RESEARCH ARTICLE OPEN ACCESS

Threat Intelligence and Internet of Medical Things(IoMT)

Alex Mathew
Dept. of Cybersecurity
Bethany College, USA

ABSTRACT
A paradigm shift in the healthcare industry is inclined towards the digital transformation of the operations. The digitalization has led to increased adoption of the Internet of Medical Things devices because of associated benefits, such as improved innovation and performance. However, the acceptability and usage of this technology face privacy and security threats. The current study adopted a systematic literature review approach to investigate the threat intelligence and IoMT in the healthcare industry. The findings showed that IoMT is a viable and intelligent application used by most of the medical organizations; however, the cybersecurity threat is a constant challenge. Nonetheless, IoMT-SAF is a recommended solution for cybersecurity threats linked to IoMT.

Keywords:- Internet of Medical Things, threat intelligence, IoMT-SAF, digital transformation

I. INTRODUCTION

The healthcare industry is facing a paradigm shift just like the rest of industries due to the emergence of advanced technologies and devices. Digital change has changed the landscape of healthcare operations, but also created potential threats, especially intelligent ones. The threat intelligence is about the skillful way to promote information security, especially because of digital transformation. The increased deployment of the Internet of Medical Things (IoMT) devices in healthcare have benefits but also poses security threats that must be addressed. Today, over 70% of healthcare institutions and agents have adopted IoMT and are using them extensively [6]. IoMT denotes the incorporation of medical applications and devices, which are linked through the Internet due to social engineering and networking capabilities. Patients and medical experts welcome IoMT as a vibrant force that is facilitating the accomplishment of many functions and operations that could not be completed by the conventional IoT platforms[2]. In simple terms, IoMT is a compilation of medical applications and appliances that join or link to healthcare IT platforms via online computer systems[1]. Empirical evidence shows that even though the emergence and increase of the IoMT have enhanced patient care and medical procedures, it has also led to increased incidences of vulnerabilities; thus, threat intelligence has become an important component of its control. Fortinet provides some strategies for healthcare institutions to prevent or tackle potential IoMT cyber-threats [1].

A. Background

IoMT characteristic components are wearable (heart monitors), ambient (door sensors), implantable (embedded cardiac monitors, or stationary [2]. The modern endpoints for IoMT are associated with integrated networking capabilities with gateways. The technology is also integrated with cloud-based platforms to facilitate smart devices' operations and applications [2]. IoMT infrastructures provide administrators-based back-end control functionalities for integrating web interfaces, reports, ecosystem administration, and analytics back up [4]. Services are used to offer edge or competitive computing for assessment and analysis of compiled data for medical analytics and finance reconciliations. Characteristically, IoMT infrastructures are built with a principle of integration [2,4]. As illustrated in Fig. 1, IoMT distinctive components are sensors, ambient motion, wearable implantable cardiac, gateway, back-end, and smart communication device.

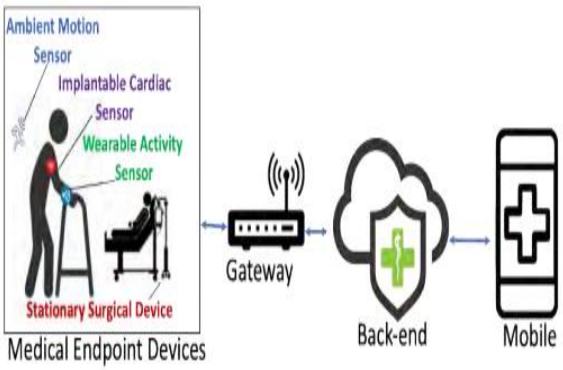

Fig. 1. IoMT Typical Components [4]

The potential of IoMT cannot be realized is the associated threats are overlooked or ignored. Studies have shown that IoMT is not immune to privacy and security because of the myriad IoMT vendors and devices in the market. The industry is full of many devices that are sharing sensitive medical information through cloud platforms virtually or wirelessly [2]. Cyber threat intelligence (CTI) is a subject of interest because many healthcare organizations are experiencing or cognizant of potential cyber-attacks [8]. The threat landscape is evolving rapidly as most of the institutions continue to adopt IoMT[8]. Therefore, there is a need to enhance the cybersecurity capacity of hospitals to minimize the end-point complexity of information sharing and boost internal stakeholder configuration. Threat intelligence entails the use of strategies for effective control of cyber vulnerability in a systematic way instead of blind troubleshooting once the security breach has occurred [7]. Security experts have demonstrated that attacks on IoMT devices can lead to fatal outcomes for patients and severe implications for healthcare providers [12]. However, it is reasonable to note that conventional IoT security solutions cannot specifically fingerprint medical devices with vulnerability to their vendors' communication protocols [12].

II. PROPOSED METHODOLOGY BLOCK DIAGRAM

The researcher has adopted a systematic literature review to gather empirical evidence, which is vital for the result analysis and completion of the paper. Fig. 2 provides a block diagram of the methodology for the study. The first step is to conduct an overview of academic research of literature associated with the topic. The second step is to extract relevant and reputable articles with relevant information and (step 3) follow up the extraction with viable references and links. Step four was to narrow the search by offering precondition for recently (2016-2020) published and reputable articles. The key terms helped to gather relevant data, which are then synthesized to present an understandable report [8].

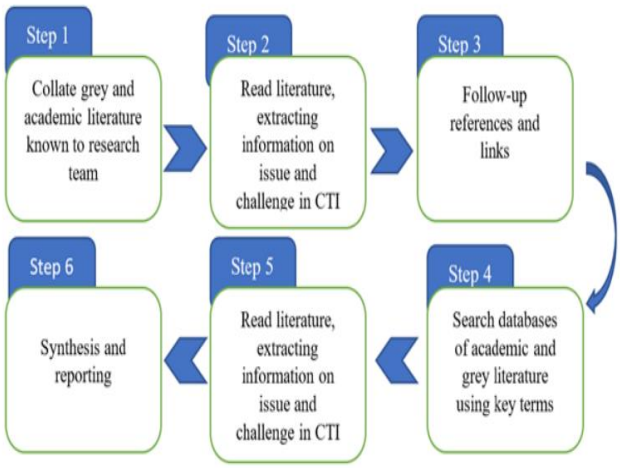

Fig. 2: Research Approach

The algorithm and flowcharts were also used to demonstrate the study objective with key terms and phrases being the guiding measures.

A. Algorithm

The path search algorithm entails the use of threat intelligence, solution, stakeholders, and infrastructures. Stakeholders are medical professionals, systems or network administrators, and patients. Solutions are devices, services, and infrastructure. The search was to analyze the threat intelligence issues and solutions for IoMT vulnerabilities.

TABLE 1: PATH SEARCH ALGORITHM [5]

Algorithm
"e: an IoMT Threat intelligence scenario
Input: $Stakeholder_e$, $Solutions_e$, $Infrastructures_e$
Output: $Measures_e$, $Attribues_e$, $Issues_e$
1: **for all** Solution in $Solutions_e$ **do**
2: **if** $Solution_{Devices\ not\ in}$ $Devices_e$ **then**
3: add $Solution_{Devices}$ to $Devices_e$
4: **end if**
5: **if** $Issues_{Solution}$ not in $Issues_e$ **then**
6: add $Issues_{Solution}$ to $Devices_e$
7: **end if**
8: **for all** Infrastructures in $Infrastructures_e$ **do**
9: **if** Infrastructures in $Solution_{Infrastructures}$ **then**
10: **if** $Device_{Infrastructures}$ not in $Devices_e$ **then**

```
11:            add Device_Infrastructures to Devices_e
12:            if Issues_Infrastructures not in Issues_e then
13:              add Issues_Infrastructure to Issues_e
14:              end if
15:          end if
16:        end if
17:      end if
18:    end if
19: Return Issues_e Solutions_e
```

B. Flow Chart

The flow chart presents the study processes to find IoMT solutions for associated threat intelligence. The literature review showed that IoMTSAF is a viable solution to IoMT cybersecurity threats. The flow chart (Fig. 3) shows that the study found a viable solution to IoMT and threat intelligence topic.

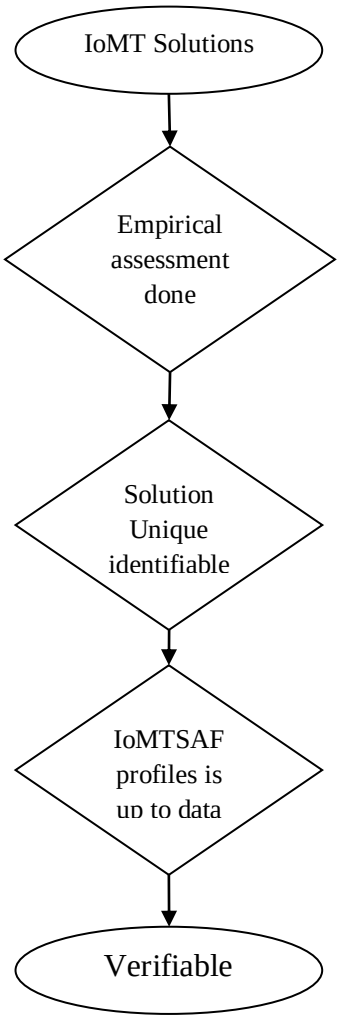

Fig. 3: IoMTSAF A Viable Threat Intelligence

III. RESULT ANALYSIS

A. IoMT Adoption Rate

The empirical findings have shown that 87% of medical institutions have adopted IoT infrastructures in their operations, which is the third-highest rate of any sector [6]. The advantages of IoT are attributed to improved innovation (80%), enhanced interoperability, and visibility across organizations (76%), and cost savings (73%), according to recent research conducted by Hewlett Packard [6]. Out of these organizations, 70% have since adopted IoMT to enhance their operations and counter the limitations of traditional IoT [6]. Experts have pointed out that IoMT is no longer a futuristic idea in the health industry. The devices and infrastructures of most healthcare institutions have been amalgamated with smart technologies as part of the current patient care ecosystems, such as sensors, ambient solutions, and wearable devices[10]. However, the sensitivity and criticality of the healthcare data and domain require that the security and privacy of the IoMT be a matter of interest in all sectors [5]. Results have shown that health organizations that have adopted security measures for their IoMT are reporting improved performance.

B. IoMT Capacity and Threat in Healthcare

A study conducted by Allied Market Research reveals that IoT healthcare market is anticipated to reach $136.8 billion US dollars by 2021, registering 12.5% of Compound Annual Growth Rate (CAGR) for the period ranging from 2015 to 2021, due to lower costs of sensory innovation and accessibility of wearable smart devices [1]. The healthcare industry is contributing to over 40% of IoT technology usage globally with over 60% investing in IoT solutions [2]. However, the high rate of IoMT usage in this industry is also linked to susceptibility to cybersecurity threats. The landscape of the Internet systems and networks is characteristically wide and open; thus, requiring efficient internal segmentation firewalls (ISFWs) for effective defense toward IoMT-oriented breaches [3]. IoMT security and privacy are dependent on emerging technologies, such as cloud hosting, augmented intelligence, digital therapeutic for better results [11]. Therefore, the healthcare industry is

adopting threat intelligence solutions toward IoMT security challenges.

C. IoMT Threat Intelligence Solutions

ISFWs run within the network rather than the edge; thus, healthcare organizations can intelligently demarcate systems between administrators, patients, guests, and healthcare professionals, and between varied devices [3]. For example, it is used between life-saving heart monitor and patient information systems to stop and detect malicious code across networks. Furthermore, integrating network access control (NAC) and ISFW solutions improves the capability of system administrators to detect when anomalous data movement from a compromised IoMT device [3]. Apart from the ISFW and NAC devices, IoMT Security Assessment Framework (IoMT-SAF) is an ideal threat intelligence application to prevent cyber-attacks [2]. The result has shown that the threat intelligence issue remains core to this study objective since it directly connects IoMT. The result shows that IoMT spans across devices (non-invasive, invasive, and active devices) and IoMT-SAF can secure all these devices intelligently [11]..

Fig. 4: IoMT Threat Intelligence Solutions

Experts assessed the efficiency of IoMT-SAF against other measures. Their findings were summarized base on recommended, not recommended, and relevant/irrelevant security measures [2]. Table 2 depicts the measurement matrix used for assessment.

TABLE 2: RECOMMENDATION CLASSIFICATION

	Relevant	Irrelevant
Recommended	a	b
Not Recommended	c	d

Recall = a/(a+c)

(1)

Accuracy = (a+d)/(a+b+c+d)

(2)

Precision = a/(a+b)

(3) [2]

Table 3 reveals that IoMT-SAF's average accuracy is very high; thus, it is an acceptable and recommended solution of the IoMT threat since it uses viable intelligence [2].

Table 3: COMPUTING THE RECOMMENDATION EVALUATION METRICS [2]

Expert	*a*	*b*	*c*	*d*	Accuracy	Precision	Recall
1	28	0	1	14	97.7%	100%	96.6%
2	18	1	1	23	95.3%	94.7%	94.7%
3	22	1	2	18	93%	95.7%	91.7%
4	32	3	1	7	90.7%	91.4%	97%
5	14	0	0	29	100%	100%	100%
6	23	1	0	19	97.7%	95.8%	100%
7	38	5	0	0	88.4%	88.4%	100%
Average					**94.7%**	**95.1%**	**97.1%**

IoMT-SAF is web-based software using a new ontological scenario-oriented strategy to guarantee cybersecurity in IoMT. It recommends essential attributes for viable security measures because of high levels of adopting emerging technologies and new stakeholders and compliance with standards [2]. The qualities of the IoMT-SAF have made it a preferred choice for IoMT [4]. The model is preferred because it allows the adopters of the system to identify all IoMT security issues carefully using a standardized IoMT taxonomy [5]. Fig. 4 presents the scenario of IoMT-SAF that complies with the adopted algorithm. The ontology regards the IoMT stakeholders as a key mediator between solutions and security requirements.

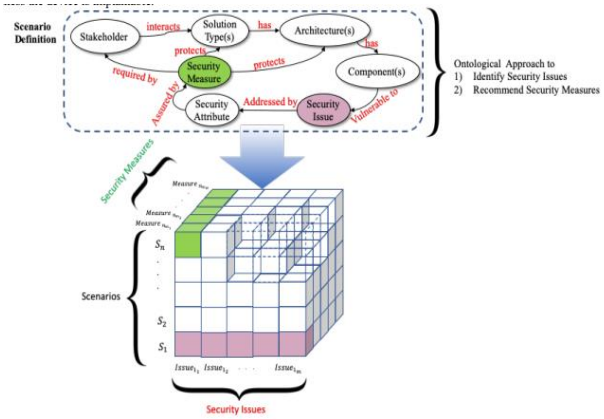

Fig. 5: Scenario of IoMT-SAF [5]

IoMT-SAF is essential for enabling users to make viable decisions regarding IoMT solutions due to its integrated functionalities. Studies about the survey-based, vulnerability-based, and expert-oriented have identified IoMT-SAF as a significant privacy and security solution for various IoT oriented healthcare devices and application scenarios [9].

IV. CONCLUSION

The recent trend of IoMT technology adoption in the healthcare industry is gaining popularity because of associated benefits. Incorporation of various healthcare devices has increased the performance and boosted the accuracy and quality outcome; however, the inadequacy of privacy and security in IoMT devices could lead to severe life-threatening consequences. Therefore, the industry is adopting threat intelligence approaches to safeguard the privacy of data and information. The study has evaluated ISFW, NAC, and IoMT-SAF, and recommended the usage of the last one because it has high accuracy for security provision.

REFERENCES

[1] InnoHEALTH Magazine, "IoMT: Protection against cyber-threats," 2018, [Online]. Available: https://innohealthmagazine.com/2018/trends/internet-of-medical-things/

[2] F. Alsubaeia, A. Abuhusseinc, V. Shandilyad , and S. Shiva, "IoMT-SAF: Internet of Medical Things Security Assessment Framework," Internet Of Things , 2019, pp. 1-32.

[3] S. Arista, "Securing the Internet of Medical Things," Inside Digital Health, 2019, [Online]. Available: https://www.idigitalhealth.com/news/securing-the-internet-of-medical-things

[4] F. Alsubaei, A. Abuhussein, S. Shiva, Ontology-Based Security Recommendation for the Internet of Medical Things, IEEE Access. 7 (2019) 48948–48960. doi:10.1109/ACCESS.2019.2910087.

[5] F. Alsubaei, A. Abuhussein, S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," in: 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), 2017: pp. 112–120. doi:10.1109/LCN.Workshops.2017.72..

[6] HIPAA Journal, "87% of Healthcare Organizations Will Adopt Internet of Things Technology by 2019," 2017, [Online]. Available: https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712/.

[7] M. S. Jalali and J. P. Kaiser, ''Cybersecurity in Hospitals: A systematic, organizational perspective,'' J. Med. Internet Res., vol. 20, no. 5, 2018, Art. no. e10059.

[8] S. Abu, S. R. Selamat, A. Ariffin , and R. Yusof, "Cyber Threat Intelligence – Issue and Challenges," Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, No. 1, 2018, pp. 371-379 DOI: 10.11591/ijeecs.v10.i1

[9] N. Nanayakkara, M. N. Halgamuge, and A. Syed, " Security And Privacy Of Internet Of Medical Things (Iomt) Based Healthcare Applications: A Review," Proceedings of 262nd The IIER International Conference, Istanbul, Turkey, 6 th -7 th, 2019, pp. 1-12.

[10] A. Ross, "Measuring Security Risk in a Medical IoT World," Security Intelligence, 2020, [Online]. Available: https://securityintelligence.com/posts/measuring-security-risk-in-a-medical-iot-world/

[11] S. Rafee, "IoMT Security: A Comprehensive Approach to Mitigate Risk and Secure Connected Devices," Security Intelligence, 2019, [Online]. Available: https://securityintelligence.com/posts/iomt-security-a-comprehensive-approach-to-mitigate-risk-and-secure-connected-devices/

[12] MEDIGATE, "The Internet of Medical Things: Why Traditional IoT security Isn't Enough," 2018, pp. 1-4.