Botnets in Healthcare: Threats, Vulnerabilities, and Mitigation Strategies

Michaela Barnett[1], James Womack[1],Christopher E. Brito[1], Khadijah Miller[1], Lucas Potter[2] and Xavier-Lewis Palmer[2]

[1]Blacks In Cybersecurity Headquarters, Inc.,VA,USA

[2]BiosView, Oswego, KS, USA

michaela@bichq.org

Abstract: The increasing digitization of healthcare systems has introduced new opportunities to improve efficiency and accessibility for medical professionals and patients. Examples include the simplified collection, storage, and organization of patient data using electronic health records (EHRs), the use of teleconferencing software like Zoom to allow patients to meet with their care providers remotely, and medical IoT devices like glucose monitors, pacemakers, and other remote patient monitoring devices that leverage software and the internet to provide patients and their healthcare providers with critical information. All of these use cases are examples of how technology can increase the quality of patient care. While the healthcare industry has realized many benefits from its increased investment in new technology, trends have shown that this increased utilization has also opened avenues for malicious cyber actors. One of these threats is botnets. These malicious networks of compromised computers, controlled by cybercriminals, can wreak havoc on all sectors of society, with the healthcare industry proving to be a desirable target. This research is a high-level analysis that investigates the threat botnets pose by employing an exploratory review. We identify the multifaceted nature of botnet threats in healthcare, analyzing their standard forms and the vulnerabilities inherent in healthcare infrastructures, ranging from outdated software to inadequate cybersecurity protocols to poor or total lack of security awareness training for staff. Moreover, the various techniques botnets use to propagate are explored to elucidate the potential points of exploitation and the damage they can cause organizations when proper controls are not implemented. These negative consequences include data breaches, service disruptions, and compromised patient confidentiality, which can endanger medical staff and patients if not addressed. This paper then discusses proven mitigation strategies such as end-user awareness, traffic monitoring, and detection response tools that organizations can employ to reduce the potential and efficacy of such threats. The threat landscape will continue to evolve; however, by staying on top of the latest trends, we can ensure the security of such critical infrastructure and save lives.

Keywords: Healthcare, Botnets, BioCybersecurity, CyberBiosecurity, Medical, IoT

1. Introduction

In an increasingly interconnected digital landscape, the emergence of botnets, malicious networks of compromised computers, have become a formidable challenge for industries across the board (Wazzan et al, 2021; Owen et al, 2022; Booth et al, 2023; Kumar and Sharma, 2023). They are often controlled by malicious actors and can wreak havoc on multiple industries, with the healthcare industry being a desirable target. This paper explores the ways in which botnets have begun to permeate the healthcare sector, posing threats to patient privacy, data security, and the overall integrity of healthcare services. Understanding the dynamics of botnets and their specific implications for healthcare is not just an academic exercise; it is a critical step in fortifying the digital defenses of an industry that plays an indispensable role in safeguarding public health.

The healthcare industry's growing reliance on technology and the internet is evident in its continued adoption of innovative digital solutions for patient care, communication and, integration into medical devices. Electronic Health Records (EHRs) have become a cornerstone of modern healthcare, improving patient record-keeping, accessibility, and data management. Another recent integration would be the standard utilization of Telemedicine, accelerated by the COVID-19 pandemic, which allows patients to access medical care remotely, increasing healthcare accessibility and reducing barriers to seeking treatment (Mueller, 2020; Finch et al, 2023; Affia et al, 2023; Hiller et al, 2024). These advancements enhance patient care as they take an active approach and contribute to the industry's cost-efficiency. The consulting industry has reported that healthcare organizations increasingly invest in digital health, data analytics and artificial intelligence to improve operational efficiency, patient engagement, and clinical outcomes (Arboleda and Shah et al., 2019).

As technology integration continues to expand, so does the overall attack surface (Potter et al, 2021; Affia et al, 2023; Potter and Palmer, 2023). Healthcare providers, while committed to patient care, often grapple with data security and privacy concerns, necessitating a robust infrastructure and security measures to safeguard sensitive medical information and devices in this increasingly digital environment. Botnets present a significant and evolving threat to healthcare systems, with potential consequences that can harm patient care and data

security (Liu et al, 2009; Ali et al, 2020; Wazzan et al, 2021; Owen et al, 2022; Kumar and Sharma, 2023). Botnets can infiltrate healthcare organizations, placing sensitive patient data at risk, disrupting vital medical operations, and potentially endangering lives.

2. Background & Methodology

Information and Data Security in healthcare is paramount due to the sensitive nature of the data involved and the potential consequences of breaches (Alhuwail et al., 2021). The integrity of computer systems is the primary concern, as the effort is concentrated on maintaining the confidentiality and integrity of the data needed to assess, track, and treat patients. Breaches to these portions of our critical infrastructure can result in the unavailability of treating patients, transferring data between facilities, or possibility of malicious threat actors to manipulate or infiltrate a system. One of the most concerning aspects of botnet attacks in healthcare is their potential to disrupt critical medical services (Liu et al, 2009; Ali et al, 2020; Wazzan et al, 2021; Owen et al, 2022; Kumar and Sharma, 2023). For example, a DDoS attack orchestrated by a botnet could overwhelm a hospital's network infrastructure, leading to the unavailability of essential systems such as electronic health records (EHR) or medical imaging systems. Such disruptions can severely affect patient care, potentially delaying treatments or compromising patient safety. In addition to internal hospital infrastructure, security measures and considerations extended to medical devices; with sensors, pumps, and or otherwise, implanted or non, which may find themselves connected to the internet for monitoring and control (Biran Achituv et al, 2016; Mavrogiorgou et al, 2019; Raju and Moh, 2020; Astillo et al, 2022; Farooq et al, 2023). Compromising these devices could have life-threatening consequences for patients, despite growing use or popularity. Implementing robust measures, including regular risk assessments, employee training, data encryption, network segmentation and continuous monitoring for threats, is crucial in mitigating these risks.

To protect patient data, healthcare providers and institutions must adhere to strict regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States (*Summary of the HIPAA security rule,* 2022). HIPAA's primary purpose is to protect individuals' sensitive health information, known as protected health information (PHI). This and the electronic version (e-PHI) includes demographic data, i.e.; physical condition or mental health status, care provided, payment information, name, address, birth date, Social Security Number (SSN), and related sensitive data (Edemekong et al, 2022). HIPAA establishes national standards for the security and privacy of this information.

Botnet attacks pose a significant threat to the healthcare sector (Ali et al, 2020; Kumar and Sharma, 2023) They leverage compromised systems or devices with access to a target network to carry out malicious activities. In recent years, the healthcare industry has increasingly become a target for botnet attacks due to its valuable patient data and critical services (Ali et al, 2020; Wazzan et al, 2021; Owen et al 2022; Kumar and Sharma, 2023). Botnets can launch various mis-actions, including distributed denial-of-service (DDoS) attacks, ransomware campaigns, and data exfiltration.

Preventing and mitigating botnet attacks in the healthcare sector requires a multi-faceted approach. This includes implementing robust cybersecurity measures such as network segmentation, intrusion detection systems, and regular vulnerability assessments to identify and patch potential entry points for malicious actors. Additionally, employee training and awareness programs can help educate healthcare staff about the risks of botnet attacks, how to recognize them and how to respond to suspicious activities.

Collaboration within the healthcare industry and with cybersecurity professionals is crucial for staying ahead of botnets' evolving threats. Sharing threat intelligence and best practices can help healthcare organizations better understand and mitigate the risks associated with these attacks.

Due to the strategies employed in initiating these attacks, certain pertinent research has yet to enter the academic domain. There is a lack of desired publicly accessible reporting in quality and quantity, which has required the authors to widen data sources to ingest additional relevant literature. This discussion will hopefully serve as guidance or reference to either contemporary non-open source analyses, or future academic works. To that end, the authors have utilized and sampled insights among authors at various points in the field.

3. Botnets in Healthcare: Threat Assessment

Common techniques for exploitation or vulnerabilities that may be exploited, that are threatening connected medical devices in the IoMT (Internet of Medical Things) are Spoofing, Tampering, Information Disclosure, Denial of Service, and Escalation/Elevation of privilege. IOMT aims to improve patient care, enhance healthcare

delivery, and enable higher function. Disabling unused, unnecessary, or unsecured network services is a simple and critical part of the device hardening process. Exposing unsecured services to the internet "could impact the confidentiality, integrity, and availability of information and increase exposure to unauthorized remote access" (Malamas et al., 2021). Another area of concern regarding IoMT is the implementation of encryption methods and the limitation of forensics that can be applied due to device constraints (Malamas et al., 2021; Yaacoub et al, 2022). This yields resource constraints that have left the deployment of strong encryption out of some IoMT devices.

Another attack vector to consider would be the many "edge" (Malamas et al., 2021) devices that make up the internet-facing networks and IoMT devices that can be included in this attack surface, such as security cameras, printers, or other monitoring devices (Malamas et al., 2021; Farooq et al, 2023; Hernandez-Jaimes et al, 2023). They often have configurations that must be changed, updated, or disabled. Configurations are often left on default settings and not adjusted, leading to possible attack path entry points if discovered. It has been noted that most administrators will harden essential network devices or appliances, but this may be insufficient in the broader scope of a healthcare network's security when other layers are considered (Filkins, 2014; Malamas et al., 2021; Affia et al, 2023). Further, in evaluating the case of a device that may not be misconfigured, an interface may be left in default configuration and can be accessed by malicious actors. Access can also be gained through plainly available credentials, manuals or configuration instructions (i,e; manufacturer support sites, online tutorials). Actors may also be able to find administration panels or access login portals via particular search engines designed to locate devices connected to the internet, such as Shodan or Censys (Al-Alami et al, 2017; Zhao et al, 2020). The resulting access could be utilized to push further into a network and move laterally through a system. Additionally, it is important to discuss the possibility of attacks that may occur at a private residence, in the absence of on-site professionals who can address specific IT configurations (Travis, 2023; Fisher, 2023). An example of this activity would be the rise in work-from-home environments where equipment is mailed or picked up by an employee and is open to remote maintenance and updates.

A unique way to demonstrate yet another risk to this infrastructure would be to examine the process by which a DDoS attack aims to deplete the battery of a glucose monitor. A DDoS (Distributed Denial of Service) attack floods a target system or network with overwhelming traffic from multiple sources, aiming to disrupt or deny legitimate access to services or resources (Farooq et al, 2023). Devices that run on battery power can be overwhelmed in this fashion and run their battery power down quickly. If attacked in this frequent/constant fashion, this can lead to life-threatening problems, especially in the case of a monitoring device outputting data essential to on-demand care such as vital signs or changes in biologically relevant chemical levels.

Disruptions to sensing capability can also be tampered with resulting in a disrupt or malfunction of hardware or software in a device. In a recent analysis of IoT health devices (IoTHDs) it is noted that certain functions and the transmission of data are intertwined. "The network layer constitutes wired and wireless networks, which connect perception devices, application-layer devices, and other network devices to transmit medical information collected at the perception layer to the application layer" (Affia et al, 2023). Thus, If a glucose monitor is attacked to the point where it is completely depleted of power and fails to function, results could be lethal either independently or combined. In a situation where a device function or sensor is impacted, proper measures, planning, configuration and monitoring can help greatly minimize the chances of success in exploiting vulnerability translating to other portions of interconnected healthcare infrastructure.

4. Mitigation and Prevention Strategies

Many facets must be addressed when discussing mitigation and prevention strategies for botnets. The study Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures acknowledges succinct tasks that IT administrators can implement to protect their systems and networks (Liu et al., 2009). Identifying the affected operating systems and the origin of network traffic can be leveraged to identify incoming attacks. Traffic can be null routed, as malicious traffic can take down critical systems (Puri, 2007). Mitigation would include an attempt to remove any unnecessary DNS hosting services as well, further restricting the resources a potential threat actor could leverage.

Organizations should continuously request and install security updates, fixes, and patches released by their vendors to ensure systems have the latest protections. End users should be regularly trained to avoid downloading software from unscrupulous sites and downloading unnecessary software. A restricted amount of software on a system would make it easier to administor, catalog and maintain, reducing the risk of malicious actors gaining unauthorized access to data or organizational infrastructure.

While it is essential for IT and security staff to be aware of how to defend the organization from cyber threats, it is also essential that the entire staff, regardless of duty or function, receive security awareness training. Healthcare organizations can facilitate this to improve end user recognition and adoption of concepts from relevant training programs (Alhuwail et al, 2021; Polis, 2023). Alhuwail et al (2021) recommends "targeted bottom-up approach via personalized outreach, in-person contacts, and frequent announcements throughout the workflow" (Alhuwail et al., 2021). In conjunction with proper training, devices in the healthcare infrastructure's network should be assessed, updated and/or configured properly prior to being introduced to the overall network, especially over time with regards to software life cycles (Otieno et al, 2023; Phiri, 2023; Harkat et al, 2024; Dadkhah et al, 2024). A core principle highlighting the necessity of this approach lies in the notion that a single vulnerability is sufficient for a malicious actor to access, move laterally or gain privileges in a system and that understanding the risk of each vulnerability allows for holistic comprehension and aids security teams as they work toward building resistance.

5. Regulatory and Compliance Considerations

The policy and compliance of Cybersecurity is to ensure best practices related to mitigating security risks, protecting sensitive data, and maintaining the confidentiality, integrity and availability of information systems and assets. The compliance enforced by policies plays a critical role in promoting trust, resilience, and accountability within organizations. Ensuring these principals play a crucial role in protecting sensitive information assets and mitigating cybersecurity risks in an increasingly complex and interconnected digital environment. In the Healthcare sector, there is a focus on the portion of HIPAA called "The Security Rule" (Craig, 2017). This rule establishes a set of security standards for protecting health information that is stored or transferred in electronic form and applies to "health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates" (*Summary of the HIPAA security rule,* 2022). Covered entities were thus tasked with heightened data management responsibilities and to note, additional importance exists in the locations of e-PHI (*Summary of the HIPAA security rule,* 2022; Fard Bahreini, 2023). This regulation requires covered entities or business associates to maintain reasonable and appropriate administrative, technical, and physical security measures for protecting e-PHI.

The HITECH Act of 2009 (Health Information Technology for Economic and Clinical Health Act) was enacted to strengthen HIPAA and promote the adoption of EHR (Electronic Health Record) systems (Mennemeyer et al, 2016; Burde, 2011; Zahedi et al, 2021). Like HIPAA, HITECH requires covered entities and business associates to implement a risk management and audit program to ensure the protection of e-PHI. In addition, HITECH results in stricter penalties for HIPAA violations and the breach notification rule, which requires covered entities and business associates to notify affected individuals within 60 days.

Healthcare providers are slated to place additional consideration on complexities surrounding choices of payment data security standards, even where not mandated. It is palpable that healthcare systems are often placed concurrently to on-site or online payment technologies, such as Point of Sales systems, ATMs, kiosks, or online processing analogs. The Payment Card Industry Data Security Standard (PCI DSS) is a standard that providers should also reference in their security considerations (Ataya, 2010; Yulianto, 2016). Though it is not mandated by law, credit card payments are ubiquitous in the healthcare industry and cannot be avoided. Coupled with the fact that credit card processors follow PCI DSS and will reduce transactions that can be made or even ban a provider from taking credit card payments, ePHI and credit card information protection needs to be a priority for providers across the healthcare industry. Although beyond the scope of this paper, it is important that healthcare providers be mindful of multisystem considerations that may emerge with enviornmental integration with payment systems (Elmas, 2023; Chitadze, 2023). In general, it is important that attack surfaces within healthcare services are regularly evaluated and examined for areas of reinforcement, ideal configuration or improvement.

6. Future Trends and Challenges

Trends in botnet activity include the sophistication in development and the methods from which the crafted botnet can interact with emerging technologies. Already, healthcare companies and important related infrastructure have been targeted. It is reasonable to expect that attacks will continue to spread and adjust with improving technologies (Baisley and Cherrat, 2023; Kalutharage et al, 2023; Suhag and Daniel, 2023; Rufai

et al, 2023; Pavelea and Negrea, 2024). The evolving threat landscape is projected to include integrations with Artificial Intelligence and corresponding Swarm Intelligence that botnets are capable of (Saini, M., & Budakoti, J., 2013; Owen et al, 2022; Hossain, 2023; Jada and Mayayise, 2023). These abilities would allow the botnet to utilize and share resources between running programs to emulate greater degrees of intelligence. Future botnet development may continue to mature in the ability to conceal actors actions through interacting and utilizing decentralized systems, advanced cryptography, or fileless protocol. The threats to predictive and diagnostic medical systems utilizing Machine Learning are also a factor in emerging threats as these are susceptible to data poisoning, model attacks and concept drift (Javaid et al, 2022; Booth et al, 2023).

Additionally, as we move toward more mobile healthcare infrastructure that may rely heavily on cellular technology in remote or emergency locations it is important to consider the vulnerabilities threat actors may identify and abuse. Specifically within the increased use of wireless broadband communication such as 5G and 6G (Moubayed et al, 2022). An example of the practical implication of these prospective routes can be expected in the development of smart cities. Parallel to the Healthcare industry and its consideration of multiple interconnected systems it is imperative that there is an examination of several additional factors influencing communications & connectivity; current and developing telecommunications technology, consideration of the quality of life (QoL) provided to those that use a system, and the integration with IOT are such areas of reflection. Defense-minded Smart City planners would need to consider systems connected, the management and configuration of each portion and potential attack paths that could be exploited (Wazzan et al, 2021; Haque et al, 2022; Acworth, 2023; Ahmad et al, 2023; de Nobrega, 2023; Kim et al, 2023). In addition, it is important to consider the techno-culture of a group as well as diversity of cybersecurity literacy of the end users who interface with and utilize the systems. A final protective and important defensive measure would be the recruiting of neurodiverse and background diverse perspective holders who can adjust and provide feedback on systems, infrastructure and processes. There must be both innovation and mindfulness in the approaches to defense, so that holistic resilience can be fostered as a mindset and in technical implementation.

7. Conclusion

Healthcare organizations must stay vigilant against the emerging threat of improved and well-integrated botnets engineered to better interface with technical advancements stemming from artificial intelligence, machine learning and further integration with the Internet of Medical Things. As medical devices continue to be designed to connect to the internet and end users are motivated to pursue connecting their devices to the internet, security measures must be well explored at both the user, staff, and technical personnel levels. Ultimately, by proactively addressing security vulnerabilities and enhancing resilience to botnet threats, the healthcare sector can better protect patient data and infrastructure to ensure the continued delivery of critical medical services.

References

Acworth, F. (2023). *National Security Policy Options For Cyber Ecosystem Resilience* Doctoral dissertation. Te Herenga Waka-Victoria University of Wellington. Available at: https://openaccess.wgtn.ac.nz/articles/thesis/National_Security_Policy_Options_For_Cyber_Ecosystem_Resilience/22313419/1/files/39696343.pdf

Affia, A.A.O., Finch, H., Jung, W., Samori, I.A., Potter, L. and Palmer, X.L., (2023). 'IoT health devices: exploring security risks in the connected landscape'. *IoT*, 4(2), pp.150-182 doi: 10.3390/iot4020009

Ahmad, M.O., Tripathi, G., Siddiqui, F., Alam, M.A., Ahad, M.A., Akhtar, M.M. and Casalino, G. (2023). 'BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities'. Sensors, 23(5), p.2757. doi: 10.3390/s23052757

Al-Alami, H., Hadi, A. and Al-Bahadili, H. (2017) "Vulnerability scanning of IoT devices in Jordan using Shodan. In 2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS) (pp. 1-6). *IEEE*. doi: 10.1109/IT-DREPS.2017.8277814

Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & AlDuaij, S. (2021). 'Information security awareness and behaviors of health care professionals at public health care facilities'. *Applied Clinical Informatics*, 12(04), 924-932. doi: 10.1055/s-0041-1735527

Ali, I., Ahmed, A. I. A., Almogren, A., Raza, M. A., Shah, S. A., Khan, A., & Gani, A. (2020). Systematic literature review on IoT-based botnet attack. IEEE access, 8, 212220-212232. doi: 10.1109/ACCESS.2020.3039985

Arboleda, P., Mukherjee, D., Shah, S., & Snyder, G. (2019). *Winning in the future of Medtech*. Deloitte Insights. Available at: https://www2.deloitte.com/content/dam/insights/us/articles/5144_Medtech-company-of-tomorro w/DI_Medtech-of-tomorrow_Report.pdf

Astillo, P.V., Duguma, D.G., Park, H., Kim, J., Kim, B. and You, I., 2022. "Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System". *Future Generation Computer Systems*, 128, pp.395-405. doi: 10.3966/160792642021012201001

Ataya, G., (2010). PCI DSS audit and compliance. Information security technical report, 15(4), pp.138-144. doi: 10.1016/j.istr.2011.02.004

Baisley, T. and Cherrat, Y., (2023). *Cyber Threats and Engagements in 202*2. Available at: https://apps.dtic.mil/sti/citations/trecms/AD1208002

Biran Achituv, D., & Haiman, L. (2016). Physicians' attitudes toward the use of IoT medical devices as part of their practice. Online Journal of Applied Knowledge Management (OJAKM), 4(2), 128-145. doi:10.36965/OJAKM.2016.4(2)128-145

Booth, J., Metz, D. W., Tarkhanyan, D. A., & Cheruvu, S. (2023). Machine Learning Security and Trustworthiness. In *Demystifying Intelligent Multimode Security Systems: An Edge-to-Cloud Cybersecurity Solutions Guide* (pp. 137-222). Berkeley, CA: Apress.

Burde, H., 2011. The HITECH act: an overview. AMA Journal of Ethics, 13(3), pp.172-175. doi: 10.1001/virtualmentor.2011.13.3.hlaw1-1103

Chitadze, N. (2023). *Basic Principles of Information and Cyber Security. In Analyzing New Forms of Social Disorders in Modern Virtual Environments* (pp. 193-223). IGI Global.

Craig, D.J. (2017). 'Ensuring compliance with the HIPAA Security Rule: Think twice when e-mailing protected health information'. *The Nurse Practitioner*, 42(6), pp.12-14. doi: 10.1097/01.NPR.0000515424.38284.e6

de Nobrega, K. (2023). *Cyber defensive capacity and capability: A perspective from the financial sector of a small state.* Masters thesis. Tilburg University. Available at https://pure.uvt.nl/ws/portalfiles/portal/75137858/Thesis.pdf

Dadkhah, S.; Carlos Pinto Neto, E.; Ferreira, R.; Chukwuka Molokwu, R.; Sadeghi, S.; Ghorbani, A. (2024) "CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security." *Preprints* 2024020898. doi: https://doi.org/10.20944/preprints202402.0898.v1

Edemekong, P.F., Annamaraju, P. and Haydel, M.J. (2022). Health Insurance Portability and Accountability Act. In StatPearls [Internet]. StatPearls Publishing.

Elmas, E. (2023). *Dijital Çağda Ödeme Sistemlerinde Siber Güvenlik ve Risk Değerlendirme*. Doctoral dissertation. Marmara Universitesi. Available at: https://www.proquest.com/openview/2b31d7ed3b321e5f277f1746014b4e3a/1

Fard Bahreini, A. (2023). Which information locations in covered entities under HIPAA must be secured first? A multi-criteria decision-making approach. Journal of Healthcare Risk Management, 43(2), pp.27-36. doi: 10.1002/jhrm.21555

Farooq, M.S., Riaz, S., Tehseen, R., Farooq, U. and Saleem, K. (2023). "Role of Internet of things in diabetes healthcare: Network infrastructure, taxonomy, challenges, and security model". *Digital Health*, 9, p.20552076231179056. doi: 10.1177/2055207623117905

Filkins, B. (2014). *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon.* Available at: https://www.redwoodmednet.org/projects/events/20150731/docs/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf

Finch, H., Affia, A.A., Jung, W., Potter, L. and Palmer, X.L.(2023) Commentary on healthcare and disruptive innovation. In International Conference on Cyber Warfare and Security (Vol. 18, No. 1, pp. 77-84).

Fisher, D. (2023). *The Fourth Industrial Revolution: A case study of the impact of the Internet of Things on road travelers in the Western Cape.* Doctoral dissertation. Stellenbosch University. Available at: https://scholar.sun.ac.za/server/api/core/bitstreams/4e058879-c944-4921-bd5d-6baa01f7613c/content

Haque, A.B., Bhushan, B. and Dhiman, G.(2022) "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends". *Expert Systems*, *39*(5), p.e12753. doi: 10.1111/exsy.12753

Harkat, H., Camarinha-Matos, L. M., Goes, J., & Ahmed, H. F. (2024). 'Cyber-Physical Systems Security: A Systematic Review.' *Computers & Industrial Engineering*, 109891. doi: 10.1016/j.cie.2024.109891

Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. Internet of Things, 100887. doi: 10.1016/j.iot.2023.100887

Hiller, J., Kisska-Schulze, K., & Shackelford, S. (2024). Cybersecurity carrots and sticks. American Business Law Journal, 61(1), 5-29. doi: 10.1111/ablj.12238

Hossain, K. A. (2023). 'Analysis Of Present And Future Use Of Artificial Intelligence (Ai) In Line Of Fourth Industrial Revolution (4IR)'. *Scientific Research Journal (SCIRJ)* doi: 10.31364/SCIRJ/v11.i8.2023.P0823954

Jada, I., & Mayayise, T. O. (2023). 'The impact of artificial intelligence on organizational cyber security: An outcome of a systematic literature review'. *Data and Information Management*, 100063. doi:10.1016/j.dim.2023.100063

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Rab, S. (2022, June 5). 'Significance of machine learning in Healthcare: Features, pillars and applications'. *International Journal of Intelligent Networks*. doi:10.1016/j.ijin.2022.05.002

Kalutharage, C.S., Liu, X., Chrysoulas, C., Pitropakis, N. and Papadopoulos, P., 2023. Explainable AI-based DDOS attack identification method for IoT networks. *Computers*, 12(2), p.32. doi:10.3390/computers12020032

Kim, D., Jeon, S., Shin, J. and Seo, J.T., 2023. Design the IoT Botnet Defense Process for Cybersecurity in Smart City. *Intelligent Automation & Soft Computing*, *37*(3). doi: 10.32604/iasc.2023.040019

Kumar, A. and Sharma, I., 2023, May. Augmenting iot healthcare security and reliability with early detection of iot botnet attacks. In *2023 4th International Conference for Emerging Technology (INCET)* (pp. 1-6). IEEE. doi:10.1109/INCET57972.2023.10170738

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., & Zhang, J. (2009) 'Botnet: classification, attacks, detection, tracing, and preventive measures'. *EURASIP journal on wireless communications and networking*, 2009, 1-11. doi:10.1155/2009/692654

Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). 'Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal'. *IEEE Access*, 9, 40049-40075. doi: 10.1109/ACCESS.2021.306468

Mavrogiorgou, A., Kiourtis, A., Perakis, K., Pitsios, S. and Kyriazis, D., 2019. IoT in healthcare: Achieving interoperability of high-quality data acquired by IoT medical devices. Sensors, 19(9), p.1978. doi: 10.3390/s19091978

Mennemeyer, S.T., Menachemi, N., Rahurkar, S. and Ford, E.W., 2016. Impact of the HITECH act on physicians' adoption of electronic health records. *Journal of the American Medical Informatics Association*, *23*(2), pp.375-379. doi: 10.1093/jamia/ocv103

Moubayed, A., Shami, A. and Al-Dulaimi, A., 2022. On end-to-end intelligent automation of 6G networks. Future Internet, 14(6), p.165. doi: 10.3390/fi14060165

Mueller, S., 2021. Facing the 2020 pandemic: What does Cyberbiosecurity want us to know to safeguard the future?. Biosafety and health, 3(01), pp.11-21. doi: 10.1016/j.bsheal.2020.09.007

Otieno, M., Odera, D., & Ounza, J. E. (2023) Theory and practice in secure software development lifecycle: A comprehensive survey. doi:10.30574/wjarr.2023.18.3.0944

Owen, H., Zarrin, J. and Pour, S.M., 2022. A survey on botnets, issues, threats, methods, detection and prevention. Journal of Cybersecurity and Privacy, 2(1), pp.74-88. doi: 10.3390/jcp2010006

Pavelea, A., & Negrea, P. C. (2024) A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications. Masters thesis. Babeș–Bolyai University. doi: 10.13140/RG.2.2.17461.65763

Phiri, L. (2023). *A framework for cyber security risk modeling and mitigation in smart grid communication and control systems.* Doctoral dissertation. The University of Zambia. Available at: https://dspace.unza.zm/items/f775ee4e-140c-4dd9-84be-bab5caa69c32

Polis, G. (2023). *Using the principles of cybersecurity ethics to mitigate cybersecurity risks*. Masters thesis. Banku Augstskola School of Business and Finance. Available at: doi:10.13140/RG.2.2.15285.86245

Potter, L., Ayala, O. and Palmer, X.L. (2021). "Biocybersecurity: a converging threat as an auxiliary to war". In *ICCWS 2021 16th international conference on cyber warfare and security* (p. 291).

Potter, L. and Palmer, X.L. (2023). Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination. In Cyberbiosecurity: A new field to deal with emerging threats (pp. 37-69). Cham: Springer International Publishing.

Puri, V. (2007). *Automated alerting for black hole routing*. Doctoral dissertation. Naval Postgraduate School. Available at: https://apps.dtic.mil/sti/citations/tr/ADA474419

Raju, R. and Moh, M. (2020) Cyber-physical systems in healthcare: Review of architecture, security issues, intrusion detection, and defenses. *Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS)*, pp.23-62.

Rufai, A.U., Fasina, E.P., Uwadia, C.O., Rufai, A.T. and Imoize, A.L.(2023) "Cyberattacks against Artificial Intelligence-Enabled Internet of Medical Things". *Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things* (pp. 191-216). CRC Press.

Saini, M., & Budakoti, J. (2013). 'Impact of social media marketing on consumer behavior.' *Procedia Economics and Finance*, 11, 677-689. https://doi.org/10.1016/S2212-5671(13)00116-1

Suhag, A. and Daniel, A., 2023. Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDOS) assault and defense. *Journal of Cyber Security Technology*, 7(1), pp.21-51. doi: 10.1080/23742917.2022.2135856

Summary of the HIPAA security rule (2022) *HHS.gov*. Available at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Travis, F. J. M. (2023). *Secure Interface Improvements Internet of Things (IoT) Vendors Need to Protect Smart Home IoT Devices from Cyber Attacks.* Doctoral dissertation. University of the Cumberlands. Available at: https://www.proquest.com/openview/52c715f15eeb29df9405a49dbf48ea17

Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). 'Internet of Things botnet detection approaches: Analysis and recommendations for future research'. *Applied Sciences*, 11(12), 5713. doi: 10.3390/app11125713

Yaacoub JP, Noura HN, Salman O, Chehab A. (2022) 'Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations.' *Internet of Things*.;19:100544. doi:10.1016/j.iot.2022.100544

Yulianto, S., Lim, C. and Soewito, B., (2016) "Information security maturity model: A best practice driven approach to PCI DSS compliance". *2016 IEEE Region 10 Symposium* (TENSYMP) (pp. 65-70). IEEE. doi: 10.1109/TENCONSpring.2016.7519379

Zahedi, Z., Mahmud, F., & Pinto, C. (2020). Systemic risk management plan for electronic medical records (EMR): Why and how? In *HTI Open Access Collection 2020* (19 pp.). IOS Press https://doi.org/10.3233/SHTI200016

Zhao, B., Ji, S., Lee, W.H., Lin, C., Weng, H., Wu, J., Zhou, P., Fang, L. and Beyah, R., 2020. "A large-scale empirical study on the vulnerability of deployed iot devices". *IEEE Transactions on Dependable and Secure Computing*, 19(3), pp.1826-1840. doi: 10.1109/TDSC.2020.3037908