International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-13, Issue-6, November 2025
DOI: https://doi.org/10.55524/ijircst.2025.13.6.5
Article ID IJIRE-1412, Pages 37-47
www.ijircst.org

Artificial Intelligence for Cybersecurity in Healthcare Systems: A Simple Review of Applications, Challenges, and Future Directions

Gnanesh Methari[1], Yawar Hayat[2], and Abdullah Mazharuddin Khaja[3]

[1] Department of Information Technology (Cybersecurity), Franklin University, Columbus, United States
[2] AI Healthcare Researcher, Institute of Business Administration, Karachi, Pakistan
[3] MS Scholar, Department of Computer Science, Governors State University, University Park, IL, United States

Correspondence should be addressed to Ganesh Methari; Metharignanesh770@gmail.com

Received: 30 October 2025 Revised: 13 November 2025 Accepted: 27 November 2025

ABSTRACT- There is increased implementation of digital systems in healthcare. Medical centers accumulate a considerable amount of patient information in database systems and computers. This data is sensitive. Hackers can steal or destroy it. Cybersecurity is, therefore, extremely critical in healthcare.

Healthcare systems may be made safer with the help of Artificial Intelligence (AI). Threats can be detected, attacks averted and rapid response provided by AI. Machine learning, deep learning, and anomaly detection are some of the AI techniques. The AI can be used to secure patient records, hospitals networks and medical devices.

AI also has challenges. Patient information confidentiality is a major issue. AI may lack adequate good data in hospitals. AI systems are subject to attack by hackers. Using AI can be costly. Legal and ethical issues, such as patient consent, are also present.

AI can also ensure the security and power of healthcare in the future. It can be assisted by new AI technologies, superior systems, and clear policies. This review examines the AI applications in healthcare cybersecurity, issues it experiences, and future actions.

KEYWORDS: Artificial Intelligence, Cybersecurity, Healthcare, Machine Learning, Data Security

I. INTRODUCTION

Healthcare is changing fast. There is increased usage of digital tools in hospitals, clinics, and health systems [1]. Electronic Health Records (EHRs), medical devices, and web platforms assist physicians and nurses to work quicker and make care superior. The patients can obtain their records online and doctors are able to share information at a quick pace. Healthcare becomes more efficient under the influence of digitalization, and it is not deprived of risks.

One big risk cyberattacks. Cybersecurity refers to the act of securing computers, networks, and data against hackers or destruction. Cybersecurity is quite significant in the healthcare sector as patient information is highly confidential [2]. In case hackers steal or modify such data, it may damage patients and destroy confidence in hospitals. Healthcare cyberattacks may consist of ransomware, phishing, malware, and medical device attacks. The threats to hospitals continue to increase since they store a lot of sensitive data, as well as many connected devices.

Artificial Intelligence (AI) develops as one of the enhancing tools to enhance cybersecurity. AI can be trained on data and be able to detect anomalous activities that are potentially indicative of attacks [3]. Some AI techniques applied in the field of cybersecurity are machine learning, deep learning, and anomaly detection. AI can assist hospitals to identify threats quicker, preserve patient documents, and guard medical equipment. Another way AI can minimize security issues is through human error that causes security issues.

Application of AI in healthcare cybersecurity is not easy. There are challenges. The good data required by AI to do well in hospitals are large [4]. Hackers can attack AI systems. There are issues of privacy, ethical and legal concerns. Artificial intelligence can also be expensive and might require one to possess special technical skills. Irrespective of these shortcomings, AI has enormous potential to transform healthcare systems into safer and more robust.

This literature review examines the application of AI in healthcare cybersecurity. It describes the key uses of AI, the issues encountered and future trends. Another aspect that the paper brings to the fore is the ability of AI to safeguard hospital networks, patient information, and medical devices. This is since it aims to provide the researchers, healthcare professionals and policy makers with a clear picture of the role of AI in healthcare security.

This review is limited to research and examples of hospitals, healthcare networks, and medical equipment. It discusses the forms of AI applied, the advantages of AI in cybersecurity, the risks and challenges, and future suggestions. Legal, ethical, and technical issues of AI implementation in healthcare are also addressed in the review.

This paper will demonstrate that AI can be used to prevent cyberattacks in hospitals and enhance patient safety by analyzing the applications and issues of AI. It also indicates the research gaps and where further research should be done. In general, the present review provides a concise yet clear picture of the present scenario and further opportunities of AI in healthcare cybersecurity.

II. OVERVIEW OF CYBERSECURITY IN HEALTHCARE

A. Digital Healthcare and Cyber Risks

The healthcare systems are filled with numerous digital devices that store, share, and process patient information. They are computer systems, server systems, mobile applications, and Internet of Things (IoT) devices [5]. Due to this reason, hospitals are exposed to numerous cyber threats. Cyberattacks may damage patients, halt hospital work, and lead to loss of money [6]. It is beneficial to know the primary categories of threats so that hospitals can plan more protection.

Cybersecurity refers to ensuring computer systems and information is secure against attacks. This is highly significant in the medical field since patient information is confidential and classified. In the case of a cyberattack in a hospital, essential medical services, patient damage, and destroyed trust can be halted.

Recent statistics indicate that data breach has been among the gravest cybersecurity threats in the healthcare industry.

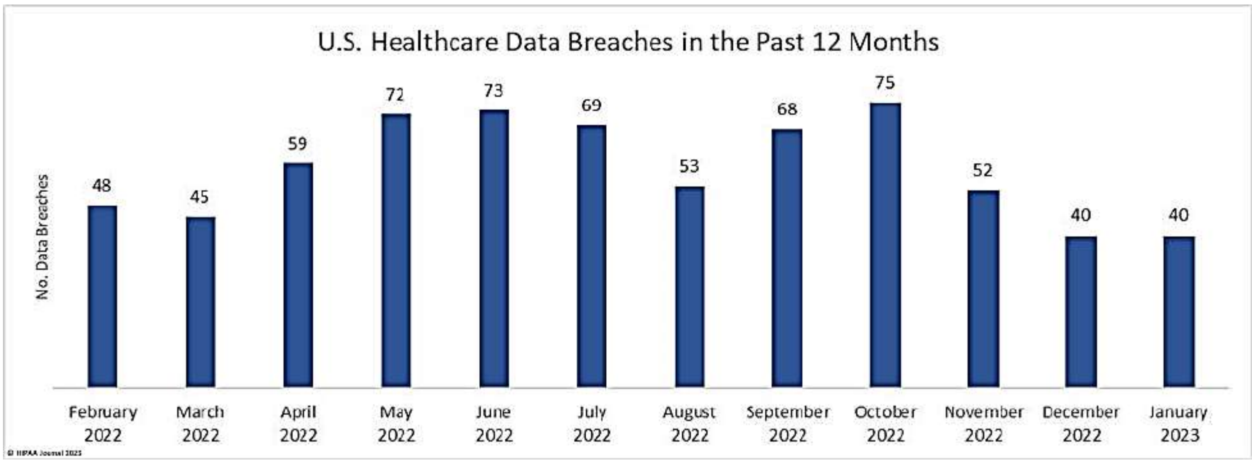

Figure 1: Number of Reported Data Breaches in the U.S. Healthcare Sector

The chart (see the Figure 1) displays the number of the data breaches reported in the American healthcare sector for 12 months. The breaches vary every month with some months reporting more incidences than others. The maximum number of breaches was in October 2022 with 75 incidents, and the minimum was 45 incidents in March 2022. This trend indicates the ongoing fight to ensure patient information is not stolen by hackers and insiders. Although there is an increase in digital security systems, the healthcare organizations remain under significant threat due to the increased adoption of electronic health records and the interconnected digital devices. Statistics indicate the significance of ensuring that cybersecurity is tightened and awareness is created to ensure that patient information is not compromised.

B. Common Cyber Threats in Healthcare

Ransomware is one of the threats that are common. The attack is used to lock the computers or data present in the hospital until money is paid to hackers [7]. It can prevent the doctor from looking at the patient records and postponing treatment. In others, hospitals have spent huge sums of money on recovering their systems. Phishing is the other significant threat. Hackers use fake emails or messages to deceive the staff to give out passwords or even trust in harmful links. These attacks are prevalent since they aim at human error.

Breach of data is also a huge issue. In the event of a patient record theft by hackers, the information may be sold away or be used in identity theft [8]. Health data of individuals would fetch a lot in the black market. Another vulnerability is IoT. Most medical equipment such as heart monitors or insulin pumps is set up on the internet. Unless these are secure, they can be used or misapplied by hackers.

In addition to damaging hospitals, patient safety and trust are also affected by these attacks. One cyberattacks is able to bring down operations, loss of data and diminished confidence among the population. See the below Table 1.

Table 1: Healthcare Cybersecurity Threats and Impacts

Threat Type	Impact on Healthcare	Example/Case Study
Ransomware	Stops access to patient data; delays treatment	WannaCry attack on UK's NHS (2017) caused hospital shutdowns
Phishing	Steals passwords and spreads malware	Fake "COVID-19 update" emails in US hospitals
Data Breach	Leaks patient records and personal data	Anthem Health breach (2015) exposed 78 million records
IoT Vulnerability	Lets hackers control medical devices	Insulin pump hack (2019) showed safety risks

C. Cybersecurity Rules and Laws

To safeguard patient information, most countries have special regulations and legislation.

The health insurance portability and accountability act (HIPAA) is a law in the United States that safeguards patient data [9]. It informs hospitals on the way to protect electronic data, as well as what they must do in case of a data breach.

The General Data Protection Regulation (GDPR) is a regulation in Europe that regulates the use and sharing of personal data, including health data (GDPR, 2018). It provides patients with increased power over their data.

There are also privacy laws in other countries. These policies are aimed at ensuring patient data security. However, most hospitals, particularly the small one's struggle to keep up with all the regulations. Others do not have a big budget or sufficient trained personnel to handle security systems.

D. Traditional Cybersecurity Methods

Various ways of protecting systems are used in hospitals. These are firewalls, antivirus programs, passwords and network monitoring [10]. These are used to prevent numerous attacks. However, contemporary cyber threats are becoming more intelligent and sophisticated.

Conventional ways have their boundaries. They frequently find out about attacks only when they take place. People must be taken up to update or check systems manually. This is time consuming and can fail to detect threats that are fast moving.

In addition, human error is the subject of numerous attacks today. As an illustration, a hectic nurse can open fake mail unknowingly. This form of error cannot be completely prevented by any software.

E. The Need for Smarter Protection

Due to these issues, hospitals are seeking more intelligent ways out. One of the new tools that has been most effective in cybersecurity is artificial intelligence (AI). The AI is able to draw conclusions on the data, identify suspicious trends, and alarm hospitals in advance [11]. It is also capable of identifying and preventing attacks earlier than human beings.

The best thing to do before implementing AI in any comprehensive way is to know the efficiencies of the existing methods and their weaknesses as well. This assists in strengthening systems in the future.

Effective cybersecurity in healthcare is not technological only. It concerns the safety of individuals, their information and their belief in healthcare.

III. ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Artificial Intelligence (AI) refers to the application of computers to think and learn as humans. AI will be able to learn information, identify trends, and make conclusions independently [12]. In cybersecurity, AI assists in identifying and preventing attacks at a rapid rate compared to human beings. It is also able to make use of the previous events and enhance its performance.

AI can be highly valuable in healthcare since hospitals receive numerous digital data daily. Human beings cannot easily look at every piece of information and discover risks [13]. AI can perform this task fast and more efficiently. It can monitor all activities within the system and investigate anything suspicious that can indicate an attack. This renders AI a significant component of the safety of healthcare systems.

A. Types of Artificial Intelligence Used in Cybersecurity

The various types of AI to defend digital systems exist. Machine Learning, Deep Learning, and Natural Language Processing are the most prevalent ones.

Machine Learning (ML) assists computers in learning based on the previous information. It researches the appearance of normal activity and then identifies anything out of the ordinary [14]. To illustrate, when a hacker attempts to penetrate the system, ML can tell that it is an abnormality.

Machine Learning is a more developed type of Deep Learning or DL. It applies numerous layers of algorithms which are referred to as neural networks [15]. It can identify sophisticated patterns of attacks which simple systems are unable to detect. Deep Learning is frequently applied to detect malware or other new threat categories.

Natural Language Processing or NLP assists computers in comprehending human language. It has the ability to read emails, messages and any other text [16]. NLP can be implemented to detect phishing emails aimed at deceiving hospital employees into providing passwords or clicking malicious links.

All these forms of AI co-exist and make systems more robust. They assist hospitals to safeguard their networks, patient records and medical equipment against various forms of attacks.

B. AI Applications in Cybersecurity

There are numerous ways AI can be applied in cybersecurity. Raising intrusion is one of its primary applications. Artificial intelligence can monitor the hospital networks around the clock and alert when a person is attempting to access the premises without authorization [17]. It gets to know what normal traffic is and alerts in case of anything different.

Anomaly detection is also done with the help of AI. This implies that it detects abnormalities that are not in line with the usual patten [18]. As an illustration, when a doctor logs in but the account is in the foreign country, the AI system will consider this as a potential threat. Malware detection is another useful application of AI. Malware refers to bad code that has the potential of corrupting computers in the hospital. AI can read files and code to detect any hidden malware and prevent its destructive effects. It is even able to identify new malware that has never been encountered.

Phishing attacks can also be identified with the help of AI. AI can detect suspicious messages by reading emails and analyzing language. It can prevent these messages and guard the staff against viewing them. The future threats can also be predicted with the help of AI. Through old attacks it can alert hospitals to weak areas in their systems. This assists hospitals to resolve issues in advance of an actual attack.

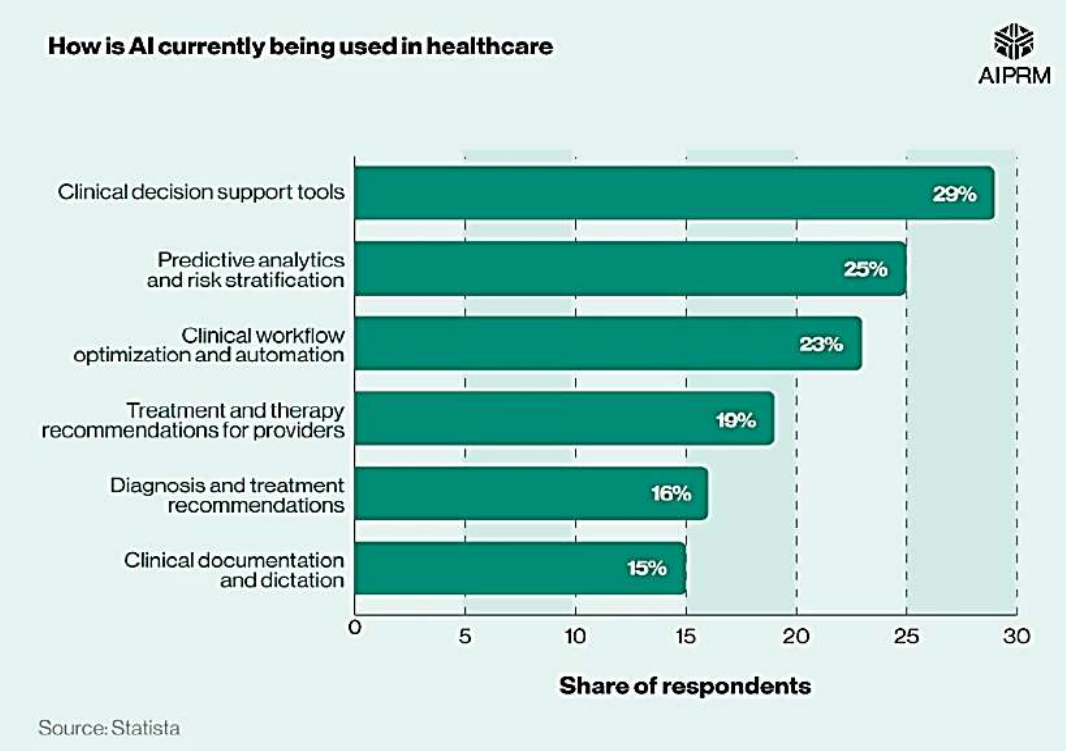

Figure 2: Current Uses of Artificial Intelligence in Healthcare

The above graph (see the above Figure 2) demonstrates the current use of AI in the healthcare sector. Clinical decision support tools (29%), that assist doctors in making more medical choices, have the highest percentage of use. In the second place, there are predictive analytics and risk detection (25%), which will assist in identifying the potential health issues at an early stage. Others are workflow automation (23 percent), treatment advice (19 percent) and diagnosis support (16 percent). A minor proportion (15%) make clinical documentation by AI.

This graph (Figure 2) demonstrates that AI already performs numerous functions in healthcare. The same AI techniques may be applied in enhancing cybersecurity. Predictive analytics and automation can be used as an example to identify and prevent cyber threats before they can cause damage. See the below Table 2.

Table 2: AI Techniques Used in Cybersecurity

AI Technique	Application in Cybersecurity	Advantages
Machine Learning	Detects unusual patterns and intrusions	Learns from data and improves accuracy
Deep Learning	Finds complex threats and malware	Handles large data and detects new attacks
Natural Language Processing	Detects phishing and fake emails	Understands and analyzes human language
Reinforcement Learning	Adjusts to changing threats	Learns from feedback and improves decisions
Neural Networks	Analyzes large security data sets	Finds hidden and complex attack patterns

C. Advantages of AI Over Traditional Methods

Traditional cybersecurity systems are less intelligent and fast than AI. The old systems will usually require individuals to verify data manually. They further respond when an attack occurs. Artificial intelligence is capable of operating in real-time and identifying problems before they get critical.

AI is able to within a short time study large volume of data. It is also able to make fewer errors than humans since it will adhere to data patterns rather than making guesses [19]. Each new attack teaches AI, and thus, it keeps up to date. It does not get tired or distracted; hence it is able to look at systems every time.

Human error is also minimized by AI. A lot of cyberattacks occur due to minor errors of individuals like clicking on a counterfeit email. Such emails can be prevented before they visit the user by AI. By doing so, AI is useful in ensuring that people work safely [20].

The other benefit is that AI is capable of identifying upcoming attacks. It does not merely solve the existing issues but also cautions on what will transpire next. This gives the hospitals early preparation and protection of the systems.

D. Challenges in Using AI

Although AI is highly potent, there are issues with it. AI requires much quality data to learn. It might cause the AI to make incorrect decisions in case the data is not good [21]. Hackers may also attempt to interfere with the AI system itself and deceive it.

Artificial intelligence is costly to develop and maintain. They require talented individuals to operate them. Not every hospital, particularly the small ones, can afford to deploy AI because of the lack of budget and specialists [22]. Privacy and ethical issues are also present due to the necessity of AI that requires massive amounts of sensitive data.

AI is now an important tool in cybersecurity. It helps hospitals detect, stop, and prevent attacks more quickly and more accurately. Machine Learning.

Natural Language Processing, and Deep Learning can be used to safeguard healthcare data. Although AI presents certain challenges, it is more secure when compared to the traditional approaches. It assists hospitals in maintaining patient information secure and establishing more reliable and dependable systems in the future.

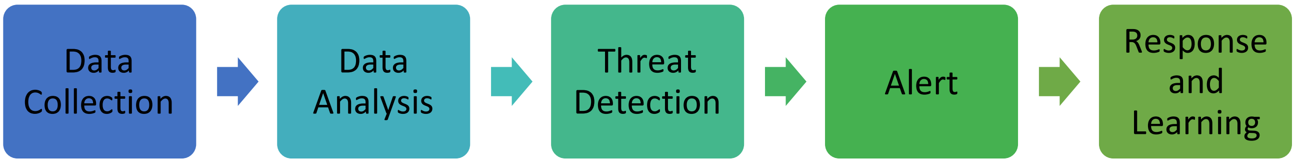

Figure 3: How AI is used to aid cybersecurity

In the above Figure 3, it shows how AI is used to aid cybersecurity in simplified form (Beginning with data collection, followed by data analysis, identifying threats, generating notifications, and then acting and learning to better the subsequent protection).

IV. APPLICATIONS OF AI IN HEALTHCARE CYBERSECURITY

A. *AI in Electronic Health Record (EHR) Protection and Access Control*

All patient data are contained in Electronic Health Records (EHRs) including medical history, testing data, and treatment plan [23]. These records are not only extremely important, but they are also a primary target of cyberattacks. This data is frequently targeted by hackers in order to make money or harm. One of the largest challenges of healthcare cybersecurity is the protection of EHR systems.

AI is very influential in the foreboding of EHRs. It is able to be tracked on who is accessing patient data and the frequency. In case the system detects ab normal access patterns, a warning can be sent. As an illustration, when an employee accesses excessive patient files that he or she does not need, AI will consider it a potentially threatening indicator.

There is access control as well, which is assisted by AI. The traditional systems apply predetermined rules such as passwords or ID cards. However, AI has the potential to make things even safer by obtaining a knowledge of how users act [24]. It examines average time of log in, gadgets, and place of location. In case something is suspicious, AI may prohibit it or request additional checks.

AI is also useful in eliminating errors. Numerous data breaches occur due to the fact that employees accidentally press on fraudulent links or other information they can share. AI can identify these activities and prevent them in the real time.

To summarize, AI can ensure the security of EHR by monitoring the actions of users, identifying suspicious actions, and stopping the misuse of information before it can occur. This provides hospitals with improved control and confidence in their digital systems.

B. *AI for Securing IoT Medical Devices*

Internet of Things (IoT) medical devices are currently becoming common in many hospitals. They are heart monitors, infusion pumps, and smart scanners that are connected to the internet [25]. These gadgets provide the healthcare with increased speed and ease, but they also result in new security threats. They can be used by hackers to gain access to the network of hospitals or steal information.

AI assists in keeping these devices safe through watching all their activities. It is able to identify a suspicious behavior on a device. As an illustration, AI will be aware when a monitor transmits excessive data or connects to an unknown IP. The weak devices that require software updates can also be detected by AI systems. The IoT devices often fail to update on a regular basis and this makes them easy targets [26]. AI can analyze each device and inform about the ones which require maintenance.

The other application of AI is in the management of devices in large numbers. One of these large hospitals may contain thousands of IoT devices. Humans cannot check every one of them. This can be done automatically using AI. It is able to monitor device performance, identify failure as well as preventing attacks before expanding.

To illustrate, in case one IoT sensor becomes infected with malware, AI will be able to exclude it off the network. This prevents the proliferation of the attack to other systems. IoT AI-based protection assists hospitals in maintaining security of patients as well as medical systems. It minimizes chances of data theft and device malfunction which may save lives in cases of emergency [27].

C. *Threat Detection in Healthcare Networks*

Healthcare networks are very complex. They are attached to computers, IoT devices, databases and communication systems [28]. Each of the connections can be a point of entry of the attackers. The conventional systems are prone to react to an attack. The internal changes involve AI identifying threats in the initial stages.

Real time network tasks are monitored by AI systems. They get to know what the normal behaviour looks like and learn about patterns that seem to be abnormal. To illustrate, in the cases when the data started to lose the network during the odd hours, AI can announce it, consequently, a possible case of data theft.

AI has the capacity to identify all sorts of threats such as ransomware or phishing attack or insider attack. In ransomware, the attackers block the hospital information and demand money [29]. The artificial intelligence can recognize the first signs, such as the uncharacteristic encryption of files or the unknown software which is running within the systems.

The second significant problem is phishing. AI can scan all incoming emails and identify the false emails, which seek to defraud employees. It authenticates the details of the sender, writing style, connections to message.

Network traffic analysis can also be performed by use of AI. It analyses the data flow between devices. An AI will raise an alarm whenever a new connection has been identified or excessive data flow where it is not, are detected [30]. The short response is what allows the hospitals to react within a short period, limit the damage and recover within a short period. With AI, healthcare networks will be more secured and impervious to any attacks on both old and new.

D. Case Studies of AI Tools in Hospitals

AI tools have become standard in various hospitals throughout the world to enhance cybersecurity. These instances demonstrate the way AI is truly changing things.

A popular example is the Mayo Clinic in the US. It employs AI-based security software to secure patient records and identify threats on the network [31]. The AI will be able to process millions of points of data each day and prevent cyberattacks before their proliferation.

Cleveland Clinic is also another example of using AI to monitor IoT devices. The system scans all devices that are connected to the system, identifies weak points and automatically blocks suspicious activities (Clinic, 2024). This has minimized breaches of data as well as making devices dependable.

The systems used in the United Kingdom to detect ransomware threats are AI-based in the National Health Service (NHS) [32]. In 2017, following a major attack (WannaCry), smarter AI monitoring tools were introduced by the NHS. These tools are now able to identify suspicious behavior much earlier and prevent it before it gets into the patient records [33].

These practical examples demonstrate that AI does not only enhance security but also assists hospitals to save time and money. They demonstrate that AI use in cybersecurity is able to secure patients, as well as, data, and the entire healthcare system.

E. Integration of AI with Cybersecurity Frameworks

AI is only effective in a comprehensive cybersecurity infrastructure. A framework is an organized strategy that has rules, tools and actions that are used to safeguard systems. The frameworks applied in most hospitals include NIST (National Institute of Standards and Technology) or ISO/IEC 27001 (NIST, 2025).

These frameworks can be enhanced with the help of AI that enhances risk detection and response. Indicatively, in the NIST model, it includes five steps namely identify, protect, detect, respond and recover. AI can help at each step. It has the capability to detect weak points within the system, secure data by controlling access to it, detection of attacks, real-time response to attack summing up to preventing the threat and learning through the experience of the event.

AI tools are also able to mingle across-systems information. This assists in forming one image of the security health of the hospital [34]. It enables the management to make decisions to be made better and enhance the strategy as time goes by.

Compliance with other healthcare regulations, including HIPAA and GDPR, which demand is a high-security protection of patient data, is also supported by integrating AI. Hospitals can fulfill these standards with the help of AI, which automates security checks and reports.

AI will become an inherent component of any cybersecurity framework of health care in the future. It will not only respond to attacks but also anticipate and other attacks automatically. See the below Table 3.

Table 3: AI Applications in Healthcare Cybersecurity

Application Area	AI Tool/Method	Example/Outcome
EHR Protection	Machine Learning for behavior monitoring	Detects unusual access to patient records
IoT Device Security	Deep Learning and anomaly detection	Finds device failures and stops attacks early
Network Threat Detection	AI-based intrusion detection	Blocks ransomware and phishing in real time
Hospital Case Study	AI security analytics tool	Used by Mayo Clinic to prevent cyberattacks
Framework Integration	AI with NIST and ISO models	Improves detection, response, and recovery

Due to the extensive adoption of AI, healthcare systems have started to be more secure. It protects patient data, IoTs and hospital networks. There is also AI that can help hospitals respond faster and minimal damage to the attack.

AI and machine learning, and Deep Learning, help uncover the issues that do not even come to the mind of a person. The real-life experience in the hospital shows that AI improves the trust and safety. With the help of AI and strong cybersecurity networks, healthcare organizations can develop a safer, smarter, and one that is ready to meet the challenges in the future.

V. CHALLENGES AND LIMITATIONS OF AI IN HEALTHCARE CYBERSECURITY

A. Data Privacy and Security Issues

AI requires much patient information to be effective. This information consists of medical history, test results and names. In case this information is not secure, it may be stolen or abused. AI systems can be attacked by hackers to access patient data or alter the decision-making process of AI.

The AI system might present incorrect outputs in case the wrong information is inputted into it [35]. The hospitals should ensure that the data is stored in a safe place and that it is accessed by the right people. They also have to comply with such data laws as HIPAA and GDPR.

The privacy of the data is highly significant in healthcare. Hospitals have their data which is kept confidential by patients. Should it leak some data, it will be detrimental to the patients and the name of the hospital.

B. Lack of Large and Good-Quality Data

AI learns from data. The better connected it is to the data the higher the performance. However, in healthcare, big and clean data are difficult to locate. Various hospitals store information in various systems. The information can be incomplete or it can contain errors. Due to privacy regulations, hospitals are not very willing to share patient information. This complicates the learning of AI [36]. Unless AI can get sufficient good data, it cannot discover novel or concealed cyber threats.

The solution to this issue is collaborative work by hospitals. They may resort to such measures as federated learning whereby AI learns many locations without the physical shifting of the actual data. This will assist in ensuring privacy and at the same time allow AI to become stronger.

C. Adversarial Attacks on AI

The AI system is also vulnerable to attacks by hackers. These are referred to as adversarial attacks. In such attacks, the hackers include minor modifications in the data in order to disorient AI [37]. The slightest variation can lead to erroneous AI results.

As an instance, there are fake emails that can be written by hackers. There is a chance that the AI will fail to notice the minor difference and assume that the email is safe. Such a trick may make AI overlook actual threats.

Such attacks are quite harmful as this is the primary section of the security system that is being attacked. Hackers can penetrate into the network easily in case AI is duped. To avoid this, the hospitals should test AI frequently and train it on numerous fake attacks. This makes AI more powerful and intelligent toward tricks.

D. High Cost and Technology Problems

AI requires good computers, high-speed internet, and large storage. These are very expensive things. A large number of small hospitals are not able to afford them. The AI also requires trained personnel to handle it. These professionals are costly and difficult to locate [38]. The AI system might not be effective, or it can remain ineffective without talented individuals.

Software update and maintenance are also cost to the hospitals. These costs keep adding up. Other hospitals have cloud-based AI to save monies, yet that may also result in privacy threats. Therefore, the price and the safety are difficult to balance.

E. Ethical and Legal Problems

Many ethical and legal issues are also associated with AI. One big issue is bias. In case the data utilized to train AI is skewed, AI will yield unjust or incorrect judgements [39]. As an example, AI can learn using data of a single hospital but not another hospital.

The other issue is responsibility. Whenever the AI commits an error, it is not easy to determine who is to be blamed whether it is the hospital, the AI company, or the user. This can cause legal trouble.

The hospitals should ensure that AI is never beyond the control of men. AI should not decide all the decisions made by humans. The AI systems must also be transparent and simple to comprehend since individuals understand how they arrive at decisions.

The other problem is ownership of data. The question of who owns the patient data whether it is the hospital, the patient or the AI company is not always obvious. This problem should be solved with clear laws. New regulations should also be enacted by governments to ensure the use of AI is fair, safe and legal.

The use of AI can be used to make healthcare safer, yet it is full of issues. Data privacy is a big risk. Large and clean data is also difficult to obtain with AI. AI systems can be hacked by attackers that will provide incorrect results. AI is as well costly to develop and maintain. Ethical as well as legal concerns are numerous. The hospitals have to rectify such issues with the help of superior rules, safe data systems and robust testing. AI, under no circumstances, should work on its own without human professionals. With proper usage, AI may be a secure and intelligent means of cybersecurity in healthcare.

VI. FUTURE DIRECTIONS AND RECOMMENDATIONS

A. Emerging AI Techniques for Healthcare Cybersecurity

AI technology is growing at a fast rate. In the future, AI methods will be created and will allow the healthcare cybersecurity to be smarter and stronger. Federated Learning is among these new fields. It allows the majority of hospitals to train AI with each other without disclosing real-life patient data. This is advantageous to maintain privacy and it gives AI more ability to learn.

Another new trend is explainable AI (XAI). This form of AI will be able to show how it makes its decisions [40]. The purpose of it is to inform the doctors and IT personnel about the need of why the AI identified a danger or avoided an action. This will create more confidence in AI systems and make them easier.

The other method that is winning popularity is Reinforcement Learning. It allows AI to become knowledgeable about past experiences and be rewarded in the positive activity [41]. To give an example, an AI will be trained to block a phishing attack in the future, in the instance where it will correctly block it.

In addition, automation based on AI will play a key role. It will help the hospitals to react to attacks faster. The AI is capable of automatically responding to threats when it identifies a threat, such as blocking the attacker or isolating the infected system.

Artificial intelligence devices will become more advanced and interconnected with other digital systems in the future. This will facilitate patient information security and make healthcare networks safe.

B. Better Integration and Adoption Strategies

AI is effective when it is integrated into a wholesome security system. Hospitals should strategize to make good use of AI. They ought to integrate AI with other cybersecurity systems and ensure that all systems are capable of working [42].

They should also prepare hospitals to make their staff use AI systems. There are numerous cyberattacks that occur due to human error. When employees know the functionality of AI tools, they will be able to use it in a more efficient way and eliminate dangerous activities.

It is also necessary to communicate well between IT specialists and the health care personnel. The two groups will have to collaborate to digest threats and resolve issues promptly. Starting with small AI projects should be considered in the hospitals. Having learned about them, they will be able to introduce additional AI tools gradually. The slow and safe adoption allows easier adjustment of hospitals.

The AI systems are also to be updated periodically. Cyber threats are evolving continuously and AI has to continue learning with new information. Hospitals can be prepared to face new forms of attacks by regularly updating their systems.

C. Policy and Regulatory Improvements

Governments and health authorities should come up with more powerful laws and definite regulations to use AI in cybersecurity. These regulations should state how hospitals can adopt AI safely and at the same time safeguard the privacy of patients.

Hospitals should also be able to share AI training data without violating privacy laws with the aid of new policies. As an illustration, the governments can help create safe data-sharing sites where hospitals can collaborate safely.

There are also rigorous regulations that AI firms should adhere to regarding the collection and storage of patient information. They are expected to be open and clarify the operations of their AI models. Hospitals that would like to use AI but lack sufficient financial resources and technical expertise could also receive government support. They are able to provide training, grants or shared cloud services to facilitate the use of AI [43].

Lastly, it should be cooperative globally. The cyber threats tend to transcend national borders and thus, countries need to exchange knowledge and collaborate to have stronger security systems.

D. Research and Innovation Opportunities

More research is still required in many areas. Researchers and colleges ought to examine ways in which AI can be used to find new forms of cyber threats earlier. They are also able to do the development of AI models that require less data to train and still perform effectively [44].

The other field of research is to ensure that AI is more resistant to adversarial attacks. There is the creation of new techniques that will make AI smarter and difficult to deceive.

Ethical AI design is another area that should be targeted by researchers. This would involve creating AI which was fair, honest and respected privacy. Research centers and hospitals can collaborate in order to develop clear ethical standards of AI safe use.

Other emerging technologies such as Blockchain could be also connected with AI. Blockchain is able to document all the activities in a secure and immutable manner. Patient data can be even more secure when implemented with the help of AI [45][46].

Low-cost artificial intelligence also requires innovation. Most developing countries have a lot of hospitals that are unable to afford expensive systems. Development of affordable AI based cybersecurity tools can be used to safeguard healthcare not only in wealthy countries.

E. Recommendations

AI tools should be applied to identify cyber threats in a timely manner and track the systems of hospitals at all times. They will have to educate all employees regarding cybersecurity and safe usage of AI. Also, one should ensure that all the systems are always updated and backed up to avoid data loss. To maintain trust and safety, hospitals should adhere to the privacy laws when managing patient data. They are also expected to collaborate with governments and research organizations to exchange information in safe and secure means that can enable them to enhance AI models and cybersecurity systems [47].

Strong policies regarding the use of AI and cybersecurity in healthcare should be clear and made by governments. They have the capability of assisting the hospitals financially, through technical assistance as well as training. Strong laws should also be established by governments to ensure sensitive data are not misused. Moreover, they are able to promote safe and useful innovation by investing in research studies that aim at developing AI to secure healthcare systems.

Researchers are significant in making AI enhance cybersecurity. They ought to create AI models which are safer, more equitable and comprehendible. Scientists will also have to research how to ensure the protection of AI systems against attacks by hackers and seek alternative ways to make AI more resistant to cyber attacks. Developing AI systems that are energy efficient and affordable to buy is another important objective on which the focus is made to enable even small hospitals and clinics to easily have them. Hospitals, governments, and researchers can cooperate to create a more secure digital future of healthcare.

The future of AI in medical cybersecurity is bright. The systems will become smarter and safer with new technologies such as Federated Learning, Explainable AI, and Blockchain. The existing issues will be resolved by powerful laws, improved training, and increased research.

AI will not supersede the human being but will collaborate with them to ensure that healthcare becomes safer. Through proper planning, free cooperation, and equitable usage, AI will save hospitals, preserve patient information, and help establish trust in electronic medical systems [48].

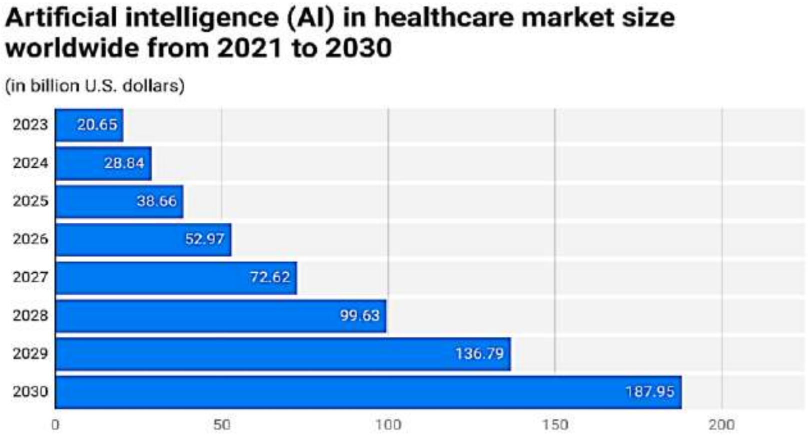

Figure 4: Projected growth of the global AI healthcare market from 2021 to 2030

AI is set to expand at a very fast rate in the nearest future, particularly in the healthcare sector. Figure 4 demonstrates that the market size of artificial intelligence in the healthcare sector in the world will continue to increase drastically between 2021 and 2030. The market is currently worth 20.65 billion, and it is expected to grow to approximately 187.95 billion by 2030. Such massive growth indicates that AI is becoming an important component of the contemporary healthcare systems. Machine learning, predictive analytics, and automation are all technologies that are used to enhance the diagnosis of the disease, treatment planning, patient monitoring, and overall healthcare delivery. The consistent increasing movement shows that AI will remain a crucial component in transforming healthcare into a more sophisticated, precise, and available one on a global level [49].

VII. CONCLUSION

The paper has defined the role of Artificial Intelligence (AI) in enhancing cybersecurity in healthcare. It demonstrated the role of AI in hospitals to secure patient records, identify cyberattacks and ensure the security of their systems. Electronic health records, medical devices, and preventing hackers are all guarded by AI. Through such technologies as machine learning and deep learning, AI can identify issues more quickly and more precisely than the previous approaches to security.

Healthcare cybersecurity has many benefits brought by AI. It is able to monitor systems 24/7 and locate unusual activities possibly of cyberattack. It also assists in minimizing the human errors and responds promptly to a threat even in case it occurs. Over time, AI will be able to learn how to attack and get more intelligent. The reason why many hospitals are using AI is that AI keeps their data secure and generates more trust among patients and employees.

Nevertheless, there are certain giant issues. Among them, data privacy is one of the major concerns. AI requires much information to be trained, and patient data sharing is not always safe. Other hospitals do not possess sufficient high-quality data to train AI systems as well. The systems can become weak through special attacks by hackers who will attempt to confuse AI. The price of using AI is also a big one, and not all hospitals possess a sufficient number of skilled individuals and powerful technology. The questions concerning the ethical and legal implications of AI data usage also exist.

The future is bright despite these issues. The healthcare systems can be safer and more open with the help of new types of AI such as Federated Learning, Explainable AI, and Blockchain. Such tools will be useful to secure data without violating privacy regulations. To ensure safe use of AI, hospitals, governments and researchers need to collaborate to make rules transparent, provide training and help their employees.

Concisely, AI plays a major part in healthcare cybersecurity in the future. It will be able to prevent attacks, safeguard patient information, and strengthen systems. Alexa intelligence will secure health care and be prepared to new challenges in cyber-crime when well planned, used fairly, and collaboratively.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] M. Khaja, H. Rafi, and M. Arikhad, “Artificial Intelligence in Neuro-Ophthalmic Healthcare: Bridging Eyesight and Brain Function,” *Int. J. Sci. Eng. Sci. Res.*, vol. 1, no. 2, pp. 1–7, Apr.–Jun. 2025. Available from: https://tinyurl.com/2krf6kra

[2] M. A. Abdullah, M. Arikhad, I. Bhatti, and T. A. Sadiq, “Algorithms with a Bedside Manner: Regulating AI’s Social and Legal Impact on U.S. Healthcare,” *IRJEMS Int. Res. J. Econ. Manag. Stud.*, vol. 4, no. 9, pp. 13–?, Sep. 2025.

[3] M. Arikhad, M. Waqar, A. H. Khan, and A. Sultana, “AI-driven innovations in cardiac and neurological healthcare: Redefining diagnosis and treatment,” *Revista Española de Documentación Científica*, vol. 19, no. 2, pp. 124–136, 2024. Available from: https://tinyurl.com/2s3kf37a

[4] Raza, “Equality before Law and Equal Protection of Law: Contextualizing its Evolution in Pakistan,” *Pakistan Law Journal*, 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5200799

[5] Raza, “Credit, code, and consequence: How AI is reshaping risk assessment and financial equity,” *Euro Vantage Journals of Artificial Intelligence*, vol. 2, no. 2, pp. 79–86, 2025. Available from: https://evjai.com/index.php/evjai/article/view/30

[6] Rasool and S. I. Haider, “Exploitation and low wages of labor migrants in Gulf countries,” *Global Management Sciences Review*, vol. 1, pp. 32–39, 2020. Available from: https://tinyurl.com/4y7yw9h9

[7] M. Khaja, H. Rafi, and M. Arikhad, “Neuro-AI synergy in visual and motor healthcare: Redefining diagnosis through brain, eye, and motion data,” *Int. J. Sci. Soc. Sci. Res.*, vol. 1, no. 2, pp. 1–7, Apr.–Jun. 2025. Available from: https://tinyurl.com/3fymuv42

[8] Raza, “AI and privacy – navigating a world of constant surveillance,” *Euro Vantage Journals of Artificial Intelligence*, vol. 1, no. 2, pp. 74–80, 2024. Available from: https://evjai.com/index.php/evjai/article/view/28

[9] H. Syed, W. A. Awan, and U. B. Syeda, “Caregiver burden among parents of hearing impaired and intellectually disabled children in Pakistan,” *Iranian J. Public Health*, vol. 49, no. 2, pp. 249–256, Feb. 2020. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC7231703/

[10] Raza, M. A. Farooqi, M. N. Rasheed, K. Shahzad, and A. A. Ansari, “Advancing legal practice: A detailed analysis of integrating AI in legal research, reasoning, and writing,” *International Journal of Social Sciences Bulletin*, vol. 2, no. 4, pp. 2525–2535, 2024. Available from: https://socialsciencesbulletin.com/index.php/IJSSB/article/view/646

[11] S. Khan, S. I. Haider, and R. Bakhsh, “Socio-economic and cultural determinants of maternal and neonatal mortality in Pakistan,” *Global Regional Review*, vol. 1, pp. 1–7, 2020. Available from: https://tinyurl.com/mtzjbf36

[12] M. Arikhad, A. H. Khan, M. Tariq, and A. Al Abrar, “AI-powered solutions for precision healthcare: Focusing on heart and brain disorders,” unpublished. Available from: https://tinyurl.com/488j89x7

[13] Raza, “Equality before Law and Equal Protection of Law: Contextualizing its Evolution in Pakistan,” *Pakistan Law Journal*, 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5200799

[14] Munir, A. Raza, S. Khalid, and S. M. Kasuri, “Automation in judicial administration: Evaluating the role of artificial intelligence,” 2023. Available from:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5209960

[15] S. I. Haider and N. K. Mahsud, "Family, peer group and adaptation of delinquent behavior," *Dialogue (Pakistan)*, vol. 5, no. 4, 2010. Available from: https://tinyurl.com/mr2ss7t5

[16] S. I. Haider and N. K. Mashud, "Knowledge, attitude, and practices of violence: A study of university students in Pakistan," *Journal of Sociology and Social Work*, vol. 2, no. 1, pp. 123–145, 2014.

[17] S. Khan, S. Mehmood, and S. I. Haider, "Child abuse in automobile workshops in Islamabad, Pakistan," *Pakistan Journal of Criminology*, vol. 12, no. 1, pp. 61–74, 2020. Available from: https://tinyurl.com/7j47z4nh

[18] Raza, M. A. Chauhan, N. Khan, G. Ali, and N. A. Tayyab, "Artificial intelligence and criminal liability: Rethinking criminal liability in the era of automated decision making," 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5376011

[19] T. A. Sadiq, A. M. Khaja, A. Tariq, and M. Arikhad, "The HIPAA Singularity: Reconciling AI, cybersecurity, and patient rights in the U.S. healthcare legal framework," *IRJEMS Int. Res. J. Econ. Manag. Stud.*, vol. 4, no. 9, pp. 9–?, Sep. 2025.

[20] UR Rahman, S. I. Haider, and A. Ali, "Tobacco farming and its social impacts on farmers in the rural Mardan, Pakistan," *Global Social Sciences Review*, vol. 4, no. 3, pp. 229–234, 2019. Available from: https://tinyurl.com/ar8rhuhm

[21] Raza, "The application of artificial intelligence in credit risk evaluation: Obstacles and opportunities in path to financial justice," *Center for Management Science Research*, vol. 3, no. 2, pp. 240–251, 2025. Available from: https://tinyurl.com/5t55347c

[22] M. Zubair, S. I. Haider, and F. Khattak, "The implementation challenges to women protection laws in Pakistan," *Global Regional Review*, vol. 3, no. 1, pp. 253–264, 2018. Available from: https://tinyurl.com/27vrnb39

[23] M. Arikhad, M. Waqar, A. H. Khan, and A. Sultana, "The role of artificial intelligence in advancing heart and brain disease management," *Revista Española de Documentación Científica*, vol. 19, no. 2, pp. 137–148, 2024.

[24] Z. Zafar, I. Sarwar, and S. I. Haider, "Socio-economic and political causes of child labor: The case of Pakistan," *Global Political Review*, vol. 1, no. 1, pp. 32–43, 2016. Available from: https://tinyurl.com/2a5ec9ud

[25] S. I. Haider, *Socioeconomic differences in drug use among older people: trends, polypharmacy, quality and new drugs*, Ph.D. thesis, Karolinska Institutet, Sweden, 2008. Available from: https://tinyurl.com/5chh3azb

[26] S. I. Haider and N. K. Mahsud, "Family, peer group and adaptation of delinquent behavior," *Dialogue (Pakistan)*, vol. 5, no. 4, 2010. Available from: https://tinyurl.com/mr2ss7t5

[27] Z. Ahmed, S. Khan, S. Saeed, and S. I. Haider, "An overview of educational policies of Pakistan (1947–2020)," *Psychology and Education Journal*, vol. 58, no. 1, pp. 4459–4463, 2021. Available from: https://tinyurl.com/2crcb8fb

[28] M. Khaja, M. Arikhad, and H. Rafi, "Artificial intelligence in neuro-ophthalmic healthcare: Bridging eyesight and brain function," unpublished.

[29] M. Khaja, M. Arikhad, Y. Hayat, and S. Rasool, "Predictive modeling for chemotherapy response using machine learning," unpublished. Available from: https://tinyurl.com/ycbnvbcm

[30] H. Khan, M. Arikhad, and M. Tariq, "Revolutionizing heart and brain healthcare with artificial intelligence: Challenges and opportunities," unpublished. Available from: https://tinyurl.com/33r6rwy2

[31] S. I. Haider and M. Ali, "Mitigating the challenges of open and distance learning education system through use of information technology: A case study of Allama Iqbal Open University Islamabad, Pakistan," *Pakistan Journal of Distance and Online Learning*, vol. 5, no. 2, pp. 175–190, 2019. Available from: https://eric.ed.gov/?id=EJ1266675

[32] Palmeri, "Divine disguises on the crossroads of Khotan: The iconographies from Dandan Oilik," *Journal of Asian Civilizations*, vol. 44, no. 2, pp. 67–107, 2021. Available from: http://jac.qau.edu.pk/index.php/jac/article/view/83

[33] S. I. Haider and F. M. Burfat, "Improving self-esteem, assertiveness and communication skills of adolescents through life skills-based education," *Journal of Social Sciences and Humanities (JSSH)*, vol. 26, no. 2, 2018.

[34] Ali, S. I. Haider, and M. Ali, "Role of identities in the Indo-Pak relations: A study in constructivism," *Global Regional Review*, vol. 2, no. 1, pp. 305–319, 2017. Available from: https://humapub.com/admin/alljournals/grr/papers/0QibDTlvAf.pdf

[35] Raza and B. Munir, "The doctrine of latent copyrights: Protecting generative AI models through representational layers," 2025. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5745922

[36] M. Liaqat, R. Kanwal, M. Ansari, and S. Munir, "Physical health-related quality of life in Pakistani physical therapists," *The Rehabilitation Journal*, vol. 2, no. 2, pp. 60–64, 2018. Available from: http://trjournal.org/index.php/TRJ/article/view/28

[37] S. I. Haider, M. Hussain, and A. Waqar, "Differential associational in learning religious extremism/violent behavior: A case study of Central Jail Rawalpindi," *Pakistan Journal of Criminology*, vol. 11, no. 3, 2019. Available from: https://tinyurl.com/4kb6aeb7

[38] Raza, "Trade secrets as a substitute for AI protection: A critical investigation into different dimensions of trade secrets," 2024. Available from: https://tinyurl.com/mvkwswwm

[39] M. Khaja, H. Rafi, and M. Arikhad, "Neuro-AI synergy in visual and motor healthcare: Redefining diagnosis through brain, eye, and motion data," unpublished.

[40] S. Khan and S. I. Haider, "Women's education and empowerment in Islamabad, Pakistan," *Global Economics Review*, vol. 5, no. 1, pp. 50–62, 2020. Available from: https://iris.unive.it/handle/10278/5104158

[41] Raza, A. Yasin, S. Khalid, S. B. R. Naqvi, and U. Noreen, *International Journal of Contemporary Issues in Social Sciences (EER)*, details not specified. Available from: https://tinyurl.com/ye564zkr

[42] S. I. Haider and A. Waqar, "Projection of CPEC in print media of Pakistan from 2014–2019," *Global Strategic Security Studies Review*, vol. 1, pp. 45–64, 2019. Available from: https://tinyurl.com/9ed6twf4

[43] Raza, "Navigating the intersection of artificial intelligence and law in healthcare: Complications and corrections," 2024. Available from: https://tinyurl.com/43dezt5m

[44] Raza and N. Bashir, "Artificial intelligence as a creator and inventor: Legal challenges and protections in copyright, patent, and trademark law," 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5376048

[45] Raza and S. Khalid, "Cognitive privacy and the architecture of AI-driven surveillance," 2025. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5745962

[46] Raza, *Artificial Intelligence, National Security, and Constitutional Governance in the United States: Reinventing the Rule of Law in the Digital Age*, Geh Press, 2025. Available from: https://tinyurl.com/4fjrfb3x

[47] M. Arikhad, M. Waqar, A. H. Khan, and A. Sultana, "AI-driven innovations in cardiac and neurological healthcare: Redefining diagnosis and treatment," *Revista Española de*

Documentación Científica, vol. 19, no. 2, pp. 124–136, 2024. Available from: https://tinyurl.com/2s3kf37a

[48] M. A. Chohan, M. A. Farooqi, A. Raza, M. N. Rasheed, and K. Shahzad, "Artificial intelligence and intellectual property rights: From content creation to ownership," 2024. Available from: https://tinyurl.com/yau78cdd

[49] Munir, "Balancing privacy and technological advancement in AI: A comprehensive analysis of the US perspective," *SSRN 5198259*, 2024. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5198259