Computing and Artificial Intelligence 2025, 3(2), 2220.
https://doi.org/10.59400/cai2220

Article

Offensive and defensive cybersecurity solutions in healthcare

Cheryl Ann Alexander[1,*], Lidong Wang[2]

[1] Institute for IT Innovation and Smart Health, Vicksburg, MS 39180, USA
[2] Institute for Systems Engineering Research, Mississippi State University, Vicksburg, MS 39180, US
*** Corresponding author:** Cheryl Ann Alexander, cannalexander68@gmail.com

CITATION

Alexander CA, Wang L. Offensive and defensive cybersecurity solutions in healthcare. Computing and Artificial Intelligence. 2025; 3(2): 2220.
https://doi.org/10.59400/cai2220

ARTICLE INFO

Received: 5 December 2024
Accepted: 28 February 2025
Available online: 9 April 2025

COPYRIGHT

Copyright © 2025 by author(s). *Computing and Artificial Intelligence* is published by Academic Publishing Pte. Ltd. This work is licensed under the Creative Commons Attribution (CC BY) license.
https://creativecommons.org/licenses/by/4.0/

Abstract: Healthcare services usually implement defensive data strategies; however, offensive data strategies offer new opportunities because they focus on improving profitability or revenues. Offensive data also helps develop new medicine, diagnosis, and treatment due to the ease of data-sharing rather than data control or other restrictions. Balancing defensive data and offensive data is balancing data control and flexibility. It is a challenge to keep a balance between the two. Sometimes, it is necessary to favor one over the other, depending on the situation. A robust cybersecurity program is contingent on the availability of resources in healthcare organizations and the cybersecurity management staff. In this paper, a cybersecurity system with the functions of both defensive cybersecurity and offensive cybersecurity in a medical center is proposed based on big data, artificial intelligence (AI)/machine learning (ML)/deep learning (DL).

Keywords: cybersecurity; defensive cybersecurity; offensive cybersecurity; artificial intelligence (AI); machine learning (ML); deep learning (DL); healthcare

1. Introduction

Cyberspace is an operational domain with confrontation, along with land, air, and sea. It is defined as being the "interdependent network of information technology infrastructures that includes the Internet, telecommunication networks, computerized systems, devices connected to the Internet, as well as processors and controllers integrated into them. It can also refer to a world, to a virtual domain or an abstract concept" (The British Security Strategy). Integrating, coordinating, and synchronizing cyberspace operations is a challenge [1]. **Table 1** [1] shows cyberspace operations, including various missions, activities, and effects in cyberspace.

Table 1. The spectrum of cyberspace operations.

Categories	Sub-categories
Missions in cyberspace	• Systems and network operations • Defensive cyberspace operations • Intelligence, surveillance, and reconnaissance in cyberspace • Offensive cyberspace operations

Table 1. (*Continued*).

Categories	Sub-categories

Activities and effects in cyberspace	• Cybersecurity
	  • Cyber hygiene
	  • Control
	  • Protection
	• Cyber defense
	  • Monitoring
	  • Detection
	  • Block
	  • Resilience
	  • Recovery
	• Cyberspace exploitation
	  • Observing
	  • Infiltration
	  • Localization
	  • Capturing
	• Cyberspace attacks
	  • Neutralize
	  • Degrade
	  • Deny
	  • Block
	  • Destroy

There are the following popular cybersecurity strategies [2]: 1) Protect and recover strategy; 2) endpoint protection strategy; 3) physical control and security clearances as a security strategy; 4) compliance as a security strategy; 5) application-centric strategy; 6) identity-centric strategy; 7) data-centric strategy; and 8) attack-centric strategy. **Figure 1** [3] shows approaches to cybersecurity.

Figure 1. Approaches to cybersecurity.

Advanced methods such as AI/ML help cybersecurity automation [4]. Automation can mitigate 1) security misconfiguration; 2) unpatched vulnerabilities; 3) insider threats and social engineering; and 4) weak, stolen, or leaked passwords [2]. With the increased utilization of AI/ML and the availability of quantum computing (QC) to boost system capabilities to new limits, there are new opportunities due to the unrealized potential. Vital areas of cybersecurity-related ML should be explored at a deeper level, including defense, offense, adversarial learning, etc. [3].

A method to build an intelligent web crawler was presented. Webpages (WPs) were categorized into two types: Irrelevant URLs (uniform resource locators) and relevant URLs by utilizing the k-nearest neighbors (KNN) (one of the ML methods).

KNN executes considerably faster than other classifiers if features are fewer. The web crawler could be improvised by making it search for hidden URLs: Dark-Web and Deep-Web [5].

DL (one of the ML methods) and extreme value theory have been applied in modeling and predicting multivariate cyber risks [6]. Automatic diagnosis of COVID-19-associated pneumonia was studied based on chest X-ray (CXR) and computed tomography (CT) scan images. An accuracy of greater than 95% was obtained by using DL. Specifically, the convolutional neural network (CNN) (one of the DL methods) was employed, and eight CNN-based DL models were used in the research [7].

Most cybersecurity research has focused on defensive approaches. Proactive approaches are also needed due to old, emerging, and unknown cyberattacks; thus, offensive security practices such as penetration testing and adversary simulation have been performed [8]. Data defense focuses on data quality, integrity, privacy, security, regulatory compliance, and governance, while data offense centers on competitive profitability and customer satisfaction [9].

Charleston Regional Medical Center in Mississippi, USA, practices cybersecurity for employees and patients. Phishing, malware, ransomware, information system disruption due to attacks, supply chain vulnerabilities, etc., are possible problems in cybersecurity at the medical center. The medical center mainly practices defensive cybersecurity, but it has started offensive cybersecurity since the beginning of the COVID-19 pandemic. The research department and areas related to biotech and new drug development and deployment are key areas and departments at the medical center now practicing more offensive cybersecurity. Other critical areas that employ an offensive cybersecurity strategy include diagnostics, mobile devices used by staff and providers, and telemedicine units.

This paper proposes a cybersecurity system with the functions of both defensive and offensive cybersecurity based on big data, AI/ML/DL. Multi-layered and multi-point defensive cybersecurity enhances protection and fosters resilience in the medical center policies and strategies. Incorporating defensive AI strategies, including multiple elements such as firewalls, advanced threat detection, intrusion detection systems, etc., is a critical part of defensive strategies. AI-based offensive cybersecurity has the potential to enhance protection and foster resilience. Offensive events typically occur more often in real-time than defensive events. The offensive cybersecurity strategy helps the cybersecurity system adjust to attacks in real time.

2. Value assessment and key improvements for systems

Research on cybersecurity-focused deepfake (DF) detection systems utilizing big data was conducted. Cybersecurity theories or principles and big data were employed to strengthen the detection system. The convolutional neural network (CNN) was employed at the frame level for feature extraction. Data collection was performed by the big data collection technique, and data analysis was conducted by big data analytics. The recurrent neural network (RNN) was trained to discriminate the temporal inconsistency resulting from the DF creation tool. The huge data sets of big data have the great potential to detect deepfake irregularity. ML-based cybersecurity practices are powerful for handling DF risks (e.g., misinformation and identity

impersonation). The integration of cybersecurity and big data helps enhance the accuracy of DF detection and guarantees the integrity and security of the processed data. Furthermore, the detection system must keep adaptability to new DF by the use of advanced technologies that are used to update the system [10]. SecureVision is a DF detection system with the innovation of using multi-modal analysis. A method of integrating DL and big data analytics was developed to detect altered information in visual and audio fields. This research is helpful for the protection of digital integrity and the defense against DF [11].

System cyber resilience is the ability to absorb, recover from, and adapt to cyberattacks. It can be more complicated due to more autonomous agents (i.e., software and hardware). Autonomous agents are elements of performing functions without human intervention and include self-activating, self-sufficient, and persistent computation. Systems enabled with autonomous agents (e.g., with the reinforcement of AI) have the potential to respond to cyberattacks with an enhanced scale or speed, but they can also introduce vulnerabilities. There are some approaches to assessing or measuring the cyber-resilience of a system with autonomous agents that can also be used in evaluating the cybersecurity system in the medical center, including the qualitative assessment, probabilistic estimates by experts (quantitative), and resource-intensive methods (e.g., modeling and simulation, wargaming, and red teaming and penetration testing) [12]. Whether or not the cost-benefit ratio of resource-intensive techniques outweighs their ability to increase cyber resilience depends on specific situations. It is suggested that these resource-intensive techniques only be used if necessary. Sometimes, it is difficult to perform a quantitative assessment for assessing cyber resilience in dynamic healthcare settings, which can be complicated. In these situations, using a qualitative method for assessing cyber resilience is often easy or convenient. The specific descriptions of the approaches are as follows [12]:

- The qualitative assessment: Evaluates cyber-resilience based on qualitative evaluations of system features, for example, a cyber-resilience matrix with four resilience abilities (plan/prepare, absorb, recover, and adapt).
- Probabilistic estimates by experts: Use probabilistic assessments from subject matter experts.
- Modeling and simulation: 1) Create a representation or "digital twin" of the business or mission processes, functions of cyberinfrastructure and systems, etc.; 2) simulate known attacks and their impacts using the created model.
- Wargaming: Fits the behaviors of autonomous cyber-attackers and defenders, with cyber-attackers being expected to maximize damage or disruption while cyber-defenders are expected to increase absorption or recovery.
- Red teaming and penetration testing: Red teaming means cyberattacks and defenses in live or test environments while penetration testing concentrates on a specific system and broadly explores many vulnerabilities.

3. A proposed cybersecurity system in the medical center

Figure 2 is the block diagram for the proposed system and **Table 1** lists the key requirements and expected benefits or their roles in the system. The specific cybersecurity data, tools and technologies, algorithms, models, and deployment

process steps in the plan specifically as to how each contributes to enhancing protection and fostering resilience for the medical center are included in **Figure 2** and **Table 2**.

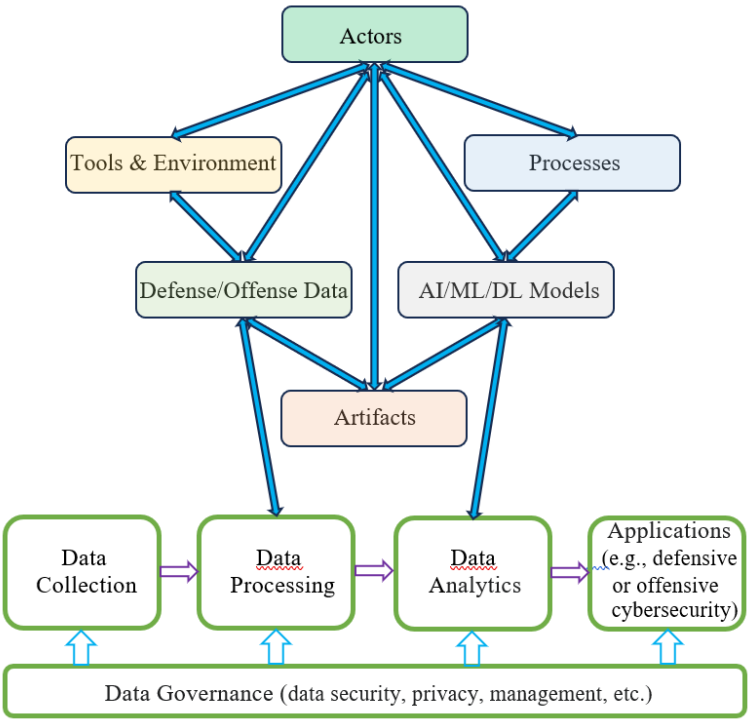

Figure 2. The block diagram for the proposed system in the medical center.

Table 2. Key requirements and expected benefits or their roles.

Key requirements	Expected benefits or their roles
Actors (physicians, nurses, researchers, third parties, etc.)	Be involved in operating, deploying, or benefiting from the system.
Defense data and offense data	Used for defensive or offensive cybersecurity, respectively.
Tools and environment	Used for creating AI/ML/DL models and data analytics.
AI/ML/DL models	Used for data analytics and predictions.
Data analytics	Supporting decision-making and defensive or offensive cybersecurity.
Applications (e.g., defensive or offensive cybersecurity)	Services and enhancing the cybersecurity of various services.

There are several types of actors, including healthcare providers (such as physicians, nurses, and managers), researchers in the medical center, third-party entities, etc. As for processes in the processed system, algorithms and data are used (following various processes). A huge amount of data is collected and applied to mathematical models and algorithms to make predictions and identify patterns/trends. Tools and environment include IDE (Integrated Development Environment) tools for AI/ML/DL, such as Visual Studio Code and PyCharm, AI/ML/DL tools, or computer language packages such as TensorFlow and R language/R packages, etc. All digital products used in an AI/ML/DL tool are described as artifacts. They can include input, output, or intermediate results processed by tools. The most common ML artifacts are

features, interference data, models, and training data. In a healthcare cybersecurity system, how might AI/ML/DL models strike a balance between real-time flexibility and prediction accuracy? It depends on specific situations and specific sectors. In most cases, prediction accuracy should be the priority. For some special situations with emergencies (e.g., medical cases during the COVID-19 pandemic), real-time flexibility is more important. There are IT/cybersecurity departments or teams in hospitals, medical centers, or healthcare agencies. Generally, outside parties are not involved in implementing and running cybersecurity systems. Even if it is necessary to ask outside parties for help, strict access (physical access and data access) control policies are implemented on a case-by-case or task-by-task basis.

4. New offensive tactics from threat actors and their impacts on the proposed system

Threat actors frequently change and improve their attack strategies and tactics using advanced technologies such as AI/ML/DL. It is necessary to pay attention to new offensive tactics from threat actors because threat actors might limit the value of the proposed system in any part/element and any step of processes. As threats evolve and new offensive tactics occur, defenders should improve their understanding of threats and develop strategies and actionable plans to handle the offensive tactics. Creating adaptive and AI-based defense mechanisms and making collaborative, interdisciplinary efforts to address cybersecurity challenges is necessary.

There are two kinds of AI: Narrow AI and general AI. General AI can achieve several tasks while narrow AI can only execute a single task. AI models are prone to three kinds of attacks: 1) Stealing; 2) evasion; and 3) poisoning (altering training data and destroying the AI's performance). Weaponized AI is defined as malicious AI algorithms that can disrupt normal functions and degrade the performance of benign AI algorithms. AI weaponization in cyberspace is dangerous [13]. Weaponized AI generally poses a bigger risk to cybersecurity compared with conventional attacks due to its speed and agility, ethical problems, etc. Classical vs. AI-powered cyberattacks are shown in **Table 3** [13]. **Table 4** [13] lists AI-powered tools for offensive cybersecurity operations. The utilization of AI in cyber defense lies in anti-phishing, cyberattack visualization, and resisting and countering possible cyberattacks using AI along the cyber kill chain.

Table 3. Classical vs. AI-powered cyberattacks.

Attack paradigm	Attack types	Attack impacts
Classical	Information disclosure	Confidentiality
	Elevation of privilege	Authorization
	Denial of service (DoS)	Availability
	Tampering	Integrity
	Spoofing	Authentication
	Repudiation	Non-repudiation

Table 3. (*Continued*).

Attack paradigm	Attack types	Attack impacts
AI-powered	Data misclassification	False positive results due to AI algorithms
	Synthetic data generation	False information for user manipulation
	Data Analytics	AI-assisted classical attack generation

Table 4. AI-powered tools that utilize data analytics for offensive cyber operations.

Names	Uses
Deep Exploit	Automates Metasploit for information scanning, gathering, exploitation, and post-exploitation
DeepGenerator	Generate the patterns of injection attacks for web applications
DeepHack	Generate the patterns of injection attacks for database applications
DeepLocker	Emulates an advanced persistent threat (APT) for initiating complicated cyberattacks
EagleEye	For social media information reconnaissance using the algorithms of facial recognition
GyoiThon	For information gathering and automated exploitation
Malware-GAN	Utilized for generating malware that can bypass security detection
uriDeep	Generating fake domains for use in various attack scenarios

Table 5 [14] shows the cases (regarding a fraud-detection system as an example) of offensive and defensive AI by attackers and defenders. Both attackers and defenders use offensive and defensive AI. For non-AI-based defenses and offenses, defenders need a defense against many possible attacks, while attackers (fraudsters) only need to find a single exploitable human or technical vulnerability. **Table 6** [15] shows major differences between adversarial, offensive, and defensive AI. **Figure 3** [16] shows attacks (data poisoning, evasion attacks, and exploratory attacks) in adversarial ML. Strict data access control, standards, policies, and regulations in healthcare, such as HIPAA, help protect the healthcare system from hostile AI-based strategies like model evasion and data poisoning.

Table 5. Cases for using offensive and defensive AI.

AI types	Offensive AI	Defensive AI
Attackers	Use AI to learn about vulnerabilities, then exploit them in a fraud-detection system	Use AI to protect attack tools and infrastructure and stop unmasking
Defenders	Use AI to hack back	Use AI to detect and learn the patterns of fraud, then act to prevent additional efforts to commit fraud

Table 6. Major differences between adversarial, offensive, and defensive AI.

Types of AI in cybersecurity	Goals	Examples
Adversarial AI	Exploits or attacks an AI system and the data of the system	Manipulates the input data and poisons the training data
Offensive AI	Uses AI methods to attack a computer system or network	Automated exploitation of vulnerabilities launches new cyberattacks
Defensive AI	Uses AI methods to protect a computer system and network from attacks	Intrusion detection systems, anti-malware

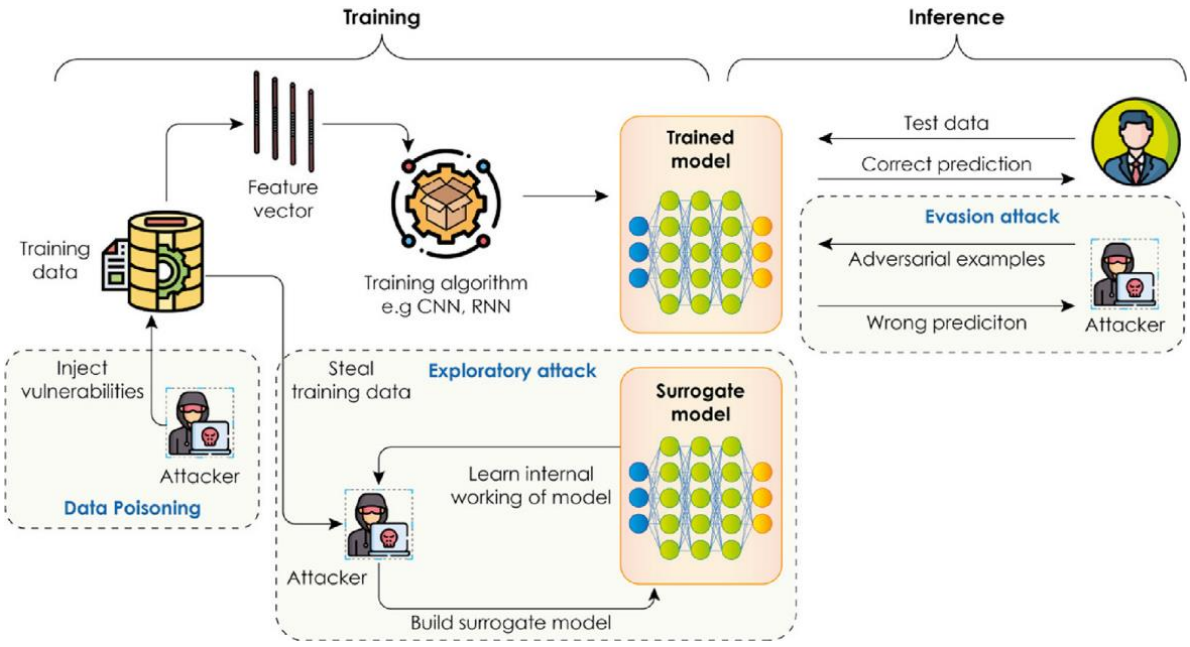

Figure 3. Attacks in adversarial ML.

5. Cybersecurity solutions in the future

Cybersecurity solutions in the future will need to adapt to new ways of operationalizing offensive and defensive tactics for the medical center. Entities must explore and evolve more robust tactics to prepare for future cybersecurity. To meet standards and HIPAA compliance, the medical center must prepare for vigorous patient data security measures, stronger encryption methods, and tougher data governance policies in AI documentation solutions. Encryption, secure transmission of patient data, and a tough authentication/access control process are necessary for strengthening cybersecurity programs. Monitoring and updating the system with regularly scheduled system audits and vulnerability assessments is also required.

Defensive and offensive strategies should be implemented appropriately in cybersecurity solutions to counter changing threats without sacrificing legal compliance. Specifically, the defensive strategy should follow standards and regulations in data privacy and data security. The offensive strategy should be fulfilled ethically and within the legal boundary. Defensive cybersecurity involves both proactively attempting to prevent cyber threats from occurring and reactively endeavoring to identify, block, and mitigate current attacks. Enacting security policies, utilizing security solutions, training employees to detect phishing, etc., fall under the defensive umbrella. Offensive cybersecurity permits entities to assess their defenses and detect security holes that should be addressed. Real-world threat simulations and offensive cybersecurity testing convey whatever vulnerabilities pose the greatest danger to an entity. Two examples of offensive cybersecurity services are described as follows:

- Penetration testing—a form of offensive security testing designed to recognize numerous vulnerabilities in an entity's defenses.
- Vulnerability scanning—an automatic process utilized to detect vulnerabilities in an entity. It can detect potentially usable weaknesses in preparation for a

cyberattack and is frequently used by malicious actors. An entity can discover and close these vulnerabilities by performing regular vulnerability scans before the vulnerabilities become exploited by malicious threat actors.

6. Discussion on offensive and defensive cybersecurity solution deployment in healthcare and the medical center

Healthcare entities with robust security programs use proactive measures to identify and address probable vulnerabilities. However, malware can not only manipulate AI's training data but can also allow the exposure of patient data on the dark web. If cyberattacks occur, these entities must proactively ensure the security of their assets, networks, and data. Therefore, the healthcare entity must implement an offensive cybersecurity strategy. An offensive cybersecurity strategy designs ideas for attacks likely to occur by modeling the attack of malicious actors. A mature cybersecurity program must incorporate both defensive and offensive cybersecurity activities. The lack of integration of defensive and offensive cybersecurity strategies makes the overall resilience of healthcare systems very weak, even destroying their resilience. This has been demonstrated by the functions and performances of the healthcare systems of all the countries in the world during the COVID-19 pandemic. In the healthcare arena, the defensive strategy was dominant in most sectors and almost all countries during the pandemic due to data privacy and security as well as policies and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the USA. There was a lack of integration or a weak integration between the defensive strategy and the offensive cybersecurity strategy, and the collaboration among various countries was very weak due to complicated factors (e.g., political and economic reasons), which resulted in many problems such as the shortage of medical supplies, the slow development of vaccines and new medicines, the death of a huge number of people, etc. As the medical center continues to establish vigorous cybersecurity programs, IT security teams must remember that generative AI also carries the following risks:

- Model manipulation—Malicious actors can affect training data or the AI model itself, resulting in biased research results, false clinical notes, or the creation of destructive content.
- Third-party risk—Some healthcare providers utilize cloud-based generative AI tools, allowing a dependence on third-party security procedures, so vulnerabilities in these vendors develop into risk points.
- Data sensitivity—Generative AI models are frequently trained on huge amounts of private patient data, encouraging most vulnerabilities in AI systems to bear this data in breaches.
- Integration vulnerabilities—Integrating generative AI tools into current healthcare systems creates further points of entry for cyberattacks; securing these points of entry is essential since the risk of patient data exposure is high.

Cyberattacks disturb patient care and associated services and lead to data leak breaches, causing healthcare entities to minimize exposure to cyber risks and

maximize data protection and integrity. The following cyber defense strategies are key to boosting security for all types of healthcare practices:

- Staff training—This should include hyperlink and redirection attacks, email attacks, online hygiene, threat and mitigation communications, authentication protections (e.g., multi-factor authentication), HIPAA digital education, etc.
- Policies—It is necessary for an annual review or when any network or organization changes occur to keep up to date including data, system, and network protections; passwords and authentication for users; privacy; technology and device use; internet use, access, and data recovery and business continuity plans.
- Communication—Among staff, leadership, and stakeholders regarding emerging threats; live channels of communication for concerns and cyber-related questions; round-table discussions; etc.
- Restoration resiliency—Healthcare entities should introduce policies that include business continuity, data backup, and disaster recovery plans.
- Redundancy—Minimizes or blocks a single point of failure, including backup (typically implemented with cloud replication and a network appliance), plus access to the Internet servers (Intranet and applications), etc.
- Security risk assessment—This should take an unbiased and analytical look into the existing network posture, which allows the IT cybersecurity team to determine resource priorities to mitigate any vulnerabilities detected.
- Hyperlink hygiene—Blocking phishing emails and other suspicious emails is necessary to protect the healthcare system from malware. Healthcare entities need a robust email filtration system to block suspicious emails. IT security teams should also develop vigorous web browser controls that block and restrict suspicious or malicious sites.
- Defense in depth—Necessary to place behind various protection mechanisms. The IT department is alerted by a monitoring system when an incident or event occurs. Monitoring servers, network devices, antivirus agents, email filtering systems, etc., should be performed.

There are indeed moral issues and ethical problems, like data abuse and privacy, when AI/ML tools and relevant data are used. Strict data access control, standards, policies, and regulations in healthcare, such as HIPAA, help address these problems. It is necessary to protect the privacy and security of patient data in a distributed health system where big data is generated from the Internet of Things (IoT), medical devices, etc. [17]. **Figure 4** [18] shows the attack surface of IoT devices. **Figure 5** [19,20] shows the security and privacy taxonomy of the Internet of Medical Things (IoMT). CIA refers to confidentiality, integrity, and availability in the figure. Healthcare providers are recommended to protect themselves as follows:

- Foresee generative AI threats.
- Run frequent security audits on AI systems with current healthcare IT infrastructure.
- Utilize a collaborative/multidisciplinary approach to improving security by having a single team to model cyberattacks and defenses.

- Provider and staff training on cybersecurity threats linked with generative AI and methods to recognize potential threats.
- Adopt data loss prevention to prevent unauthorized utilization or access to sensitive data.
- Employ a zero-trust architecture; hence, accessing sensitive data is limited to a restricted basis and is continually verified.

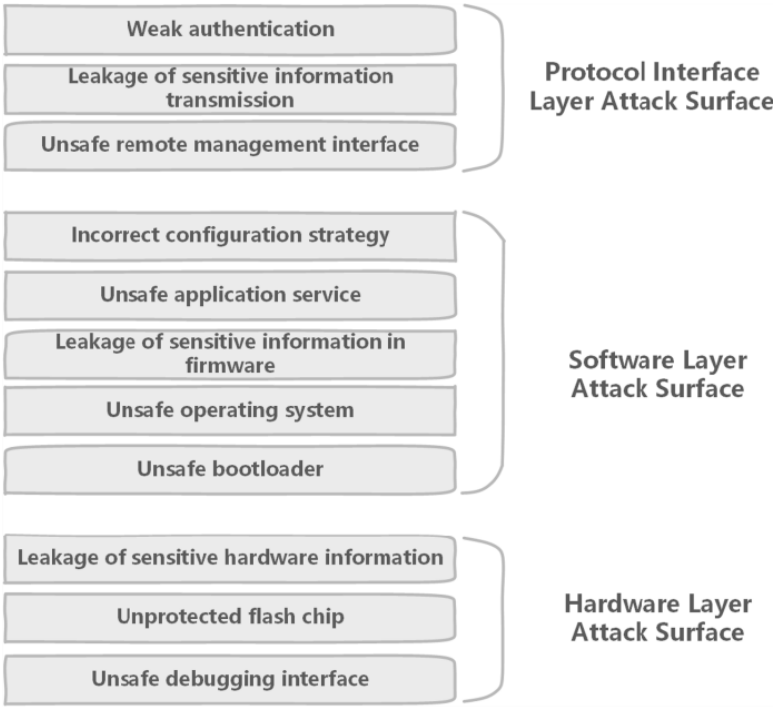

Figure 4. The attack surface of IoT devices.

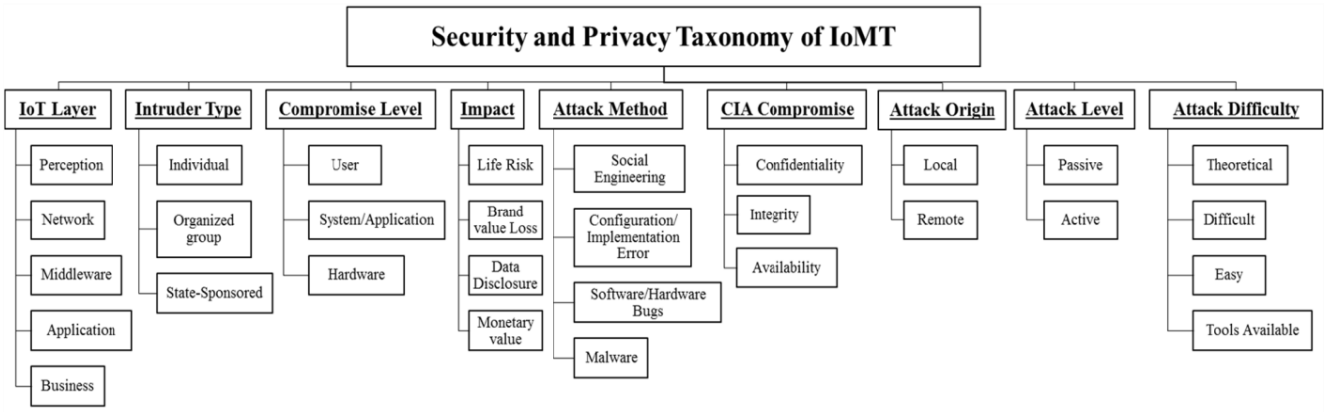

Figure 5. The security and privacy taxonomy of IoMT.

7. Conclusion and future research

Generative AI carries risks. Both attackers and defenders use offensive and defensive AI. Cyberattacks disrupt patient care and associated medical center services. A brisk cybersecurity plan includes both defensive and offensive security tasks. The defense data strategy in healthcare lies in protecting patient data, maintaining privacy, and following federal standards such as HIPAA, national laws, etc., while the offense

data strategy focuses on making hospitals more competitive and maintaining patient satisfaction. The medical center mainly practices defensive cybersecurity, but there will be more offensive cybersecurity operations, deployment, and practices at the organization with the increase of new cyberattacks and tactics from threat actors, the availability of more resources for healthcare cybersecurity, and the improved management skills at the administrative level for medical center cybersecurity. Because there is a lack of enough experimental devices and data, experiments and simulations/predictions based on AI/ML/DL have not been completed. The capabilities of AI/ML, especially DL, have not been demonstrated adequately in this paper. These are the limitations of the paper, and they have been our future research topics. Simulations or experiments have been ongoing. We plan to write a separate paper to report on this work and its progress soon.

Author contributions: Conceptualization, CAA; methodology, CAA; formal analysis, CAA and LW; resources, CAA and LW; writing—original draft preparation, CAA; writing—review and editing, LW; visualization, CAA and LW; project administration, CAA. All authors have read and agreed to the published version of the manuscript.

Institutional review board statement: Not applicable.

Informed consent statement: Not applicable.

Conflict of interest: The authors declare no conflict of interest.

References

1. Dumitrescu B. Operationalising Cyberspace–From Cyber Security to Operational Success. Romanian Military Thinking. 2019; (1): 50–73.
2. Rains T. Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks. Packt Publishing Ltd; 2020.
3. Buchanan B. A national security research agenda for cybersecurity and artificial intelligence. Center for Security and Emerging Technology. 2020. doi: 10.51593/2020ca001
4. Sarker IH. Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. Security and Privacy. 2023; 6(5). doi: 10.1002/spy2.295
5. Kumar N, Aggarwal D. LEARNING-based Focused WEB Crawler. IETE Journal of Research. 2023; 69(4): 2037–2045. doi: 10.1080/03772063.2021.1885312
6. Zhang Wu M, Luo J, Fang X, et al. Modeling multivariate cyber risks: Deep learning dating extreme value theory. Journal of Applied Statistics. 2021; 50(3): 610–630. doi: 10.1080/02664763.2021.1936468
7. Kumar N, Hashmi A, Gupta M, et al. Automatic diagnosis of Covid-19 related pneumonia from CXR and CT-Scan images. Engineering, Technology & Applied Science Research. 2022; 12(1): 7993–7997. doi: 10.48084/etasr.4613
8. Ajmal AB, Shah MA, Maple C, et al. Offensive security: Towards proactive threat hunting via adversary emulation. IEEE Access. 2021; 9: 126023–126033. doi: 10.1109/access.2021.3104260
9. DalleMule L, Davenport TH. What's your data strategy. Harvard Business Review. 2017; 95(3): 112–121.
10. Kumar N, Kundu A. Cyber security focused deepfake detection system using big data. SN Computer Science. 2024; 5(6): 752. doi: 10.1007/s42979-024-03105-8
11. Kumar N, Kundu A. SecureVision: Advanced Cybersecurity Deepfake Detection with Big Data Analytics. Sensors. 2024; 24(19): 6300. doi: 10.3390/s24196300
12. Ligo AK, Kott A, Linkov I. How to measure cyber-resilience of a system with autonomous agents: Approaches and challenges. IEEE Engineering Management Review. 2021; 49(2): 89–97. doi: 10.1109/emr.2021.3074288

13. Yamin MM, Ullah M, Ullah H, et al. Weaponized AI for cyber attacks. Journal of Information Security and Applications. 2021; 57: 102722. doi: 10.1016/j.jisa.2020.102722
14. Michael JB, Wingfield TC. Defensive AI: The future is yesterday. Computer. 2021; 54(9): 90–96. doi: 10.1109/mc.2021.3092480
15. Malatji M, Tolah A. Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI. AI and Ethics. 2024; 1–28. doi: 10.1007/s43681-024-00427-4
16. Macas M, Wu C, Fuertes W. Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems. Expert Systems with Applications. 2024; 238: 122223. doi: 10.1016/j.eswa.2023.122223
17. Uriawan W, Adriansyah S, Maulidiyah SJ, et al. Challenges and opportunities: Improve patient data security and privacy in distributed systems. 2024. doi: 10.20944/preprints202407.0163.v1
18. Yu M, Zhuge J, Cao M, et al. A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. Future Internet. 2020; 12(2): 27. doi: 10.3390/fi12020027
19. Alsubaei F, Abuhussein A, Shiva S. Security and privacy in the internet of medical things: Taxonomy and risk assessment. In: Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops); 9 October 2017; Singapore, Singapore. pp. 112–120.
20. Taheri S, Asadizanjani N. An Overview of medical electronic hardware security and emerging solutions. Electronics. 2022; 11(4): 610. doi: 10.3390/electronics11040610