, security mechanisms and the data processing without encryption. In addition, the authors provided an overview of the entry points into a MBAN offered to an attacker and discussed the attacks on nodes typically used in MBAN applications. In order to assess the IEEE 802.15.6 standard's vulnerabilities across a large number of dimensions, the authors adopted a structured analysis method and a number of physical requirements that represent special node types. They used three distinct realistic scenarios to reflect against the application-specific requirements. The analysis resulted in various recommendations, which may combine with the standard body.

New techniques for encoding and compressing data have been presented in [31] for healthcare systems using IoT sensors and devices in order to enhance security. The proposed solution is based on discrete Rajan transform (DRT) which is essentially a fast algorithm developed on the lines of Decimation-In-Frequency Fast Fourier Transform algorithm. To recover the original data, inverse DRT is used to decrypt the uncompressed data. According to the results, IoMT data can be encrypted and compressed to a minimum of 12.4%; while at the same time being decrypted to its original form with minimal errors.

As digital healthcare platforms are vulnerable to cyber-attacks such as ransomware. a new framework was proposed [32] to provide security at multiple levels for securing future healthcare environments. The platform prototype consists of four different mechanisms (Layers). Performance was reduced by 10 percent compared with unsafe mechanisms, but on the other hand, this prototype improved security, efficiency, and management of services, such as deployment, replication, and migration.

The use of IoT in combination with cloud-based electronic medical records (EMRs) in healthcare industry is leading to improve quality of healthcare environmental services. However, the author [33] found that while healthcare organizations are still vulnerable to several known IoT security threats, a new factor is appeared which is "the fear of not knowing how IoT devices work". Depending on that factor, the author investigated its influence decision-making concerning the security policy. Although the number of interviewees for the investigation (ten senior information security engineers from the largest group of hospitals) seems small, the author tried to gather insights from the most knowledgeable person at each organization. According to the results, the biggest threat is outdated firmware, employees not understanding how to secure outdated software and hardware, multiple types of connectivity, and fear of IoT devices. Due to the rapid development of IoT devices as well as EMRs, the fear of the unknown is associated with IoT devices.

To make the information of the patient in cloud servers more secure, the authors of [34], proposed an architecture with two different models (security and prediction). In order to implement the security model, a random diagonal elliptical curve cryptography together with homomorphic encryption was used. The second model was implemented using the Multi-nomial smoothing Naive Bayes model that requires the training data in order to generate the efficient prediction model. The authors enhanced the security of patient data and key words by encrypting and decrypting them using the novel homomorphic encryption algorithm with random diagonal elliptical curve cryptography. The doctor remotely deciphers the data with the decryption key. Using the generated matrix as a basis, both the public and private keys are generated based on the logarithmic probability with smoothing conditions. In particular, the proposed model can be applied to the integration of IoT with cloud-based health systems.

Due to insufficient power, many IMDs today operate without basic security defenses. Trying to solve this problem the authors of [35] proposed a system model. The proposed system based on the consideration of energy limitations and the availability of each device, the authors propose a system model consisting of four layers: perception, network, data processing and application layer. Case study from the proposed system, where each device manages keys in an asymmetrical manner depending on the energy limitations of the device, demonstrates the effectiveness of managing keys on power-constrained devices to encrypt or decrypt the messages.

The authors of [36] identified the weaknesses in IoMT environment and IoMT edge network security threats. The major objective of their research was to identify an attack vector for the IoMT edge network. They used the Chapman-Kolmogorov equation to find the transient probabilities (number of probabilities distribution is 13 security attacks including countermeasures) and to examine how attacker exploits system vulnerabilities to change the state of the system from Safe state to Attack state. Depending on the distribution of security threat probability in the IoMT edge network and on the attack vector, quantifying the likelihood of attacks that will exploit these threats could be found.

For cancer disease prediction, the authors of [37] utilized IoT and cloud computing. In order to improve health care computations, they developed a framework that enhanced the security and flexibility of accessing cancer patient details. By using Virtual Machines (VMs), framework simulation (using CloudSim) showed that task completion time is reduced from 400 to 160.

The existing encryption techniques are too strict to handle and ensure the suitable encoding for images in the IoMT framework. A security paradigm in the IoMT for medical images is presented in Figure 4. To protect the security and privacy of the patient's image, the authors of [38] used 256 bits for encryption and divided the image's binary value into 16 segments of 16 bits. The encryption procedure contains the following steps: configuration the parameters, applying key for the brain images, starting key and image nomination operation then computing the segment-based image encryption transformation and finally applying the lightweight Image encryption algorithm. The algorithm was experimented at the cybersecurity laboratory showing better efficiency than conventional techniques.

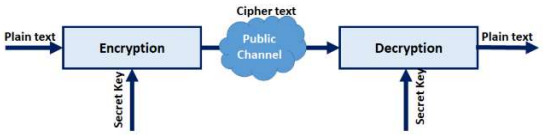

Figure 4. Representation of the image security paradigm of IoMT

The rapid growth of IoMT led to the occurrence of many security threats. The authors of [39] suggested a new authentication system as recommendations such as filtering for anonymity.

The healthcare industry in the United States is considered the most affected sector by digital security breaches (four data breaches per week). Which prompted HIPAA to call for creating a checklist of current security practices in order to use it to identify the gaps in these practices. In this context the authors of [40] highlighted serious gaps in the literature with an emphasis on the need to bring further research to support better understand the risk management method applied to control cybercrimes in the healthcare sector.

An evaluation framework for evaluating the General Data Protection Regulations (GDPR) requirements against the different types of blockchains was proposed in [41]. The obtained results showed that; despite the use of blockchain, legal risks and ethical allegations remain unsolved. In addition, they mentioned there is a lack of existing literature on cross-border movement towards ownership of health certificate of COVID-19.

Pseudonymization technique was used in [42] for protecting EHRs. The proposed module works as follows: the pseudonymization module removes all identifiers and quasi-identifiers related to a patient are removed from the patient's health record, before storing it into the Patient Controlled Pseudonym Based HER (PcPbEHR) database, this guaranties that the patient's identity is hidden from any intruder. The patient identity is unique and generated randomly using the Pseudonym Generation mechanism.

A system based on blockchain for protecting EHR was proposed in [43], the proposed system offered some characteristics such as decentralization, security, secrecy, immutability and tamper-proof. The proposed system used an InterPlanetary File System (IPFS) and cloud computing to store patients 'data and files.

Employing the Web in virtual health care was explored in [44], the prospective such as tendencies, technologies, apparent challenges, and ethical issues were studied and explored. Moreover, emerging technologies such as AI, IoT, IoMT, fifth generation technology, big data and cloud computing were explored and studied also.

This section summarized most research papers on IoMT security from different prospective such as: Wireless Body Area Network, Medical Devices Communication, Medical Embedded Systems, Healthcare National Infrastructure, Wearable Bluetooth Low Energy (BLE) Enabled Health Monitoring Devices, Implantable Medical Devices (IMD), Medical Information System, Electronic Health Record (EHR) and Security of medical data on the cloud.

3. RESULTS AND DISCUSSIONS

The vast advances in IoT and communication technologies helped improving healthcare and can save patients' lives by offering remote health care warning about the status of the patient's to healthcare providers. But IoMT had its drawbacks especially concerning medical data privacy and data security during data transfer or storage. Several researches were done since the last years, in the beginning the researches concentrated on the architecture of the IoMT, BAN and wearable medical devices. After that, there emerged new trends in the researches such as security of the transmitted data, ability of the medical sensors and implantable devices to be have some security measures, developing new lightweight encryption and authentication techniques designed for resource-constrained devices. Latest research trends were about the adoption of blockchain for security, cloud computing (with its associated huge storage capabilities) for storing EHR.

As shown in Table 1 this paper categorized the surveyed papers according to their E-Health domains, for each domain, the features of each surveyed paper were listed.

From Table 1 it clear that Implantable medical devices (IMD), Electronic Health Record (EHR) and IoMT areas of Privacy gained First place of researches attention, while Medical embedded systems, Wearable Bluetooth Low Energy (WBLE) enabled health monitoring devices came in the second place. Finally, areas such as Medical embedded systems, Wearable Bluetooth Low Energy (BLE) enabled, Security of medical data on the cloud and health-monitoring devices need further researches with more emphasis on new technologies such as blockchain.

Table 1: Proposed Features from the Related Research Efforts According to E-Health Domains

E- Health Domain	Ref.	Features
Wireless Body Area Network	9	Framework for WBAN security
	30	Improvements to enhance the security of (BAN) applications
Medical Devices Communication	10	Long distance (more than 10 km) data communications.
	29	Secure communication between IoMT nodes
Medical Embedded Systems	11	Software-based Architectural Framework For Ensuring Security
	20	Remote software-based verification for real-time constrained embedded devices
	23	An architecture for ECG remote monitoring
	27	Authenticate the smart medical monitoring devices,
Healthcare National Infrastructure	12	security defense strategies against attacks aimed to harm the Healthcare Critical National Infrastructure (HCNI)
	31	Encoding and compressing data in healthcare systems
	32	Security platform prototype consists of four different mechanisms (Layers).
	40	highlighted serious research gaps in the healthcare industry
Wearable Bluetooth Low Energy (BLE) Enabled Health Monitoring Devices	14	Framework based on Penetration Testing Execution Standard (PTES).
	15	A wearable sensor system: strong end-to-end communication security
Implantable Medical Devices (IMD)	16	Evaluating cyber threats targeted IMD
	17	Efficient data access control protocol for IMD
	22	A Four-layer architecture model for skin monitoring system
	25	Some of the IMD attacks were explored
	35	Proposed systems based on the consideration of energy limitations and the availability of each device
Medical Information System	18	Security framework for medical information system in hospitals
	24	E-health care systems with the two constrained protocols
Electronic Health Record (EHR)	19	Security system for protecting medical EHR
	41	An evaluation framework for evaluating the General Data Protection Regulations (GDPR)
	42	Pseudonymization technique for protecting EHR
	43	System based on blockchain for protecting EHR
	44	Tendencies, technologies, apparent challenges, and ethical issues in EHR were studied.
IoMT Areas of Privacy Concerns	21	Addressed the areas of concerns to improve the IoMT model
	26	Privacy, security, and storage management in IoMT infrastructure exploration
	28	Exploration and classification of IoMT security threats
	33	Exploration of healthcare organizations known vulnerabilities.
	36	Identify an attack vector for the IoMT edge network
	38	Encoding framework for medical images.
	39	A new authentication system for IoMT.
Security of medical data on the cloud	34	Security architecture with two different models (security and prediction)
	37	Framework that enhanced the security and flexibility of accessing cancer patient details

4. IoMT PROBLEMS AND RESEARCH AREAS

As a new emerging technology, IoMT poses problems that still open areas of research such as how to control huge data generated from large number of connected medical devices and sensors, protecting and maintaining patient safety, maintain connectivity between connected sensors and devices continuously, minimizing human factor errors, lack of Interoperability between different vendors , lack of standardization and regulations and finally the biggest issues of medical devices security and medical records privacy.

This paper tried to highlight the importance of IoMT and its problems. It could be further improved by performing a multivocal literature review and focusing on recent research areas such as blockchain and Artificial Intelligence (AI).

5. CONCLUSION AND FUTURE DIRECTIONS

Recent advances in electronics have made IoMT an increasingly popular application to improve patient experience and efficiency of healthcare systems. Patients' data can be collected by wearable IoMT devices for condition monitoring and alerts, while implanted devices can be used to remotely inject medicine. An IoMT is a network of embedded objects, sensors, and actuators for transmitting and receiving medical data. However, security and privacy are significant concerns when it comes to wireless communication systems. Security of data and computation overhead remain the two main issues of the IoMT-cloud-based system. Traditionally, network security involves encryption, authentication, and authorization. However, these approaches may not be feasible for IoMT devices with severe power constraints.

Bearing in mind the importance of security and privacy parameters in IoMT, we explored and analyzed the factors that could negatively impact security and privacy. Accordingly, a literature review of IoMT security challenges has identified numerous challenges that have been addressed with cryptographic techniques, algorithms, and approaches proposed by recent researchers. With the rise in the usage of IoMT devices, this study aimed to identify new threats and patterns that arise, both technical and behavioral. A review of different e-Health domains has been done regarding the weaknesses in IoMT devices edge network security threats. It has also been noted that insufficient power in IMDs led to the operating of these devices without proper security defenses. Moreover, new factors have emerged, such as "the fear of not knowing how IoMT devices work," making these devices more vulnerable to security threats. Additionally, the paper illustrates the suggested improvements to enhance the security of future Medical Body Area Network (MBAN) applications based on IEEE 802.15 TG6.

Between different Future work could be to perform a multivocal literature review, determining the success factors of secure IoMT and identifying further challenges. In addition, we will collect best practices for secure IoMT by conducting case studies with experts.

REFERENCES:

[1] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain," J. Commun., vol. 12, 2017, pp. 240-247.

[2] Rubí, Jesús & R. L. Gondim, Paulo. "IoMT Platform for Pervasive Healthcare Data Aggregation, Processing, and Sharing Based on OneM2M and OpenEHR," Sensors, 2019. 19. 4283. 10.3390/s19194283.

[3] D. Kalra, "Electronic health record standards," Yearbook of medical informatics, vol. 15, 2006, pp. 136-144.

[4] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical internet of things: a review," Security and Communication Networks, vol. 2018, 2018.

[5] W. Khan, E. Muntimadugu, M. Jaffe, and A. J. Domb, "Implantable medical devices," in Focal controlled drug delivery, ed: Springer, 2014, pp. 33-59.

[6] H. A. Owida, J. I. Al-Nabulsi, N. M. Turab, F. Alnaimat, H. Rababah, and M. Y. Shakour, "Autocharging Techniques for Implantable Medical Applications," International Journal of Biomaterials, vol. 2021, 2021.

[7] D. I. Fotiadis, C. Glaros, and A. Likas, "Wearable medical devices," in Wiley Encyclopedia of Biomedical Engineering, ed: Wiley Hoboken, NJ, USA, 2006.

[8] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. Leung, "Body area networks: A survey," Mobile networks and applications, vol. 16, 2011, pp. 171-193.

[9] P. C. Paul, J. Loane, F. McCaffery, and G. Regan, "A Data Security And Privacy Risk Management Framework For WBAN Based Healthcare Applications," in 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 2021, pp. 704-710.

[10] N. C. Gaitan, "A Long-Distance Communication Architecture for Medical Devices Based on LoRaWAN Protocol," Electronics, vol. 10, 2021, p. 940.

[11] A. Rao, "A Software Framework for Security Risk Assessment and Management in Life-critical Embedded Systems," The University of Arizona, 2021.

[12] Y. He, R. S. Camacho, H. Soygazi, and C. Luo, "Attacking and defence pathways for Intelligent Medical Diagnosis System (IMDS)," International Journal of Medical Informatics, vol. 148, 2021, p. 104415.

[13] (2022, Feb). OpenEMR. Available: https://www.open-emr.org/

[14] G. A. Zendehdel, R. Kaur, I. Chopra, N. Stakhanova, and E. Scheme, "Automated Security Assessment Framework for Wearable BLE-enabled Health Monitoring Devices," ACM Transactions on Internet Technology (TOIT), vol. 22, 2021, pp. 1-31.

[15] J. Winderickx, P. Bellier, P. Duflot, and N. Mentens, "Communication and Security Trade-Offs for Battery-Powered Devices: A Case Study on Wearable Medical Sensor Systems," IEEE Access, vol. 9, 2021, pp. 67466-67476.

[16] M. N. Sabra, "Cyberthreats on Implantable Medical Devices," Journal of Information Security and Cybercrimes Research, vol. 4, 2021, pp. 36-42.

[17] J. Kar, X. Liu, and F. Li, "Dac-Pre: Practical Anonymous Data Access Scheme Control with Proxy Re-Encryption For Implantable Medical Devices," Available at SSRN 4005069.

[18] Y. Kim, J. Kim, and H. Chang, "Design of an Information Security Service for Medical Artificial Intelligence," CMC-COMPUTERS MATERIALS & CONTINUA, vol. 70, 2022, pp. 679-694.

[19] A. T. Kalpally and K. Vijayakumar, "Privacy and security framework for health care systems in IoT: originating at architecture through application," Journal of Ambient Intelligence and Humanized Computing, 2021, pp. 1-11.

[20] S. Surminski, C. Niesler, F. Brasser, L. Davi, and A.-R. Sadeghi, "RealSWATT: Remote Software-based Attestation for Embedded Devices under Realtime Constraints," in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, 2021, pp. 2890-2905.

[21] S. M. Karunarathne, N. Saxena, and M. K. Khan, "Security and privacy in IoT smart healthcare," IEEE Internet Computing, vol. 25, 2021, pp. 37-48.

[22] S. Juyal, S. Sharma, and A. S. Shukla, "Security and privacy issues in unified IoT-based skin monitoring system," Materials Today: Proceedings, vol. 46, 2021, pp. 10815-10820.

[23] N. C. Gaitan and I. Ungurean, "Internet of M-Health Things System for Remote EKG Monitoring," in 2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI), 2019, pp. 1-4.

[24] A. Hussain, T. Ali, F. Althobiani, U. Draz, M. Irfan, S. Yasin, et al., "Security framework for IoT based real-time health applications," Electronics, vol. 10, 2021, p. 719.

[25] V. Hassija, V. Chamola, B. C. Bajpai, and S. Zeadally, "Security issues in implantable medical devices: Fact or fiction?," Sustainable Cities and Society, vol. 66, 2021, p. 102552.

[26] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology," The Journal of Supercomputing, vol. 77, 2021, pp. 7916-7955.

[27] P. Kumar and L. Chouhan, "A privacy and session key based authentication scheme for medical IoT networks," Computer Communications, vol. 166, 2021, pp. 154-164.

[28] M. A. Akbar, A. Alsanad, S. Mahmood, and A. Alothaim, "A Multicriteria Decision Making Taxonomy of IOT Security Challenging Factors," IEEE Access, vol. 9, 2021, pp. 128841-128861.

[29] A. Nazir, S. Sholla, and A. Bashir, "An Ontology based Approach for Context-Aware Security in the Internet of Things (IoT)," International Journal of Wireless and Microwave Technologies (IJWMT), vol. 11, 2021, pp. 28-46.

[30] G. Hahn, M. A. Siddiqi, S. Hamdioui, W. A. Serdijn, and C. Strydis, "Assessing the Security of the IEEE 802.15. 6 Standard for Medical BANs," arXiv preprint arXiv:2201.06354, 2022.

[31] M. Shankar Lingam, G. Raghavendra, A. Kumar, V. Anand, and A. Sudhakara, "Data Encryption as Security Measure in IoT-Enabled Healthcare," in Smart Trends in Computing and Communications: Proceedings of SmartCom 2020, ed: Springer, 2021, pp. 69-81.

[32] N. Vithanwattana, G. Karthick, G. Mapp, and C. George, "Exploring a new security framework for future healthcare systems," in 2021 IEEE Globecom Workshops (GC Wkshps), 2021, pp. 1-6.

[33] C. Graham, "Fear of the unknown with healthcare IoT devices: An exploratory study," Information Security Journal: A Global Perspective, vol. 30, 2021, pp. 100-110.

[34] M. Vedaraj and P. Ezhumalai, "HERDE-MSNB: a predictive security architecture for IoT health cloud system," Journal of Ambient Intelligence and Humanized Computing, vol. 12, 2021, pp. 7333-7342.

[35] I. Jellen, J. Callenes-Sloan, and D. Fang, "Heterogeneous System Model for Security in E-Health Applications," in 2021 IEEE International Conference on Communications Workshops (ICC Workshops), 2021, pp. 1-6.

[36] M. A. Allouzi and J. I. Khan, "Identifying and modeling security threats for IoMT edge network using Markov chain and common vulnerability scoring system (CVSS)," arXiv preprint arXiv:2104.11580, 2021.

[37] M. Anuradha, T. Jayasankar, N. Prakash, M. Y. Sikkandar, G. Hemalakshmi, C. Bharatiraja, et al., "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," Microprocessors and Microsystems, vol. 80, 2021, p. 103301.

[38] M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A.-H. A. Hashim, S. Habib, et al., "Lightweight encryption technique to enhance medical image security on internet of medical things applications," IEEE Access, vol. 9, 2021, pp. 47731-47742.

[39] R. Karthick, R. Ramkumar, M. Akram, and M. V. Kumar, "Overcome the challenges in bio-medical instruments using IOT–A review," Materials Today: Proceedings, vol. 45, 2021, pp. 1614-1619.

[40] F. M. Dias, M. L. Martens, S. F. de Paula Monken, L. F. da Silva, and E. D. R. Santibanez-Gonzalez, "Risk management focusing on the best practices of data security systems for healthcare," International Journal of Innovation, vol. 9, 2021, pp. 45-78.

[41] M. Foy, D. Martyn, D. Daly, A. Byrne, C. Aguneche, and R. Brennan, "Blockchain-based governance models for COVID-19 digital health certificates: A legal, technical, ethical and security requirements analysis," Procedia Computer Science, vol. 198, 2022, pp. 662-669.

[42] B. K. Rai, "Patient-Controlled Mechanism Using Pseudonymization Technique for Ensuring the Security and Privacy of Electronic Health Records," International Journal of Reliable and Quality E-Healthcare (IJRQEH), vol. 11, 2022, pp. 1-15.

[43] N. Alrebdi, A. Alabdulatif, C. Iwendi, and Z. Lian, "SVBE: searchable and verifiable blockchain-based electronic medical records system," Scientific Reports, vol. 12, 2022, pp. 1-11.

[44] E. Mbunge and B. Muchemwa, "Towards emotive sensory Web in virtual health care: Trends, technologies, challenges and ethical issues," Sensors International, vol. 3, 2022, p. 100134.