International Journal of Computer Applications Technology and Research
Volume 11–Issue 09, 01-07, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1109.1001

AI-Driven Cybersecurity Frameworks for Protecting Electronic Health Records Against Ransomware Attacks

Pelumi Oladokun
Department of Computer Science
Southeast Missouri State University
USA

Getrude Alielo Shabiha
Montclair State University
USA

Abstract: In an attempt to improve efficiency and care delivery, the healthcare industry has adopted the digitization of patient data through Electronic Health Records (EHRs). However, due to this digital revolution, EHR systems are becoming more appealing targets for ransomware attacks, which jeopardize patient safety, interrupt clinical operations, and jeopardize data integrity. The purpose of this review is to explore the AI-driven cybersecurity frameworks to prevent ransomware attacks on EHRs. The findings indicate that AI technologies improve cybersecurity by enabling proactive defense tactics, lowering false positives, and offering real-time threat detection. While deep learning models enhance the detection of complex infections, machine learning and behavioural analytics are excellent at spotting unusual activity. Although issues like data privacy concerns, resource needs, and the demand for ongoing system training still exist, integrating AI with conventional security measures may further increase organizational resilience.

Keywords: Healthcare; artificial intelligence; software; cyberattacks; information systems

1. INTRODUCTION

More effective and precise healthcare delivery is now possible due to the substantial changes that have occurred with the digitization of healthcare in terms of the management, access, and storage of medical data (Junaid et al., 2022). Since they offer a streamlined repository for patient data, medical histories, and treatment plans, electronic health records (EHR), have emerged as a key component of this change (Dash et al., 2019; Vos et al., 2020).

Specifically, a thorough store of patient data, including imaging studies, prescriptions, treatment plans, laboratory findings, and medical histories, is made available via these digital records. EHRs facilitate the easy exchange of data between healthcare providers, which improves teamwork and patient outcomes in contrast to conventional paper-based systems. EHR systems also facilitate telemedicine programs, integrate decision-support tools, and expedite administrative procedures, all of which improve the effectiveness and patient-centeredness of healthcare delivery (Ratwani, 2020).

The Information technology breakthroughs and laws encouraging healthcare digitization have fuelled the use of EHRs. However, emerging threats have also been introduced forth by this digital transformation (Junaid et al., 2022). EHRs, which hold protected health information and personally identifiable information, are extremely sensitive in addition to being essential for clinical operations. Therefore, owing to their dual significance, EHRs are a popular target for cybercriminals, especially during ransomware attacks, where losing access to records can have detrimental consequences (Seh et al., 2020; Basil et al., 2022).

In addition to the reliance of the healthcare industry on digital systems and the high value of its data, ransomware assaults are becoming a bigger problem. Malicious malware known as ransomware encrypts data belonging to an organization and prevents access until a ransom is paid, usually in cryptocurrency (Neprash et al., 2022). The healthcare industry is especially susceptible to these attacks because of its dependence on constant access to electronic health records and other digital resources. Ransomware attacks in the healthcare industry have repercussions that go beyond monetary losses. They disrupt critical operations, delay diagnoses and treatments, and, in extreme situations, jeopardize patient lives when EHRs are compromised (Minnaar & Herbig, 2022; (Argaw et al., 2020). Additionally, ransomware tactics have become increasingly complex, emphasizing the urgent need for effective cybersecurity solutions catered to the particular difficulties faced by healthcare systems.

Artificial intelligence (AI) can potentially improve EHR system security in the healthcare industry. In this regard, machine learning algorithms can identify unusual network traffic patterns, like abrupt increases in data encryption activity or unauthorized access attempts, that might point to a ransomware infestation (Murdoch, 2021). By seeing intricate patterns in encrypted communications or file signatures that conventional systems would overlook, deep learning models further improve these capabilities. This review therefore explores the cybersecurity frameworks powered by AI to prevent ransomware attacks on electronic health records.

2. RANSOMWARE THREATS IN HEALTHCARE

Considering its reliance on digital systems, the importance of patient data, and the pressing need for operational continuity, the healthcare sector has grown more appealing as a target for ransomware attacks (Seh et al., 2020). Malicious software known as ransomware is made to encrypt data on a victim's computer, making it unusable until a ransom is paid, typically in cryptocurrency. Such assaults have the potential to have disastrous effects on the healthcare industry, including the interruption of essential services, large financial losses, and jeopardized patient safety (Connolly & Wall, 2019).

Attacks using ransomware against healthcare institutions have become more frequent in recent years. Given that their operations cannot afford extended downtime, hospitals, clinics, and other healthcare providers are often the targets of attacks (Neprash et al., 2022). However, compared to other businesses, reports show that healthcare organizations have some of the highest incidences of ransomware occurrences, and attackers are using more advanced techniques to compromise systems (Connolly et al., 2020).

In addition, social security numbers, insurance information, and medical histories are a few examples of the extremely private and sensitive data that may be found in electronic health records, or EHRs. With regard to the black-market value of this data, fraudsters find healthcare institutions to be an attractive target (Abdulhameed & Al, 2021). Medical data is unchangeable and may have long-term repercussions if disclosed, in contrast to financial data, which can be deleted or changed (such as credit card information). Furthermore, a breach could have a greater impact because healthcare organizations frequently keep a lot of historical documents.

Ransomware attacks have a variety of effects on the healthcare industry. Operationally encrypted systems may result in the interruption of vital services including emergency care, treatment planning, and diagnostics. Patients may be denied prompt care or relocated to other facilities as a result of this interruption, which could have fatal implications and raise rates of morbidity and mortality (Neprash et al., 2022). The financial implications of ransom payments, data recovery, legal liability, and reputational harm are high for healthcare organizations.

Several variables make healthcare systems especially susceptible to ransomware assaults. Many businesses use antiquated legacy systems with weak cybersecurity defenses, which makes them more vulnerable to attack. Additionally, since Internet of Medical Things (IoMT) devices sometimes lack strong security protocols, integrating them expands the attack surface. Human error is also a major factor since ransomware frequently enters systems through social engineering techniques and phishing emails (Argaw et al., 2020).

3. THE EMERGENCE OF RANSOMWARE TECHNIQUES

Techniques used by ransomware have overcome conventional security measures. Advanced persistent threats (APTs), in which attackers infiltrate networks and stay hidden for a long time before releasing ransomware, are a common component of modern attacks. Attackers are increasingly using double extortion tactics, in which they encrypt stolen material and threaten to reveal it (Alawida et al., 2022). Therefore, the pressure on healthcare institutions to abide by ransom demands is increased by these tactics.

The healthcare industry has been severely disrupted globally by ransomware assaults. The 2017 WannaCry assault, which impacted the National Health Service (NHS) in the United Kingdom and resulted in the cancellation of thousands of doctor's appointments, is one such instance (Collier, 2017). Similarly, Universal Health Services in the United States had operational disruptions across institutions due to the 2020 Ryuk ransomware outbreak (Alder, 2020). These illustrations show how urgently improved cybersecurity safeguards in the healthcare industry are needed.

A proactive, multifaceted strategy is needed to mitigate ransomware threats. Businesses need to make investments in strong cybersecurity infrastructure, which includes advanced threat detection tools, frequent security assessments, and staff development initiatives (Cremer et al., 2022). Backup plans are therefore crucial to guarantee a speedy recovery in the case of an attack. Additionally, by examining patterns and spotting irregularities instantly, the combination of AI and machine learning might improve ransomware detection and prevention. Ultimately, healthcare ransomware threats are a serious issue that requires a quick and thorough response. In an increasingly digital environment, healthcare organizations can secure patient data, guarantee operational continuity, and protect lives by comprehending the nature of these threats and establishing effective defenses

3.1 Ransomware Threats on EHR

The effects of ransomware attacks on EHR systems are extensive and significant. The most direct effect is the loss of patient records, which can cause important medical operations to be postponed or stopped entirely (Basil et al., 2022). Clinicians may find it difficult to coordinate care, make accurate diagnoses, or deliver the right therapies if they do not have timely access to EHRs, endangering patient outcomes. If backups or decryption keys are not accessible, ransomware attacks have the potential to permanently destroy critical patient data in addition to causing operational problems (Farringer, 2017). Since compromised data might result in identity theft and data protection violations, the exfiltration of EHR data also presents serious privacy threats. Ransomware attacks also have substantial financial cost, including ransom payments, recovery expenses, and reputational harm, all of which can reduce patient confidence in medical professionals (Yeo & Banfield, 2022).

Specifically, the complexity of contemporary ransomware assaults frequently surpasses the capabilities of healthcare cybersecurity solutions. Static rule-based detection systems, which are the foundation of conventional approaches like firewalls and antivirus software, are ineffective against new threats like polymorphic malware and zero-day vulnerabilities (Beaman et al., 2021; Kapoor et al., 2021). Additionally, these systems produce a lot of false positives, which can overburden security staff and cause them to take longer to respond to real threats. As such, protecting EHR systems from ransomware attacks is made more difficult by the growing interconnectedness of medical devices, many of which were not designed with cybersecurity in mind. Legacy systems, which are common in the healthcare industry, further exacerbate vulnerabilities because they may lack critical updates and patches . Healthcare organizations also frequently struggle with resource constraints, such as limited budgets and a lack of qualified cybersecurity professionals (He et al., 2021; Kapoor et al., 2021).

.

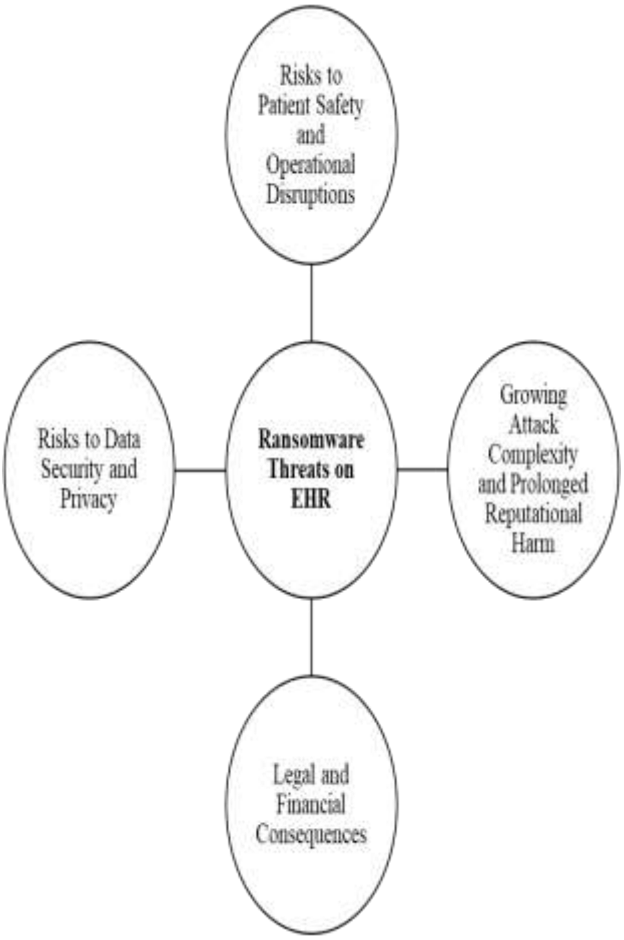
Risks to Patient Safety and Operational Disruptions
Risks to Data Security and Privacy
Ransomware Threats on EHR
Growing Attack Complexity and Prolonged Reputational Harm
Legal and Financial Consequences

Figure 1: Ransomware Threats on EHR

4. ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Artificial intelligence (AI) has become a disruptive force in cybersecurity due to its advanced skills in precisely and quickly detecting, ending, and reacting to cyber threats (Dalal, 2018). The opposite is also true, as cybercrimes and attacks are growing alarmingly due to the rapid advancement of internet technology and systems (Mooney et al., 2022). Therefore. to combat cybercriminal activities, AI-based techniques are required in cybersecurity systems to improve cyberspace security effectively. Table 1 presents a concise overview of AI methods and uses.

Table 1: Synopsis of AI Techniques and Applications in Cybersecurity

AI Techniques	**Description**	**Uses**	**References**
Identifying anomalies	Detects variations in the typical behaviours of systems or networks.	Identifying anomalous network activity, insider threats, and zero-day attacks.	Sarhan & Altwaijry, (2022); Tucker et al., (2016); Khan et al., (2020)
Predictive Analytics	Forecasts possible future risks using historical data.	Identifying weaknesses, foreseeing potential points of attack, and stopping breaches.	Barati & Yankson, (2022); Sarker (2021b)
Natural language processing (NLP)	Evaluates and deciphers speech and text data in the human language.	Recognizing social engineering techniques, identifying phishing emails, and examining threat intelligence data.	Sarker, (2021a); Syafitri et al., (2022); Mittal et al., (2022)
Machine Learning	To forecast or categorize results, algorithms learn from data.	Creating fraud detection, malware classification, and intrusion detection systems.	Yeboah-Ofori, (2020); Akhtar & Feng, (2022)
Deep Learning	Neural networks are used in advanced machine learning to analyze complex data.	Recognizing ransomware, examining file signatures, and identifying encrypted malware.	Urooj et al., (2021);
Automated Threat Intelligence	Combines and evaluates data on global threats to produce insights that can be used.	Prioritization, vulnerability assessment, and real-time threat updates.	Cremer et al., (2022)

Several AI security models, including neural networks, expert systems, machine learning, deep learning, and data mining, can be employed to address threats and assaults successfully. Therefore, developing informed choices in cyberspace is possible with AI-based techniques.

4.1 Artificial Neural Networks (ANNs)

Frank Rosenblatt developed Artificial Neural Networks (ANNs) in 1957 as a statistical learning method that mimics how neurones in the human brain work (Averkin & Yarushev, 2018). ANN is a technology that simulates neurones using a mathematical equation. To generate a goal value, the model reads massive amounts of data. ANNs usually can comprehend, learn, and resolve issues in various fields (Dell'Aversana, 2019). Additionally, it can solve incomplete and noisy data samples. ANNs have been employed in the early warning, prevention, detection, and response phases of the cyber defence system. Due to their versatility, ANNs are highly beneficial in intrusion-detection systems (IDS). ANNs could be utilized in cybersecurity to analyze security traffic flow (Buczak & Guven, 2016; Khraisat et al., 2019). Therefore, by studying traffic flow in security networks, artificial neural networks (ANNs) have the potential to be utilized in cybersecurity to identify breaches before they happen and thwart cyberattacks through perimeter defence (Haddaji et al., 2022).

ANNs have a higher classification rate than manual methods and may identify patterns in extremely nonlinear issues (Sarker, 2021c). ANNs can automatically identify both normal and problematic network patterns using previously sent data over the network. Network security products including firewalls, network hubs, and intrusion detection systems use ANNS to scan network traffic (Ahmad et al., 2022). The Deep Neural Network (DNN) was further described as a more advanced version of ANN that has the added benefit of anticipating future cyberattacks in addition to defending the security system against them (Wu et al., 2020).

4.2 Intelligence Agents

Self-governing systems with an internal decision-making process and a personal goal are known as intelligent agents (IAs). IAs use sensors to assess dangers and actuators to keep an eye on the area, while also regulating the activities until a specific goal is accomplished (Wirkuttis & Klein, 2017). These systems are proactive and responsive and can comprehend and react to changes in their domain when interacting with other autonomous agents. Therefore, intelligent agents can learn from and interact with their surroundings, making them adaptive and successful in thwarting Distributed Denial of Service (DDoS) assaults (Singh & Gupta, 2022).

4.3 Deep Learning (DL) and Machine Learning (ML) Techniques

A subfield of artificial intelligence refers to machine learning that focuses on teaching machines to learn new things and use algorithms to make judgements based on data (Sarker, 2021d). The mathematical methods that enable data extraction, pattern recognition, and inference are all strongly associated with machine learning (Pugliese et al., 2021). Hence, Sarker (2021d) further stated that the two most significant applications of machine learning technology are classification and regression. In this regard, learning is categorized as supervised, unsupervised, semi-supervised, and reinforcement.

5. FRAMEWORKS FOR AI-POWERED CYBERSECURITY

Frameworks for cybersecurity driven by AI are revolutionizing how organizations protect their systems from cyber-attacks. These frameworks improve the capacity to identify, evaluate, and reduce attacks more successfully than conventional systems by utilizing AI. They are especially useful in complicated settings where a breach could have serious consequences, such as healthcare, finance, and vital infrastructure (Manoharan & Sarker, 2022). AI-powered frameworks are essential for protecting sensitive data and preserving system integrity because they provide scalability, agility, and a proactive approach to cybersecurity (Cremer et al., 2022). AI-powered systems are dynamic and able to learn from changing attack patterns, in contrast to existing frameworks that mostly rely on static rules and human monitoring. To offer a complete security solution, these frameworks combine several elements, such as automatic response systems, anomaly detection algorithms, and machine learning models.

5.1 AI Models and Frameworks for Instantaneous Threat Intelligence

Several machine learning models are used by AI-driven threat intelligence to identify and react to threats in real time. The sorts of machine learning models used in cybersecurity and their particular uses in detecting, categorizing, and reducing cyber threats are covered in the sections that follow.

Models of Supervised Learning

Labelled datasets are necessary for supervised learning models to train algorithms that correctly classify threats such as model training on labelled threat data in which supervised learning models learn from historical data by linking particular inputs with known outcomes (Sarker et al., 2020; Mohammed et al., 2016). However, according to Peng et al., (2018), this is especially useful for identifying malware or phishing attack types where attack signatures are already available. Commonly used techniques include decision trees, support vector machines (SVMs), and neural networks. For example, neural networks can analyze the content and sender information of a phishing email, learning to flag emails with suspicious characteristics (Mittal et al., 2022).

Unsupervised and Semi-supervised Learning

Models Unsupervised models are essential for anomaly detection, which is a fundamental component of cybersecurity applications such as clustering and anomaly detection which is a fundamental component of cybersecurity applications: clustering and anomaly detection in which unsupervised models allow for greater flexibility in threat detection because they are not limited to labelled datasets (Goldstein & Uchida, 2016). For instance, clustering algorithms can identify outliers in network traffic, which aids in the detection of patterns suggestive of cyberattacks. Semi-supervised Learning with Limited Labelled Data: Since cybersecurity data frequently lacks thorough labelling, semi-supervised learning enables models to learn from a small set of labelled data along with a greater volume of unlabelled data, improving detection capabilities for unknown threats (Fan et al., 2021).

Natural Language Processing (NLP)

NLP can be used to interpret unstructured data, including threat reports, social media, and cybersecurity forums including text mining for threat intelligence: NLP-based text mining identifies keywords and entities associated with potential attacks in textual data, extracting threat information (Rahman et al., 2020).

6. CONCLUSION

The current healthcare system is becoming more dependent on EHRs, which has improved patient outcomes and efficiency. However, intruders take advantage of the weaknesses brought about by this digital transition, especially through ransomware assaults. In addition to jeopardizing the availability, confidentiality, and integrity of vital patient data, these attacks often interfere with healthcare activities, sometimes with potentially fatal results. outcomes. With a focus on the revolutionary potential of AI-powered cybersecurity frameworks in reducing ransomware threats to EHR systems, this study has examined the role of artificial intelligence (AI) in tackling these issues.

Several important discoveries are highlighted in this research review. Machine learning, deep learning, and natural language processing are examples of AI technologies that improve ransomware attack detection and prevention. These systems are excellent at detecting unusual activity, identifying complex malware, and responding to threats in real time.

Additionally, AI-powered frameworks enable layered and proactive defenses that lessen the impact of ransomware on EHR systems, integrating seamlessly with conventional security measures. AI technologies also enable businesses to efficiently handle enormous volumes of data, which lowers false positives and allow cybersecurity professionals to concentrate on real risks.

Furthermore, certain ramifications for cybersecurity in healthcare include the need for healthcare institutions to urgently implement AI-driven solutions so as to overcome the shortcomings of conventional approaches to ransomware risk mitigation. AI-powered systems' scalability, speed, and agility make them essential for protecting EHRs, especially as the amount and complexity of medical data continue to increase. Similarly, using AI into cybersecurity frameworks for healthcare helps improve adherence to regional mandates and data protection laws. AI can assist businesses in lessening the operational, financial, and reputational effects of ransomware attacks by enabling proactive defenses and automated threat responses. However, problems like data privacy, high resource requirements, and the requirement for qualified staff to manage and maintain AI systems must be addressed for successful deployment.

7. REFERENCE

1. Abdulhameed, I. S., & Al, E. (2021). The Security and Privacy of Electronic Health Records in Healthcare Systems: A Systematic Review. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 1979–1992. https://doi.org/10.17762/turcomat.v12i10.4701
2. Ahmad, I., Ul Haq, Q. E., Imran, M., Alassafi, M. O., & AlGhamdi, R. A. (2022). An Efficient Network Intrusion Detection and Classification System. *Mathematics*, *10*(3), 530. https://doi.org/10.3390/math10030530
3. Akhtar, M. S., & Feng, T. (2022). Malware Analysis and Detection Using Machine Learning Algorithms. *Symmetry*, *14*(11), 2304. https://doi.org/10.3390/sym14112304
4. Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003
5. Alder, S. (2020). *Universal Health Services Ransomware Attack Cripples IT Systems Across United States*. The HIPAA Journal. https://www.hipaajournal.com/universal-health-services-ransomware-attack-cripples-it-systems-across-united-states/
6. Argaw, S. T., Pastoriza, J. R. T., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O’Leary, C., Chauvin, B. E., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/s12911-020-01161-7
7. Averkin, A., & Yarushev, S. (2018). *Evolution of Artificial Neural Networks*. https://libeldoc.bsuir.by/bitstream/123456789/30338/1/Averkin_Evolution.PDF
8. Barati, M., & Yankson, B. (2022). Predicting the Occurrence of a Data Breach. *International Journal of Information Management Data Insights*, *2*(2), 100128. https://doi.org/10.1016/j.jjimei.2022.100128
9. Basil, N., Ambe, S., Ekhator, C., & Fonkem, E. (2022). *Health records database and inherent security concerns: A review of the literature*. Nih.gov. https://pmc.ncbi.nlm.nih.gov/articles/PMC9647912/
10. Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*(1). https://doi.org/10.1016/j.cose.2021.102490
11. Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/comst.2015.2494502
12. Collier, R. (2017). NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal*, *189*(22), E786–E787. https://doi.org/10.1503/cmaj.1095434
13. Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568
14. Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa023
15. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber Risk and cybersecurity: a Systematic Review of Data Availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3). https://doi.org/10.1057/s41288-022-00266-6
16. Dalal, A. (2018). Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity To Improve Detection And Response To Cyber Threats. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *9*(3), 1416–1423. https://doi.org/10.61841/turcomat.v9i3.14670
17. Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: Management, analysis and future prospects. *Journal of Big Data*, *6*(1), 1–25. springer. https://doi.org/10.1186/s40537-019-0217-0
18. Dell’Aversana P. (2019). *ARTIFICIAL NEURAL NETWORKS AND DEEP LEARNING. A SIMPLE OVERVIEW*. https://doi.org/10.13140/RG.2.2.20898.38080/1
19. Fan, C., Liu, Y., Liu, X., Sun, Y., & Wang, J. (2021). A study on semi-supervised learning in enhancing performance of AHU unseen fault detection with limited labeled data. *Sustainable Cities and Society*, *70*, 102874. https://doi.org/10.1016/j.scs.2021.102874
20. Farringer, D. (2017). *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals*. https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2416&context=sulr
21. Goldstein, M., & Uchida, S. (2016). A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data. *PLOS ONE*, *11*(4), e0152173. https://doi.org/10.1371/journal.pone.0152173
22. Haddaji, A., Ayed, S., & Fourati, L. C. (2022). Artificial Intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey. *Computers and Electrical Engineering*, *104*, 108460. https://doi.org/10.1016/j.compeleceng.2022.108460
23. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review

(Preprint). *Journal of Medical Internet Research*, *23*(4). ncbi. https://doi.org/10.2196/21747

24. Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar, G., Abdulkarim, M., Shuaibu, A. N., Garba, A., Sahalu, Y., Mohammed, A., Mohammed, T. Y., Abdulkadir, B. A., Abba, A. A., Kakumi, N. A. I., & Mahamad, S. (2022). Recent Advancements in Emerging Technologies for Healthcare Management Systems: A Survey. *Healthcare*, *10*(10), 1–45. https://doi.org/10.3390/healthcare10101940
25. Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. *Sustainability*, *14*(1), 8. https://doi.org/10.3390/su14010008
26. Khan, M. I., Foley, S. N., & O'Sullivan, B. (2020, November 4). *Database Intrusion Detection Systems (DIDs): Insider Threat Detection via Behavioural-based Anomaly Detection Systems -- A Brief Survey of Concepts and Approaches*. https://doi.org/10.48550/arXiv.2011.02308
27. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1–22. https://doi.org/10.1186/s42400-019-0038-7
28. Manoharan, A., & Sarker, M. (2022). REVOLUTIONIZING CYBERSECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR... *International Research Journal of Modernization in Engineering Technology and Science*, *4*(12), 2151–2164. https://www.researchgate.net/publication/379308659_REVOLUTIONIZING_CYBERSECURITY_UNLEASHING_THE_POWER_OF_ARTIFICIAL_INTELLIGENCE_AND_MACHINE_LEARNING_FOR_NEXT-_GENERATION_THREAT_DETECTION
29. Minnaar, A., & Herbig, F. J. (2022). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica*, *34*(3), 154–185. https://doi.org/10.10520/ejc-crim_v34_n3_a10
30. Mittal, A., Engels, D., Kommanapalli, H., Sivaraman, R., Chowdhury, T., & Chowdhury, T. (2022). Phishing Detection Using Natural Language Processing and Machine Learning. *SMU Data Science Review*, *6*(2), 14. https://scholar.smu.edu/cgi/viewcontent.cgi?article=1215&context=datasciencereview
31. Mohammed, M., Khan, M. B., & Bashier, E. B. M. (2016). Machine Learning. In *Crc Press*. https://doi.org/10.1201/9781315371658
32. Mooney, Z. R. A., Zhang, X., & Crabtree, J. D. (2022). UNDERSTANDING CYBERCRIME: A THREE-GENERATION APPROACH. *Issues in Information Systems*, *23*(3). https://doi.org/10.48009/3_iis_2022_103
33. Murdoch, B. (2021). Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era. *BMC Medical Ethics*, *22*(1). https://doi.org/10.1186/s12910-021-00687-3
34. Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum*, *3*(12), e224873. https://doi.org/10.1001/jamahealthforum.2022.4873
35. Peng, T., Harris, I., & Sawa, Y. (2018). *Detecting Phishing Attacks Using Natural Language Processing and Machine Learning*. IEEE Xplore. https://doi.org/10.1109/ICSC.2018.00056
36. Pugliese, R., Regondi, S., & Marini, R. (2021). Machine learning-based approach: Global trends, research directions, and regulatory standpoints. *Data Science and Management*, *4*, 19–29. Sciencedirect. https://doi.org/10.1016/j.dsm.2021.12.002
37. Rahman, M. R., Mahdavi-Hezaveh, R., & Williams, L. (2020). A Literature Review on Mining Cyberthreat Intelligence from Unstructured Texts. *2020 International Conference on Data Mining Workshops (ICDMW)*. https://doi.org/10.1109/icdmw51313.2020.00075
38. Ratwani, R. M. (2020). Electronic Health Records and Improved Patient Care: Opportunities for Applied Psychology. *Current Directions in Psychological Science*, *26*(4), 359–365. https://doi.org/10.1177/0963721417700691
39. Sarhan, B. B., & Altwaijry, N. (2022). Insider Threat Detection Using Machine Learning Approach. *Applied Sciences*, *13*(1), 259. https://doi.org/10.3390/app13010259
40. Sarker, I. H. (2021a). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, *Springer*. https://www.academia.edu/45623331/AI_Driven_Cybersecurity_An_Overview_Security_Intelligence_Modeling_and_Research_Directions
41. Sarker, I. H. (2021b). Data Science and Analytics: an Overview from Data-Driven Smart Computing, Decision-Making and Applications Perspective. *SN Computer Science*, *2*(5). Springer. https://doi.org/10.1007/s42979-021-00765-8
42. Sarker, I. H. (2021c). Deep Learning: a Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. *SN Computer Science*, *2*(6). Springer. https://doi.org/10.1007/s42979-021-00815-1
43. Sarker, I. H. (2021d). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, *2*(3), 1–21. Springer. https://doi.org/10.1007/s42979-021-00592-x
44. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1). https://link.springer.com/article/10.1186/s40537-020-00318-5
45. Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), 133. NCBI. https://doi.org/10.3390/healthcare8020133
46. Singh, A., & Gupta, B. B. (2022). Distributed Denial-of-Service (DDoS) Attacks and Defence Mechanisms in Various Web-enabled Computing Platforms. *International Journal on Semantic Web and Information Systems*, *18*(1). https://doi.org/10.4018/ijswis.297143
47. Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, *10*, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594
48. Tucker, J., Coughlan, M., Nelson, T., & Klimkowski, B. (2016). Implementing an Anomaly-Based Intrusion Detection System: Focus on Internal Threat -Masquerade Attacks. *American International Journal of Contemporary Research*, *6*(4).

https://aijcrnet.com/journals/Vol_6_No_4_August_2016/1.pdf

49. Urooj, U., Al-rimy, B. A. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2021). Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions. *Applied Sciences*, *12*(1), 172. https://doi.org/10.3390/app12010172
50. Vos, J. F. J., Boonstra, A., Kooistra, A., Seelen, M., & van Offenbeek, M. (2020). The influence of electronic health record use on collaboration among medical specialties. *BMC Health Services Research*, *20*(1), 1–11. https://doi.org/10.1186/s12913-020-05542-6
51. Wirkuttis, N., & Klein, H. (2017). *Artificial Intelligence in Cybersecurity. Cyber, Intelligence, and Security, 1, 103-119. - References - Scientific Research Publishing*. Scirp.org. https://www.scirp.org/reference/referencespapers?referenceid=3617952
52. Wu, Y., Wei, D., & Feng, J. (2020). Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey. *Security & Communication Networks*, 1–17. https://doi.org/10.1155/2020/8872923
53. Yeboah-Ofori, A. (2020). Classification of Malware Attacks Using Machine Learning In Decision Tree. *International Journal of Security (IJS)*, *11*(2), 10–25. https://repository.uwl.ac.uk/id/eprint/8022/1/IJS-155.pdf
54. Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*, *19*(Spring), 1i. https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/