Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 15s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Cyber Security In Healthcare Using Iomt

Dr. Shivanand Pujar[1], Dr. Savitha C K[2], Prof. Rekha S[3], Dr. Dinesha H.A[4]

[1]Department of Computer Science and Engineering, Navkis College Of Engineering (NCE), Visveswaraya Technological University (VTU), Karnataka, India

[2]Professor and Head Department of CS&E(AI & ML) KVG College of Engineering, Sullia, D. K, VTU Belagavi

Email ID: cksavithaharish@gmail.com

[3]Department of Computer Science and Engineering, Navkis College Of Engineering (NCE), Visveswaraya Technological University (VTU), Karnataka, India

[4]Department of Artificial Intelligence and, Machine Learning, Navkis College Of Engineering (NCE), Visveswaraya Technological University (VTU), Karnataka, India

***Corresponding Author:**

Dr. Dinesha H.A

Professor, Computer Science and Engineering Department, Navkis College of Engineering Hassan, Karnataka, India.

Email ID: sridini@gmail.com

.Cite this paper as: Dr. Shivanand Pujar, Dr. Savitha C K2, Prof. Rekha S, Dr. Dinesha H.A, (2025) Cyber Security In Healthcare Using Iomt. *Journal of Neonatal Surgery*, 14 (15s), 1722-1729.

ABSTRACT

Internet of Medical Things (IoMT) is one such realistic application of IoT in healthcare domain, which provides an opportunity to evolve the existing healthcare system and provide better healthcare services and quality life to the patients. It opens a way for the potential security attacks to the ongoing IoMT communication where the adversaries can get unauthorised access to the personal, confidential and sensitive health related information that can be utilised for malicious purposes. To overcome security issues of IoMT, various security protocols have been proposed and designed in the recent couple of years. This paper discussed about healthcare analytics using IoT. The Internet of Medical Things (IoMT) refers to the network of interconnected medical devices, sensors, and applications that transmit health data over the internet for improved healthcare delivery.

Keywords: *IoMT, nCyberSecurity, SmartPills, Healthcare*

1. INTRODUCTION

Cybersecurity in healthcare is becoming increasingly important as healthcare organizations adopt more digital systems and store sensitive patient information electronically. The healthcare industry is a prime target for cyberattacks because of the sensitive and valuable nature of the data they possess [1]. This includes personal health information (PHI), financial information, and other sensitive information that can be used for malicious purposes. To mitigate these risks, it is important for healthcare organizations to implement strong security measures such as encryption, secure data storage, regular software updates, employee training, and incident response plans [2].

2. CYBER ATTACKS HEALTH INFORMATION

Cyber-attacks on health information can have serious consequences, including theft of sensitive information, loss of trust in healthcare organizations, and financial losses. Health information is a valuable target for cyber criminals because it can be used for identity theft, fraud, and other illegal activities [3]. Additionally, many healthcare organizations store large amounts of financial information, making them a prime target for cyber-attacks. To prevent these attacks, healthcare organizations must implement strong security measures, such as encryption, secure data storage, regular software updates, employee training, and incident response plans [4]. It is also important for individuals to protect their own health information by using strong passwords, being cautious about sharing personal information online, and monitoring their financial accounts for unusual activity [5].

1.1 Cyber Attacks Health Sensitive Information

Cyberattacks on health sensitive information can have serious consequences, including theft of personal health information (PHI), loss of trust in healthcare organizations, and financial losses. Health sensitive information is a valuable target for cyber criminals because it can be used for identity theft, fraud, and other illegal activities [6]. Additionally, many healthcare organizations store financial information, making them a prime target for cyberattacks. To prevent these attacks, healthcare organizations must implement strong security measures, such as encryption, secure data storage, regular software updates, employee training, and incident response plans. It is also important for individuals to protect their own health information by using strong passwords, being cautious about sharing personal information online, and monitoring their financial accounts for unusual activity [7].

The security of connected care devices and systems, such as the Internet of Medical Things (IoMT) and Internet of Things (IoT) devices, is a crucial concern for healthcare organizations. This includes securing operational technology (OT) systems and ensuring visibility of IT assets. Threat mitigation strategies aim to reduce the risk of security incidents and minimize their impact if they occur. These strategies include implementing strong passwords and authentication protocols, using encryption for sensitive data, conducting regular security assessments, and regularly updating software and firmware to address known vulnerabilities. Additionally, organizations should have incident response plans in place to quickly respond to security incidents and minimize their impact [8]. The below figure.1 shows the devices that are mainly responsible for internet of medical things. These devices the way they are interconnected and the way they respond to each other and to the external world is signified by this figure 1.

Strong Security Measures
Secure Data Storage
Regular Software Updates
Strong Passwords
Employee Training
Incident Response Plans

Figure 1. Connected Devices of Internet of Medical Things

The Internet of Medical Things (IoMT) refers to the network of medical devices, such as wearable health monitors, smart pills, and telehealth devices, that are connected to the internet and other networks. These devices gather and transmit health data to healthcare providers, allowing for remote monitoring and treatment [9]. However, the use of IoMT devices also introduces new security risks, as sensitive health information is being transmitted over the internet and stored in cloud-based systems. To mitigate these risks, it's important to ensure that IoMT devices are secure and that the data they transmit is protected. This can be done through secure software design, regular security updates, encryption, and secure data storage and transmission protocols. Additionally, healthcare organizations should regularly assess the security of their IoMT systems and implement incident response plans in the event of a security breach [10]. The figure 2. Shows the different forms of the layers that are appearing within the internet of medical things. It also notifies the attacks that are appearing with respect to the each of the layers.

The different forms of the attacks that are appearing within the IoT are physical attacks, network attacks, software attacks and data attacks. These attacks are listed into different categories depending upon the respective layers. Cyber attacks mainly notify the risk which is an integrated version of vulnerabilities, threats along with the potential impact. It is also noticied that the threat appearing is recognized to be a cyber-Attack that make use of the system vulnerabilities [11].

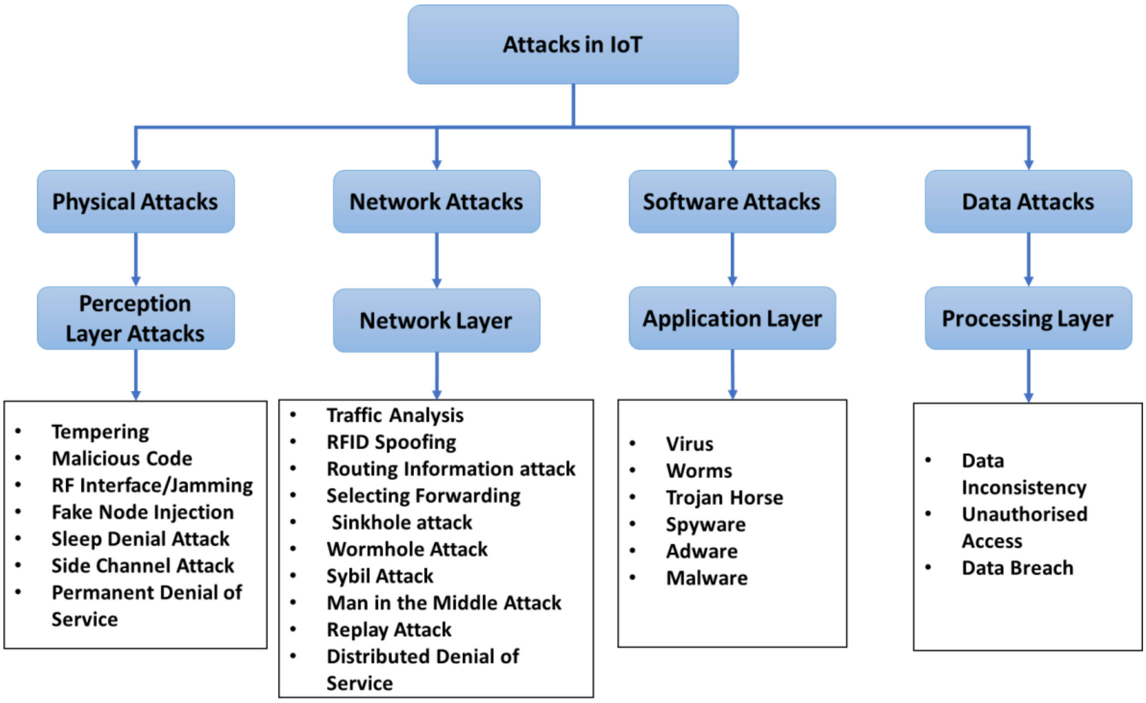


Figure 2. IoT attacks based on each layer

The Internet and Internet of Things (IoT) are key contributors to growing security risks. As web applications expand, the potential for data breaches intensifies. Vulnerabilities in certain plugins and add-ons can also provide entry points for malware to compromise systems. Phishing techniques are evolving and becoming increasingly deceptive, making passwords alone insufficient for securing sensitive information. The main threat actors behind these risks include cybercriminals, nation-states, and hacktivists, each with their own motivations and methods [12]. From the figure 3 it can be noticed the things that are responsible to create internet of medical things. Table 1 signifies the level of attacks for each of the layers within the IoMT. These levels are categorized into different types as confidentiality, integrity and availability.

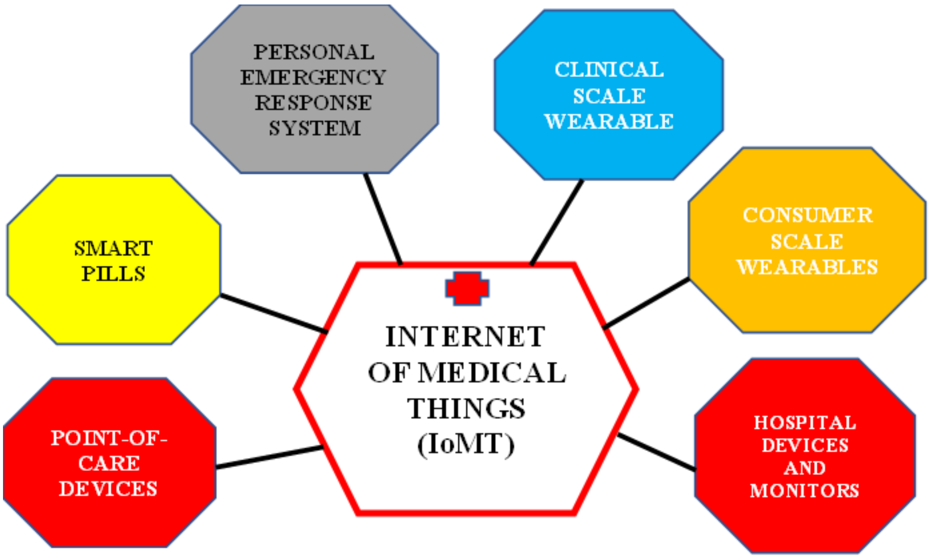

PERSONAL EMERGENCY RESPONSE SYSTEM
CLINICAL SCALE WEARABLE
SMART PILLS
CONSUMER SCALE WEARABLES
INTERNET OF MEDICAL THINGS (IoMT)
POINT-OF-CARE DEVICES
HOSPITAL DEVICES AND MONITORS

Figure 3. Internet of Medical Things (IoMT)

Table 1. Attacks for Each IoMT Layer

IoMT Layer	Medical Things	Attack type	Confidentiality, Integrity, Availability (CIA) type
Perception	Wearable, Implantable, Ambient, and Stationary	Side channel	C
		Tag Cloning	C, I
		Tampering devices	I, A
		Sensor Tracking	C, I
Network	Wearable, Implantable, Ambient, and Stationary	Eavesdropping	C
		Replay	C, I
		Man-in-the-middle	C, I
		Rogue access	C
		DoS	A
		Sinkhole	C
Middleware	All	CSRF	C
		Session Hijacking	C, I
		XSS	C, I
Application	All	SQL Injection	C, I, A
		Account Hijacking	C
		Ransomware	A
		Brute force	C
Business	All	Information Disclosure	C
		Deception	I
		Disruption	A

From the table.2 a real incident concerned to IoMT is being notified were each of the device like pacemaker and blood sugar monitor is notified with the attacks like side-channel, tampering along with the network like 10 and 5 and the protocol prone that is responsible. The overall count of heterogenous systems involved are mainly the 5 and 10 with repect to the pacemaker and blood sugar monitor. The security of the devices is notified to be 10 and 5 involving the risk factor 8 and 6. Figure 4 clearle shows the pictorial representations of the side-channel and the tampering that is being caused by both of the IoMT devices. The blue-coloured line signifies side-channel for the pacemaker were as the yellow-coloured line signifies tampering for the blood sugar monitor. From the figure 4 it is also clearly observed the CIA to be equivalent to 5 and 5 for both of the devices.

Figure 5 illustrates the risk impact in relation to side-channel attacks and tampering. The risk associated with tampering is considered minimal, whereas the risk impact from side-channel attacks is identified as significantly higher. The analysis of the memory is recognized to be a promising technique which gives a comprehensive view concerned to the malware and also it serves as the majority within the malware analysis. The contributions so for analysed are 1) providing an overview of malware types and malware detection approaches (2) discussion of the current malware analysis techniques 3) study of malware obfuscation 4) expoling the memory-based analysis [13].

Table 2. IoMT real incident

IoMT device	Attack	Network	Protocol prone	Count of heterogeneous systems involved	Device Security	CIA	Risk impact
Pacemaker	Side-channel	10	10	5	10	5	8
Blood sugar monitor	Tampering	5	5	10	5	5	6

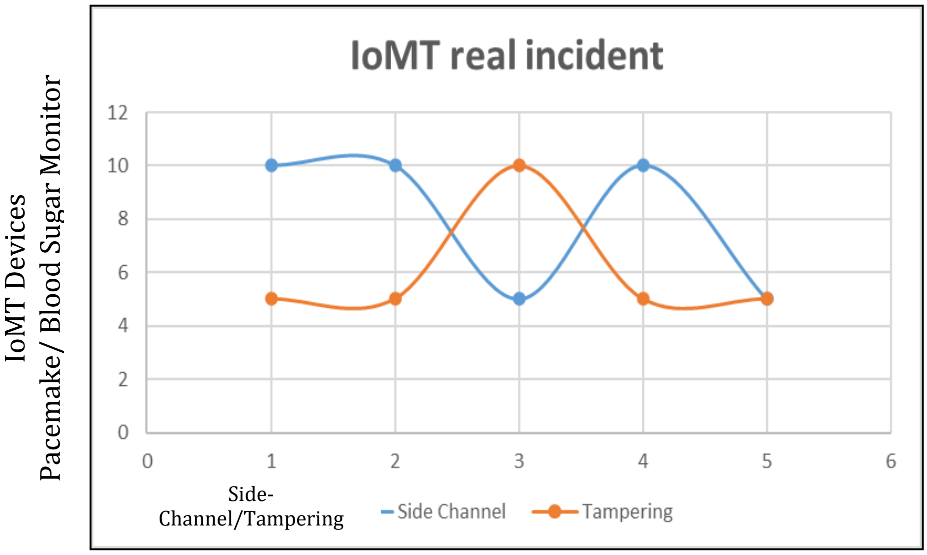
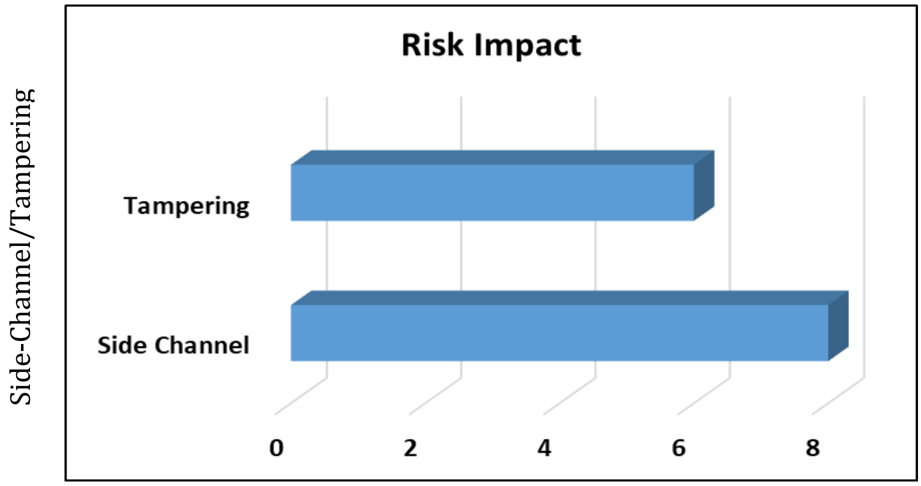


Figure 4. IoMT Real Incident



IoMT Devices

Pacemake/ Blood Sugar Monitor

Figure 5. Risk Impact

Table 3 outlines essential factors concerning device risk, including risk factor, likelihood, score, and overall risk level. These factors are specifically associated with devices like pacemakers and blood sugar monitors. Figure 6 illustrates the computational time for various devices, with devices plotted along the x-axis and computational time on the y-axis. Figures 7 and 8 offer insights into the accuracy and F1-score across different device types. Together, these figures provide a comprehensive evaluation of the key parameters for each device.

Table 3 Risk Classification

IoMT device	Attack	Past attacks	IoT layer	Sector	Device risk factor	Risk likelihood	Risk score	Risk level
Pacemaker	Side-channel	10	10	8	9	9	72	High
Blood sugar monitor	Tampering	5	5	8	6	6	36	Medium

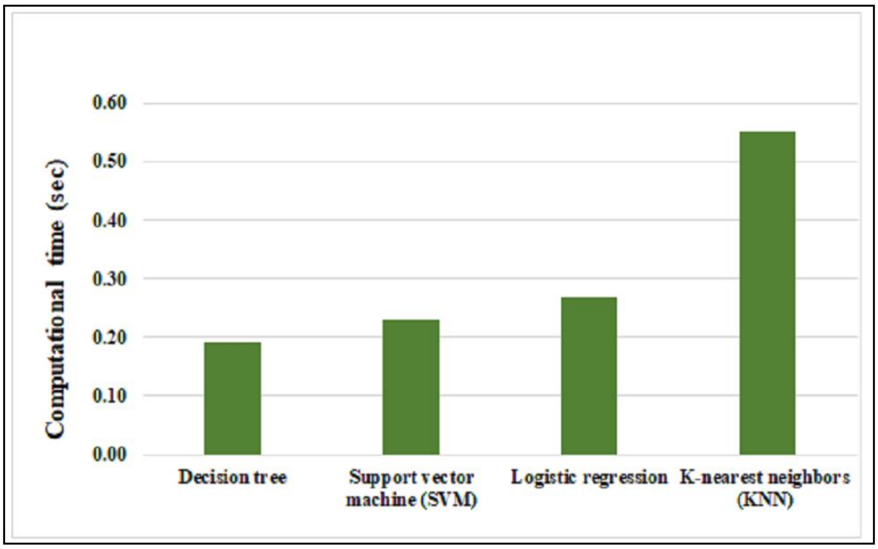


Figure 6. Computation Time

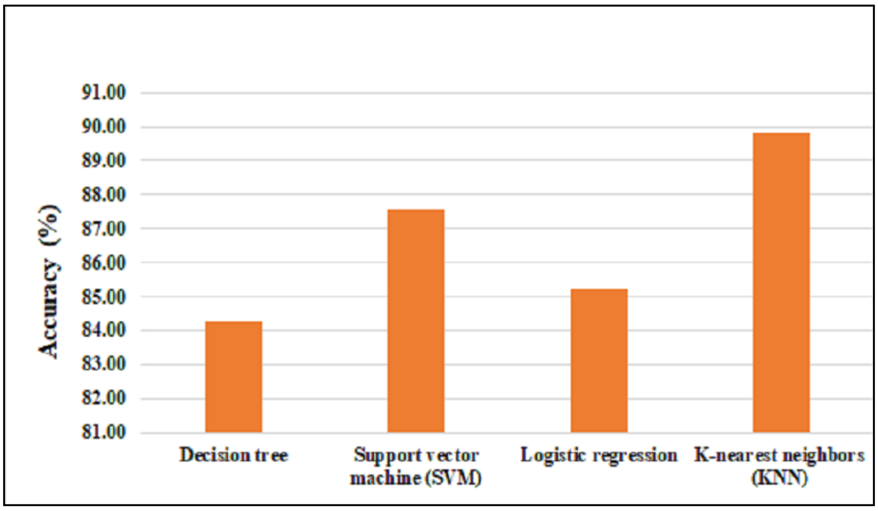


Figure 7. Accuracy

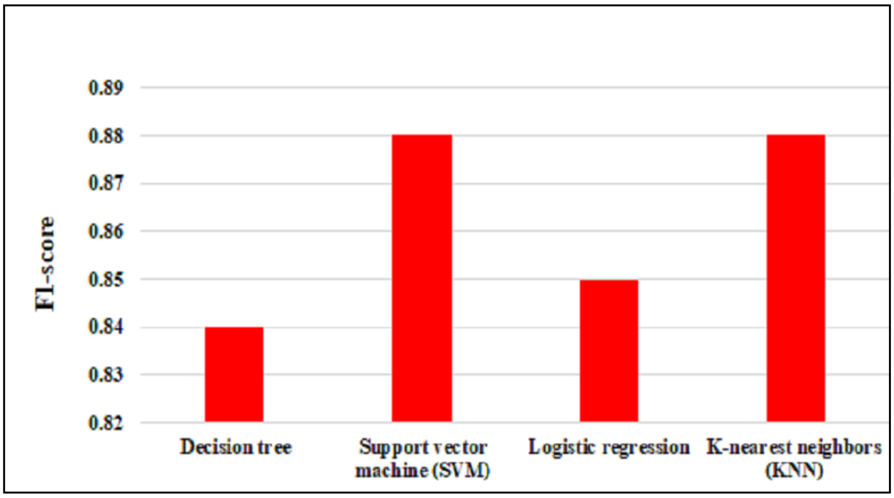


Figure 8. F1-Score

3. CONCLUSION

A critical analysis of the cyber-security risk assessment frameworks suitable for IoT systems is presented. Applications of IoT risk assessment frameworks in finance and healthcare sectors are discussed to demonstrate the maturity of the IoT risk domain. The major part of the benefits of IoT risk assessment framework in finance and healthcare includes proactive threat identification, compliance assurance, Data integrity and privacy protection, operational continuity and improved device management. IoT risk considerations of these frameworks are explained along with their strengths, weakness, and focus areas. A solid treatment of the IoMT risk domain is included with the intention of bringing critical risk issues connected with the IoMT domain to the fore.

REFERENCES

[1] A. Sardi, A. Rizzi, E. Sorano, and A. Guerrieri, “Cyber Risk in Health Facilities: A Systematic Literature Review,” Sustainability, vol. 12, no. 17, p. 7002, Aug. 2020, doi: https://doi.org/10.3390/su12177002.

[2] P. Ambrose and C. Basu, “Interpreting the impact of perceived privacy and security concerns in patients’ use of online health information systems,” Journal of Information Privacy and Security, vol. 8, no. 1, pp. 38–50, Jan. 2012, doi: 10.1080/15536548.2012.11082761.

[3] R. K. Pathinarupothi, ``Clinically aware data summarization at the edge for Internet of Medical Things,'' in Proc. IEEE Int. Conf. Pervasive Comput. Commun.Workshops (PerCom Workshops), Mar. 2019, pp. 437_438, doi: 10.1109/PERCOMW.2019.8730765.

[4] D. Birnbaum, E. Borycki, B. T. Karras, E. Denham, and P. Lacroix, “Addressing Public Health informatics patient privacy concerns,” Clinical Governance an International Journal, vol. 20, no. 2, pp. 91–100, Apr. 2015, doi: 10.1108/cgij-05-2015-0013.

[5] Q. W. Cao, ``Description of SA weak password's harm and solution in the SQL server system,'' J. Xingtai Polytech. College, vol. 29, no. 1, Feb. 2012.

[6] A. S. Salsabila, M. D. Fikri, M. S. Andika, and N. A. Harahap, “Potential and threat analysis towards cybersecurity in South East Asia,” Journal of ASEAN Dynamics and Beyond, vol. 1, no. 1, p. 1, Dec. 2020, doi: 10.20961/aseandynamics.v1i1.46794.

[7] W. Burke, T. Oseni, A. Jolfaei, and I. Gondal, “Cybersecurity indexes for eHealth,” Proceedings of the Australasian Computer Science Week Multiconference, Jan. 2019, doi: 10.1145/3290688.3290721.

[8] A. Raghavan, M. A. Demircioglu, and A. Taeihagh, “Public Health Innovation through Cloud Adoption: A Comparative Analysis of Drivers and Barriers in Japan, South Korea, and Singapore,” International Journal of Environmental Research and Public Health, vol. 18, no. 1, p. 334, Jan. 2021, doi: 10.3390/ijerph18010334.

[9] T. A. Mattei, ``Privacy, con_dentiality, and security of health care information: Lessons from the recent wannacry cyberattack,'' World Neuro-surgery, vol. 104, pp. 972_974, Aug. 2017.

[10] Y. He, A. Aliyu, M. Evans, and C. Luo, ``Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review,'' J. Med. Internet Res., vol. 23, no. 4, Apr. 2021, Art. no. e21747.

[11] Prasad, Ramjee, and Vandana Rohokale. &quot;Cyber Threats and Attack Overview.&quot; In Cyber Security: The Lifeline of Information and Communication Technology, pp. 15-31. Springer, Cham, 2020.

[12] Vyawahare, M., &amp; Chatterjee, M. (2020). Survey on Detection and Prediction Techniques of Drive-by Download Attack in OSN. In Advanced Computing Technologies and Applications (pp. 453-463). Springer, Singapore.

[13] R. Sihwail, K. Omar, and K. A. Z. Ariffin, “A survey on malware analysis techniques: static, dynamic, hybrid and memory analysis,” International Journal on Advanced Science Engineering and Information Technology, vol. 8, no. 4–2, pp. 1662–1671, Sep. 2018, doi: 10.18517/ijaseit.8.4-2.6827.

[14] Tahir, Rabia. &quot;A study on malware and malware detection techniques.&quot; International Journal of Education and Management Engineering 8, no. 2 (2018):20.

[15] C. T. Thanh and I. Zelinka, “A survey on Artificial Intelligence in Malware as Next-Generation Threats,” MENDEL, vol. 25, no. 2, pp. 27–34, Dec. 2019, doi: 10.13164/mendel.2019.2.027.

[16] P. Bory, “Deep new: The shifting narratives of artificial intelligence from Deep Blue to AlphaGo,” Convergence the International Journal of Research Into New Media Technologies, vol. 25, no. 4, pp. 627–642, Feb. 2019, doi: 10.1177/1354856519829679.

[17] Y.-T. Hou, Y. Chang, T. Chen, C.-S. Laih, and C.-M. Chen, “Malicious web content detection by machine learning,” Expert Systems With Applications, vol. 37, no. 1, pp. 55–60, May 2009, doi: 10.1016/j.eswa.2009.05.023.

[18] K. Singh and N. Goyal, &quot;A Comparison of Machine Learning Attributes for Detecting Malicious Websites,&quot; 11th International Conference on Communication Systems &amp; Networks (COMSNETS 2019), Bengaluru, India, 2019, pp. 352-358.

[19] Ma J, Saul L.K., Savage S. and Voelker, 2009, June. Beyond blacklists: learning to detect malicious websites from suspicious URLs. In Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining(pp.1245-1254). ACM.

[20] David, Eli, Nadav Maman, and Guy Caspi. &quot;Methods and systems for detecting malicious webpages.&quot; US Patent Application 15/641,851, filed January 10, 2019.

[21] Al-Yaseen, W., Othman, Z., Ahmad Nazri, M.Z.: Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system. Expert Systems with Applications 67 (01 2017).

[22] Banu, R., M, A., C, A., S, A., Ujwala, H., N, H.: Detecting phishing attacks using natural language processing and machine learning. pp. 1210–1214 (05 2019).

[23] I. Baptista, S. Shiaeles, and N. Kolokotronis, “A novel malware detection system based on machine learning and binary visualization,” 2022 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6, May 2019, doi: 10.1109/iccw.2019.8757060.

[24] Barbara, D., Couto, J., Jajodia, S., Popyack, L., Wu, N.: Adam: Detecting intru-sions by data mining pp. 5–6 (07 2001).

[25] Bose, S., Barao, T., Liu, X.: Explaining ai for malware detection: Analysis of mechanisms of malconv. In: 2020 International Joint Conference on Neural Networks (IJCNN). pp. 1–8 (2020).