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.2025.13.6.6
Article ID IRP-1691, Pages 48--57
www.ijircst.org

Securing Smart Healthcare: The Role of Artificial Intelligence in Protecting Patient Data and Medical IoT Devices

Gnanesh Methari[1], and Yawar Hayat[2]

[1] Department: Information Technology (Cybersecurity), Franklin University, Columbus, United States
AI Healthcare Researcher, Institute of Business Administration, Karachi, Pakistan

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

Received: 31 October 2025 Revised: 14 November 2025 Accepted: 28 November 2025

ABSTRACT- Every year, healthcare is becoming digitalized. Smart devices and Web-based systems are now employed to gather, store, and share patient information in hospitals. These tools simplify and speed up the process of treatment, yet they lead to the emergence of new risks. Cyberattacks, theft of data, and system failure can be detrimental to both the patients and the healthcare providers. In this paper, we will review the way Artificial Intelligence (AI) can be used to protect the healthcare system against such issues. It describes how AI can detect and prevent attacks, secure medical equipment, and ensure patient data is secure. The paper also examines how AI can analyze previous attacks and forecast future attacks in order to prevent them. Certain challenges such as the need for powerful rules, ethical issues, and data privacy are also addressed. The paper demonstrates that AI can be used to ensure safe and more reliable healthcare, as long as it is utilized reasonably and conscientiously.

KEYWORDS: Artificial Intelligence, Cybersecurity, Smart Healthcare, Medical IoT, Patient Data, Machine Learning, Data privacy, Healthcare security.

I. INTRODUCTION

The healthcare industry is evolving at a very fast rate because of the development of new digital resources [1]. Medical centers and hospitals have become smart in their patient care systems. Another name of these devices is smart healthcare or Internet of Medical Things (IoMT). They entail the use of things such as heart monitors, blood pressure watches and wearable watches, and hospital machines which send information via the Internet. Doctors will have an opportunity to check patients at any place and patients can get assistance quickly. Digital records also facilitate easy storage of health information as well as sharing the information. This will save time and promote treatment. Nevertheless, due to the growing number of devices that are connected to the internet, the risk of cyberattacks is also multiplying. Patient information can be stolen by hackers, as well as hostage systems and even medical machines [2]. These attacks can cause serious harm and lack of confidence in patients. Owing to this fact, security of smart healthcare systems has emerged a big and pressing need.

Not all hospitals are ready to fight against the modern cyberattacks. The old methods of security like passwords and antivirus software cannot be used nowadays. Modern tricks that have been employed by cybercriminals to gain access to systems are phishing emails, ransomware and fake software [3]. These attacks can spread quickly across interconnected networks and devices. The attack can also pose a threat to the life of patients either due to draining of the hospital or tampering of the information of the patients. This is the reason why health care needs to be protected more vigorously and wisely. Such issues can be addressed by introducing Artificial Intelligence (AI). Artificial intelligence can be used to analyze data masses, identify suspicious activity, and forecast attacks before they happen. It will be capable of studying how the hackers work and respond promptly to the emergence of new types of threats. For example, AI can track the network traffic and alert the personnel in case they find some unusual activity. AI may also be used to detect the weaknesses in systems and deal with them quickly. This explains why AI is very important in terms of protecting healthcare information and equipment [4].

Even though AI would significantly help, it is not applied to the appropriate extent concerning cybersecurity in healthcare. The majority of hospitals use AI to treat patients, diagnosing a disease or medical imaging but not safeguarding their systems. Most of the studies on AI and healthcare focus on treatment and diagnosis, but not on data security. Some researchers are focused on testing AI for detecting attacks, but they are done in labs on smaller scale. Some hospitals do not have the finances, knowledge and confidence to adopt these tools [5]. Another issue is privacy. To make AI efficient a lot of data is needed, but patient data is confidential and must be maintained. There are no global regulations/ standards on AI application in healthcare security. Not all the potential of AI in healthcare system security has been wielded yet because of these factors.

The opportunities of AI that can make smart healthcare systems more secure will be discussed in this paper. It will touch upon how AI is able to protect patient data, detecting attacks, and securing medical equipment. The paper will address what has been done and what the researchers must improve. It will also outline the major concerns of privacy, ethics, and cost and suggest the way of its solution. The simplified descriptions of the AI techniques related to machine learning and deep learning will be discussed and how they will be used to support the process of

cybersecurity will be demonstrated. The paper will also discuss new ideas that will be implemented in healthcare safety involving blockchain and cloud computing using AI [6]. It is also geared towards showing that AI is not a future issue, but it is already helping in the development of stronger and more secure medical systems. Being aware of its place and restrictions, hospitals and researchers will be able to cooperate in order to protect patient data and make healthcare more credible.

II. BACKGROUND AND LITERATURE REVIEW

A. From Traditional Healthcare to Smart Systems

Previously, hospitals were utilizing paper-based files to store patient data [7]. Notes were written by hand, and nurses stored these files in shelves or folders. This system was not fast and might lead to errors. The exchange of patient information between hospitals was also quite difficult. In case a patient transferred to a different city, the records would remain.

With the passage of time, computers replaced paper files. Electronic Health Records (EHRs) began to be used by hospitals where data was stored and updated [8]. This simplifies the work. Doctors can access patient data with just one click now. This is made possible by the internet to share data between hospitals and clinics.

After that, a new wave of change in the Medical Internet of Things (MIoT) entered. It implies that medical machines, sensors, and devices are now able to connect to the internet [9]. For instance, a smartwatch can monitor the heart of an individual, and a device to monitor sugar level can send the results to a doctor immediately. Smart systems are now becoming part of smart healthcare.

This new system is also majorly driven by Artificial Intelligence (AI). The AI is used to assist physicians in scans reading, predicting conditions, and identifying optimal treatment options in every patient [10]. It can analyze vast data in a shorter period than humans. Due to AI and MIoT, the healthcare is more than ever in a digital, connected, and efficient state. However, with this transformation it brings with it new threats. When machines and information are linked to the internet, they may be attacked by hackers.

The fast development of Internet of Things (IoT) devices has become one of the main factors that have contributed to the further digitalization of healthcare, as they connect medical sensors, wearables, and hospital systems [11]. Such devices constantly gather and send patient information, which allows real-time monitoring and distant care. The growth, however, escalates cyber threats and data breach, which makes it essential to incorporate Artificial Intelligence (AI) to enhance security systems.

At the world level, Figure 1 below illustrates the increase in the number of IoT-connected devices between the year 2015 and 2025. Connected devices have increased by an average of 15.41 billion in 2015 and to 75.44 billion in 2025, which is almost five times.

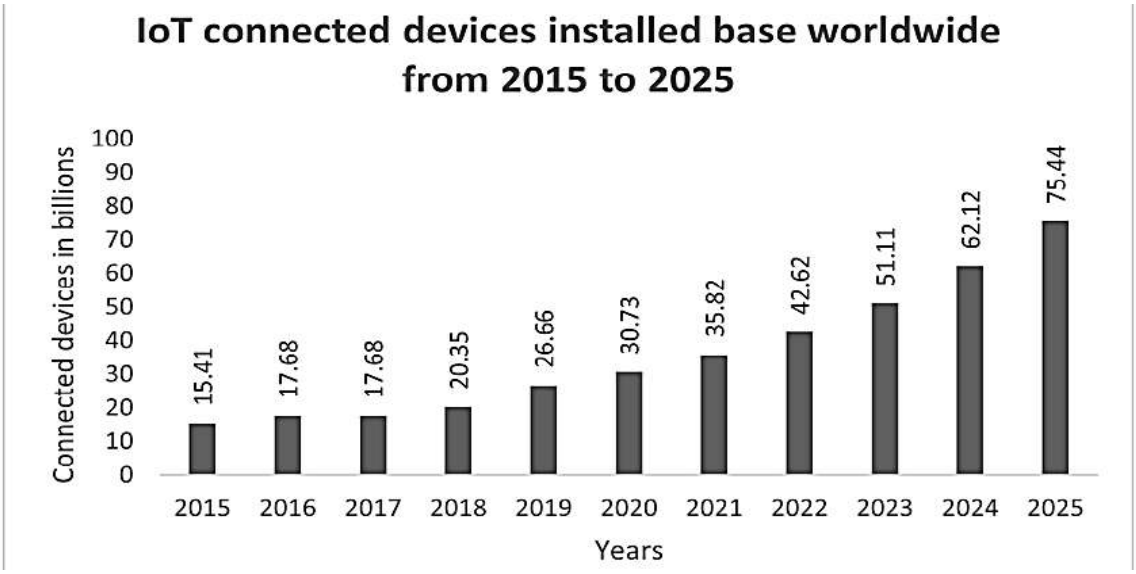

Figure 1: IoT connected devices installed base worldwide from 2015 to 2025

B. Cyber Risks in Healthcare Systems

The field of security in cybercrime has been a very serious issue in contemporary healthcare. Hospitals possess a considerable amount of personal information, including medical records, ID numbers, and payment information [12]. When this data is in the hands of hackers, they may sell it or use it illicitly. Hospital systems may also be paralyzed by cyberattacks. In others, physicians might be unable to retrieve patient information or machines may end up not functioning which endanger lives.

Most of the hospitals are unprepared to manage these risks. They tend to have outdated computer systems that are ineffective with security measures. Others are using insecure passwords or outmoded software. There are various tricks or tricks that attackers employ to gain access to systems such as phishing emails, malware, or ransomware. With ransomware attacks, the hackers encrypt the hospital files and request money to decrypt.

The Medical Internet of Things (MIoT) is also riskier. Any hospital network can become the target of all smart devices. They are cardio monitors, insulin pumps, and health bracelets. Most of these devices lack good passwords and security systems. Hacking of one system can provide access to the entire hospital network.

Numerous research indicates that cyberattacks have been increasing annually in the healthcare sector. As an illustration, in 2023, it was reported that the hospital sector in most of all industries lost data due to cyberattacks [13]. This indicates the extent to which these attacks have become serious and expensive. Hospital data security and patient protection nowadays are one of the key challenges in healthcare.

III. RESEARCH ON AI-BASED CYBERSECURITY

To address these issues, scholars are considering Artificial Intelligence (AI) as the means of enhancing the safety of healthcare systems [14]. AI can identify trends in data, identifying abnormal behavior, and respond promptly to prevent cyberattacks. In contrast to human beings, AI can perform around the clock and act quicker in case of something out of the ordinary.

Research indicates that machine learning and deep learning, the subsections of AI, can be used to identify and avert cyber threats [15]. Machine learning models have the potential to understand a normal activity within a hospital network. In the case of an uncommon occurrence, such as when a mysterious device attempts to gain access to files, AI can send a notification. Signals of medical devices can also be studied using deep learning and discovered whether a person is attempting to modify or intercept them.

Indicatively, a research study created an AI system that learned on previous attacks. It has improved with time in the detection of new types of threats [16]. In another study, AI was utilized to secure medical information, such as X-rays and MRIs, by determining whether they were altered prior to saving them. These illustrations demonstrate that AI will be able to assist healthcare systems to be safer and respond to the issues quicker.

Other domains where AI is being tested in cybersecurity are also present. As an example, AI will be able to view and interpret email messages to identify phishing [17]. It is also able to verify the health of the hospital networks and identify areas of weakness that require repair. These capabilities enable AI to provide hospitals with the means of averting attacks rather than responding to the damage after it occurs.

IV. CHALLENGES AND GAPS IN RESEARCH

As AI is presented as highly beneficial, it is not fully applied in hospitals yet. Most AI security systems are not used in real health care settings, only laboratory testing. They are commonly difficult to use in hospitals due to their cost, untrained staff, and the concern of data privacy [18].

The amount of data required to train AI is also quite big, whereas patient data is highly sensitive. Sending it to AI systems may lead to legal and moral issues. The other problem is that AI occasionally makes decisions that are not easily explained by human beings. In case AI blocks access to a system or falsely claims that there is a threat, it can influence the work of the doctors and the safety of patients.

The scholars also indicate that there are no worldwide regulation or criteria for utilizing AI in healthcare cybersecurity. Different systems are used by each hospital or country, hence making it difficult to develop a shared protection plan. Ai will require more efforts to become safe, fair, and explainable before it becomes the standard approach to healthcare.

V. THE FUTURE OF AI IN SMART HEALTHCARE SECURITY

Despite these issues, AI is still promising a lot in the future. Recent research indicates that AI should be used along with blockchain and cloud computing to create more robust protection systems [19]. Blockchain will render hackers more difficult to alter patient records since they are stored in encrypted blocks. Cloud systems have the potential to provide the hospitals with improved storage and shorter recovery time post attacks. Working with such tools, AI can make healthcare more secure, flexible, and smart.

It is the opinion of experts that healthcare cybersecurity will be shaped in the future by the ability of systems to learn, adapt, and react to emerging threats within a short period of time [20]. Such systems can be built with the assistance of AI. It will be able to transform the healthcare cybersecurity process into a reactionary process to a proactive process. To do this, hospitals, researchers and governments need to collaborate to develop simple rules, share knowledge and develop trust.

In conclusion, paper-based healthcare has been replaced by intelligent and AI-driven healthcare. This online expansion has numerous advantages and novel threats. Attack incidents on hospitals and equipment are increasing very quickly. Healthcare protection can occur through AI that identifies threats and mitigates them preventing damage to the system. Nevertheless, it has issues including privacy threat, nonexistence of standards and high-cost obstacles. The application of AI in healthcare cybersecurity requires more studies and international collaboration to operate AI in a safe and holistic way.

VI. TYPES OF SECURITY THREATS IN SMART HEALTHCARE

Smart healthcare involves the use of the internet to integrate machines, applications and patient information. This assists physicians and patients to work more efficiently. However, it also makes the way to numerous types of cyberattacks. By hacking into the systems of hospitals, hackers are able to steal the information, shut down the work of machines and even damage people. These attacks may occur at three primary levels, data, device and network.

Over the last ten years, the healthcare sector has been experiencing an accelerating rate of cyberattacks. Digital tools and online databases are adding more connectivity to hospitals, clinics, and other medical systems and increasing their vulnerability to hackers. The following graph was used to illustrate the number of healthcare data breaches in the United States between 2009 and 2023. In all these cases, over 500 records of patients were exposed.

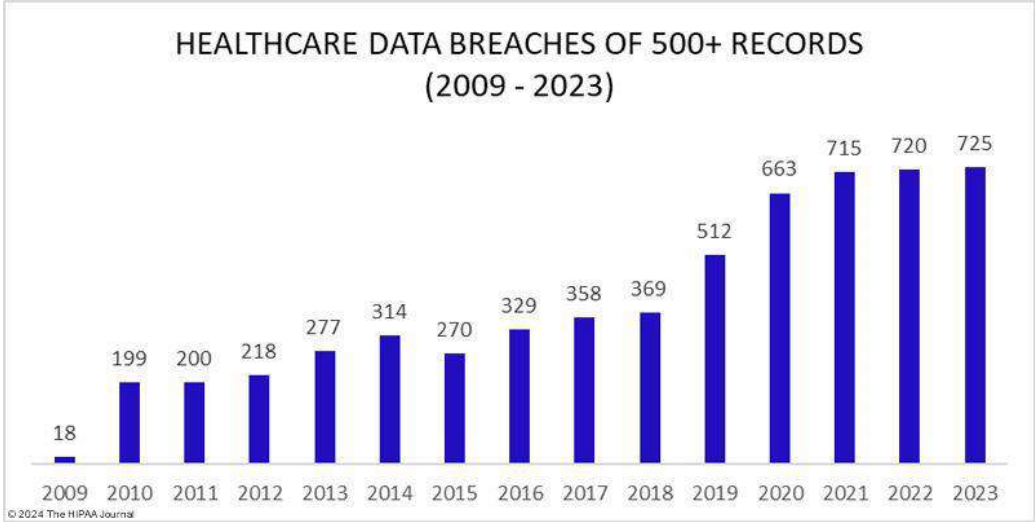

Figure 2: Healthcare Data Breaches of 500+ Records (2009–2023)

In the above Figure 2, this is an illustration of the increasing data breaches in healthcare. In 2009, the number was limited to 18 breaches, and in 2023, it had increased to 725. Such consistent rise is indicative of the fact that cyber threats in healthcare are not only persisting but are getting more threatening. This sharp increase after 2019 also indicates the impact of increased digitalization during and after the COVID-19 pandemic.

With the increasing use of electronic health records (EHRs), and the use of the IoT medical devices in hospitals, attackers discover new methods of obtaining sensitive patient data. This underscores why better cybersecurity mechanisms (particularly the ones that will be underpinned by AI technologies) are highly required to help identify and prevent such attacks before they can do substantial damage.

A. Data-Level Threats

Theft of patient information is one of the largest issues in smart healthcare. Electronic Health Records (EHRs) contain a lot of private data about the names, addresses, medical history and treatment of people kept by hospitals. In case hackers obtain such data, they may sell it or commit identity theft [21]. As an illustration, they may make fraudulent insurance claims or purchase medicine under the name of another person.

Patient data may also be altered or damaged by hackers. This is referred to as data tampering [22]. In case a medical record is being edited secretly (such as altering the blood type or allergy of a patient) this may result in incorrect treatment and grave damage. The slightest changes in data can ruin the patient-doctor's trust.

Tricks such as SQL Injection are applied by many hackers to gain access to the databases of hospitals [23]. This implies that they send embedded instructions to them enabling them to read or duplicate confidential information. There are also others with the use of forged emails that appear authentic to fool hospital employees into providing passwords. Once they enter, they can steal or destroy anything.

Data encryption and strong passwords, as well as multi-step logins, can help hospitals eliminate this. The staff also needs to be trained to identify fake emails and suspicious links. Patient data safety is not a technical task per se; it is a collective responsibility of people working in the healthcare sector.

B. Device-Level Threats

Smart hospitals have numerous devices, such as heart rate monitors, blood sugar sensors, X-ray machines, and fitness watches connected to it. All of them belong to the Medical Internet of Things (MIoT). They gather and transmit data at all times. However, all connected devices are vulnerable to being attacked unless they are secured.

A common danger is malware. It is malicious software that may be introduced into a device via internet or via a USB drive [24]. It may cause the device to behave abnormally or break down after getting inside. As an illustration, a virus on the heart monitor can display incorrect figures and mislead the clinicians.

One more form of attack is referred to as spoofing. In spoofing, the hackers impersonate a legitimate user or device. They transmit misleading information that appears to be real. And, as an example, a hacker can create a falsified medical sensor transmitting incorrect readings to the hospital system. This may make a physician prescribe the wrong medicine or fail to notice a true emergency.

Most of the devices are not updated or use weak passwords and are therefore easy to hack. One of the things that should be maintained in the hospital is the software updates, strong logins, and periodic device inspection. The makers of the devices are also supposed to make their products safe in consideration, rather than only about medical use.

C. Network-Level Threats

The hospital network integrates all devices and computers. Everything can just come to a halt in case hackers attack this network.

A network attack that is referred to as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack is one of the common types of attacks. The hackers overwhelm the hospital network with bogus traffic making it too busy to work. Physicians are unable to open files, computers crash down, and services to patients are slowed down.

Man-in-the-Middle (MITM) attack is also another attack that is dangerous. In this case, a hacker covertly remains in the middle of two two-person or between two-system communication [25]. The hacker interprets or alters the

messages that are being sent. As an illustration, when a physician transmits patient results to a nurse, the hacker can manipulate the figures prior to their delivery to her.
The hospitals can minimize these risks through employing safe communication systems, firewalls and network monitoring applications. Frequent testing enables identifying areas of weakness before the attackers.

D. Real-World Cases

In 2021, the ransomware attack struck Scripps Health, which is a large California-based hospital network. Hackers disabled the computers nearly one month. Doctors could not see the records of the patients and numerous surgeries were postponed. Patients were exposed to severe challenges, and the hospital has lost a great deal.
Ireland also suffered the attack by ransomware in the same year by its Health Service Executive (HSE). The entire public hospital systems were required to be shut down (Office of Information Security, 2022). Patients could not get access to patient records, test results, or appointments in weeks. This hack demonstrated why hospitals may not be as secure as they could be without solid cybersecurity.
Ransomware was used to attack a hospital in Düsseldorf, Germany in 2020. Due to the failure of the computers, physicians could not serve emergency patients in a timely manner [26]. Unfortunately, one patient succumbed to death after referring to another hospital. This case demonstrated that cyberattacks in healthcare are not only fatal in terms of money.
In 2018, a huge data breach happened in Sing Health in Singapore. The personal information of approximately 1.5 million patients including the Prime Minister was stolen by hackers. They caused them to take names, ID figures, and information about medicines. Following this attack, the government began to be much more concerned with data protection and cybersecurity.
These incidences demonstrate the severity of cyberattacks in the healthcare sector. They do not only cost money; they can take the lives of people. See the below Table 1.

Table 1: Classification of Cyber Threats in Smart Healthcare

Threat Type	Example Attack	Target	Impact	Mitigation
Data Breach	SQL Injection	EHRs	Identity theft	Encryption
Malware	Ransomware	Servers	Service disruption	Patches
Network Attack	DoS	IoT Devices	Data loss	Secure protocols

Smart healthcare is both strong and weak at the same time. Attacks may occur on any tier, data, device, or network. Data theft breaks privacy. Attacks on the devices may provide inaccurate readings. Whole hospitals can be put out of business by network attacks. Such acts as WannaCry are real cases that demonstrate that such threats are real and dangerous.
The hospitals should maintain the systems up to date, educate the employees, and apply effectively powerful security software. Safety in healthcare does not only refer to the protection of data, but the lives of people as well.

VII. THE ROLE OF ARTIFICIAL INTELLIGENCE IN SECURING SMART HEALTHCARE

The concept of Artificial Intelligence (AI) is transforming the way healthcare systems operate. It assists hospitals to handle large volumes of data, make decisions in real time, and the care provided to patients [27]. However, cybersecurity is one of the greatest applications of AI nowadays. The numerous interconnected devices and digital records involved in Smart healthcare can be hacked. AI would be useful in identifying and preventing such threats before they occur.
AI functions through the learning of data. It can learn trends, identify suspicious activity and react promptly. In contrast to people, AI can oversee thousands of activities simultaneously and detect even minor hints of attack. This is why AI can be a potent solution to ensure the safety of healthcare systems and patient data.
The AI assists in making healthcare systems based on the IoT more intelligent and secure. Below the Figure 3 represents a straightforward design of how smart healthcare devices are going to gather and transfer information securely. It is also demonstrated how AI (as a fuzzy neural network) is employed to treat and secure patient information.

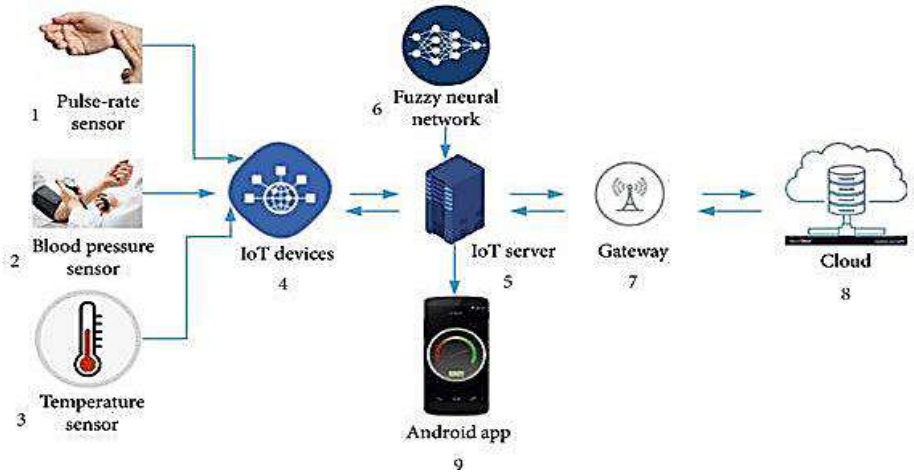

Figure 3: Fuzzy Neural Network Model in Smart Healthcare IoT System

This section describes the way AI safeguard smart healthcare in four sections, namely various AI methods, key security uses, their purpose in securing the medical IoT devices, and practical use cases.

A. AI Techniques Used in Healthcare Security

AI has many elements or processes that can be applied in cybersecurity. They include the most common - Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL), and Natural Language Processing (NLP). They have all played a different but great part in guaranteeing safety in healthcare.

Machine learning helps computers to learn without necessarily being coded to learn. ML in cybersecurity analyzes the past and comprehends the characteristics of suspicious activity (Mohamed, 2025). To illustrate, in case where the activity of the specific employee is a sudden change, the ML can identify it as abnormal. The ML models could be used to monitor network traffic, user activity, or the activity of the medical device to detect the first signs of a hacking.

Deep learning is another advancement of ML that includes a series of computer neurons (neural networks) which emulate the human brain [28]. DL can determine the advanced attack patterns which other security systems might not. As an example, the case of a deep learning model that could scan several millions of files or messages and find any malware or phishing email even in cases where they might seem normal can be used.

Reinforcement helps the systems to make superior decisions depending on the experience. It relies on the trial and error through rewarding on the right action [29]. Cybersecurity in healthcare may use RL to design smarter firewalls and dynamically encrypt the data, which responds differently to a new type of attack detected.

NLP allows computers to be aware of the human language. Cybersecurity It can be used in reading system logs, user messages, and alerts. One of them includes the fact that the NLP can scan through emails or text messages to detect social engineering or phishing. It can also identify fraudulent internet capture or malicious orders within the network of hospitals.

Together, these artificial intelligence techniques change smart healthcare systems and make them smarter, quicker, and more aware of potential risks.

B. AI Applications in Healthcare Cybersecurity

There are numerous fields of healthcare security that use AI. Not only can it detect threats, but it can also prevent and predict them. The three primary applications are data encryption, anomaly recognition and intrusion detection.

A system of intrusion detection monitors the activities of hospital networks. Conventional IDS systems rely on pre-set rules, whereas the AI-based systems can learn about new threats [30]. Based on ML and DL, such systems can detect abnormal login attempts, data flows, or network indicators. As an example, data patterns can be processed using a Convolutional Neural Network (CNN) to easily identify evidence of cyberattacks that can be difficult to detect by humans. Artificial intelligence-based IDS systems can prevent or notify personnel on-the-fly.

Encryption helps to secure patient information by converting it into inaccessible ciphers. AI is smarter encryption because it can adjust to emerging threats. Reinforcement Learning enables the AI systems to alter their encryption mechanisms based on circumstantial events (Balachandran et al., 2025). As an illustration, when a hacker attempts to crack the encryption, AI will automatically change to a stronger or a different code. This can be used to guard against unauthorized access of Electronic Health Records (EHRs) [31].

Artificial intelligence is also quite proficient at detecting anomalies, or any activity that is unusual and suspicious. At a hospital, it may be an unexpected increase in network traffic, a log in at an unusual place, or a machine acting strangely. Machine learning models can contrast normal patterns and current activity and issue an alert in case something appears amiss. This prevents ransomware and data attacks at an early stage before they proliferate.

C. Protecting IOT Devices With AI

Medical Internet of Things (MIoT) devices play an important part in Smart healthcare. They are sensors, smart monitors, and wearable devices, which gather and transmit patient data. They are easy to use in treatment, but at the same time, they are weak areas of hackers. Most of the devices have small memory, low security and are left unprotected. AI assists in enhancing their security along three primary lines authentication, traffic monitoring, and predictive defense.

Authentication is a process of verifying whether the user or the device is authentic. Machine learning and NLP are AI systems that can analyze communication between devices [32]. In case a device begins to transmit unusual or counterfeit data, AI will block it. As an illustration, in case the hacker attempts to emulate a sensor of a hospital, the system may identify the difference in writing style, time, or data pattern and prohibit it from connecting.

AI will be able to track the flow of data among devices on a continuous basis. It can identify minor changes that can indicate an attack using deep learning. In case there is excessively high data flow across devices, or vice versa, the AI systems can automatically isolate the suspicious device to avoid destruction. It would come in handy to identify malware or Denial-of-Service (DoS) attacks.

AI is also capable of anticipating the time and place of an attack. Machine learning systems examine previous data regarding the attacks and generate the values that predict upcoming threats. These predictions can enable hospitals to rectify loose links within their networks prior to their accessibility by hackers. Such a defense is preventative - it prevents problems rather than reacts to them [33].

D. Real-World Case Studies

The use of AI in healthcare security is a reality, as technology is already being implemented in the real world. The most famous ones are IBM Watson Health, Google DeepMind, and the Philips AI Systems.

IBM Watson studies big data in medical research. It can identify uncharacteristic system behavior by processing millions of events per second in security [34]. Watson is also able to read reports and discover concealed risks to hospital systems. It studies each new cyberattack and automatically renews its defense models.

Another AI system that can assist healthcare organizations is DeepMind. It involves deep learning in data security within a cloud. DeepMind can identify when an individual tries to access patient data by an unknown source or files

are transferred in an unusual manner. It is also useful in controlling the accessibility of specific data to individuals, which makes healthcare systems safer.

Philips has developed AI devices which are used to track devices and networks in hospitals. ML and DL are employed in their systems to identify anomalous signals in medical machines (Philips, 2024). As an example, when an MRI machine starts malfunctioning, Philips AI tools could alert the hospital prior to its total malfunction or hacking by vandals. Such systems also trace the way information flows across devices to avoid ransomware or virus infections.

These are just some of the examples demonstrating that AI is already safeguarding actual hospitals and healthcare systems. It assists in timesaving and minimizing human error, as well as makes data safer [35]. See the below Table 2.

Table 2: AI Applications in Smart Healthcare Security

Security Function	AI Method	Description	Example
Intrusion Detection	CNN	Detecting unusual activity	Hospital IDS
Data Encryption	Reinforcement Learning	Adaptive encryption	EHR Security
Threat Prediction	Machine Learning	Predict attacks	Predictive Analytics
Device Authentication	NLP + ML	Validate IoT communication	Smart Monitor Systems

Smart healthcare is also in the form of Cybersecurity through Artificial Intelligence. It makes systems faster, smarter and threat conscious. AI can identify attacks, anticipate risks and even automatically protect itself without human intervention. Healthcare can use machine learning, deep learning, reinforcement learning, and NLP to ensure that it has secured its data, devices, and networks like never before.

Still, AI is not perfect. It must have good data, regular updating and human input to be safe. But its potential is huge. In the future, AI systems in hospitals can be used as the main barrier to cyber threats. AI is not only assisting in saving computers but also saving lives since healthcare systems have become secure and dependable.

VIII. ETHICAL, LEGAL, AND PRIVACY CONSIDERATIONS

The additional implementation of Artificial Intelligence within smart healthcare is beneficial in many ways and, at the same time, has certain concerns. The use of AI in securing the information of the patients must be in care, respect and responsibility to ethics, privacy and law. It is essential that patients be assured that their health care records are dealt with in a fair and secure way.

One of the main ethical issues is prejudice. The learning process in AI works with information, and the system can also be unjustly judged in case of unfair or unbalanced information [36]. Indicatively, the AI model which has been trained basically on the data of one group of people might not work with the other members. This can lead to discrimination or falseness of the health care systems.

The other issue is explainability. Many AI systems are black box systems, especially deep learning systems. They are decision makers, but it can hardly be understood how they achieved such results. This can be a serious problem within the healthcare industry. The patients and doctors can know why an AI system has locked them out of operation, detected an action or made a special recommendation. Developing trust by creating AI systems that are more transparent and comprehensible.

Consent and Trust are also highly essential. Patients are also to be told how their information will be used and agree to it [37]. Businesses and hospitals should be open regarding the application of AI systems to personal information. Once it turns out to the people that AI is being installed secretly and illegally, people will not trust healthcare technologies anymore.

There are also effective statutes that regulate patient information gathering and dissemination. The Health Insurance Portability and Accountability Act (HIPAA) protect the health privacy in the US (Centers for Disease Control and Prevention, 2024). It requires hospitals and health applications to keep the information confidential and use it for the intended purpose.

General Data Protection Regulation (GDPR) is European legislation, according to which individuals have the right to control their personal data [38]. It must be given a clear authorization to use data and people must be able to understand how their data is being used. In most nations, local legislation has been passed to protect digital health information. AI systems ought to comply with these legislations. They are expected to be developed keeping in mind the aim of meeting all the privacy regimes and possessing sound policies on data protection.

The intelligent artificial intelligence can make healthcare smarter, faster, and safer but must not be disrespectful towards human rights. Innovations should not be put at the cost of privacy or fairness. This is geared towards coming up with systems which will protect people and not only data. Ethical standards of AI working should have a well-defined system, fair and considerate of the dignity of all patients [39][40].

Finally, AI implementation in smart healthcare is not only as successful as it is powerful but also well responsible.

IX. FUTURE TRENDS AND RESEARCH DIRECTIONS

Smart healthcare is a rapidly expanding field of AI. Numerous new concepts and technologies are being created to ensure that systems are even safer and smarter. The future of healthcare cybersecurity will rely on the ways of collaborating of new technologies such as Blockchain, Federated Learning, Edge AI, and 5G networks.

One of the potential data protection tools is blockchain. It stores data in small digital blocks, which are interconnected with each other and extremely difficult to alter [41]. This will ensure that patient records will not be tampered with. All the modifications that are made to the data are logged and are transparent such that it becomes easy to monitor the individuals who accessed the information.

Another emerging technology that assists in training AI systems is federated learning that does not require relocating data between different locations. Rather than gathering all patient data on a large server, in federated learning, hospitals can train AI models locally and receive only results. This secures privacy and minimizes the chances of data leakages [42].

Edge AI brings smartness nearer to devices. Rather than transmitting all the data to a central system, AI can compute information directly on the IoT devices or close servers [43]. This allows the response time to be quicker, and sensitive data is stored with the hospital or even on the machine itself, which enhances privacy and security.

The future of healthcare will also be different with the use of 5G. As the internet is getting faster and has improved connectivity, hospitals can connect thousands of devices in real time. With 5G, AI and IoT can transfer medical data in a fast and safe manner. Physicians will be able to keep track of patients remotely without any delays, and AI will process the information immediately to identify the first indications of threat [44].

X. RESEARCH GAPS AND FUTURE NEEDS

Despite all these advances, gaps still exist which should be filled. Explainable AI (XAI) is one of the significant requirements. The current generation of AI systems performs quite effectively, and individuals cannot readily comprehend the way they arrive at their choices. The researchers must develop models that would clarify their logic. This will assist the doctors and patients to have more faith in AI [45].

The other gap is the development of international standards of AI safety and privacy within the healthcare industry. Various nations have varying regulations, and this makes it hard to work with each other. On the one hand, the common framework can assist hospitals and companies under the same ethical and technical guidelines [46].

The AI will only keep expanding into the future as a major contribution to healthcare security. However, it should be built in a responsible manner, i.e. with fairness, privacy, and human well-being in mind.

XI. DISCUSSION AND IMPLICATIONS

AI applications in healthcare security are increasing at a rapid pace. At this point it is evident that AI is more effective in guarding hospitals than the outdated security systems. Old-fashioned cybersecurity measures, such as firewalls and passwords, are applicable, but they are incapable of fighting new attacks [47]. These tools do not respond to an attack but wait until the attack occurs. AI is different. It can monitor systems continuously, identify suspicious activities, and prevent attacks before they can harm anyone. This increases the strength of AI and enhances it in safeguarding patient information and equipment.

AI also brings speed. It can handle several thousands of notifications and locate actual threats quicker than humans. As an illustration, machine learning models can analyze the information of hospitals and instantly identify an anomaly like a hacker attempting to access the system. Deep learning has the potential to consider the trends which standard software may not. This rapid reaction is useful in saving time and damages by hospitals.

However, AI is not perfect. It requires much quality information to learn. In case of incomplete or biased data, AI can be erroneous [48]. The construction and training of AI systems is also expensive. This is not available in many hospitals, particularly in the small ones, due to lack of funds and skilled personnel. AI systems are also complex. IT employees and physicians must be trained to know how to deal with them. Even the strong AI system can be misused without training.

In the case of hospitals, the takeaway is that AI should be implemented gradually. They must begin with minor AI projects that secure patient records or network attacks. Thereafter, they can develop gradually as they get to know more. To policymakers, clear laws and standards should be made to govern the safe application of AI to the healthcare industry. Governments can also intervene by sponsoring AI training and providing financial relief to hospitals. A developer should aim at coming up with easy, transparent, and less expensive AI systems that are easily accessible by hospitals [49].

The collaboration of AI and people must exist. AI can process big data and identify threats within a short period of time, whereas humans can make final decisions in a careful and ethical manner. Working together, healthcare strengthens and becomes more credible. The point is obvious, AI may transform the sphere of healthcare security, but it should be applied wisely, planning, training, and without injustice.

XII. CONCLUSION

The present paper demonstrated the ability of AI to make smart healthcare systems safer and more trusted. AI can be used to identify cyber threats, identify patient data, and secure hospital devices. It is superior to the antique security system since it learns and responds quicker. Attacks can be prevented in time by using machine learning, deep learning, and other AI systems.

Nevertheless, they still have a few boundaries. AI systems require a significant amount of clean data to be effective, and hospitals must spend funds to create and maintain them. A significant number of hospitals also do not have trained staff members that are aware of AI. The other issue is that the usage of AI in the medical field is not represented by any unified global regulations. Various countries have diverse standards, and it is difficult to establish a powerful system.

Despite such restrictions, the hope of AI in healthcare security is bright. Hospitals can safeguard data with more aids with new technologies such as blockchain, edge AI, and federated learning. The second thing is to ensure that AI is more transparent and just to allow both patients and doctors to trust it.

To be brief, AI is not merely a novel technology, but a strong collaborator of healthcare. It will be able to design a more privacy-conscious, speedy, and safer system in which patients will feel secure and where data will not be lost.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] 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 AIOU Islamabad, Pakistan," *Pak. J. Distance Online Learn.*, vol. 5, no. 2, pp. 175–190, 2019.

[2] 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

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

[4] Raza, "AI and privacy – navigating a world of constant surveillance," *Euro Vantage J. Artif. Intell.*, vol. 1, no. 2, pp. 74–80, 2024. Available from: https://evjai.com/index.php/evjai/article/view/28

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

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

[7] 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

[8] 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/2t83ven8

[9] 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

[10] S. I. Haider, "Socioeconomic differences in drug use among older people," Karolinska Institutet, 2008. Available from: https://tinyurl.com/5chh3azb

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

[12] M. Khaja, H. Rafi, and M. Arikhad, "Neuro-AI Synergy in Visual and Motor Healthcare," *Int. J. Sci. Soc. Sci. Res.*, vol. 1, no. 2, pp. 1–7, Jun. 2025.

[13] 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*, vol. 4, no. 9, pp. 1–3, Sep. 2025.

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

[15] M. Liaqat, R. Kanwal, M. Ansari, and S. Munir, "Physical health related quality of life in Pakistani physical therapists," *Rehabil. J.*, vol. 2, no. 2, pp. 60–64, 2018. Available from: https://doi.org/10.52567/trj.v2i02.28

[16] 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

[17] Raza and B. Munir, "The application of artificial intelligence in credit risk evaluation: Obstacles and opportunities in path to financial justice," *Cent. Manag. Sci. Res.*, vol. 3, no. 2, pp. 240–251, 2025. Available from: https://tinyurl.com/5t55347c

[18] S. I. Haider and A. Waqar, "Projection of CPEC in print media of Pakistan (2014–2019)," *Glob. Strat. Secur. Stud. Rev.*, vol. 1, pp. 45–64, 2019. Available from: https://tinyurl.com/9ed6twf4

[19] Raza et al., "Artificial Intelligence and Criminal Liability: Rethinking criminal liability in the era of automated decision making," working paper, Jul. 31, 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5376011

[20] Z. Ahmed, S. Khan, S. Saeed, and S. I. Haider, "Educational policies of Pakistan (1947–2020)," *Psychol. Educ. J.*, vol. 58, no. 1, pp. 4459–4463, 2021. Available from: https://tinyurl.com/2crcb8fb

[21] S. Khan and S. I. Haider, "Women's education and empowerment in Islamabad," *Glob. Econ. Rev.*, vol. 5, no. 1, pp. 50–62, 2020. Available from: https://tinyurl.com/msnkeszt

[22] Raza, "Equality before Law and Equal Protection of Law: Contextualizing its evolution in Pakistan," *Pakistan Law J.*, 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5200799

[23] M. Arikhad et al., "The role of AI in advancing heart and brain disease management," *Rev. Esp. Doc. Cient.*, vol. 19, no. 2, pp. 137–148, 2024.

[24] Munir, A. Raza, S. Khalid, and S. M. Kasuri, "Automation in judicial administration: Evaluating the role of AI," working paper, Jul. 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5209960

[25] Raza and B. Munir, "The Doctrine of Latent Copyrights: Protecting Generative AI Models," working paper, Aug. 2025. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5745922

[26] M. Khaja et al., "Predictive modeling for chemotherapy response using machine learning," 2025. Available from: https://tinyurl.com/2j4t2jye

[27] Rasool and S. I. Haider, "Exploitation and low wages of labor migrants in Gulf countries," *Glob. Manag. Sci. Rev.*, vol. 1, pp. 32–39, 2020. Available from: https://tinyurl.com/4y7yw9h9

[28] Raza et al., "Advancing legal practice: Integrating AI in legal research," *Int. J. Soc. Sci. Bull.*, vol. 2, no. 4, pp. 2525–2535, 2024. Available from: https://socialsciencesbulletin.com/index.php/IJSSB/article/view/646

[29] M. Arikhad et al., "AI-driven innovations in cardiac and neurological healthcare," *Rev. Esp. Doc. Cient.*, vol. 19, no. 2, pp. 124–136, 2024. Available from: https://tinyurl.com/wjrb3nsv

[30] Raza, "Credit, Code, and Consequence: How AI Is reshaping risk assessment," *Euro Vantage J. Artif. Intell.*, vol. 2, no. 2, pp. 79–86, 2025. Available from: https://evjai.com/index.php/evjai/article/view/30

[31] M. Arikhad et al., "AI-powered solutions for precision healthcare." Available from: https://tinyurl.com/488j89x7

[32] Raza and N. Bashir, "AI as a creator and inventor: Legal challenges," working paper, Dec. 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5376048

[33] H. Khan, M. Arikhad, and M. Tariq, "Revolutionizing heart and brain healthcare with AI." Available from: https://tinyurl.com/33r6rwy2

[34] Raza, "Navigating AI and law in healthcare: Complications and corrections," 2024.

[35] T. A. Sadiq et al., "The HIPAA singularity," *IRJEMS*, vol. 4, no. 9, pp. 1–9, Sep. 2025.

[36] Raza, "Equality before Law and Equal Protection of Law," *Pakistan Law J.*, 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5200799

[37] M. A. Chohan et al., "AI and IPR: From content creation to ownership," 2024. Available from: https://tinyurl.com/yau78cdd
[38] S. I. Haider and F. M. Burfat, "Improving self-esteem and communication skills of adolescents," *JSSH*, vol. 26, no. 2, 2018.
[39] S. I. Haider, M. Hussain, and A. Waqar, "Differential associational learning in extremism," *Pak. J. Criminol.*, vol. 11, no. 3, 2019.
[40] Raza et al., "International Journal of Contemporary Issues in Social Sciences EER." Available from: https://tinyurl.com/ye564zkr
[41] S. Khan, S. Haider, and R. Bakhsh, "Maternal and neonatal mortality determinants," *Glob. Reg. Rev.*, vol. 1, pp. 1–7, 2020. Available from: https://tinyurl.com/mtzjbf36
[42] Palmeri, "Divine disguises: Iconographies from Dandan Oilik," *J. Asian Civilizations*, vol. 44, no. 2, pp. 67–107, 2021. Available from: http://jac.qau.edu.pk/index.php/jac/article/view/83
[43] Raza, "Artificial Intelligence and Constitutional Governance in the U.S.," Geh Press, 2025.
[44] M. A. Abdullah et al., "AI's social and legal impact," *IRJEMS*, vol. 4, no. 9, 2025.
[45] Raza, "Navigating the intersection of AI and law in healthcare," 2024.
[46] H. Syed et al., "Caregiver burden among parents of disabled children," *Iran J. Public Health*, vol. 49, no. 2, pp. 249–256, 2020.
[47] M. Khaja et al., "Neuro-AI Synergy – Visual & Motor Healthcare," *Int. J. Sci. Soc. Sci. Res.*, 2025.
[48] M. Khaja et al., "AI in Neuro-Ophthalmic Healthcare," *Int. J. Sci. Eng. Sci. Res.*, 2025.
[49] K. ur Rahman, S. I. Haider, and A. Ali, "Tobacco farming and social impacts," *Glob. Soc. Sci. Rev.*, vol. 4, no. 3, pp. 229–234, 2019.