AI-Driven Solutions for Enhancing Cybersecurity in Healthcare Systems: A Comprehensive Review

Thangaraj Petchiappan
Chief Technology Officer -SIMS
iLink Digital

ABSTRACT

As healthcare businesses face more and more cyber hazards as a result of digital technology's increasing integration into healthcare systems, cybersecurity is taking on more significance. This analysis looks at how AI may improve cybersecurity in the healthcare industry. AI technologies, such as ML, DL, and NLP, have become effective instruments for identifying, evaluating, and reducing cyber threats. The study demonstrates the efficacy of AI applications in cybersecurity, including automated incident response, anomaly detection, and predictive maintenance, in protecting sensitive patient data and guaranteeing the provision of essential healthcare services. Additionally, a paper discusses the regulatory frameworks that govern healthcare data security, including HIPAA and GDPR, which further emphasize the need for robust cybersecurity solutions. By exploring the current landscape of AI-driven cybersecurity challenges with solutions, this review aims to provide insights into best practices, emerging trends, and future directions for research and implementation in healthcare cybersecurity.

Keywords

Cybersecurity and AI-driven solutions in cybersecurity, AI-driven solutions for Cybersecurity in Healthcare Systems, Challenges.

1. INTRODUCTION

The whole of the methods and tools used to protect networks, software, and data against threats is known as cybersecurity [1][2]. There are cyber defence mechanisms accessible at the network, data, host, and application levels [3]. In order to detect security breaches and thwart assaults, some cybersecurity instruments, such as firewalls, IDS, intrusion protection systems, etc., are always in use at both ends [4][5]. The development of IoT networks has made cybersecurity more crucial than before[6]. Numerous security risks may affect computer networks, including the IoT [7]. Furthermore, in addition to being safeguarded against external threats, the system must also be secured against internal risks, which include abuse of authorised access by individuals or those who work for the company[8].

Criminals are always on the lookout for vulnerabilities in healthcare systems, making cybersecurity of all personal information, financial data, social security numbers, and contact details important[9][10]. The pandemic has made many hospitals, research facilities, and healthcare facilities vulnerable; thus, businesses should have a modern, albeit complex, cybersecurity strategy. Healthcare is facing new cybersecurity threats as a consequence of digital transformation[11][12]. A growing number of major players in the healthcare sector are putting their faith in a wider range of technologies, including public cloud services and mobile applications [13]. While the advantages are clear, new cybersecurity risks are emerging as a consequence of the increasing complexity of the computer environment [14][15]. The healthcare industry has heavily relied on cybersecurity measures to provide the utmost patient safety in several healthcare environments. In the last decade, cybersecurity has been all over the news due to the growing number of threats and the determined efforts of hackers to evade authorities[16][17]. Hackers have enhanced their methodologies despite the fact that the initial motivations for conducting cyberattacks have generally remained consistent over time. The identification and prevention of evolving threats using conventional cybersecurity instruments is becoming increasingly challenging. The advancement of AI methodologies provides cybersecurity professionals with the opportunity to prepare for the constantly changing threat posed by assailants [18].

Biomedical applications and medical AI systems use AI, which is based on "data acquisition, ML, and computing infrastructure," to gradually revolutionise medical practice [19][20]. AI has already been implemented in significant disease areas, including neurology, cardiology, and cancer [21]. AI has the "transformative potential" of a technological revolution comparable in magnitude to the industrial revolution [22][23]. In this change, "the provision of healthcare services in resource-poor settings" is being addressed, and of particular interest is the potential to address health system challenges by using AI and other developing technologies that complement one another [24].

This review paper aims to evaluate AI-driven solutions for enhancing cybersecurity in healthcare systems, analysing their applications in detecting, preventing, and responding to cyber threats. The growing prevalence of cyber risks that endanger patients' privacy and safety, in tandem with the healthcare industry's increasing dependence on digital technology, is driving this research. As recent data breaches highlight vulnerabilities in the sector, there is a critical need for effective cybersecurity measures. By exploring the potential of artificial intelligence in fortifying healthcare systems against cyberattacks, this paper seeks to inspire organisations to adopt innovative strategies that safeguard sensitive health information and maintain trust in digital healthcare services.

Organization of the paper

The following paper is structured as follows: Sections II and III provide the Overview of cybersecurity and the Overview of AI-driven cybersecurity; Section IV gives the AI-driven cybersecurity in healthcare systems; Section V discusses the AI-driven challenges and solutions for cybersecurity in healthcare systems; Section VI provides the. Literature Review and Section VII summarised the Conclusion and Future Scope.

2. OVERVIEW OF CYBERSECURITY

Cybersecurity refers to the system of measures put in place to safeguard information systems and cyberspace itself against threats that might compromise the integrity of de jure and de facto property rights [25][26]. Naturally, the word "cybersecurity" necessitated that we provide a level of security that allows regular people to communicate with businesses over a network or the internet. It may be deployed using a variety of tackles and castoff procedures. Some Types of cybersecurity threats are as follows, shows in Figure 1 [27]:

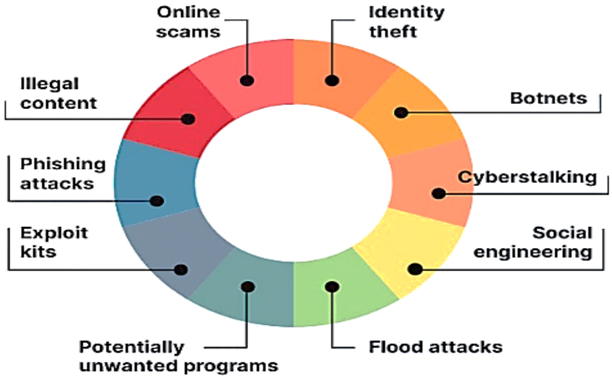

Fig. 1. Types of cyber attacks

- Phishing is the practice of disseminating phoney emails that seem to be from reliable sources. The objective is to negotiate sensitive information like as login credentials and credit card information.
- Ransomware Malicious software falls under this category. To make money, one must first pay in order to have access to records or the computer system. No assurance of data recovery or system restoration will be provided by paying the ransom.
- Malware A system's security may be compromised or unauthorised access gained by using this software.
- Social engineering, in conjunction with the aforementioned pressures, may make you more likely to click on links, spread malware, or believe in a malevolent cause.

A. Some techniques to improve cybersecurity:

There are some techniques to improve cybersecurity are as follows[28]:

- **Access control and "password security":** The usage of a login and password is a basic method of data assurance. It might be the most important step for cybersecurity.
- **Data's Authentication:** The papers that must be reliably verified before to transmission. The "antivirus" software that comes with most devices checks these data. Consequently, it is also essential to have good "antivirus" software to protect the devices from infections.
- **Anti-virus software:** It is a computer program that recognises, steers clear of, and takes action to damage or remove harmful software applications, such as viruses and worms.
- **Malware scanners:** The program in question is a virus scanner that checks all of the system's files and folders for malicious code. Examples of "malicious software" that often assemble and are referred to as malware include viruses, worms, and Trojan horses.
- **Firewall:** An item of hardware or "software program" that aids in the detection and prevention of computer viruses, malware, and worms of all kinds that attempt to infect computers over the Internet. Nowadays, the firewall is a must for all data going to or from the internet.

3. OVERVIEW OF AI-DRIVEN IN CYBERSECURITY

AI has developed into a cornerstone of computer science, with an emphasis on utilising sophisticated mathematical algorithms to mimic human thought processes. AI is revolutionising cybersecurity by augmenting human capabilities to meet the challenges of an intensifying threat landscape[29]. AI technologies like ML, neural networks, and NLP are enabling security systems to detect, analyse, and respond to emerging dangers with unprecedented speed, scale, and accuracy[30][31]. Whereas legacy tools rely on simple signatures and rules, AI introduces data-driven adaptability and autonomy to keep pace with attackers' increasing creativity and persistence. The radical potential of AI has spurred extensive cybersecurity research and increased real-world deployments.

B. Applications of AI in Cybersecurity:

Investigate the Applications of AI in Cybersecurity are as follows[32]:

- The many uses of AI in cybersecurity, including threat detection, vulnerability assessment, incident response, and predictive analysis, should be carefully investigated.
- Look at real-world examples, studies, and applications to show how AI is being used to strengthen cybersecurity and lessen the impact of cyberattacks.
- In order to shed light on the ever-changing cyber defence scenario, it is important to identify important trends, new technology, and creative ways in AI-driven cybersecurity.

C. Efficacy and Impact of AI in Cybersecurity

Evaluate the Use and Effect of AI in Cybersecurity:

- Assess how well AI-powered cybersecurity solutions reduce cyber risks, protect digital assets, and maintain cyberspace's integrity.
- Combine the results of studies in analysing effectiveness, adaptability and reliability of the AI based solutions to cybersecurity issues while considering data, opinions of experts and tendencies in the IT industry.
- Identify the best and worst practices associated with cybersecurity frameworks and their future potential and vulnerabilities.

D. The Role of AI and ML in Cybersecurity

The cybersecurity analysis process is greatly enhanced by AI and ML. It has the ability to analyse server logs, network traffic, and other disparate data points from an organisation's digital infrastructure in order to reveal hidden dangers. Most importantly, it can process this data more meticulously and within a shorter time than human analysts could by applying complex formulas. Organisations may improve their strategic response by comprehending the context and complexity of the attack vectors thanks to this thorough study. The response to security issues may be further automated using AI and ML.

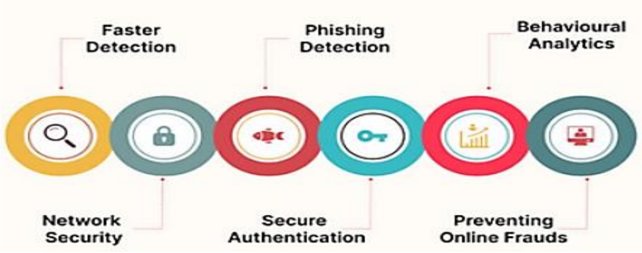

Fig. 2. AI in cybersecurity

Figure 2 outlines the key areas where artificial intelligence (AI) is being used to enhance cybersecurity. Here's a breakdown of each element:

- **Faster Detection:** The real-time analysis of such large data sets, as capability of most AI algorithms ensures the quick identification of potential risks like threats, weaknesses, diseases among others. This speed is important in order to intercept the attacks before they begin to inflict a lot of harm.

- **Phishing Detection:** Machine learning is capable of understanding the body of an email and the behaviour of senders to flag phishing emails. Phishing attempts may have a much lower success rate because of this.

- **Behavioral Analytics:** AI can monitor a user's behaviours and look for changes that may suggest that the system has been compromised. For instance, attempts to login, or any pattern of data that needs more scrutiny could be flagged.

- **Network Security:** The traffic of networks could be monitored and analysed by an AI to look for ab norms – more specifically, events such as attempts at unauthorised access or acts of malware. This helps in a battle against different forms of cyber threats in a network.

- **Secure Authentication:** Applying biometric data, for instance, fingerprints, face, or recognising behaviour patterns, AI might enhance the methods of users' authentications and control the identity of a user. This could enhance security by often reaching it unprohibited users to achieve pedestal to systems.

- **Preventing Online Frauds:** AI can receive transaction information, identify certain trends, and inform about possible fraud, thus aiding in the detection of online fraud. Companies and individuals could gain from it since it lessens the chances of losing money.

In general, and as seen in AI's role in machine learning and cyber threat detection, AI is slowly assuming an essential role in strengthening cybersecurity.

Machine learning (ML) computer science is a subfield of AI that focuses on teaching computers to do tasks automatically via the development of algorithms and statistical models [33][34]. There are essentially three types of ML techniques used in the field of cybersecurity: supervised and unsupervised learning, respectively.

- Supervised learning is a technique in which a model is trained on a dataset that already contains the matching output labels (y) and input data (X). Learning about a mapping function f that approximates f(X) y is the aim [35].

- Datasets without labelled responses are the domain of unsupervised learning methods, as opposed to supervised learning. Finding the underlying structure inside a set of data points is the goal. An important part of cybersecurity is the use of clustering and anomaly detection.

To automate the detection of cyber threats, DL-enhanced defence mechanisms are being used more and more in cybersecurity as DL is a component of ML. These systems are constantly changing and becoming more effective over time [36][37]. The input, hidden, and output layers make up DL's fundamental architecture; the exact number of layers depends on the computational layers' AI models, including ANNs and DNNs[38].

E. Benefits of AI in Cybersecurity

These benefits of AI in cybersecurity are as follows:

- **High data capacity:** An important advantage of AI is its high data processing capacity, which enables the offloading of tiresome data analysis, review procedures, and 24/7 security monitoring without compromising security.

- **Learning over time:** Cybersecurity software may improve itself over time by learning from its mistakes and other experiences, thanks to ML and DL. With this kind of learning capability, cybersecurity apps can see patterns and make associations between historical events and current threat data. Additionally, DL algorithms can monitor trends and patterns in passwords in order to detect weak or readily guessable passwords and notify the appropriate staff.

- **Improved threat detection:** When cybersecurity solutions that are driven by AI provide constant monitoring of networks and devices. Some of the threat response steps may take time, and time is a critical factor, so steps like blocking malicious traffic, isolation of infected devices, and imparting notifications can all be done by AI.

- **Improved threat detection:** Continuous network and device monitoring by cybersecurity systems driven by AI allows them to spot possible threats or indications of compromise instantly. It can automate threat response procedures like banning distasteful traffic, isolating devices, and sending out notices, which can be efficient or decrease contaminated data.

- **Better user experience:** Customer satisfaction is the end aim, and automated monitoring, incident response, and troubleshooting may help get you there. As a result of the use of generative AI, customer support is getting new tools for feedback collection, such as interactive chat choices.

4. AI-DRIVEN FOR CYBERSECURITY IN HEALTHCARE SYSTEMS

AI is starting to play a significant role in healthcare, from organising medical activities and diagnosing patients to developing new medications. Numerous medical data sets may be analysed by AI methods like ML and DL to identify trends and make predictions. Healthcare cybersecurity should be a top priority for every company operating in the medical field, including insurance, pharmaceutical, biotech, and medical device operations. In addition to ensuring that medical services are available, medical systems and equipment are operating properly, patient data confidentiality and integrity are maintained, and industry rules are followed, it entails a number of steps to safeguard organisations from both internal and external cyberattacks.

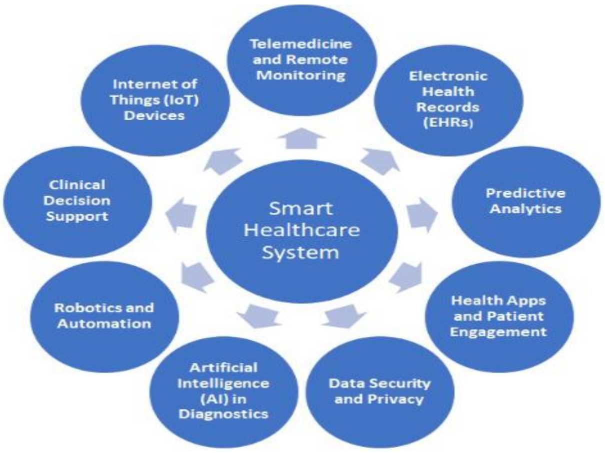
Telemedicine and Remote Monitoring
Electronic Health Records (EHRs)
Predictive Analytics
Health Apps and Patient Engagement
Data Security and Privacy
Artificial Intelligence (AI) in Diagnostics
Robotics and Automation
Clinical Decision Support
Internet of Things (IoT) Devices
Smart Healthcare System

Fig. 3. Applications of Smart Healthcare System

A smart healthcare system's essential elements are shown in Figure 3. The core component of the system is the Smart Healthcare System, which combines many technologies to improve the quality of healthcare. Surrounding the central component are several interconnected elements: IoT devices allow for the collecting and analysis of data in real time, while telemedicine and remote monitoring allow for the remote treatment and monitoring of patients. EHRs allow for the digital preservation of a comprehensive patient medical history. It is the intention of clinical decision support systems to assist medical professionals in making decisions based on evidence. Predictive Analytics utilises data patterns to forecast future health outcomes. Robotics and Automation streamline processes and tasks within healthcare settings. Patients may take an active role in their treatment and see better results with the help of health apps and other patient engagement tools. Artificial Intelligence (AI) in Diagnostics aids in the diagnosis and treatment of diseases. Data Security and Privacy ensure the protection of sensitive patient information. Together, these components work synergistically to create a more efficient, effective, and personalised healthcare experience.

F. AI-Driven Threat Detection in Healthcare

AI offers unique capabilities for identifying and mitigating cyber threats that traditional methods cannot match. As cyber threats to healthcare systems have evolved in sophistication, the use of effective cyber analysis has become the bread and butter of robust cybersecurity practices [39]. Key AI technologies employed in healthcare data security include:

1) Predictive Maintenance and Anomaly Detection:

The use of AI in healthcare facilities for anomaly detection and predictive maintenance is a recurrent subject in the literature. Using ML, scientists have developed models that can foresee when machinery will break down and identify any suspicious patterns in energy use [40].

2) Natural Language Processing (NLP):

NPL is another branch of AI that compels computers to understand and even read human speech. Applications in the healthcare sector include medical research, clinical documentation, and correspondence with the patient. Further, NLP may be adopted in developing artificial assistants such as virtual assistants and chatbots in the management of patient's health.

3) Machine Learning:

It depends on inference and patterns from data. Using historical patient data, ML algorithms are used in forecasting their prognosis and disease evolution alongside the response to treatment so as to guide treatment and resource utilisation. Healthcare professionals may identify high-risk patients and put preventative measures in place by using ML algorithms to divide patient groups according to risk profiles. Use of ML in healthcare

- Disease prediction and treatment
- Medical imagery and testing services
- Developing and discovering novel medicines

4) Deep Learnings:

Includes multi-layer neural networks that excel in extracting complex representations and patterns from data. Image types such as X-rays, MRIs, and CT scans are analysed using DL algorithms, in particular CNNs. T helps diagnose and accurately detect patterns related to different medical conditions[41].

G. Regulations of Healthcare on AI Cybersecurity

These are the organisations to protect personal data are as follows:

- **The Health Insurance Portability and Accountability Act (HIPAA):** Physicians are required by a clearly defined Security Rule to safeguard patients' electronically stored, protected health information. The regulations mandate that the doctors apply the proper technological, administrative, and physical precautions to guarantee the security, confidentiality, and integrity of this data. Any healthcare provider that sends health information electronically is subject to the HIPAA Security Rule.
- **The General Data Protection Regulation (GDPR):** It is the world's most robust privacy and security legislation. It guarantees that businesses properly handle and preserve personally identifiable information (PII).

H. Benefits of AI for Cybersecurity in Healthcare

There are some benefits to enhancing cybersecurity in healthcare systems, as follows:

- **Gather information more quickly:** The use of wearable technology is assisting healthcare personnel in collecting real-time data that ML algorithms may subsequently assess and learn from. For a similar rationale, the FDA has been trying to integrate ML and AI into software for medical goods. The massive demand for healthcare diagnosis has resulted in an abundance of data.
- **Research and development of new drugs at a faster pace:** Combining deep learning with machine learning allows researchers to build models that can more accurately predict which medicinal molecules will be beneficial. The discovery of novel pharmaceuticals is accelerated as a result of this.
- **Cost-Effective Methods:** Appointments for patients, data searches within electronic health records, and other duties can all be handled by machine learning algorithms. The ability to concentrate on more vital problems allows healthcare staff more autonomy.
- **A Tailored Solution:** ML technology can analyse large datasets to aid doctors in developing personalised medicine therapies for their patients. By using ML

algorithms to forecast how patients would respond to certain drugs, doctors may better anticipate their patients' requirements [42].

5. AI-DRIVEN CHALLENGES AND SOLUTIONS FOR CYBERSECURITY IN HEALTHCARE SYSTEMS

Enhancing cybersecurity in healthcare systems through AI involves addressing several challenges and implementing various solutions. Here's a detailed overview:

Table I. Challenges and Solutions for Cybersecurity in Healthcare Systems through AI

Challenges	Description	Solutions	Benefits
Data Sensitivity and Privacy	Healthcare data is subject to strict regulations (e.g., HIPAA), making compliance crucial.	Implement AI-powered threat detection for compliance monitoring.	Enhances compliance with regulations and protects sensitive data.
Complex IT Infrastructure	Legacy systems and diverse technologies complicate security efforts.	Use AI to integrate legacy systems with modern cybersecurity solutions.	Streamlines security management across platforms.
Insider Threats	Employees may unintentionally or maliciously compromise data security.	Employ behavioural analytics to detect anomalies in user actions.	Identifies potential insider threats before they escalate.
Evolving Threat Landscape	Cyber threats are continuously evolving, requiring adaptive security measures.	Apply predictive analytics to forecast and mitigate potential security incidents.	Proactively addresses emerging threats.
Limited Resources	Many healthcare organisations lack sufficient cybersecurity personnel and funding.	Automate security processes using AI to optimise resource allocation.	Increases efficiency and reduces manual effort.
False Positives	High rates of false positives can lead to alert fatigue and missed real threats.	Enhance machine learning algorithms to minimise false alarms.	Improves the accuracy of threat detection.
Integration and Interoperability Issues	Ensuring compatibility between new AI solutions and existing systems can be challenging.	Develop AI-driven solutions that facilitate interoperability.	Simplifies deployment and enhances overall security posture.
Automated Incident Response	Delays in response can exacerbate the impact of security breaches.	Implement automated incident response systems for rapid threat mitigation.	Reduces response time and limits damage from breaches.
Enhanced Authentication Mechanisms	Traditional authentication methods may be insufficient against modern threats.	Utilise AI for advanced authentication methods like biometrics and behavioural recognition.	Strengthens access controls and reduces unauthorised access.
Regular Security Assessments	Continuous monitoring is essential for identifying vulnerabilities.	Conduct ongoing security assessments using AI tools for threat intelligence.	Maintains an up-to-date security posture.
Education and Training	Staff awareness is critical in preventing security incidents.	Leverage AI to create personalised training programs for employees.	Enhances cybersecurity awareness and reduces human error.
Collaboration and Information Sharing	Lack of shared threat intelligence can hinder effective security measures.	Foster collaboration among healthcare organisations for shared threat intelligence.	Strengthens collective security efforts and knowledge sharing.
Data Encryption and Masking	Protecting sensitive data is essential, especially during breaches.	Automate data encryption and masking with AI for data protection.	Safeguards sensitive information even in the event of a breach.
Compliance Automation	Manual compliance processes are time-consuming and error-prone.	Use AI to streamline compliance processes and automate audits.	Improves compliance efficiency and reduces risks of non-compliance.

Table I comprehensively outlines the key challenges healthcare systems face in enhancing cybersecurity, the corresponding AI-driven solutions, and the benefits of implementing these solutions. Healthcare organisations may greatly enhance their cybersecurity posture and safeguard sensitive patient data by using effective solutions to solve these concerns.

6. LITERATURE REVIEW

This section provides a literature review on AI-driven solutions for Cybersecurity in Healthcare Systems; summary is shown in Table II.

This paper, ElSayed, Elsayed and Bay, (2024) presents an innovative architecture that utilises ML specifically to rectify and lessen security flaws in healthcare-related IoT devices. Proactively monitoring and detecting potential threats, the proposed architecture uses advanced convolution ML architecture to safeguard sensitive healthcare information, reduce costs, and increase portability in healthcare and emergency settings. The results of the experiments show that various kinds of attacks may be predicted with an accuracy of up to 93.6%. Using the CICIoT2023 dataset, the findings demonstrate a tenfold reduction in cost and a simulation of zero-day detection accuracy[43].

The paper, Sabillon and Barr, (2024) outlines the structure of CSAM 2.0 in detail, including its architecture. CSAM 2.0 has undergone testing, implementation, and validation in research scenarios. The study concludes by demonstrating that the validation of the CSAM 2.0 model provides valuable insights for future decision-making, enabling organisations to address cybersecurity weaknesses and enhance their cybersecurity domains and controls[44].

The paper, Sangwan, (2024) suggests a middle way that embraces both technology and human supervision and explores the connection between technological advances and human behaviour. In the end, it finishes with some recommendations for enhancing cybersecurity awareness by pointing out policy implications, educating particular audiences, and sharing good practices. For successful combating of cyber threats, the study emphasises the need for an integrated strategy that synchronises human actions, corporate values, technological innovations, and legislative systems[45].

This paper, Rajamäki et al., (2024) presents a master's program titled "Managing Digital Transformation in the Health Sector" (ManagiDiTH) jointly implemented by universities in four different countries. The innovative master's program includes 3 focus areas- health sector skills, societal skills and digital skills.

The ManagiDiTH programme integrates cybersecurity education into a broader framework of digital transformation skills for health professionals with interconnectedness of cybersecurity and healthcare innovation. The programme emphasises practical learning through hands-on exercises and case studies, allowing students to apply cybersecurity principles to real-world healthcare scenarios[46].

In this paper, Pirbhulal, Abie and Shukla, (2022) IoT-based healthcare cybersecurity is improved with the help of DT technology, which is utilised to build a new automated conceptual framework. It entails conceptualising and analysing the proposed framework that might provide an adaptive and dynamic security solution for healthcare systems that rely on the IoT to identify vulnerabilities and threats in real time[47].

This study, Ugwu et al., (2022) found that the most common forms of healthcare data breaches are hacking and IT incidents, followed by unauthorised access and disclosures, in order to determine the main causes of these breaches. Given the many significant implications of this work for future discoveries, additional thorough research is thus important to confirm the results. The reliability of the dataset under analysis affects all of the findings[48].

This paper, Mohamed et al., (2023) investigates the potential of digital twins to improve several facets of healthcare systems via the use of engineering methods and results. The paper delves into the difficulties faced by healthcare systems engineers and how digital twins can alleviate some of those difficulties. It then goes on to build a theoretical framework for how to use digital twins to enhance healthcare systems engineering procedures and results, and it concludes by discussing the possibilities of using digital twins to accomplish healthcare systems engineering's objectives. The implications of this utilisation are also briefly discussed in the article, along with future goals for digital twin research and development in healthcare systems engineering[49].

Table 2. Literature Review Summary for AI-Driven Solutions for Enhancing Cybersecurity in Healthcare Systems

Ref	Focus	Challenge	Methodology	Key Findings	Limitations	Future Work
[43]	Security enhancement of IoT devices in healthcare	Security vulnerabilities in IoT healthcare devices	Convolution ML architecture, CICIoT2023 dataset	Achieved 93.6% accuracy in detecting attacks and reduced costs by 10x	Security vulnerabilities in IoT healthcare devices	Improve generalisation across various datasets, real-time performance
[44]	Comprehensive cybersecurity audits in multiple domains	Cybersecurity auditing across diverse domains	Audits in cybersecurity domains, including governance, risk, and technology	Demonstrated effectiveness in addressing cybersecurity weaknesses	Cybersecurity auditing across diverse domains	Develop broader applications of CSAM 2.0 across industries
[45]	Cybersecurity awareness and policy integration	Cybersecurity auditing across diverse domains	Exploration of human-technology synergy, policy recommendations	Emphasised need for integrated human, corporate, technological, and legislative approaches	Balancing technological advancements and human supervision	Further study of the impact of policy recommendations
[46]	Cybersecurity education in digital healthcare transformation	Integrating cybersecurity into digital transformation in health	Master's program integrating health, societal, and digital skills with cybersecurity	Practical learning in cybersecurity for healthcare professionals	Integrating cybersecurity into digital transformation in health	Expanding to more countries, developing more case studies
[47]	Testing in real-world healthcare environments	Real-time threat detection and dynamic security in IoT healthcare	Development of DT-based adaptive security for IoT healthcare	Provided an adaptive solution to identify real-time threats	Real-time threat detection and dynamic security in IoT healthcare	Testing in real-world healthcare environments
[48]	Healthcare data breach prevention and understanding	Predominance of hacking/IT incidents in healthcare data breaches	Analysis of healthcare data breach reports	Identified major factors leading to healthcare breaches	Predominance of hacking/IT incidents in healthcare data breaches	Deeper investigation and validation of breach factors
[49]	Use of digital twins for healthcare systems engineering	Challenges in Healthcare Systems Engineering processes	Conceptual framework for using digital twins in healthcare systems	Showed potential for improving healthcare systems engineering with digital twins	Challenges in Healthcare Systems Engineering processes	Future research on the impact and scalability of digital twins

7. CONCLUSION AND FUTURE SCOPE

The primary focus of this review paper is, therefore, to present a comprehensive literature review of AI approaches for enhancing healthcare cybersecurity. Last but not least, organisations within the healthcare sector where they deal with a vast number of threats have a revolutionary aspect available by integrating AI in the line of securing their corporate network. Over time, AI technologies allow for recognising potential cyber threats on their own and preventing them from compromising the security level of patient data and disrupting the continuity of healthcare services. The efficacy of patient care applications using AI, including predictive analytics, the ML algorithm, and the DL model, is a reason why healthcare institutions should embrace advanced tools as cybersecurity measures. Also, treating patients' information as MIPAACT and GDPR compliant is critical to avoiding compromises on patient data confidentiality and integrity. Since the healthcare sector is on its way to becoming more digitalised, further research and development to secure AI systems from cyber threats will be critical. Me, this review shows that healthcare stakeholders should pay much attention to using AI for cybersecurity purposes to protect patients' data and ensure people's trust in the digital healthcare space.

8. REFERENCES

[1] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Commun. Surv. Tutorials*, 2016, doi: 10.1109/COMST.2015.2494502.

[2] S. A. and A. Tewari, "Security Vulnerabilities in Edge Computing: A Comprehensive Review," *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 936–941, 2022.

[3] S. Bauskar, "A Review on Database Security Challenges in Cloud Computing Environment," *Int. J. Comput. Eng. Technol.*, vol. 15, pp. 842–852, 2024, doi: 10.5281/zenodo.13922361.

[4] S. Arora and P. Khare, "AI/ML-Enabled Optimization of Edge Infrastructure: Enhancing Performance and Security," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, pp. 230–242, 2024.

[5] N. Richardson, V. K. Yarlagadda, S. K. R. Anumandla, and S. C. R. Vennapusa, "Harnessing Kali Linux for Advanced Penetration Testing and Cybersecurity Threat Mitigation," *J. Comput. Digit. Technol.*, vol. 2, no. 1, pp. 22–35, 2024.

[6] J. Thomas, K. V. Vedi, and S. Gupta, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–879, 2021.

[7] V. V. Kumar, A. Sahoo, S. K. Balasubramanian, and S. Gholston, "Mitigating healthcare supply chain challenges under disaster conditions: a holistic AI-based analysis of social media data," *Int. J. Prod. Res.*, 2024, doi: 10.1080/00207543.2024.2316884.

[8] P. Podder, S. Bharati, M. R. H. Mondal, P. K. Paul, and U. Kose, "Artificial Neural Network for Cybersecurity: A Comprehensive Review," 2021.

[9] P. Khare, "Enhancing Security with Voice : A Comprehensive Review of AI-Based Biometric Authentication Systems," vol. 10, no. 2, pp. 398–403, 2023.

[10] S. S. Pranav Khare, "Enhancing Biometric Authentication: Deep Learning Models For Human Iris Recognition," *Int. J. Creat. Res. Thoughts*, vol. 11, no. 8, pp. h148–h153, 2023.

[11] P. Khare, "Signature-Based Biometric Authentication: A Deep Dive Into Deep Learning Approaches," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 04, no. 08, pp. 2414–2424, 2022.

[12] Sahil Arora and Apoorva Tewari, "Fortifying Critical Infrastructures: Secure Data Management with Edge Computing," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 2, pp. 946–955, Aug. 2023, doi: 10.48175/IJARSCT-12743E.

[13] S. Bauskar, "Advanced Encryption Techniques For Enhancing Data Security In Cloud Computing Environment," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 05, no. 10, pp. 3328–3339, 2023, doi: : https://www.doi.org/10.56726/IRJMETS45283.

[14] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends," *Cyber Secur. Appl.*, vol. 1, no. February, 2023, doi: 10.1016/j.csa.2023.100016.

[15] S. S. Gopalan, A. Raza, and W. Almobaideen, "IoT Security in Healthcare using AI: A survey," *ICCSPA 2020 - 4th Int. Conf. Commun. Signal Process. their Appl.*, vol. 2021-January, pp. 1–6, 2021, doi: 10.1109/ICCSPA49915.2021.9385711.

[16] S. Arora and P. Khare, "THE IMPACT OF MACHINE LEARNING AND AI ON ENHANCING RISK-BASED IDENTITY VERIFICATION PROCESSES," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 06, no. 05, pp. 8246–8255, 2024.

[17] R. Goyal, "EXPLORING THE PERFORMANCE OF MACHINE LEARNING MODELS FOR CLASSIFICATION AND IDENTIFICATION OF FRAUDULENT INSURANCE CLAIMS," *Int. J. Core Eng. Manag.*, vol. 7, no. 10, 2024.

[18] S. Taheri and N. Asadizanjani, "An Overview of Medical Electronic Hardware Security and Emerging Solutions," *Electronics (Switzerland)*. 2022. doi: 10.3390/electronics11040610.

[19] J. Thomas, K. V. Vedi, and S. Gupta, "Artificial Intelligence and Big Data Analytics for Supply Chain Management," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 06, no. 09, 2024, doi: DOI : https://www.doi.org/10.56726/IRJMETS61488.

[20] J. Thomas, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 9, 2021.

[21] J. Thomas, P. Patidar, K. V. Vedi, and S. Gupta, "Predictive Big Data Analytics For Supply Chain Through Demand Forecasting," *Int. J. Creat. Res. Thoughts*, vol. 10, no. 06, pp. h868–h873, 2022.

[22] R. Tandon, "Face mask detection model based on deep CNN techniques using AWS," *Int. J. Eng. Res. Appl.*, vol. 13, no. 5, pp. 12–19, 2023.

[23] K. R. V. K. Raghunath Kashyap Karanam, Dipakkumar Kanubhai Sachani, Vineel Mouli Natakam, Vamsi Krishna Yarlagadda, "Resilient Supply Chains: Strategies for Managing Disruptions in a Globalized Economy," *Am. J. Trade Policy*, vol. 11, no. 1, pp. 7–16, 2024.

[24] P. Radanliev and D. De Roure, "Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2)," *Health Technol. (Berl).*, 2022, doi: 10.1007/s12553-022-00691-6.

[25] A. P. A. S. and N. Gameti, "Digital Twins in Manufacturing: A Survey of Current Practices and Future Trends," *Int. J. Sci. Res. Arch.*, vol. 13, no. 1, pp. 1240–1250, 2024.

[26] R. Goyal, "Software Development Life Cycle Models: A Review Of Their Impact On Project Management," *Int. J. Core Eng. Manag.*, vol. 7, no. 2, pp. 78–87, 2022.

[27] A. Alshehri, N. Khan, A. Alowayr, and M. Y. Alghamdi, "Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics," *Comput. Syst. Sci. Eng.*, 2023, doi: 10.32604/csse.2023.026526.

[28] M. Sonntag, "Cyber security," *IDIMT 2016 - Inf. Technol. Soc. Econ. Strateg. Cross-Influences - 24th Interdiscip. Inf.*

Manag. Talks, vol. 10, no. 2, pp. 313–323, 2016, doi: 10.4324/9781315753393-25.

[29] V. K. Y. Nicholas Richardson, Rajani Pydipalli, Sai Sirisha Maddula, Sunil Kumar Reddy Anumandla, "Role-Based Access Control in SAS Programming: Enhancing Security and Authorization," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 6, no. 1, pp. 31–42, 2019.

[30] V. K. Yarlagadda and R. Pydipalli, "Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity," *Eng. Int.*, vol. 6, no. 2, pp. 211–222, 2018.

[31] R. Goyal, "THE ROLE OF REQUIREMENT GATHERING IN AGILE SOFTWARE DEVELOPMENT: STRATEGIES FOR SUCCESS AND CHALLENGES," *Int. J. Core Eng. Manag.*, vol. 6, no. 12, pp. 142–152, 2021.

[32] N. G. Camacho, "The Role of AI in Cybersecurity: Addressing Threats in the Digital Age," *J. Artif. Intell. Gen. Sci. ISSN3006-4023*, vol. 3, no. 1, pp. 143–154, 2024, doi: 10.60087/jaigs.v3i1.75.

[33] H. Sinha, "An examination of machine learning-based credit card fraud detection systems," *Int. J. Sci. Res. Arch.*, vol. 12, no. 01, pp. 2282–2294, 2024, doi: https://doi.org/10.30574/ijsra.2024.12.2.1456.

[34] H. Sinha, "Benchmarking Predictive Performance Of Machine Learning Approaches For Accurate Prediction Of Boston House Prices : An In-Depth Analysis," *ternational J. Res. Anal. Rev.*, vol. 11, no. 3, 2024.

[35] H. Sinha, "Predicting Employee Performance in Business Environments Using Effective Machine Learning Models," *IJNRD - Int. J. Nov. Res. Dev.*, vol. 9, no. 9, pp. a875–a881, 2024.

[36] A. P. A. Singh, "Best Practices for Creating and Maintaining Material Master Data in Industrial Systems," vol. 10, no. 1, pp. 112–119, 2023.

[37] H. Sinha, "Advanced Deep Learning Techniques for Image Classification of Plant Leaf Disease," *J. Emerg. Technol. Innov. Res. www.jetir.org*, vol. 11, no. 9, pp. b107–b113, 2024.

[38] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, *Advancing cybersecurity: a comprehensive review of AI-driven detection techniques*, vol. 11, no. 1. Springer International Publishing, 2024. doi: 10.1186/s40537-024-00957-y.

[39] S. Arefin, "Strengthening Healthcare Data Security with Ai-Powered Threat Detection," vol. 12, no. 10, pp. 1477–1483, 2024, doi: 10.18535/ijsrm/v12i10.ec02.

[40] V. Dinesh, R. Kalli, and E. Jonathan, "AI-Driven Energy Management Solutions for Healthcare: Optimizing Medical Device Software [1]," *Int. J. Adv. Eng. Technol. Innov.*, vol. 01, no. 01, p. 1, 2023.

[41] D. A. Ramalingam, D. A. Karunamurthy, D. T. Amalraj Victoire, and B. Pavithra, "Impact of Artificial Intelligence on Healthcare: A Review of Current Applications and Future Possibilities," *Quing Int. J. Innov. Res. Sci. Eng.*, vol. 2, no. 2, pp. 37–49, 2023, doi: 10.54368/qijirse.2.2.0005.

[42] H. Narne, "AI-DRIVEN SOLUTIONS FOR HEALTHCARE : IMPROVING DIAGNOSTICS AND TREATMENT," vol. 12, no. 1, pp. 1295–1307, 2021.

[43] Z. ElSayed, N. Elsayed, and S. Bay, "A Novel Zero-Trust Machine Learning Green Architecture for Healthcare IoT Cybersecurity: Review, Analysis, and Implementation," in *SoutheastCon 2024*, 2024, pp. 686–692. doi: 10.1109/SoutheastCon52093.2024.10500139.

[44] R. Sabillon and M. Barr, "Planning and Conducting Cybersecurity Audits to Assess the Effectiveness of Controls," in *2024 IEEE International Systems Conference (SysCon)*, 2024, pp. 1–6. doi: 10.1109/SysCon61195.2024.10553588.

[45] A. Sangwan, "Human Factors in Cybersecurity Awareness," in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, 2024, pp. 1–7. doi: 10.1109/ISCS61804.2024.10581139.

[46] J. Rajamäki, P. Rathod, J. C Ferreira, O. Ahonen, C. Serrão, and M. do Carmo Gomes, "Enhancing Cybersecurity Education for the Healthcare Sector: Fostering Interdisciplinary ManagiDiTH Approach," in *2024 IEEE Global Engineering Education Conference (EDUCON)*, 2024, pp. 1–7. doi: 10.1109/EDUCON60312.2024.10578769.

[47] S. Pirbhulal, H. Abie, and A. Shukla, "Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, pp. 1–5. doi: 10.1109/VTC2022-Spring54318.2022.9860581.

[48] A. O. Ugwu, X. Gao, J. O. Ugwu, and V. Chang, "Ethical Implications of AI in Healthcare Data: A Case Study Using Healthcare Data Breaches from the US Department of Health and Human Services Breach Portal between 2009-2021," in *2022 International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC)*, 2022, pp. 343–349. doi: 10.1109/IIoTBDSC57192.2022.00070.

[49] N. Mohamed, J. Al-Jaroodi, I. Jawhar, and N. Kesserwan, "Leveraging Digital Twins for Healthcare Systems Engineering," *IEEE Access*, vol. 11, pp. 69841–69853, 2023, doi: 10.1109/ACCESS.2023.3292119.