A blue and orange logo

Description automatically generated

The Role of Deep Learning in Cybersecurity for Healthcare Organizations - March 2024

**Tharindu D. Nanayakkara.**

**Undergraduate in Cybersecurity, Faculty of Computing, Sri Lankan Institute of Information Technology, Malabe, Sri Lanka.**

***Abstract*: When everything gets digitalized, the healthcare sector also increasingly digitizes patient records and adopts interconnected systems for improved patient care and operational efficiency, they become vulnerable targets for cyber threats. As result traditional cybersecurity measures are often insufficient in safeguarding against sophisticated attacks, necessitating the integration of advanced technologies such as deep learning. Cybersecurity challenges faced by healthcare organizations, including data breaches, ransomware attacks, and insider threats. It then delves into the fundamentals of deep learning, highlighting its capabilities in processing large volumes of data, identifying complex patterns, and adapting to evolving threats.**

**Furthermore, the report discusses various deep learning methodologies applicable to cybersecurity, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs). It examines how these models can be utilized for tasks such as anomaly detection, malware classification, and intrusion detection within healthcare networks. Advantages and limitations of deploying deep learning solutions in healthcare cybersecurity, including scalability, interpretability, and resource requirements. It also addresses ethical considerations and regulatory compliance issues associated with the use of AI in sensitive healthcare environments. A review of case studies and real-world examples of healthcare organizations implementing deep learning-based cybersecurity solutions. These case studies highlight the effectiveness of deep learning in detecting and mitigating cyber threats, reducing response times, and enhancing overall security posture.**

**In conclusion, the report emphasizes the significance of integrating deep learning technologies into cybersecurity strategies for healthcare organizations. By leveraging the power of deep learning, healthcare institutions can bolster their defenses against cyber threats, safeguard patient data confidentiality, and ensure the continuity of critical healthcare services.**

***Keywords:* Artificial Intelligence, Cybersecurity, Cyberthreats, Data Breach, Deep Learning, Healthcare, Internet of Medical Things, Post-Incident.**

# Introduction

In the rapidly evolving landscape of cyberspace, the convergence of deep learning and cybersecurity emerges as a critical domain, particularly within the healthcare sector. With the production of digital technologies and the increasing reliance on electronic health records (EHR), medical devices, and telemedicine platforms, healthcare organizations have become prime targets for cyber threats [1]. From ransomware attacks compromising patient data to insider threats jeopardizing the integrity of medical systems, the urgency for robust cybersecurity measures in healthcare has never been more apparent.

Against this backdrop, deep learning, a subset of artificial intelligence (AI) that mirrors the neural networks of the human brain, has garnered significant attention for its potential to bolster the defenses of healthcare organizations against cyber threats. By harnessing vast datasets and sophisticated algorithms, deep learning techniques offer a promising avenue for real-time detection and mitigation of cybersecurity risks. From anomaly detection and malware analysis to intrusion detection and threat intelligence, deep learning algorithms hold promise for enhancing the security posture of healthcare systems and safeguarding the confidentiality, integrity, and availability of patient information [1] [2].

However, the potential benefits of deep learning in healthcare cybersecurity are accompanied by significant challenges and ethical considerations. As organizations deploy deep learning algorithms to protect sensitive medical data, concerns arise regarding data privacy, algorithmic bias, interpretability, and susceptibility to adversarial attacks. Moreover, the adoption of deep learning in healthcare cybersecurity necessitates robust infrastructure, skilled personnel, and ongoing refinement to ensure efficacy and reliability in the face of evolving cyber threats [3].

## What is Deep learning, fundamentals, and applications.

Deep learning is a subset of machine learning that involves training artificial neural networks to learn from large amounts of data. At its core, deep learning utilizes neural networks, which are computational models inspired by the structure and function of the human brain [4]. In the deep learning there are fundamentals and applications. Further studies are in the appendix about the artificial neural network.

### Fundamentals

Neural Networks are the building blocks of deep learning models. These networks are composed of interconnected layers of nodes, or artificial neurons, each performing simple mathematical operations. Layers are typically organized into an input layer, one or more hidden layers, and an output layer. The connections between nodes are associated with weights, which are adjusted during the training process to optimize the network's performance [4].For training backpropagation is a fundamental algorithm used in neural networks. It involves calculating the gradient of the loss function with respect to the network's parameters and using this information to update the parameters in the direction that minimizes the loss and helps to improve its performance over time.

Same as backpropagation there are some optimization techniques, such as gradient descent, are employed to iteratively adjust the parameters of the neural network to minimize the loss function during training [5]. Regularization techniques, such as L1 and L2 regularization, are used to prevent overfitting, a common problem in deep learning where the model performs well on the training data but generalizes poorly to unseen data. Regularization adds a penalty term to the loss function that discourages overly complex models, helping to improve generalization performance [4].

The loss function quantifies the difference between the predicted outputs of the neural network and the actual targets. Common loss functions include mean squared error for regression tasks and cross-entropy loss for classification tasks. By minimizing the loss function during training, the neural network learns to make more accurate predictions [4].

### Applications

In Neural networks learning models, such as convolutional neural networks (CNNs), have revolutionized computer vision tasks such as image classification, object detection, and image segmentation. Convolutional neural networks are capable of automatically learning hierarchical features from raw pixel data, enabling them to achieve state-of-the-art performance on a wide range of visual recognition tasks. Normally in Natural Language Processing (NLP, such as recurrent neural networks (RNNs) and transformers, are widely used to perform tasks such as language translation, sentiment analysis, and text generation [4] [2]. These models can help us to understand and generate human-like text by processing large amounts of textual data [4] [1].

Same as in the Recommendation Systems deep learning models, such as collaborative filtering and deep neural networks, are used to provide personalized recommendations for products, movies, music, and other items. These models analyze user behavior and preferences to generate recommendations that are tailored to individual users' tastes and preferences [4].

## Deep Learning in Cybersecurity.

With the help of deep learning fundamentals and applications they have utilized deep learning in the cybersecurity to do mostly impossible. Mostly it is used to detect the changes in the systems that cannot be hooked by naked eye [6].

### Detecting Anomalies:

Intrusion Detection is one which is a detection of anomalies in the system which indicative of cyber-attacks, such as denial-of-service attacks or data exfiltration. Then it can also be used to prevent intrusion in real-time.

Vulnerability detection

Vulnerability detection in cybersecurity encompasses various techniques, among which deep learning plays a pivotal role. Specifically, deep learning models excel in two critical areas: malware detection and phishing detection.

In malware detection, deep learning models leverage their capability to analyze file characteristics comprehensively. By scrutinizing file attributes such as code patterns, behavior, and structural anomalies, these models can effectively identify malicious software. Furthermore, deep learning enables the classification of detected malware into distinct families, facilitating targeted mitigation strategies and enhancing overall cybersecurity posture.

Similarly, deep learning models are instrumental in combating phishing attacks, a prevalent threat vector in cybersecurity. Through the analysis of email content and metadata, these models can discern subtle indicators of phishing attempts. By scrutinizing language patterns, sender attributes, and contextual cues, deep learning models can swiftly identify suspicious emails and preempt potential threats. By bolstering phishing detection capabilities, organizations can mitigate the risk of data breaches and protect sensitive information from compromise.

### Security Analytics

Deep learning in threat intelligence lies in its ability to automatically analyze and correlate data from diverse sources. By assimilating information from disparate sources, such as network traffic logs, incident reports, and threat feeds, deep learning models can uncover hidden patterns and relationships indicative of potential security threats. This holistic approach enables security analysts to gain a comprehensive understanding of the threat landscape, facilitating proactive measures to mitigate risks and bolster defense mechanisms [6] [7].

Moreover, deep learning models aid in enhancing security by enabling automated analysis and prioritization of identified threats. By swiftly identifying and categorizing potential risks based on their severity and impact, these models empower security analysts to allocate resources more effectively and respond to threats in a timely manner. This streamlines the incident response process, enabling organizations to mitigate risks promptly and minimize the potential impact of cyberattacks.

## Healthcare and Cybersecurity

Healthcare has witnessed significant advancements in recent years, particularly with the digitalization of medical data and the integration of interconnected devices into healthcare systems.

### Development

Looking from the progressive side, most of the improvements helped to develop the medical sector. Electronic Health Records (EHRs) have become commonplace, allowing healthcare providers to access and manage patient information more efficiently [5]. Additionally, the proliferation of Internet of Things (IoT) devices, such as wearable health monitors and remote patient monitoring systems, has revolutionized patient care by enabling continuous health monitoring and remote consultations. These developments have improved patient outcomes, enhanced diagnostic capabilities, and increased the efficiency of healthcare delivery. Figure 1 shows the simple medical ecosystem [8] [7].

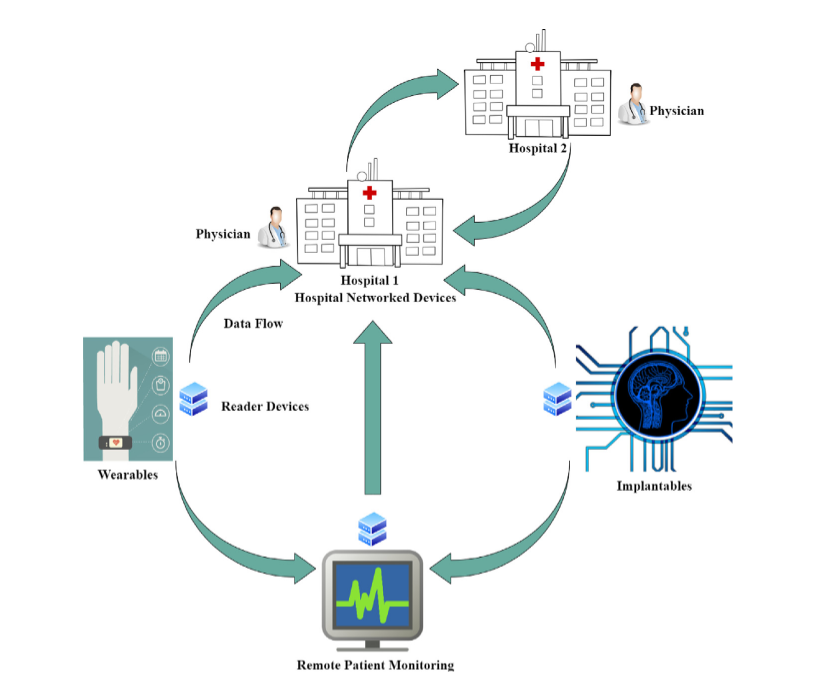


Figure 1 Internet of medical things ecosystem [5]

With the time medical Centers, hospitals and healthcare organizations are evolving into a paperless environment with the introduction of the electronic health records (EHR) for patients [3].

As mentioned above deep learning helped mostly in enhanced threat detection in real-time, helping healthcare organizations respond more effectively to security incidents. Deep learning techniques hold tremendous potential for bolstering patient privacy within healthcare systems by automating processes such as de-identification of sensitive information in medical records and enhancing access controls to prevent unauthorized access. These advanced algorithms can analyze large datasets and detect anomalies in user behavior, aiding healthcare organizations in proactively identifying and mitigating security threats. Additionally, deep learning can assist in the development of more robust encryption protocols and data protection mechanisms by analyzing historical cybersecurity incidents and identifying patterns to strengthen security measures. By leveraging deep learning, healthcare entities can effectively safeguard patient data, ensuring compliance with regulatory requirements while maintaining patient trust and confidentiality in an increasingly digital healthcare landscape [8].

### Impact

However, with these advancements mentioned above comes the challenges of ensuring the security and privacy of patient data. The increasing interconnectedness of healthcare systems and the digitization of medical records have made healthcare organizations more vulnerable to cyber threats. Cybercriminals target healthcare institutions to gain unauthorized access to sensitive patient information, disrupt operations, and even demand ransom through ransomware attacks. Moreover, insider threats, whether intentional or unintentional, pose significant risks to patient data security. The consequences of a data breach in healthcare can be severe, including financial losses, reputational damage, and compromised patient safety.

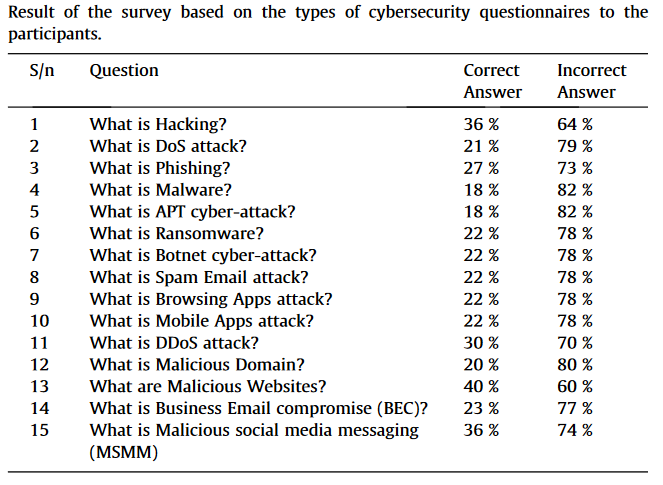


Figure 2 Survey on awareness. [9]

As mentioned above table a survey conducted by King Saud University [9] mostly of the attacks happen due to the lack of the awareness on the cyberthreats. Like Hacking, where individuals gain unauthorized access to systems or networks with the intention of stealing data, disrupting operations, or causing damages. Phishing is another prevalent tactic, involving the deceptive masquerading of trustworthy entities to trick individuals into divulging sensitive information like login credentials or financial details.

Botnet attacks utilize networks of compromised computers, or botnets, to execute coordinated assaults such as distributed denial of service (DDoS) attacks, spamming, or malware dissemination. Ransomware, a particularly disruptive form of malware, encrypts files or systems, demanding payment of a ransom for their release. These attacks can inflict significant financial losses and operational disruptions on individuals, businesses, and organizations.

Advanced Persistent Threats (APTs) represent a sophisticated breed of cyber-attack orchestrated by highly skilled adversaries. These attacks are often targeted and clandestine, with specific objectives such as espionage, sabotage, or data theft. APTs can operate stealthily for extended periods, enabling attackers to gather intelligence and execute their aims undetected.

Malicious social media messaging exploits the trust and social connections inherent in social media platforms to distribute malware, phishing links, or other malicious content to unsuspecting users. Similarly, in business email compromise attacks, cybercriminals impersonate legitimate email accounts or domains to deceive employees into carrying out fraudulent activities like fund transfers or disclosing sensitive information.

Malware, encompassing viruses, worms, Trojans, and spyware, is designed to disrupt, damage, or gain unauthorized access to computer systems or data. Denial of Service (DoS) attacks flood target systems or networks with excessive traffic or requests, rendering them unavailable to legitimate users. Distributed denial of service (DDoS) attacks, conducted from multiple sources, exacerbate the challenge of mitigation [10].

Finally, vulnerabilities within the technology sector represent weaknesses or flaws in software, hardware, or systems that cyber attackers exploit to gain unauthorized access or carry out malicious activities. Addressing these vulnerabilities through robust cybersecurity measures is essential to safeguarding against cyber threats and protecting digital assets.

### Damages

Depending on the attack and damage that is done by the cybercriminals the whole sector will be affect with in it can be Individuals, business, organizations, governments, and service providers [11]. Most of the damages cause

Security and privacy concerns breaches of sensitive data can lead to identity theft, fraud, or exposure of personal information, raising concerns about privacy and data security. According to the U.S. Department of Health and Human Services (HHS), there's been a 93% increase in large breaches from 2018 to 2022. In that same period, there's been a 278% increase in breaches involving ransomware [11] [12].

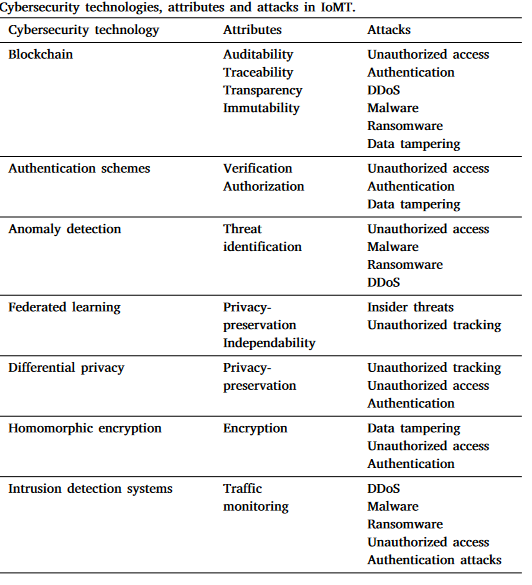


Figure 3 Cybersecurity technologies, attributes, and attacks in healthcare [13].

Then Cyber-attacks can result in financial losses due to theft of funds, disruption of operations, costs associated with recovery and remediation efforts, and potential regulatory fines or legal liabilities. The stolen data will be more valuable more than 10 - 20 times than credit card data [3]. With that Organizations may suffer damage to their reputation and brand image following a cyber-attack, leading to loss of customer trust, investor confidence, and business opportunities [11]. The below show the cost of the ransomware that taken place 2020 to 2022 worldwide [14] [15].

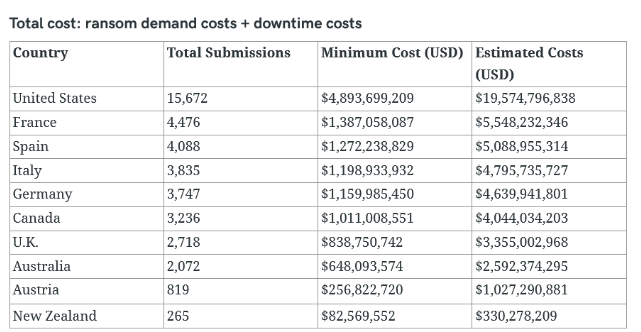


Figure 4 Ransome attacks on healthcare in 2020 [15]

Additionally National security Cyber-attacks are mainly targeting critical infrastructure, government agencies, or defense systems can pose significant threats to national security, potentially disrupting essential services, compromising classified information, or undermining public safety [12]. They can stifle innovation and technological advancement by undermining trust in digital technologies, discouraging investment in research and development, and creating barriers to collaboration and information sharing [11].

### Mitigate

To address these challenges, healthcare organizations must prioritize cybersecurity measures to protect patient data and mitigate the risk of cyber-attacks. There are mostly responses from the professionals and agencies that they make more awareness about the problem [3]. Robust cybersecurity frameworks encompassing encryption technologies, access controls, and regular security audits are essential to safeguard sensitive information from unauthorized access, disclosure, and tampering. Moreover, compliance with regulations like HIPAA is crucial to ensure patient privacy and avoid penalties associated with non-compliance [12]. Integrating cybersecurity practices with regulatory compliance initiatives enables healthcare organizations to effectively mitigate risks and uphold patient trust.

# Review of the literature

According to the topics we discussed mostly the healthcare organizations have these incidents that can help them to learn and study for the future development.

Improved Detection and Response Capabilities with the evolving landscape of cyber threats, healthcare organizations are investing in advanced technologies and methodologies to enhance their ability to detect and respond to cyber-attacks promptly. This includes the implementation of intrusion detection systems, security information and event management (SIEM) solutions, and threat intelligence platforms [16]. By leveraging real-time monitoring, threat hunting techniques, and automated incident response mechanisms, organizations can detect and mitigate security breaches more effectively, minimizing the impact on patient data and healthcare operations. Mostly they will also be affected to the attacked mentioned above in the threat sector mostly [16] [17].

Enhanced Data encryption plays a crucial role in protecting sensitive patient information from unauthorized access or disclosure. Healthcare organizations are increasingly adopting encryption techniques, such as end-to-end encryption and data-at-rest encryption, to secure data both in transit and at rest [5] [16]. By encrypting data stored in databases, electronic health records (EHR), and communication channels, organizations can prevent data breaches and ensure compliance with regulatory requirements, such as HIPAA and GDPR [18] [17].

Healthcare organizations must comply with a myriad of regulatory requirements and industry standards aimed at protecting patient privacy and data security. However, navigating the complex regulatory landscape can be burdensome, requiring significant time, resources, and expertise. Organizations must stay abreast of evolving regulations, such as the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Cybersecurity Act of 2015, to ensure compliance and avoid potential fines or penalties for non-compliance. Mostly these regulations are yet to be developed including in U.S.A and worldwide counties [3] [19].

Mainly human error remains one of the leading causes of cybersecurity breaches in healthcare. Awareness programs aim to educate employees about common cyber threats, phishing scams, and best practices for safeguarding sensitive information [19]. These programs may include interactive training sessions, simulated phishing exercises, and regular security awareness newsletters. By fostering a culture of cybersecurity awareness and accountability, organizations can empower employees to recognize and report potential security incidents, reducing the risk of data breaches and insider threats [11] [19].

Legacy System Vulnerabilities, such as outdated software, operating systems, and medical devices, often lack the latest security patches and updates, making them vulnerable to cyber-attacks, like insulin pump, cardiac implantable device vulnerabilities will speak as facts [3]. Healthcare organizations face the challenge of securing legacy systems while maintaining critical patient care services. This may involve implementing compensating controls, such as network segmentation, intrusion detection systems, and vulnerability management programs, to mitigate the risk of exploitation by cybercriminals [13] [20].

Ransomware attacks have indeed gained notoriety in recent years, with notable incidents such as Proxy Logon, Clop Ransomware, and WannaCry leaving a significant impact on the healthcare industry too [18] [21].

Proxy-Logon was a vulnerability found in Microsoft Exchange servers that allowed threat actors to gain unauthorized access to email accounts and potentially execute malicious code. Exploiting this vulnerability, cybercriminals could deploy ransomware or exfiltrate sensitive data, leading to significant data breaches and financial losses for affected entities [21].

Clop Ransomware is another prominent example of ransomware that has caused widespread damage. Clop not only encrypts files on infected systems but also threatens to publish stolen data if the ransom demands are not met. This tactic, known as "double extortion," adds another layer of pressure on victims to pay the ransom, amplifying the impact on affected organizations [14] [17] [21].

The WannaCry ransomware attack, which occurred in 2017, targeted vulnerable Windows systems worldwide, including healthcare organizations. The attack exploited a known vulnerability in the Windows operating system to encrypt files and demand ransom payments in Bitcoin for decryption keys [15] [18]. WannaCry installs the Double-Pulsar backdoor, which means that infected machines may still be vulnerable to future attacks. In addition to making these machines vulnerable to future ransomware attacks that would deny healthcare providers access to their systems and devices, this could make hacker-targeted medical records vulnerable to theft [15]. The WannaCry attack highlighted the importance of timely patch management, network segmentation, and data backup strategies in mitigating the impact of ransomware attacks on healthcare systems [15].

Insider threats, whether intentional or unintentional, pose a significant risk to healthcare data security. Insider threats may include employees, contractors, or trusted third parties who abuse their access privileges to steal sensitive information, sabotage systems, or compromise patient privacy. Healthcare organizations must implement robust access controls, user monitoring, and privilege management mechanisms to detect and mitigate insider threats effectively [18] [15].

Healthcare organizations rely on third-party vendors for various products and services, including medical devices, software applications, and cloud services. However, vendor security incidents, such as data breaches or supply chain attacks, can pose significant risks to patient data security and operational continuity. Healthcare organizations must conduct thorough due diligence when selecting vendors, assess their security posture, and establish contractual agreements to hold vendors accountable for maintaining security standards and responding to security incidents promptly [18].

Coronavirus Crisis has exacerbated cybersecurity challenges in healthcare, with cybercriminals exploiting the pandemic to launch phishing scams, ransomware attacks, and misinformation campaigns [10]. Healthcare organizations have faced increased pressure to rapidly deploy telehealth solutions, remote work infrastructure, and digital health technologies to support patient care during the crisis. This rapid digital transformation has introduced new security risks, including vulnerabilities in telehealth platforms, remote access systems, and medical IoT devices. Healthcare organizations must prioritize cybersecurity amidst the ongoing pandemic, implementing robust security measures to protect patient data and ensure the integrity of healthcare services.

Always cybercriminals have taken advantage of social flaws, and thus, the coronavirus pandemic. A one study shows the detailed impact this has done on the healthcare sector and done damages like data breaches [9] [11] [10].

Many types of cyber-attack took place day and night during the peak period of the global COVID-19 crisis. Hackers were busy launching and trying their hands on different variants of cyber-attacks such as phishing, malware, distributed-denial-of-service (DDoS), denial-of-service (DoS), advanced persistent threat (APT), malicious social media messaging (MSMM), business email compromise (BEC), botnet, ransomware amongst many others [10]. In the case of the phishing attack, hackers used harmful links hidden in carefully designed emails to target company employees. Unfortunately, when employees click on such links, they ignorantly download keylogging software onto their computers or devices, giving hostile actors access to their credentials. Hackers can then gain unrestricted access to critical business assets and data of the victim’s organization by impersonating a genuine employee. [9]

## Challenges and limitations

Deep learning models in healthcare cybersecurity present several challenges that must be addressed for successful implementation. One significant obstacle is data availability and quality, as accessing diverse and comprehensive datasets is hindered by privacy concerns and regulatory restrictions, while data quality issues can impact model performance [6] [22]. Additionally, scalability is a concern due to the computational intensity of deep learning models, posing challenges for organizations with limited IT infrastructure [17] [22]. Interpretability and explainability are crucial, especially in healthcare, where understanding model decisions is essential for trust and accountability. Ethical implications arise regarding patient privacy and potential biases, necessitating careful design and validation across diverse populations. Lastly, resource requirements for implementing and maintaining deep learning solutions, including skilled personnel and specialized hardware, can strain healthcare organizations, particularly in resource-constrained environments. Addressing these challenges is essential to leverage the potential of deep learning in healthcare cybersecurity effectively [17].

# Future research

Apart from the things mentioned above, mostly some topics were not covered as needed. With time we should also look at these topics. Morely they will help in the advancements.

## Areas needed improvement.

Regulatory Compliance and Data Privacy: Compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) is critical for ensuring the privacy and security of patient data. Healthcare organizations need to improve their compliance efforts by implementing comprehensive policies, procedures, and technical controls to protect patient privacy and prevent data breaches [17].

Securing the Internet of Medical Things (IoMT) Devices: The production of Internet-connected medical devices, such as wearable health monitors, implantable devices, and remote patient monitoring systems, poses significant security risks to healthcare organizations. There is a need to improve the security of IoMT devices by implementing authentication, encryption, and vulnerability management measures to mitigate the risk of cyber-attacks and ensure patient safety.

Cybersecurity Training and Awareness: Human error remains a significant factor in healthcare cybersecurity breaches, highlighting the importance of cybersecurity training and awareness programs for healthcare employees. Organizations need to invest in comprehensive training programs to educate employees about common cyber threats, phishing scams, and best practices for protecting patient data.

Supply Chain Security: Healthcare supply chains are increasingly interconnected, with third-party vendors providing a wide range of services and products to healthcare organizations. Strengthening supply chain security requires improved vendor risk management practices, including thorough vetting of vendors, contractual agreements, and ongoing monitoring of vendor security practices to mitigate the risk of supply chain attacks and data breaches.

These sectors must have more upgrades and research due to their vast vulnerabilities.

# Conclusion

Overall, addressing the complex challenges and evolving threats in healthcare cybersecurity requires a multifaceted approach that encompasses technological innovation, regulatory compliance, and organizational readiness. Throughout this discussion, we have explored the fundamentals of deep learning and its applications in cybersecurity, particularly within the healthcare sector. We have also identified key challenges and areas needing improvement, ranging from data privacy and regulatory compliance to the security of Internet-connected medical devices and supply chain integrity.

Moving forward, it is imperative for healthcare organizations to prioritize investments in advanced cybersecurity technologies, robust compliance frameworks, and comprehensive training programs to mitigate risks and safeguard patient data. Collaboration between stakeholders, including healthcare providers, cybersecurity experts, regulatory agencies, and technology vendors, is essential for developing and implementing effective cybersecurity strategies that address the unique needs and complexities of the healthcare ecosystem.

By leveraging the power of deep learning and embracing a proactive and holistic approach to cybersecurity, healthcare organizations can enhance their resilience to cyber threats, protect patient privacy and safety, and uphold the trust and integrity of the healthcare system. As we continue to navigate the ever-evolving landscape of cyberspace, let us remain vigilant, adaptable, and committed to advancing cybersecurity in healthcare for the benefit of all stakeholders.

# Appendix

What is Artificial Neural Network?

<https://www.mit.edu/~kimscott/slides/ArtificialNeuralNetworks_LEAD2011.pdf>

# Acknowledgement

This review paper has given me the experience and knowledge about the topic, hereby I give my appreciation to my parents who helped me throughout my life. And additionally special thanks to the lecturer in charge, Mr. Kanishka Yapa, for his unwavering guidance throughout the duration of this module assignment. Lastly, I would like to express my heartfelt appreciation for the opportunity to work on this report. It has been a truly enlightening and rewarding experience, allowing me to explore the details of deep learning, cybersecurity, and their intersection with healthcare. I am thankful for the knowledge gained and the skills honed throughout this process.

# References

|  |  |
| --- | --- |
| [1] | A. H. R. P. S. R. S. Mohd Javaid, "Towards insighting cybersecurity for healthcare domains: A comprehensive," *Cyber Security and Applications,* p. 13, 2023. |
| [2] | A. K. S. K. P. T. Sita Rani, "Federated learning for secure IoMT-applications in smart healthcare," *Knowledge-Based Systems,* p. 28, 2023. |
| [3] | C. J. Kumar, "New Dangers in the New World: Cyber Attacks in the," *Intersect,* p. 15, 2017. |
| [4] | I. H. Sarker, " A Comprehensive Overview from Neural Network and Deep Learning Perspective," *Deep Cybersecurity,* 2021. |
| [5] | F. A. M. A. F. \*. ,. A. B. Alyazia Aldhaheri, "Deep learning for cyber threat detection in IoT networks:," *Internet of Things and Cyber-Physical Systems,* p. 9, 2024. |
| [6] | G. A. ,. Y. Y. ,. Y. L. Zhenyang Sun, "Optimized machine learning enabled intrusion detection 2 system for internet of medical things," *Franklin Open,* p. 11, 2024. |
| [7] | A. E. A. M. M. H. M. G. Emna Baccour, "Reinforcement learning-based dynamic pruning for distributed inference via explainable AI in healthcare IoT systems," *Future Generation Computer Systems,* p. 17. |
| [8] | Z. C. a. D. B. N. Daniel Zeng, "Artificial intelligence–enabled public health surveillance—from local detection to global epidemic monitoring and control," 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7484813/. |
| [9] | A. e. o. O. I. A. Moatsum alawida, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," 2022. |
| [10] | INTERPOL, "Covid 19 Cybercrime INTERPOL," 2020. |
| [11] | TheHackerNews, "Cybersecurity for Healthcare—Diagnosing the Threat Landscape and Prescribing Solutions for Recovery," FEB 2024. [Online]. Available: https://thehackernews.com/2024/02/cybersecurity-for-healthcarediagnosing.html. |
| [12] | U. D. o. H. a. H. Services, "HEALTHCARE SECTOR CYBERSECURITY," 2022. |
| [13] | N. T. N. E. P. I. R. Sotirios Messinis, "Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review," *Computers in Biology and Medicine,* p. 21, 2024. |
| [14] | P. Hannah T. Neprash, M. Claire C. McGlave, P. Dori A. Cross, P. Beth A. Virnig and M. Michael A. Puskarich, "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," 2022. |
| [15] | O. o. C. a. I. Analysis., "OTENTIAL IMPACTS OF WANNACRY RANSOMWARE ON CRITICAL INFRASTRUCTURE," p. 5, 2017. |
| [16] | A. A. D. J. P. K. S. I. Randhir Kumar, "Digital Twins-enabled Zero Touch Network: A smart contract and explainable AI integrated cybersecurity framework," *Future Generation Computer Systems,* p. 15, 2024. |
| [17] | O. o. t. A. S. f. P. a. Response, "2017-2022 Health Care Preparedness and Response Capabilities," 2022. |
| [18] | A. J. Cartwright, "The elephant in the room: Cybersecurity in healthcare," *Journal of clinical monitoring and computing,* p. 10, 2023. |
| [19] | S. V. B. S.-S. B. ˇ. Samanta Mikuletiˇ, "Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees," *Computers & Security,* p. 14, 2024. |
| [20] | O. o. i. Security, "2022 Healthcare Cybersecurity Year in review, and a 2023 look-ahead," HSS, 2023. |
| [21] | D. o. h. a. h. s. U. Health, "Health Sector Cybersecurity 2021 Retrospective and 2022 look ahead," 2022. |
| [22] | www.thelancet.com/digital-health, "The challenges of cybersecurity in health care: the UK National Health Service as case study," 2019. |

# Author

**Tharindu D. Nanayakkara** ([dilz.nanayakkara@gmail.com](mailto:dilz.nanayakkara@gmail.com)) Currently an undergraduate who follows a B.Sc. Hons. Information Technology degree program specializing in Cybersecurity at Sri Lankan Institute of information technology.

As the first report done on the based topic your feedback will very much appreciated. You can contact Author from his contacts in his website <https://DilzNanayakkara.github.io>.