HSPI The Open Access Publisher

JAIRI ISSN 3069-762X JOURNAL OF ARTIFICIAL INTELLIGENCE RESEARCH AND INNOVATION

Research Article

Assessing Techniques for Reducing Cyber Risks and AI Applications

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

[1]Institute for IT Innovation and Smart Health, Mississippi, USA
[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA

More Information

***Corresponding author:** Cheryl Ann Alexander, Institute for IT Innovation and Smart Health, Mississippi, USA,
Email: cannalexander68@gmail.com

Submitted: August 10, 2026
Accepted: August 14, 2026
Published: August 17, 2026

Citation: Alexander CA, Wang L. Assessing Techniques for Reducing Cyber Risks and AI Applications. J Artif Intell Res Innov. 2026; 2(2): 108-114. Available from: https://dx.doi.org/10.29328/journal.jairi.1001024

Keywords: Artificial intelligence (AI); Machine learning (ML); Federated learning; Cybersecurity; Cyber risk; Privacy; Data encryption; Multi-factor authentication (MFA); Access control; Healthcare

Abstract

This paper introduces techniques specifically designed to reduce cyber risks and presents techniques for reducing cyber risks and for artificial intelligence (AI) applications in healthcare. A case study introducing the reduction of cyber risks and the use of artificial intelligence (AI)/ machine learning (ML)/deep learning (DL) in healthcare is also presented. The case study includes techniques and countermeasures for reducing cyber risks and protecting data assets in the Emerald Healthcare System in the USA; provisions for giving access and extending access to suppliers and customers in the healthcare system; and the implications of outsourcing, consulting, service providers, and/or other external links that have access to privileged areas. Extended access to data will increase cyber risks. Access to privileged areas puts data at a higher cyber risk. Data encryption is necessary for important data in motion and at rest to prevent hijacked data. Cybersecurity and techniques for reducing cyber risks in this paper are significant, especially in the healthcare industry. The methodology of the case study also applies to most other healthcare systems.

Introduction

Various types of controls (including preventive, detective, corrective, and compensating) can mitigate cyber risks. Preventive controls (e.g., firewalls and intrusion prevention systems) help prevent attacks on a specific information asset. Detective controls can determine whether an attack is imminent, the nature of the attack, where it started, what is utilized in the attack, and, if possible, individuals finishing the attack. Corrective controls help lessen the destruction from an attack. They include backup and restore, security upgrades or fixes, system patches, and updates on application operating systems and hardware drivers. Compensating controls can offset the failures or lack of other controls and reduce the loss of an incident. This kind of control includes having hot failover locations, separating a key system from the Internet, and fulfilling a backup or disaster recovery plan. Utilizing a layered method is a recommended mechanism of cyber defense [1].

It is important to align the goals of a company with cyber risk management strategies for cybersecurity defense. Governance is a collective set of principle-guided behaviors, while management is the application of the principle-guided behaviors into the company's operations. The three S's: strategy, steering, and standards (known as the governance triad) are often employed when aligning business and technology. The four C's: competencies (skill sets), conditions (environments), conduct (the set of actions), and capabilities (the measurement of competency throughput) represent the critical success factors [1].

Named data networking (NDN) is a promising Internet architecture. The Interest Flooding Attack (IFA) is an exhaustive attack that targets the forwarding strategy of NDN. IFA countermeasures can be classified as statistical-based, centralized-based, threshold-based, reputation value-based, and machine learning-based [2]. Technical efforts have been made in key areas such as MFA, anti-malware, robust patching, network hardening, and ransomware detection applications to detect, prevent, and recover from potential cyber risks [3].

Artificial Intelligence (AI)/machine learning (ML) can perform sophisticated pattern recognition, anomaly detection, and learning about new types of cyberattacks [4]. AI can improve edge security significantly by enabling the implementation of intelligent, context-aware rules that help to detect and respond to threats locally. An AI-enabled multi-layered security framework for 5G Networks was proposed [5].

With the help of AI/ML/deep learning (DL), IT professionals can detect attacks in real-time and take proper action. However, AI integration for security systems faces challenges, such as the compatibility of AI with existing infrastructure. In addition, AI requires a lot of data for training, which is difficult to arrange, maintain, and protect [6].

The primary purpose of the research in this paper is to address techniques for reducing cyber risks and AI applications. The originality and specific contribution of this paper lie in synthesizing the fundamental concepts, methodologies, and the body of knowledge in both cybersecurity (focus on reducing cyber risks) and AI/ML/DL, and extending them to applications in key aspects of a medical center through a case study. The remainder of this paper will be organized as follows: the second section introduces techniques specified to reduce cyber risks and a federated learning model; the third section presents techniques for reducing cyber risks and AI-powered protection in healthcare; the fourth section is a case study regarding reducing cyber risks and AI applications in healthcare, including techniques and countermeasures for reducing cyber risks and protecting data assets in Emerald Healthcare System, provisions for giving access and extending access to suppliers and customers, and implication of external links that have access to privileged areas; and the fifth section is the conclusion.

Techniques specified to reduce cyber risks and a federated learning model

To reduce cyber risks, a multi-faceted approach should be implemented, including proactive risk management strategies, robust security measures, and employee training. In addition, establishing clear security policies, conducting regular risk evaluations, and minimizing the attack surface are critical to practicing robust cybersecurity. Major techniques to reduce cyber risks are as follows: 1) the least privilege principle (granting users only the necessary access permissions to perform their tasks), 2) strong passwords and multi-factor authentication (MFA), 3) encrypting data and backing it up, 4) updating software and systems regularly, 5) minimizing the attack surface (reducing the number of entry points into systems and data by removing unnecessary software and access), 6) monitoring threat intelligence (monitoring threat intelligence feeds and staying informed about the latest cyber threats and attack techniques), 7) network segmentation (dividing the network into smaller segments to limit the spread of a potential cyberattack), 8) securing networks and devices (network access controls, utilizing firewalls, and employing antivirus and malware protection), 9) employing security tools such as intrusion detection systems (IDS) and security information and event management (SIEM) systems, 10) using endpoint detection and response (EDR) (providing real-time monitoring and analysis of endpoint activity to detect and respond to threats), 11) vendor risk evaluation (evaluating third-party vendors to guarantee they meet security standards), etc. [7-11].

Federated learning is a distributed machine learning (ML) framework. A federated learning system includes multiple participants and an aggregation server. A federated learning model faces cyber risks or attacks (e.g., model poisoning, data poisoning, etc.) in the training period, as illustrated in Figure 1 [12,13]. Perturbation technology and encryption have been used to safeguard privacy in federated learning [12,13].

Software-defined networking (SDN) is an agile networking technology. SDN features support cybersecurity. SDN's dynamic flow control feature enables dynamic access control without needing a firewall [14]. This feature helps network separation, as shown in Figure 2 [14]. Network-wide visibility with centralized control is another feature of SDN that allows you to monitor the entire network. The complete view of the network helps to detect and defend against cyberattacks such as distributed denial-of-service (DDoS)[14], as illustrated in Figure 3 [14].

Three kinds of privacy concerns were studied: privacy concerns raised by user cyberspace activities, privacy concerns in a personal cyber-physical system, and privacy

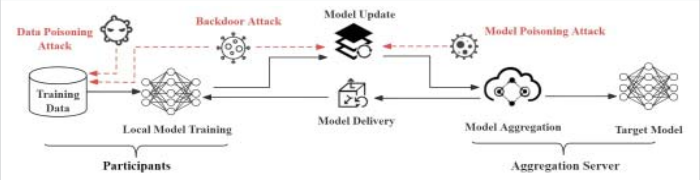

Figure 1: Attacks in the training period of a federated learning model.

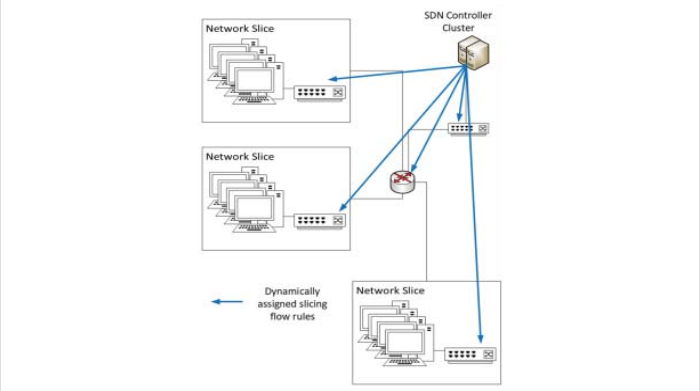

Figure 2: Network slicing utilizing the dynamic control of SDN.

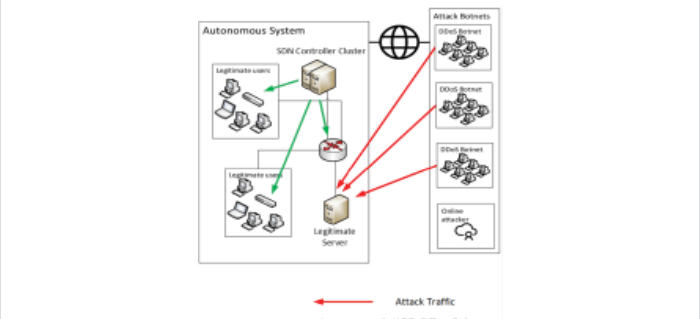

Figure 3: Network-wide visibility of ADN supports protection against DDoS.

concerns during user-driven data collection [15]. Details regarding these privacy concerns are summarized in Table 1 [15].

In summary, main techniques or approaches discussed in this paper can reduce general cyber risks and also include the following suggestions: 1) using advanced security technology such as firewalls, anti-virus software, and an intrusion detection system; 2) regular patches and updates to systems, devices, and software; 3) using strong passwords and changing them regularly, or implementing multi-factor authentication; 4) encrypting sensitive information at rest and in transit; 5) establishing network access controls; 6) continuously monitoring network traffic; 7) performing risk assessment; 8) closely monitoring third-party access and assessing and monitoring vendors; 9) regular data backups; 10) minimizing the attack surface; 11) using endpoint detection and response (EDR); and 12) fostering partnerships and sharing information.

Techniques for reducing cyber risks and AI-powered protection in healthcare

To mitigate cyber risks in healthcare, robust security measures should be implemented, including strong passwords, multi-factor authentication, and regularly updated software. In addition, regular security evaluations, data encryption, and network segmentation are significant. Major techniques to reduce cyber risks in healthcare are as follows: 1) multi-factor authentication, 2) data backups, 3) regularly patching systems and software, 4) minimizing supply chain risks (evaluating vendors and implementing measures to mitigate risks related to third-party providers), 5) AI-powered threat protection, 6) HIPAA compliance, 7) connected device security (implementing security measures for medical devices), 8) securing the network (using firewalls, intrusion detection systems, intrusion prevention systems, and network segmentation), 9) endpoint security (using antivirus software, anti-malware protection, and endpoint detection and response systems to secure individual devices and systems), 10) securing remote access (utilizing secure methods for remote access, such as VPNs, to protect data transmitted over public networks), 11) adopting zero-trust architecture (reducing the attack surface by using a zero-trust model, where access is granted based on the principle of least privilege), etc. [16-20].

Table 1: Three categories of privacy concerns.

Categories	Countermeasures
Privacy & user activity in cyberspace	Web privacy protection using browser extensions: shielding a user's digital interactions from intrusive third-party tracking by blocking methods (list-based, algorithm-based, and ML-based blocking).
	Local differential privacy: a refinement of differential privacy, guaranteeing that removing an individual entry will not drastically change the overall distribution of data.
Privacy in a personal cyber-physical system	Access-control implementation for wearable devices
	The lightweight encryption of healthcare equipment
Privacy in user-driven data collection	Location privacy in participatory sensing: based on three main techniques, including dummy location (sending a query with a user's actual location & some fake locations), obfuscation (negotiating the degradation of location information), and *k*-anonymity (concealing the user's location within the locations of *k*-1 other users).
	Anonymous authentication for OppNets: anonymity protects users' identities while authentication validates nodes & secures the network.

Many hospitals in the USA are not prepared for cyber risks. Recommendations include training and educating employees in cybersecurity and cyber protocols, increasing advanced technical protections, cooperating with various experts, etc. [20]. Figure 4 shows risky technologies, associated vulnerabilities, current risk management, and recommended strategies [20].

Identity Management (IdM) systems based on blockchain (BC) can potentially be more secure and privacy-aware compared with a centralized IdM system. Research has been conducted to create a decentralized IdM system for the Health Internet of Things (HIoT). A framework of cyber risk management for an HIoT BC-IdM system has been presented [21]. Figure 5 illustrates the major aspects (requirements, threats, vulnerabilities, attacks, controls, and countermeasures) of the HIoT BC-IdM system [21]. Table 2 [21] lists details of some of the major aspects. All the aspects of security (e.g., assets/components) are presented in detail for every system layer. For example, the assets/components of the User layer include issuers, verifiers, holder custodians, data subjects, system owners, holders, relying parties, and orders [21]. Zero Trust is a major principle of cybersecurity in many areas, especially in healthcare. Every user, device, or

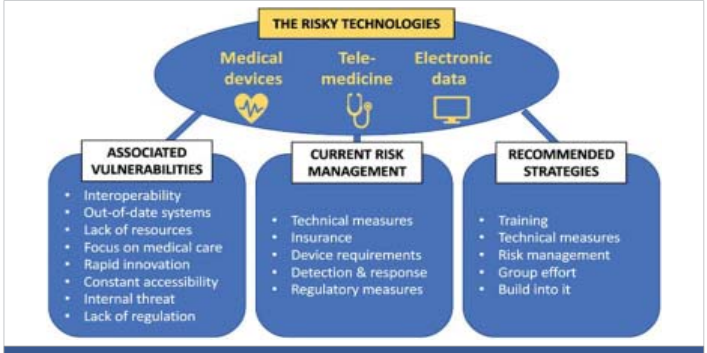

Figure 4: Risky technologies, vulnerabilities, risk management, and recommended strategies.

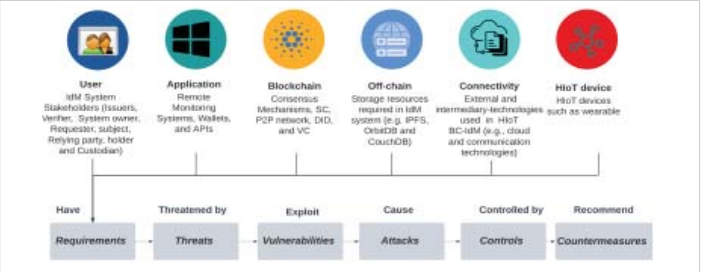

Figure 5: The security framework of an HIoT BC-IdM system.

application requires continuous verification and has the least privileged access. This is critical in healthcare due to sensitive patient data and many cyberattacks.

Bring Your Own Device (BYOD) refers to utilizing employee-owned mobile devices to get access to business content or networks. There are challenges when mobile devices are brought to hospitals. The challenges are associated with technologies, human factors, and policies [22,23]. Table 3 shows the challenges and solutions [22,23]. Table 4 lists mitigation strategies that are grouped into categories and well-defined by the NIST (National Institute of Standards and Technology) Cybersecurity Framework [24]. The mitigation techniques in the table ought to be recommended to medical device manufacturers and healthcare delivery organizations to ensure appropriate safeguards [24].

There are many cyber risks in the healthcare sector due to complex factors such as the high value of healthcare

Table 4: Mitigation categories, security capabilities, and mitigation techniques.

Mitigation categories	Security capabilities	Mitigation techniques
Identify	Personal authentication Node authentication	Digital signature Authentication
Protect (Protect-prevent)	Authorization Automatic logoff Physical lock on a device Health data integrity & authenticity Health data storage & confidentiality	Authorization Encryption De-identification Filtering Message authentication code Do not store secrets
Protect (Protect-limit)	Guidelines for security Software & application hardening Security features configuration	Input validation Input sanitization Least privilege Throttling Service quality Physical tamper-resistant
Detect	Audit Physical lock on a device	Audit trail Physical tamper evidence
Respond	Emergency access Malware detection & protection	End-user signalization Invalidate compromised security
Recover	Cybersecurity product update Data backup & disaster recovery	Re-establish security

Table 2: The details of the security framework of an HIoT BC-IdM system.

Layers	Part of the major aspects	Description
User	Threats or risks	Tampering (malicious input, patient data), spoofing (user device impersonation)
	Control & Countermeasures	Authorization, authentication/MFA, auditing, and ABE (attribute-based encryption) key management
Application	Threats or risks	Insecure APIs (privilege elevation); unsecured components of software (tampering, spoofing, information disclosure, & privilege elevation); lack of input/output filtering in HIoT & APIs (tampering & information disclosure)
	Control & Countermeasures	Logging & access control
Blockchain	Threats or risks	Insider threats, Sybil attacks, quantum threats, replay attacks (tampering), consensus mechanism vulnerabilities, 51 attacks (majority attacks), double-spending threats, Decentralized Identifier (DID) defects, Smart Contract/Chaincode threats, & advanced persistent threat (APT)
	Control & Countermeasures	Encryption, authentication, strict access, session management, input validation, infeasible service endpoint attributes, secure Membership Service Provider (MSP), utilizing SC (smart contract) analysis tools, utilizing SC countermeasure analysis tools, utilizing one of 51 attack prevention techniques, & utilizing quantum-safe cartographic mechanisms
Off-chain	Threats or risks	Transaction privacy leakage, wallet theft, data delivery problems (repudiation), log deletion (repudiation), & medical information disclosure
	Control & Countermeasures	Restricting access, data encryption, & using privacy techniques (e.g., zero-knowledge proof)
Connectivity	Threats or risks	Tampering (replay attacks, communication modification); information disclosure (side-channel attacks, data eavesdropping); tampering and information disclosure (lack of input/output filtering in the HIoT and APIs)
	Control & Countermeasures	Third-party data distribution policies, monitoring, & the review of third-party services
HIoT	Threats or risks	Tampering (device failure, device tampering); denial of service (DoS) (signal-jamming flooding, battery-drain attack); information disclosure (HIoT tracking, HIoT type determination); elevation of privilege (maintenance compromise)
	Control & Countermeasures	Authorization, authentication, protection of host & device security

Table 3: Challenges and solutions of BYOD.

	Technology factors	Human factors	Policies
Challenges	Insecure devices	Unsuitable behaviors	Lack of policy
	Absence of locking	Lack of awareness	Compliance
	Unsecure network	User's poor experience	Sanctions for breaches
	Suspicious app installed	Shortage of skills	
	Management of mobile devices	Culture of security	BYOD strategies & governance
	Containerization	Awareness & training	Users' agreements
Solutions	Management of identity & access	Improvement in skills	BYOD policies
	Tools of endpoint security		
	Secure communication platforms		

and research data, widely distributed data, numerous vulnerable Internet of Medical Things (IoMT) endpoints, many connected devices ripe for exploitation, supply chain risks, and unprotected legacy systems. In addition, healthcare organizations rely heavily on third-party vendors and suppliers. A contract should be required, especially if the cloud is used. In summary, the following main techniques or approaches will reduce cyber risks in health healthcare:

- Artificial intelligence (AI)/machine learning (ML)/ deep learning (DL) is used to identify cyber-attack patterns and make immediate decisions on how to stop the attacks.
- Using biometrics (such as fingerprints, facial recognition, and iris scanning) and MFA, and enforcing least-privilege access based on work responsibilities and roles to guarantee only authorized access to sensitive information.
- Fundamental network security in healthcare (e.g., firewalls).
- Keeping systems up to date with the latest security patches.
- Limiting network access, limiting employee access privileges, controlling access to protected healthcare information, and implementing data use controls.
- Logging all access and usage data for monitoring users, auditing, and evaluating cyber risks.
- Mitigating the cyber risks of connected medical devices, installing mobile security software, and securing mobile devices
- Backing up healthcare data to a secure and off-site location.
- Following HIPAA security rules and HIPAA privacy rules.
- Information sharing for stronger collective defense in healthcare.
- Conducting regular security assessments and preventing health data breaches.

A case study regarding reducing cyber risks and ai applications in healthcare

Emerald Healthcare System is a not-for-profit corporation dedicated to developing medical programs, healthcare services, research, etc. The system's three hospital campuses, plus several outpatient facilities, provide a broad spectrum of care. Services provided by over 1,550 medical staff members and more than 10,300 employed professionals make Emerald Healthcare System one of the largest healthcare providers in Texas, USA.

Techniques and countermeasures for reducing cyber risks and protecting data assets in the Emerald Healthcare System

Data assets in Emerald Healthcare System include patient data, biometric data, passwords, clinical diagnostic and treatment data, pharmaceutical data, research data, third-party supply chain-generated data, etc. HIPAA standards protect patient data; clinicians, staff, and employees with limited access to patient data are given passwords or biometric scans that protect the data. Biometric data is protected by vigorous encryption. Passwords are employee-specific and are protected by the staff; for example, they are required to change passwords every 90 days. Clinical diagnostic and treatment data is protected by HIPAA, encrypted data while in motion and at rest, biometric scans, and passwords. Pharmaceutical data is protected by HIPAA, biometric data, passwords, and contracts with third-party vendors. Passwords and biometric scans protect research data. Third-party supply chain data is protected by HIPAA, biometric data, and passwords. The primary method of protection, aside from encryption, is third-party background checks and third-party contracts. In addition, data gathered from satellite locations and telemedicine must adhere to HIPAA standards and encryption in motion and at rest. Emerald Healthcare System has implemented rigorous cybersecurity measures and policies based on advanced techniques (such as AI/ML/DL), countermeasures, and HIPAA standards to reduce cyber risks in healthcare. Cyber risk incidents were reduced by 38% in 2025 compared with those in 2024.

AI/ML/DL has been used to identify cyber-attack patterns and predict various cyber-attacks in the Emerald Healthcare System. The quality of training datasets is very important for the performance of AI/ML/DL. For example, a DL model's architecture and DL hyperparameters (such as the number of layers and nodes, the batch size, the dropout rate, and the learning rate) also affect the performance of DL. DL methods and models, such as multilayer perceptrons (MLPs), recurrent neural networks (RNNs), deep belief networks (DBNs), and convolutional neural networks (CNNs), have been used in the healthcare system. Accuracy, precision, recall, the false positive rate (FPR), the false negative rate (FNR), and F1-score are often used as evaluation or performance metrics, providing a comprehensive evaluation of the performance of DL models.

Provisions for giving access and extending access to suppliers and customers

Customers in the Emerald Healthcare System include patients, physicians, nurse practitioners, physician assistants, nurses, clinicians, third-party suppliers and vendors, employees, and staff. Third-party access is given according to the contract established by the Healthcare System. Data access for patients is limited by Medical Records staff, HIPAA

standards, Healthcare System standards, and access to their data only. Physicians and other clinical providers have access to their patients' data only, research data, clinical data such as clinical notes, diagnostic data, telemedicine and off-site patient data, and imaging data, which is limited by HIPAA and regulated with biometric scanning and passwords. Nurses and clinicians—access is limited to patients they are directly caring for and are responsible for. Data is restricted to HIPAA standards, passwords, biometric data, and encrypted data. Third-party suppliers and vendors can only access the data outlined in a well-planned contract submitted and agreed on by upper management and IT security teams. Employees and staff can only access patient data or billing data according to their role in the Healthcare System. Customers are limited to data access by management and IT security. Customers must seek and gain IT security permission and upper management approval for extended access. AI/ML/DL needs much data for training and testing. Extended access to data introduces a higher cyber risk.

Implications of outsourcing, consulting, service providers, and/or other external links that have access to privileged areas

Sometimes the Emerald Healthcare System has limited access to specialized providers. For example, one hospital may not have access to a cardiologist for a patient who needs a stress test. Therefore, outsourcing or consulting is necessary for this patient, and data must be transmitted, putting it at higher cyber risk. The implication of introducing third-party access to data is that it puts data at a higher cyber risk. Data must be encrypted. Data is in motion and may be subject to any malicious actor. Data may be exposed verbally; for example, an employee of a third party may speak of the data in an elevator, at a water cooler, etc. AI/ML/DL can be used for defense, but malicious actors and scammers can also use AI/ML/DL and access exposed data while at rest. Data encryption while data is in motion and at rest is necessary to prevent hijacked data.

Conclusion

A federated learning model faces cyber risks or attacks (e.g., data poisoning). Perturbation technology and encryption help safeguard privacy in federated learning. SDN's dynamic flow control enables dynamic access control without needing a firewall. This SDN-holistic view of the network helps detect and defend against attacks. Many hospitals in the USA are not prepared for cyber risks. Training and educating employees in cybersecurity and cyber protocols, increasing sophisticated technical protections, and cooperating with various experts in both cybersecurity and healthcare are highly recommended. IdM systems based on blockchain can potentially be more secure and privacy-aware compared with a traditional centralized IdM system.

The originality and specific contribution of this paper lie in synthesizing the fundamental concepts, methodologies, and the body of knowledge in both cybersecurity (focus on reducing cyber risks) and AI/ML/DL, and extending them to applications in key aspects of a medical center through the case study. AI/ML/DL is powerful in threat protection. In the Emerald Healthcare System, there are various techniques and countermeasures for reducing cyber risks and protecting data assets, as well as the applications of AI/ML/DL, which depend on specific data assets. Extended access to data will increase cyber risk. Access to privileged areas puts data at a higher cyber risk. The methodology in the case study can also be used in most other healthcare systems.

Acknowledgment

The authors would like to express thanks to Technology and Healthcare Solutions, USA, for its help and support.

Declaration of the use of AI tools

The authors declare that they did not use AI tools in writing this paper.

Ethics: In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

References

1. Moschovitis C. Cybersecurity program development for business. Wiley; 2018.
2. Jeet R, Arun Raj Kumar P. A survey on interest packet flooding attacks and its countermeasures in named data networking. Int J Inf Secur. 2022;21(5):1163-1187.
3. Angafor GN, Yevseyeva I, Maglaras L. Securing the remote office: reducing cyber risks to remote working through regular security awareness education campaigns. Int J Inf Secur. 2024;1-15.
4. Alnaabi AA, Al Mahruqi AA. Artificial intelligence methods for enhancing cybersecurity in Oman: A comprehensive review. J Cloud Comput. 2026;15(1):48. Available from: https://doi.org/10.1186/s13677-026-00860-2
5. Alam A, Umer A, Ullah I, Alsayat A. AI-enabled cybersecurity framework for future 5G wireless infrastructures. Sci Rep. 2026;16(1):7055. Available from: https://doi.org/10.1038/s41598-026-37444-8
6. Ali A, Shah MH, Foster M, Alraja MN. Artificial intelligence for cybersecurity in banking: A taxonomy of barriers and possible mitigation strategies. Cybern Syst. 2026;1-42. Available from: https://doi.org/10.1080/01969722.2026.2626804
7. Conteh NY, Schmick PJ. Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In: Ethical hacking techniques and countermeasures for cybercrime prevention. IGI Global; 2021. p.19-31. Available from: https://doi.org/10.19101/IJACR.2016.623006
8. Eling M, McShane M, Nguyen T. Cyber risk management: History and future research directions. Risk Manag Insur Rev. 2021;24(1):93-125. Available from: https://doi.org/10.1111/rmir.12169
9. Evans A. Managing cyber risk. Routledge, Taylor & Francis Group; 2019. Available from: https://doi.org/10.4324/9780429057632
10. Gallo N. Considering security measures mitigations in automatic cyber risk assessment [doctoral dissertation]. Politecnico di Torino; 2025.
11. Islam E, Rudolph C, Oliver G. Managing cyber harm: a survey of

challenges, practices, and opportunities. Inf Secur J Glob Perspect. 2025;1-31. Available from: https://doi.org/10.1080/19393555.2025.2484348

12. Jagielski M, Oprea A, Biggio B, Liu C, Nita-Rotaru C, Li B. Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. In: 2018 IEEE Symposium on Security and Privacy (SP). IEEE; 2018. p.19-35.
13. Wu J, Jin J, Wu C. Challenges and countermeasures of federated learning data poisoning attack situation prediction. Mathematics. 2024;12(6):901.
14. Abdelrahman AM, Rodrigues JJ, Mahmoud MM, Saleem K, Das AK, Korotaev V, et al. Software-defined networking security for private data center networks and clouds: Vulnerabilities, attacks, countermeasures, and solutions. Int J Commun Syst. 2021;34(4):e4706.
15. Jiang Y, Rezazadeh Baee MA, Simpson LR, Gauravaram P, Pieprzyk J, Zia T, et al. Pervasive user data collection from cyberspace: Privacy concerns and countermeasures. Cryptography. 2024;8(1):5.
16. Al-Qarni EA. Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. Int J Adv Comput Sci Appl. 2023;14(5).
17. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, Flahault A. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak. 2020;20:1-10. Available from: https://doi.org/10.1186/s12911-020-01161-7
18. Jawad LA. Security and privacy in digital healthcare systems: Challenges and mitigation strategies. Abhigyan. 2024;42(1):23-31. Available from: https://doi.org/10.1177/09702385241233073
19. Pendyala SK. Strengthening healthcare cybersecurity: Leveraging multi-cloud and AI solutions. J Comput Sci Appl Inf Technol. 2025;10(1):1-8. Available from: https://doi.org/10.15226/2474-9257/10/1/00163
20. Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Front Digit Health. 2022;4:862221.
21. Alamri B, Crowley K, Richardson I. Cybersecurity risk management framework for blockchain identity management systems in health IoT. Sensors. 2022;23(1):218.
22. Burke G, Saxena N. Cyber risks prediction and analysis in medical emergency equipment for situational awareness. Sensors. 2021;21(16):5325.
23. Rodrigues GAP, Serrano ALM, Vergara GF, Albuquerque RDO, Nze GDA. Impact, compliance, and countermeasures in relation to data breaches in publicly traded US companies. Future Internet. 2024;16(6):201.
24. Wani TA, Mendoza A, Gray K. Hospital bring-your-own-device security challenges and solutions: Systematic review of gray literature. JMIR Mhealth Uhealth. 2020;8(6):e18175.