Received: 6 March 2026 | Revised: 25 June 2026 | Accepted: 2 July 2026 | Published online: 17 July 2026

REVIEW

Artificial Intelligence and Applications
2026, Vol. 00(00) 1–15
DOI: 10.47852/bonviewAIA62029545

Cyber Threats in E-healthcare and an Autonomous Cybersecurity Agent: A Comprehensive Review

Divya Sharma[1,*], Chander Prabha[2,*], Amna Bamaqa[3], Wedad O. Alahamade[3] and Mohammad Zubair Khan[4]

[1] *Department of Computer Science and Engineering, Amity University – Punjab, India*

[2] *Chitkara University Institute of Engineering and Technology, Chitkara University – Punjab, India*

[3] *Department of Computer Science and Information, Taibah University, Saudi Arabia*

[4] *Faculty of Computer Science and Information Systems, Islamic University of Madinah, Saudi Arabia*

Abstract: In the future, an AI-driven security agent could be designed to face cyberattacks for small-scale E-healthcare systems. With the evolution of the Internet, E-healthcare information is made available within seconds on any electronic device, irrespective of the user's geographical location. Since E-healthcare information can be accessed flexibly by individuals on the Internet, as such these are prone to cyberattacks by hackers and even the critical healthcare infrastructure. This study is a critical narrative review of the threats faced by the E-healthcare sector while proposing autonomous AI-driven security agents for improving cyber resilience. The major attacks faced by the E-healthcare systems are ransomware, phishing, data breaches, malware, Distributed Denial of Service, Structured Query Language injection, and Man-in-the-Middle, together with their influence on privacy, confidentiality, authenticity, and patient safety. In this article, a seven-stage cybersecurity response framework consisting of identification, protection, detection, response, recovery, procurement, and security audit is introduced. This architecture is capable of sensing, analyzing, responding to, and learning from the changing attack patterns to ensure security from future attacks. This article also highlights the significance of AI-assisted security mechanisms, staff awareness, and privacy-preserving practices in enhancing defenses of the electronic healthcare sector. In the future, the proposed framework could be implemented and validated as eventually cybersecurity needs to be adaptive to cyberattacks.

Keywords: E-healthcare, cyberattacks, autonomous security agent, privacy, secrecy

1. Introduction

In recent years, cybersecurity concerns have risen, which target the E-healthcare sector with ransomware and data breaches resulting in disruption of clinical services and compromising millions of patient records worldwide. Computers nowadays are connected to the Internet, which has increased cybersecurity [1–23] concerns. A cyberattacker tries to steal, destroy, or alter confidential data through unauthorized access [15]. Internet users are easily deceived by attackers as they are not trained on such cybersecurity [1–23] risks.

With the advent of the Internet, the number of attacks on hospitals has tripled. The most vulnerable is the E-healthcare sector, which deals with critical and lifesaving information of a patient. Cyberattacks that leak Personal Identifiable Information are a growing threat in healthcare. The healthcare sector has attracted the attention of cybercriminals due to the data value and sensitivity of patient information [11]. These are stored on the cloud or in-house storage devices. Data stored on Google Drive and Dropbox is secured using AES-256 algorithms, but time has shown us that even the strongest algorithm can be broken [24]. Further, it is known that the AES-256 algorithm is secure, but implementation flaws, poor key management, weak authentication mechanisms, and security against brute force attacks are still compromised [1–4, 8, 9, 11, 13–18, 25–31] such as brute force attacks [3, 7, 32]. AES with fewer rounds is susceptible to biclique attack, related key attack, and algebraic attack.

1.1. Research motivation

This research addresses the security crisis faced by the E-healthcare sector because of the various cyberattacks resulting in a threat to patient privacy and hospitals.

***Corresponding author:** Divya Sharma, Department of Computer Science and Engineering, Amity University – Punjab, India. Email: dsharma2@pb.amity.edu and Chander Prabha, Chitkara Institute of Engineering and Technology, Chitkara University, India. Email: chander.prabha@chitkara.edu.in

1.2. Common types of E-healthcare data

E-healthcare data is classified as either sensitive or non-sensitive in nature. Table 1 helps get a detailed understanding of the sensitive and non-sensitive information with respect to their characteristics such as privacy, legal protection, encryption, and examples. It can be concluded that protecting sensitive information is necessary as this prevents future attacks or loss of trust in an organization.

1.3. Research questions

In the referred research paper, the authors observed that previous researchers have not clearly discussed the following research questions:

Research Question 1: Why is privacy in E-healthcare of great importance?

Research Question 2: What is the technical impact of privacy, secrecy, authenticity, and confidentiality on any user?

Research Question 3: What cyberattacks are currently faced by the E-healthcare sector?

Research Question 4: What framework should the E-healthcare sector follow in case of an active cyberattack?

1.4. Research objective

The overall research objective of this article is as follows:

Research Objective 1: Evaluate the critical role of privacy in E-healthcare and its direct impact on patient trust.

Research Objective 2: To analyze the technical outcome of privacy, secrecy, authenticity, and confidentiality on cybersecurity of the end user.

Research Objective 3: To identify and categorize the current landscape of cyberattacks targeting E-healthcare.

Research Objective 4: To propose a framework for ensuring data security in case of an active attack.

1.5. Research gap

The following research gaps were found during the literature study of this paper:

1) This paper studies more than 20 attack types.
2) Here, a study on privacy analysis is conducted.
3) A seven-stage response framework.
4) An AI-based autonomous agent is proposed.

1.6. Structure of paper

This article has been divided into six sections. In Section 2, the literature analysis on popular cyberattacks on E-healthcare is done with respect to the research article, and in Section 3, a discussion on the various cyberattacks and privacy is elaborated. Section 4 presents the framework for the proposed method. Section 5 presents the findings, and finally, the conclusion in Section 6 summarizes this paper.

2. Literature Reviews

This research article focused on major scientific databases, including Scopus and Google Scholar, from 2020 to 2025. Search keywords were "cyberattacks" such as "ransomware," "DDoS," "MITM," and "IoMT," where an "AI-based defense system" is or is not being used for cyber defense of "privacy in healthcare," while some limitations have been discussed in this article. Only peer-reviewed journal articles published in the English language were included. The study selection followed the PRISMA guidelines.

The technology advances have led to increased vulnerability to attacks. Verma and Shri [15] identified five prevalent attacks: Internet of Things (IoT) attacks, phishing attacks, malware attacks, Distributed Denial-of-Service (DDoS) attacks, and Structured Query Language (SQL) injection attacks. Here, the author analyzed 60 articles and then proposed a word tree for

Table 1
Sensitive and non-sensitive E-healthcare information

Sensitive information	Non-sensitive information
Loss of such information will harm any individual and cause privacy violations. Susceptible to identity theft	Such information bears minimal risk to any individual
Examples like medical reports: MRI, X-ray images, blood test reports, behavioral health perspectives, address, insurance policy number, biometric details, payment details, medication, treatment plan, genetic data, date of birth, name, etc.	Examples are hospital policies, marketing materials, public stats, hospital location, phone number, marital status, hospital name, general phone number, hospital location data, medical record number, hours of working, list of services, etc.
Legally regulated under HIPAA, GDPR, and DISHA, etc., and legally protected	Not subjected to legal protection and are not protected legally
It is mandatory to protect them when stored or when being transmitted	General security measures are taken
Data access should be restricted	Available to the general public
Explicit consent is required	Implicit consent is not required
Clinics, hospitals, and researchers use this data	Researchers, policy makers, and public health agencies use them.
Result in identity theft, discrimination, and legal consequences	Minimal or no harm
Restricted information sharing	Often shareable for analysis
Encryption is a must	Could or could not be encrypted, as it's not valuable
Generate medical records, diagnoses, lab results, genetic data, biometric data, insurance details, payment details, etc.	Generate for aggregate analysis, anonymized research data, public health information, etc.

security threats, helping to navigate between security solutions and control measures. This can be used by organizations as a ready tool to detect attacks and provide a specific solution to cyberattacks, such as regular audits, staff training, setting up an advisory board, installing antivirus software, and performing two-factor authentication, while enhancing security infrastructure. Here, a bibliometric analysis is combined with qualitative research and expert opinions. An emphasis is made on the need for ready-to-refer tools to be available to counter the cyber threats, which are updated in correlation with the attacks.

Legal privacy-preserving acts like Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), European Union Agency for Cybersecurity (ENISA), etc., are studied in Figure 1 based on the number of times they are mentioned in the referred papers. In Figure 2, the number of times various attacks, such as Man-in-the-Middle (MITM) [1, 4, 5, 7, 9, 12, 23, 24, 30, 33], botnet [8, 12, 15], phishing attacks [1, 2, 4–6, 9, 15, 25, 26], etc. have been depicted with the respect to their frequency. It can be concluded that most researchers have mentioned cybersecurity threats in E-healthcare, with malicious attacks [1–4, 7–9, 21, 25, 30, 31, 33–35] occurring most frequently. These attacks are done with the intent to harm an organization. The PRISMA analysis has been depicted in Figure 1. A detailed literature review has been conducted in Table 2, summarizing the major cyberattacks, AI-based defense mechanisms, healthcare applications, key findings, and limitations of previous studies.

Figure 1
PRISMA for this research article selection criteria

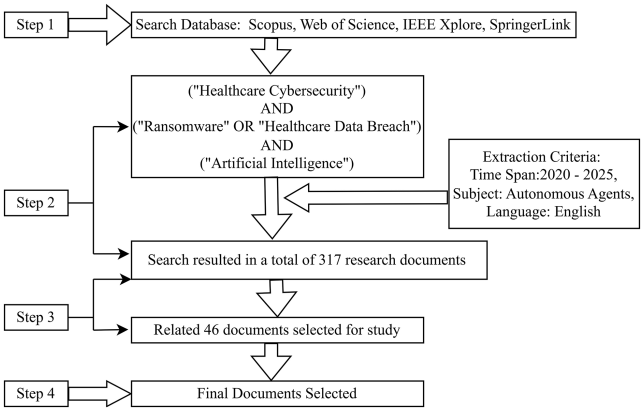
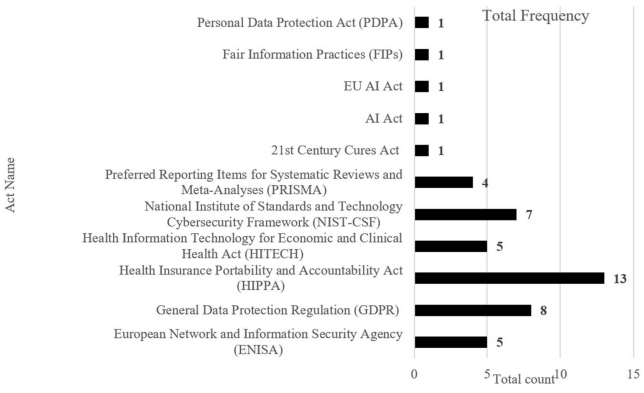


Figure 2
Privacy-protecting acts for E-healthcare data



3. Discussion

The evolution of the Internet has made it necessary for authorities to ensure the privacy and security of E-healthcare data from cyberattacks. Based on the literature in Section 2, Figure 2 shows that previous researchers have discussed the HIPAA Act for privacy preservation, which legally protects E-healthcare information. This graph also depicts the frequency with which these acts have been cited in the previously studied research works.

Figure 3 depicts those research works that have focused on cybersecurity threats and data breaches occurring in the E-healthcare sector. It is observed as a whole that malicious hacking attacks, MITM attack, DDoS, and ransomware attacks are the most frequently occurring attacks nowadays, which result in loss of security and privacy.

3.1. Privacy aspects of an E-healthcare system

Research Question 1: Why is privacy in E-healthcare of great importance?

Privacy is the fundamental right of a person to their personal information. It controls who can and cannot access a patient's information. Loss of privacy can harm any organization's reputation among the general public.

Hence, it is important to gain an understanding of what and why privacy in E-healthcare is of great importance. Privacy in E-healthcare ensures:

Protection against misuse: Privacy ensures no discrimination, no harassment, and no financial loss to an individual.

Safety and security: It prevents stalking and stops people from targeting any individual or individuals, which ensures their physical and emotional well-being, hence ensuring trust among its users.

Builds trust in an organization: The safety of a patient's information increases it could be trust in E-healthcare services, wearable devices, and Electronic Health Records (EHR) Thus, enhancing confidence promotes a positive opinion of an organization as a whole.

Data integrity and safety: Ensures accuracy and prevents errors leading to incorrect treatment of a patient, which could be dangerous or life-threatening in extreme cases.

Legal and ethical compliance: E-healthcare data must legally comply with HIPAA, GDPR, etc., which are strict legal frameworks. They improve the privacy and secrecy of sensitive information. These are followed to avoid heavy penalties and uphold ethical obligations regarding confidentiality and patient autonomy.

Control data access: Robust privacy measures such as role-based access control ensure the authenticity of personal data, especially focused on patient information.

Freedom of expression and thought: Privacy ensures mental freedom, allowing an individual to form independent beliefs, explore, and express their belief without the fear of being judged.

3.2. Consequences of privacy loss

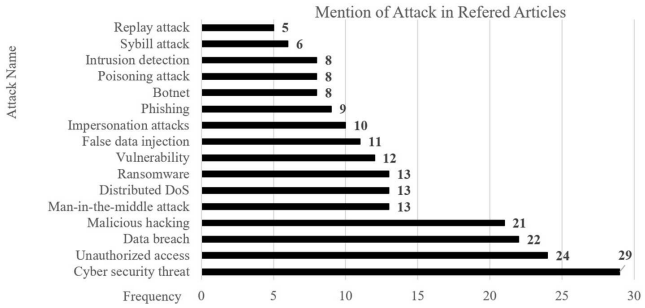
Unauthorized access: Hospital staff accesses the data without the permission of the authorized users. This results in a loss of confidentiality and trust in an organization.

Data breaches [1, 2, 4, 9, 10, 12, 20, 25, 26, 30, 34, 35, 38]: The attackers store, expose, or transmit the data records. For

Table 2
Literature review

Refs.	Attack/security area	Healthcare focus	AI used	Key findings	Limitation
[2]	Healthcare Data Breaches	Healthcare Information Systems	No	Identified major causes of healthcare data breaches and mitigation mechanisms	Limited discussion of AI-based defenses
[4]	Cyberattacks in Healthcare	Hospitals and Clinical Systems	No	Discussed ransomware, malware, phishing, and insider threats	Mostly descriptive review
[6]	IoMT Security	Healthcare IoT Devices	Reinforcement Learning (RL)	RL improved cybersecurity and reduced unauthorized access	Simulation-based validation only
[8]	Botnet Attacks	IoT Networks	Stacked Ensemble Learning	Achieved high botnet detection accuracy with low false positives	Not healthcare-specific dataset
[12]	IoMT Risk Assessment	Internet of Medical Things	Partial	Proposed frameworks for managing IoMT security risks	Lack of implementation details
[14]	DDoS Attacks	Healthcare Network Infrastructure	SVM, Random Forest	High DDoS-detection accuracy using supervised ML	Dataset limitations
[18]	AI Regulations and Security	Digital Healthcare Systems	Yes	Reviewed cybersecurity regulations for AI deployment in healthcare	Focused on policy rather than implementation
[19]	Adversarial Attacks	Medical AI Systems	Yes	Demonstrated vulnerabilities of deep-learning healthcare models	No practical mitigation framework
[20]	Healthcare Cyber Threats	Healthcare Systems	No	Identified socio-technical vulnerabilities and attack vectors	Limited AI discussion
[21]	IoT Cybersecurity Attacks	IoT-enabled Healthcare	Multiple AI Techniques	Systematic review of AI-based attack detection methods	Few healthcare-specific case studies
[23]	Secure Routing Attacks	Smart Healthcare IoT	No	Cross-layer cryptography improved secure communication	Increased computational overhead
[27]	Hospital Cyberattacks	Hospital Systems	No	Reviewed ransomware and operational disruptions in hospitals	Narrative review only
[28]	Healthcare Cybersecurity Threats	Healthcare Organizations	No	Classified healthcare cybersecurity challenges and threats	Limited quantitative analysis
[29]	Pandemic-Related Cyberattacks	Healthcare during COVID-19	No	Highlighted rise of cyberattacks during the pandemic	Focused on COVID-19 period
[31]	Medical AI Agent Attacks	Medical AI Agents	Yes	Identified emerging threats targeting AI agents	Early-stage research
[32]	Privacy Engineering	Healthcare Data Protection	Yes	Reduced re-identification risks using privacy-preserving techniques	Computational complexity
[33]	DDoS Attacks	IIoT Healthcare Systems	Reinforcement Learning	Adaptive defenses significantly reduced attack success rates	Tested in simulated environments
[34]	Ransomware	Healthcare Information Systems	No	Reviewed ransomware attack patterns and impacts	Limited AI-based solutions
[35]	Ransomware	Healthcare Organizations	No	Discussed patient-care disruptions caused by ransomware	Lacks technical evaluation
[36]	Privacy-Preserving AI	High-Risk Healthcare Systems	Yes	Combined privacy protection with attack-aware AI mechanisms	Regulatory focus
[37]	Man-in-the-Middle (MITM)	Healthcare Communication Systems	Hybrid Deep Learning	High accuracy in detecting MITM attacks	Requires extensive training data

Figure 3
Attacks mentioned in the studied articles



example, ransomware or WannaCry [1, 2, 4, 9, 12, 20, 21, 25, 26, 29, 34, 35] attacks. They also result in identity theft, financial losses, and reputational damage to an organization.

Insiders' threats: These occur due to the misuse of data by authorized users or individuals who work for the organization. Employee selling patients' data results in legal penalties and reputational damage for hospitals.

Insecure data transmission: Data is transmitted without applying any proper encryption algorithm, where telemedicine consultation is made over an insecure communication channel, which is prone to an attack. Here, data interception and leakage are done.

Weak authentication: Passwords set by the authorized users are weak or have been shared with third parties. Compromising a user's account and its related data (such as lab. reports, MRI, X-rays, personal sensitive information like payment details, etc.) to hackers.

Data re-identification: Anonymous data gets re-linked to an authentic individual's public EHR; hence, they suffer from loss of anonymity.

Third-party data sharing: Information is shared with third-party applications or vendors without any prior consent from the authentic users.

Cloud storage vulnerability: A less secure cloud storage is used for storing EHR, exposing a huge amount of data publicly, which results in loss or manipulation [1, 9, 10, 33].

Lack of user awareness: Patients are not clearly informed in their consent forms about the data sharing policy and hence are unaware of how their data is being used and by whom.

Device loss and theft: Electronic devices like laptops or mobile devices containing E-healthcare information are stolen, which increases security risk.

3.3. Privacy, secrecy, authenticity, and confidentiality

Research Question 2: What is the technical impact of privacy, secrecy, authenticity, and confidentiality on any user?

Table 3 tabulates the four commonly used terms in cybersecurity: privacy, authenticity, confidentiality, and secrecy. Table 3 infers privacy, confidentiality, authenticity, and secrecy with respect to the various properties. Privacy affects an individual directly and needs to be ensured as per acts such as GDPR. Establishing privacy secures any individual's rights, protecting them from attacks and theft.

3.4. Popular cyberattacks on E-healthcare

The various cyberattacks in E-healthcare, as quoted by the studied research papers, are presented here.

Research Question 3: Cyberattacks currently faced by the E-healthcare sector?

The E-healthcare sector is regularly suffering from phishing, MITM, ransomware, and SQL injection attacks; these are depicted in Figure 4, which is followed by their detailed discussion. Here, the cyberattacks were studied based on their characteristics, how to protect against them, the side effects they result in, how these attacks take place, and so on.

Malicious attacks [2]: These attacks are done with the intent to harm and often include ransomware attacks. Complete access to cloud resources [10] is given. They often harm patient safety and clinical outcomes.

Ransomware [25] or WannaCry attack [1, 12, 20]: The attacker encrypts the data and asks for money as ransom; otherwise, they will delete the data. Exploiting the Windows vulnerability called Eternal Blue. The attacker locks the devices, making the service inaccessible to all users. Results in loss of reputation for hospitals and any other industry. To prevent these attacks, organizations should maintain offline backups following the 3-2-1 backup rule, regularly update systems, deploy endpoint protection, and prepare an incident response plan.

Malware [12, 34]: An application software that does not do what it is intended for or allows unauthorized users to access your computer, who disrupt and destroy data. Malware is usually attached to an email sent by a suspicious sender; it could be an unknown freeware, a plug-in, or an unknown USB drive, resulting in the installation of malware on your system, for example, botnet, worm [36], spyware, and Trojan horse [4, 5, 15]. Preventive measures include setting up a firewall [3, 10, 29], installing antivirus software, providing staff with proper training, restricting admin rights, removing redundant software, setting up a security advisory board, implementing anti-ransomware, and implementing an anti-exploit system to ensure the safety of E-healthcare data.

Phishing [1, 26]: Gathering information by social engineering [4] or disguising oneself as an authorized entity through email or any form of communication to steal passwords, banking information, or credit card details. Phishing attacks mostly target Software as a Service (SaaS), Webmail, Financial institutions, cloud storage, and social media. To prevent such attacks, employee activity should be monitored, and employees should be trained to identify and report fake phishing emails.

1) Types of phishing attacks

Spoofing email: Forged email that appears legit, resulting in the reader opening it, hence, loss of personal information.

Spear-phishing: The attacker targets a specific group of individuals (such as senior citizens, etc.) who are a more vulnerable part of society.

Whaling: Targeting the high-ranking officers with the spear phishing attack.

SMiShing: SMS phishing impersonating law officials and bank authorities, leading to the victim downloading malware.

Vishing (voice phishing): Here, VoIP is used by an attacker to impersonate trusted authorities like banks and law enforcement agencies and trick them into surrendering confidential information.

Search engine phishing: A fake website with incredible deals is indexed by legit search engines, which leads the victim to give away their confidential information [9].

Pharming: The Domain Name System (DNS) file of the victim is modified, which makes the legit user open a bogus website [38].

Table 3
Study on privacy, authenticity, confidentiality, and integrity

Privacy	Authenticity	Confidentiality	Secrecy
When, how, and to what extent their personal data can be shared with others. Regulated under GDPR and the Digital Personal Data Protection Act (DPDPA)	It refers to the truth of an electronic record irrespective of its exposure to third-party attacks	Protect medical history and treatment details during diagnosis	Maintaining trade secrets is an alternative to patents
Control over browser history	Using a password to log in	HIPAA-protected medical records	Hiding information
The individual	System/protocol	Organization/professionals	Anyone
Personal boundaries	Verification of identity	Protection from disclosure	Intentional concealment
Keeps information hidden	Ensures the sent and received information is the same	State of being apart from the company or observation, or prevents information from being disclosed to unauthorized users	Intentional withholding of information from others
Restrict a person from accessing people's personal information	Technique to ensure information security	Restrict unauthorized users from accessing confidential information	Imply with the intent to avoid consequences
Personal choice	Authenticity is a trade	Professional obligation	Personal choice
It is right	It's an assurance	It is an agreement or obligation	It's a barrier
State of being away from people's attention	State of being sure that the message received is the same as the one sent	State where certain information is kept secret	State of hiding, concealing information from others
Example: privacy setting on social media	Admitting your failure openly	Example: ATM pin and bank account number	Example: sexuality, substance dependencies, and abortion history
Privacy is about people	Authenticity is about the data or information	Confidentiality is about information	Secrecy is about people
Patients have the right to choose whether their data should be disclosed or not	The doctor ensures patient records are safe	Using a fingerprint scan or a password to unlock your mobile	Doctor intentionally hides medical error
A personal right	Professional duty	Security check	Tactical choice
To maintain autonomy and personal boundaries	Fulfill trust or legal contract	To prevent spoofing or impersonation	To gain strategic advantages

2) Phishing attacks result

Losses: Loss of sensitive information of patients and stakeholders, which could lead to money theft, computer breakdown, etc.

Loss in customer trust: Decreases E-healthcare users' trust in an organization.

Loss in brand reputation: Even when phishing sites are removed, the lack of customer trust leads to blacklists.

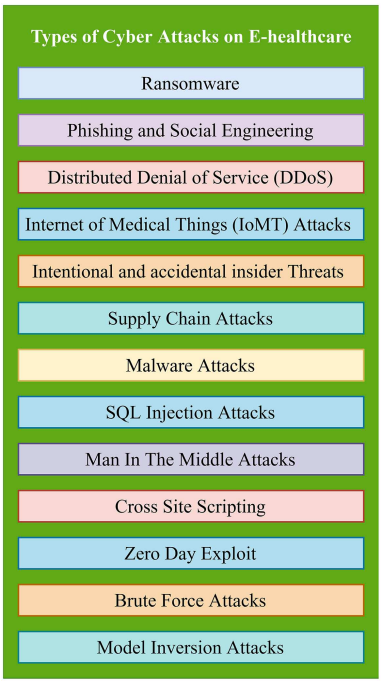
Identity theft [5, 34]: Resulting in financial theft, psychological, and even emotional damages to an individual.

Distributed Denial of Service (DDoS) [1, 2, 4, 5, 7–9, 12, 14, 15, 21, 23, 26, 28, 29, 33]: The targeted server is overwhelmed with requests, resulting in flooding of requests, rendering it unusable to authentic users. To avoid DDoS attacks, companies need to have multilayer security controls, train employees on DDoS attacks, build a strong security infrastructure, and have an incident response team. Network traffic should be monitored regularly, and the firewall security and a content delivery network should be used, which can manage the traffic on a network irrespective of the data volume being transmitted. In case such attacks have already taken place, then remove malicious elements trying to access the services, restore the service to the previous state before the service was attacked, improve the mitigation strategies, and use a more secure encryption algorithm. Support vector machine (SVM), Logistic Regression, Random Forest (RF), K-Nearest Neighbors (KNN), Decision Trees, supervised, and principal component analysis machine learning models help detect the DDoS [14].

Internet of Things (IoT) attacks [36]: Here, the attacker tries to sniff information by targeting smart devices or IoT devices. To prevent such attacks, a response plan should be kept ready, while the use of complex passwords should be mandatory, a secure environment should be set up, and two-factor authentication should be used. Attack types on IoT are:

a. Device hijacking: An attacker gains access to IoT devices and uses them for spying, gaining access to passwords and their services.

Figure 4
Popular cyberattacks in E-healthcare



b. Data breaches: Personal or healthcare data collected from wearable or smart devices is stolen or lost and then sold to those who exploit the stored data.
c. Firmware exploitation: Old firmware that has not been updated and patches that need to be fixed have not been applied. Attackers use them to gain deep control of a device.

SQL injection attacks [5, 8, 9, 12, 15, 23]: Attackers exploit the query application made to the database by inserting a malicious SQL query. To prevent them, delete database functions not required anymore, perform penetration testing, change pre-installed passwords, update passwords regularly, and reboot systems frequently. It is a good practice for account holders to regularly update their password and select a strong password and avoid extended organizational URLs (avoid including deep file paths, session IDs, and tracking parameters in URLs).

Man in the Middle (MITM) [12, 23]: The attacker intercepts the message and then alters it without the knowledge of the intended parties to steal the data. This attack results in fooling and spoofing information [23]. Here, medical devices (pacemakers and infusion pumps) are manipulated, which often results in misdiagnosis or could even lead to death. Internet of Medical Things (IoMT) devices are vulnerable because they lack encryption and are often targeted by Address Resolution Protocol (ARP) and DNS spoofing attacks. The hospital's Wi-Fi is public, hence prone to being set as an evil twin, which tricks staff and the public into sharing their login and credentials with it. The use of an outdated Windows OS or an old OS that is not updated with patches results in these attacks. To make sure they do not occur, stronger encryption, such as TLS 1.3, should be made mandatory while allowing only specific server users to use it on their specific devices.

3) Protect against MITM

Strong awareness training of the staff on phishing and malware attacks.

Apply TLS 1.3 to ensure security while transmitting and securing data stored with an encryption algorithm such as AES.

Certificate pinning that ensures that mobile healthcare applications that have specific and verified servers can access such information.

Using a server that follows a zero-trust network access, where no user is trusted, and continuous verification is done to ensure authentic users.

Multi-factor authentication (MFA) ensures that even if the passwords are stolen by MITM, they cannot access the account without the second verification.

Endpoint security: The device should have the firewall set up, and regular patch work updates should be done while constantly checking the firewall. Cloud Access Security Broker: It can identify unauthorized system access and detect anomalies. Account Cleanup: Regular password updates and set up a strong password.

Cross-Site Scripting (XSS): An attacker injects a malicious script into content viewed by users (steal cookies, session tokens, or redirect users).

4) Types of XSS

Stored XSS: A malicious script is permanently stored on the target server.

Reflected XSS: Here, a malicious script is a part of the URL.

DOM-based XSS: The Document Object Model (DOM) on the client side is manipulated.

Fallout of XSS attack: (i) Session hijacking, (ii) credential theft, (iii) defacement, (iv) malware distribution, (v) unauthorized actions, and (vi) sensitive data exfiltration.

5) Measures to safeguard against XSS

Input validation must be done in order to remove harmful characters (<, >, etc.), output must be encoded and CSP which will limit execution of only trusted scripts on a webpage.

Zero-day exploits [34]: An attacker targets previously unknown vulnerabilities, hence giving developers no time to patch the website before the attack.

Brute force attack [3, 7]: Systematically trying to crack the password or encryption key by all possible combinations until found. It is the most popular attack on the cloud [10]. Table 4 states the types of brute force attacks and how to prevent and defend against these attacks.

Table 3 helps infer that generally attackers exploit human habits of users and use personal details for setting passwords. MFA, hence granting access only after authentic password and a combination of mobile verification has been done, is the best defense against cyberattacks. Reverse brute force attacks can only be prevented if the correct details like IP address, device fingerprint, or timing are right; otherwise, it could be an attack. Also, users are advised to add salt before their passwords to prevent a rainbow table attack.

Insider attack: Here, hospital staff (nurses, doctors, lab technicians, etc.) misuse patient or patient's sensitive information. Often resulting in loss of secrecy and privacy, therefore decreasing patient trust in the hospitals.

Membership interference attack or tracing attack: Disclosure of this information facilitates discriminatory practice, which exploits the existing vulnerability of a particular dataset. This dataset has been used for developing the machine learning model. The attacker targets the model, focusing on exploiting the weakness in the existing dataset.

Differencing attack: Focusing on comparing the output. The attacker learns insider information about individuals and compares them. It is a privacy breach attack where sensitive information is isolated about a specific patient compared after aggregating information.

Model inversion attacks: Reconstruction of sensitive features of the training data. For example, for a face recognition model, what were the initial feature criteria that form the basis of how software recognizes a face?

Man in the cloud: This is a modified version of the MITM attack that is aimed at cloud storage systems. The process entails the following: 1) The attacker installs a malware tool or application on the cloud system. 2) Token theft: The token is stolen by the attacker, who later uses it to conduct attacks. 3) Account takes over: They use the stolen token to connect their devices to the victim's cloud storage devices. 4) Malicious payload: Malware-infected files are stored on the E-healthcare cloud, and these infected files are synchronized with the cloud. They can remove the switcher malware and erase evidence of an attack.

Unintentional disclosure [2]: Illegal access that causes loss of privacy and secrecy of the patient's information. Accidental leakage of sensitive patients' information caused by human error or technical slipups. The reasons are: 1) Human error: Leaving their computer with patients' data unattended and open to all. 2) Sharing sensitive data to misaddressed emails: Hacking [1, 2, 4, 8–10, 12, 14, 20, 22, 25, 31] like ransomware and malware, which exposes personal healthcare data, theft of laptops, disks, and

Table 4
Classification of brute force attacks

	Characteristics	How these attacks work	Prevention and defense
Simple brute force attacks	• Manual Guessing • No Intellectual Strategy • Targeting Weak Credentials Scale	• Password guessing is done manually • Passwords are a combination of personal details • Successful, as most people use weak passwords or the same password on multiple websites	• **Adding Multi-Factor Authentication (MFA)** makes password loss insufficient • **Account Lockout Policies:** after 3–5 wrong attempts, the account is locked temporarily • **Complex Passwords/ Passphrases:** Using a password that has 12–15 characters and a special symbol and number will increase the time to crack the password • **CAPTCHA:** They help block bots- based attacks • **Progressive Delays:** Increasing the time between allowed login attempts after each failure to frustrate attackers
Dictionary attacks	• Predefined Wordlists • Targeted Human Habits • High Efficiency and Speed • Automation • Hybrid Mutations • Regional Customization • Two Modes of Operation: Online and Offline	• A target is selected to test possible passwords • A dictionary is used by the hacker, which is time-consuming, and the success rate is low	• **Multi-Factor Authentication (MFA)** • **Strong Passphrases:** Use long, random strings of 12–15 + characters rather than single words • **Account Lockout and Rate Limiting:** Automatically locking an account after 3–5 failed attempts stops automated guessing in its tracks • **Salting Hashes:** adding "salt" will prevent rainbow table attacks
Hybrid brute force attacks	• Predictive Pattern Matching • Intelligence-Led Wordlists • Computational Efficiency • Automated Variations	• Combination of simple and dictionary attack methods • Hacker tries a list of expected passwords and then a combination of letters and characters • Most commonly used passwords can be found by them	• **Zero Trust Architecture** • **AI-Powered Monitoring:** to identify login attempts from unknown IP addresses • **Salting Hashes:** addition of "salt" followed by password makes password detection impossible • **Account Lockouts and Rate Limiting:** lock the account after 3–5 failed login attempts • **Multi-Factor Authentication (MFA):** Even if a hybrid attack successfully guesses a password, MFA acts as a final barrier to unauthorized entry
Reverse brute force attacks	• Targeting the "Least Common Denominator." • Evasion of Lockout Policies • High Efficiency • Leverages Predictable Healthcare Username • Credential Source	• An attacker tests the known password found during network breaches and then weak passwords	• **Multi-Factor Authentication (MFA)** • **Unique Usernames:** make unique passwords other than the first and last name • **Behavioral Analytics:** AI tools could stop users from using the same password across multiple accounts • **IP Rate Limiting:** A tool to block IPs trying to log in to multiple accounts

(*Continued*)

Table 4
(*Continued*)

	Characteristics	How these attacks work	Prevention and defense
Credential stuffing	• Reliance on Password Reuse: • High Success Probability • Massive Automation • Bypassing Traditional Brute Force Defenses • Geographic Distribution (Proxy Use)	• The Attacker exploits the weak passwords. Mostly successful in case the same passwords are used on multiple websites, or use identity-driven passwords	• **Multi-Factor Authentication (MFA)** • **Bot Management and Detection:** real-time AI tools to differentiate human from bot login • **Device and Connection Fingerprinting:** Identifying suspicious sessions by analyzing parameters like OS, browser version, and time zone to flag bot-like patterns • **Breached Password Screening:** Services like Have I Been Pawned or Application Programming Interfaces (APIs) that block users from selecting passwords already found in public leak databases • **Unpredictable Usernames:** Avoiding the use of email addresses as usernames, email/password pairs are the most common data leaked in breaches

portable drives containing patient personal data [25], and sending email, faxes, and medical charts to a third-party user. This is caused by working too quickly or trusting the autofill feature. 3) Technical and procedural issue**:** Malware application shares patient data without the knowledge of the patient and the hospital. 4) Lack of training and awareness: Inadequate staff training and lack of awareness of digital tools. 5) Incorrect disposal of electronic devices (such as USB, memory cards, or hard disks) without erasing them before throwing them in the trash. This leads to data confidentiality breaches, distrust in patients, incorrect or delayed treatment, and legal and financial penalties. Preventive measures, such as regular training of staff, enforcing clear policies, automatic screen lock, secure communication policies, and regular review of logs, will help identify and correct potential vulnerabilities.

Channel attack [13]: Stealing sensitive information while disrupting critical lifesaving devices is a side channel attack. Injection of electromagnetic interference into a pacemaker or pump can result in a lethal shock to a patient. Most medical devices can be vulnerable to attack. Side-channel attacks can be thwarted using AI-powered monitoring systems that will detect abnormal IoMT device signals, disable unnecessary ports in the hardware, and use tamper-proof casing to stop side-channel attacks.

Differential attacks [13]: This method is used against block ciphers, stream ciphers, and hash ciphers, which exploit the relative difference between the plain and the encrypted text.

Botnet attacks [12]: It is a strategy-based attack that makes detection and prevention difficult. The diverse nature of the IoT devices on the network and protocol makes it challenging to analyze a large volume of network traffic and system logs for botnet detection.

Common attacks carried out by Botnets:

a. DDoS attack: Server is targeted with a large amount of traffic, leading to a crash and disrupted services.
b. Spam and phishing: Spam links are used to spread the malicious software.
c. Data theft: Bots steal confidential financial information.
d. Crypto-currency mining: Bots help mine cryptocurrency.
e. Ad fraud [39]: Bots create fake clicks on online advertisements.
f. Adversarial attacks [3, 39]: Where the input is modified such that the machine learning model makes an inaccurate prediction. Types of adversarial attacks:
g. Evasion attack: Here, the input is modified
h. Poisoning attack [12]: Manipulating the trained dataset.
i. Inference attack [44]: Querying the model to steal parameters and reconstruct the sensitive data.

The inference of this section gives an understanding of the most popular kinds of cyberattacks, such as malware, phishing, ransomware, DDoS, and MITM attack. To prevent attacks, the user must use an updated version of their operating system, the firewall should be active, regularly scan the system with antivirus and malware detection software, and they should use MFA, which will ensure the privacy and security of any user.

4. Proposed Method: Stages for Dealing with Cyberattacks in E-healthcare

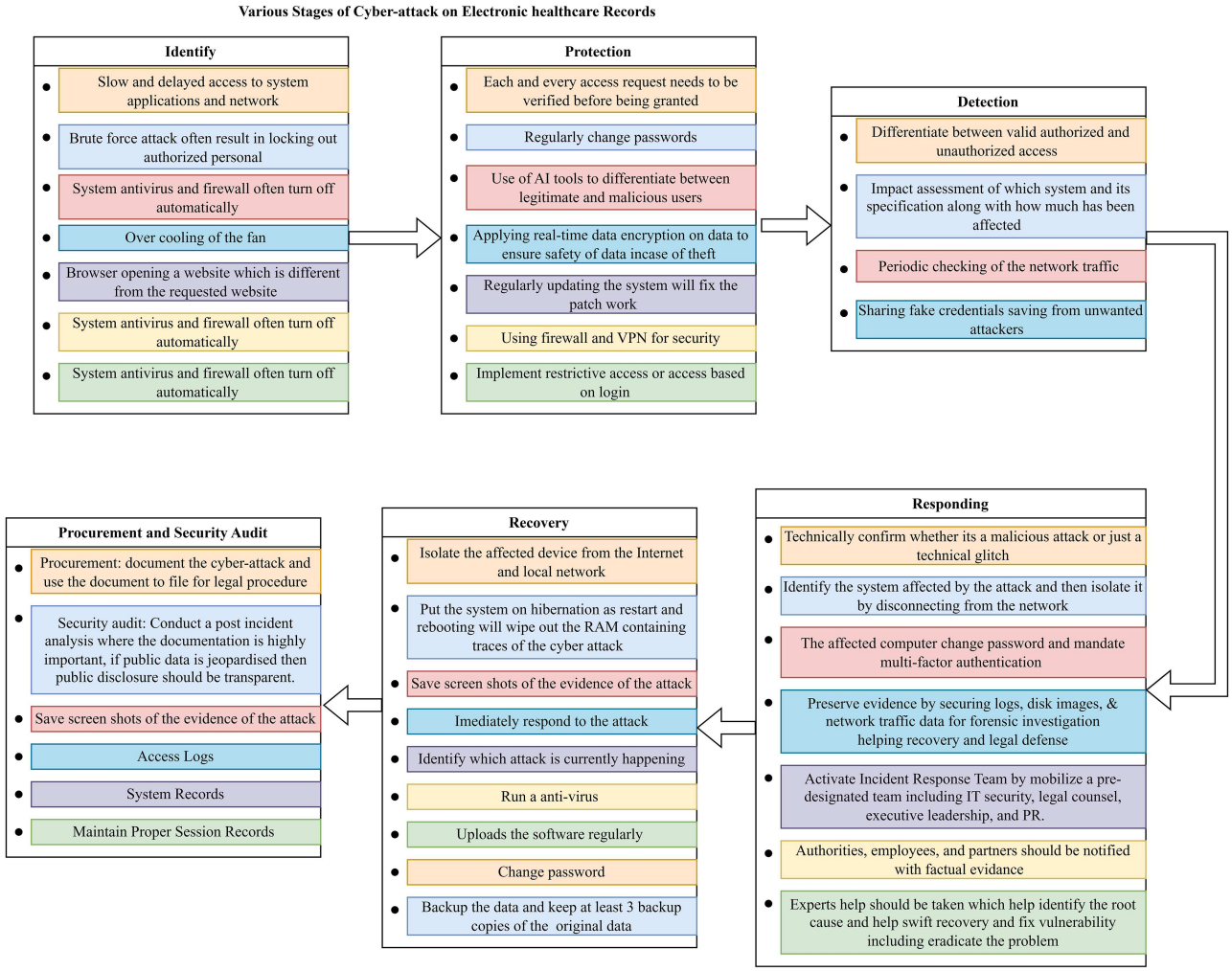
Research Question 4: What framework should the E-healthcare sector follow in case of an active cyberattack?

Figure 5 depicts the stages of the framework that should be taken in case of a cyberattack on E-healthcare.

Identify: How cyberattacks are identified: 1) The computer system performance reduces significantly, 2) there is an unusual amount of network traffic, 3) sudden and unexplained mouse movement on screen, 4) antivirus software and firewall [30] get turned off automatically, 5) unexpected pop-ups open up, 6) passwords get changed suddenly, 7) bots can even create and send messages which the users have no previous knowledge of, 8) unrecognized financial transactions take place in the bank account, and 9) the browser opens a website other than the one requested. Any one of these occurrences is a sign of an attack happening on the computer system.

Protection: To safeguard against cyberattacks, a user should be trained on: 1) Use of a multi-factor authentication (MFA), 2) a strong password, 3) changing passwords after every 3 months, 4) regularly update software, 5) back up critical data regularly to ensure concurrency, 6) train staff and doctors to not to click on spurious links received as email or messages, 7) install and run an antivirus and anti-malware software regularly and firewall, and 8) have an incident response team ready with an action plan in case of an active cyberattack is spotted.

Figure 5
Steps taken when a cyberattack happens in E-healthcare



Detection [12]: To be able to find out if an attack is happening or not. When the system is under a cyberattack, usually its performance is slowed; it frequently freezes or crashes suddenly, and in some cases, the device restarts itself. Resources like memory, CPU, etc., are used up, the number of pop-ups increases, and there is a spike in network activity. Changes in device: unknown application installed, missing or changes in files, browser redirected, firewall, and antivirus software have been disabled without the authorized users' knowledge. If confidential information is demanded (such as personal details, banking details, credit card numbers, etc.) by a spurious email, SMS, WhatsApp, etc., based on the nature of the service affected, the type of attack could be pinpointed, and hence, an appropriate response can be selected.

Responding: The first thing is to remain calm, confirm the identity of the sender before opening or replying to the mail, avoid giving out any confidential information (bank account number, etc.), notify the appropriate authorities about the attack, do not give access remotely to the system, keep up-to-date with software in your electronic gadgets, conduct a scan of your gadgets now and then, check the phone numbers while calling through SMS or WhatsApp, and for the websites, always confirm the URL and also check for padlock symbol, confirm any grammatical mistakes in the URL, isolate the infected system (disconnect internet connection, use an incident response plan that isolates the affected gadget, and attempt recovering the gadget from the cyber-attack), and record the cyber-attack as it needs to be reported to the authorities along with notifying the stakeholders and customers with the help of a legitimate expert dealing with the cyber-attack.

Recovery: To safely recover the information that was targeted, users should run antivirus software, use Windows' built-in malware removal tool to remove malware software, review account login history, monitor network connections in case of an unknown network, immediately disconnect, regularly back up their data, and change passwords. In certain cases, it is advised to reformat the operating system. Eradicate the system by formatting or removing the malware software and then patch the vulnerability so that future attacks can be stopped. This will restore the system to a safe state or load a safe version from the backup.

Procurement: Document the cyberattack and use the document to file for a legal procedure.

Security Audit: Conduct a post-incident analysis where the documentation is highly important; if public data is jeopardized, then public disclosure should be transparent.

The cyber defense strategies in E-healthcare are of great importance.There is an urgent need for intelligent cybersecurity agents capable of responding autonomously to evolving cyber threats in healthcare environments.

5. Findings, Synthesis, and Future Research Directions

Composite framework: It is a multilayered cybersecurity architecture that combines traditional risks. This multilayer architecture has robust defenses. It is a protective, ready-to-use framework that protects organizations from the most frequently occurring attacks, where staff training is highly emphasized [1]. Various components of the composite framework are:

1) Physical components: Direct interfacing with the IoMT uses the AES encryption algorithm and a tamper detection mechanism to secure data at the source.
2) Virtual component (digital twin): Creating a real-time virtual replica to monitor operational cost.
3) Blockchain components: In blockchain, Hyperledger, or using a smart contract to automate access control, ensuring medical logs cannot be altered by attackers.
4) Analytical components: AI-driven employs machine learning to identify threats and predict future vulnerabilities based on past attacks.

Expert elicitation protocol:Step-by-step process for consulting an expert in dealing with the uncertainty. Cybersecurity experts should be hired and trained on cyberattacks and their vulnerabilities. Real-world examples for mitigating the threat if an attack occurs. This process will help in developing a better risk management process. The use of Anti-Phishing Working Group (e.g., Kaspersky) will help in detecting anti-malware. Mock drills and simulations were conducted where cyberattacks were simulated to find weaknesses. The mitigation technique reduces overfitting and adds privacy. It can be done with:

1) Minimum access is granted: As per the user's job profile.
2) Software update and patch management on outdated software could ensure security.
3) Employee training and awareness: Human error causes breaches, and how to identify phishing attacks, using secure passwords.
4) Data encryption and backup of sensitive data when stored or while being transmitted over a network, making it non-understandable or non-readable to an attacker for quick recovery.
5) Firewall and network segmentation: Set a barrier and control incoming traffic, blocking unauthorized access.

Darktrace AI for Threat Detection is an AI-based security platform that learns users' behavioral patterns to detect anomalies and cyber threats in IoMT environments. CrowdStrike Falcon is an AI-driven endpoint protection platform deployed on laptops and other endpoints to defend against ransomware and malware attacks. IBM QRadar AI provides intelligent security information and event management (SIEM) and incident response capabilities, serving as the central security operations platform for e-healthcare organizations. Microsoft Defender AI is a cloud-integrated security platform that protects cloud and hybrid environments and is widely used to secure telemedicine services and cloud-based health records. Palo Alto Cortex XDR is an AI-driven extended detection and response platform that provides security across endpoints, networks, cloud platforms (including AWS, Google Cloud, Microsoft Azure), and Kubernetes environments within hospital networks. Designing an autonomous cybersecurity agent begins with detecting an ongoing attack in real time. This is done by continuously monitoring the network traffic and checking session log files for corruption or unusual activities. Then, thinking using the already available dataset, it should be able to identify an anomaly. Followed by the act, here the agent acts as per the attack pattern that is taking place. Finally, it learns and records the observation of the attack into the dataset for future timely response and learning. This has been depicted in Figure 6. A framework suitable for a small sector organization having stages like identification, protection, detection, response, recovery, procurement, and security audit needs to be designed as per the needs. In Table 5, the various frameworks have been compared to cybersecurity features.

The available framework is not customized as per the needs of the E-healthcare sector. A framework having stages like identification, protection, detection, response, recovery, procurement, and security audit needs to be designed as per the needs of the E-healthcare sector. Table 6 presents the various works done by

Figure 6
Design of the autonomous cybersecurity for E-healthcare

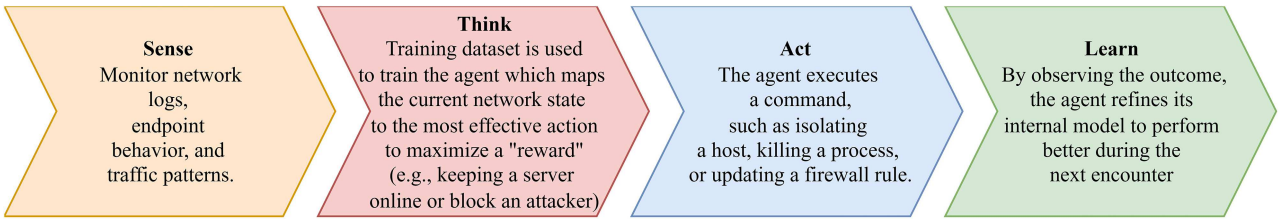


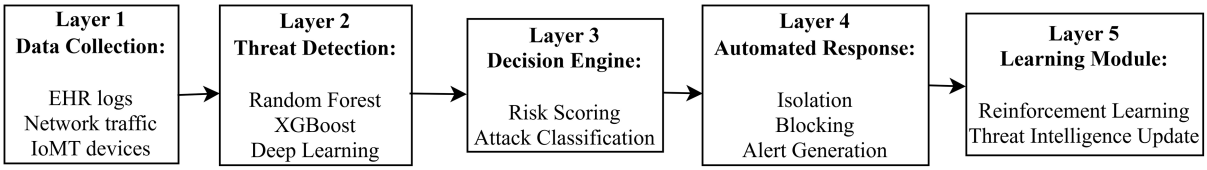
Table 5
Framework analysis

Feature	NIST CSF	ISO 27001	Proposed framework
Generic Cybersecurity Controls	✓	✓	✓
Healthcare Data Protection	Partial	Partial	✓
EHR-Specific Security Focus	✗	✗	✓
IoMT Device Security	Limited	Limited	✓
Patient Safety Consideration	✗	✗	✓
Healthcare AI Threats	✗	✗	✓
Autonomous Cybersecurity Agent	✗	✗	✓

Table 6
Findings and inferences from researcher's work

Specific areas	Findings	Inferences
AI-driven threat detection in healthcare and IoT	Hybrid deep-learning models for network-attack detection report accuracies above 98% and FPRs below 0.08 on benchmark datasets (e.g., CICIDS-2017), outperforming traditional ML models such as KNN or SVM In IoT-botnet-detection work, stacked ensemble-learning models can achieve F-measures above 0.95 and very low false-positive rates on large-scale IoT traffic DDoS-detection models using supervised ML (e.g., SVM, Random Forest) on healthcare-related infrastructure data show detection rates of 90–97%, with precision and recall both above 90% in selected configurations	Deep and ensemble models significantly improve the ability to distinguish legitimate traffic from attacks in highly imbalanced datasets, which is typical in healthcare IoT environments Low False Positive Rate (FPR) is critical in healthcare so that Intrusion Detection System (IDS) alerts do not overwhelm clinicians; model architectures that jointly optimize recall and FPR are preferred for operational deployment
Security of AI/ML models in healthcare applications	Experimental work on "evasive adversarial attacks" against Android-malware-detection models shows that small, carefully crafted perturbations can reduce model accuracy by 15–30 percentage points while remaining visually or functionally indistinguishable from benign samples Studies on medical-AI-agent security report that adversarial examples can increase misclassification rates by 20–40% under certain constraints, particularly when the adversary has query access to the model Privacy-preserving AI frameworks (e.g., under EU-AI-Act-style constraints) can reduce re-identification risk by >70% via differential privacy or homomorphic encryption, albeit at a modest drop in prediction accuracy (often 2–5 percentage points)	AI-based defenses in healthcare are powerful but introduce new attack surfaces; adversarial robustness and model-inspection metrics must be part of any clinical-AI deployment Privacy-enhancing AI techniques trade off some model performance for compliance and privacy, suggesting that "operational" AI models in healthcare should be tuned per use case (e.g., risk tolerance for false-positive clinical alerts)
Data breaches and ransomware in healthcare systems	Reviews of healthcare data breaches report that >70% of incidents involve hacking/IT incidents (including ransomware and phishing), while insider threats and loss/theft account for <20% combined in many datasets Ransomware-related downtime in hospitals can cause >70% of affected institutions to experience delays in care delivery, with typical downtime measured in days to weeks Systematic reviews of cyber threats to health information systems show that phishing and credential-harvesting attacks are the most common initial vectors, responsible for ~40–60% of analyzed breaches	The dominance of external hacking and ransomware implies that perimeter-focused defenses (firewalls, endpoint detection, and incident response planning) are as critical as staff-training programs The high proportion of phishing-driven breaches supports investment in simulated-phishing exercises and continuous security-awareness training, especially among clinical staff
Security frameworks, regulation, and policy-driven controls	Reviews of digital health cybersecurity regulations note that >80% of recent AI in healthcare guidelines explicitly require risk assessment, transparency, and audit trails but provide few quantitative testing standards Privacy engineering studies for anonymized healthcare data show that re-identification risk can be reduced by two orders of magnitude (e.g., from >1% to <0.01%) when strong k anonymity or differential privacy mechanisms are applied Policy-oriented reviews of hospital cybersecurity risk gaps find that ~60–80% of identified vulnerabilities are software and configuration related rather than hardware level, indicating that configuration management and patching are high-impact levers	The concentration of risk in software/-configurations and the lack of explicit quantitative AI testing standards point to a need for standardized "AI security test beds" and continuous compliance automation Strong privacy engineering substantially lowers re-identification risk, suggesting that de-identification pipelines in healthcare should be treated as part of the core security architecture, not just an administrative step
IoT-enabled and Industrial Internet of Things (IIoT)-secured healthcare infrastructures	Reinforcement learning-based security schemes for healthcare IoT can reduce unauthorized access attempts by >80% in simulated environments, at the cost of a small increase in authentication latency (e.g., <50 ms) Cross-layer cryptography and secure routing protocols for smart healthcare IoT report <1% packet loss increase and <3% delay overhead under attack conditions, while maintaining near 100% data integrity on simulated traffic Adaptive moving target defense strategies for IIoT-based DDoS mitigation can reduce successful attack volume by >75% while maintaining service availability above 95%	Lightweight crypto and adaptive defense schemes can provide strong security for resource-constrained medical devices without degrading clinical usability RL-based and adaptive mechanisms are promising for dynamic healthcare environments where threat profiles change over time, but they require careful tuning to avoid service quality degradation

Figure 7
Architecture components an autonomous system should have



researchers. Their findings are summarized, and inferences have been drawn.

The basic architectural components that an autonomous agent should focus on have been depicted in Figure 7.

6. Conclusion and Future Scope

A detailed study on cyberattacks currently happening on E-healthcare systems and the importance of privacy in E-healthcare has been included in this article. Privacy should be ensured legally, as per HIPAA, GDPR, etc. In this article, a study on privacy, secrecy, authenticity, and confidentiality is conducted. This article contributes by providing a detailed understanding of the various cyberattacks on E-healthcare, such as malware, phishing, ransomware, DDoS, IoT, SQL injection, MITM, Cross-Site Scripting, and brute force attacks, which have been discussed in detail, followed by the types of brute force attacks, such as simple, dictionary, hybrid, reverse, and credential brute force attacks, which have been tabulated, and then the steps to deal with cyberattacks, including identification, protection, detection, response, recovery, procurement, and security audits. A vital need for an organization is to train staff on cyberattacks as they try to steal, modify, and alter information, resulting in cyber risks. There is a need to develop robust cybersecurity measures and also enhance technology awareness and preparedness to protect against attacks. Finally, an autonomous cyber defense agent was discussed as a solution that has seven stages for response against cyberattacks faced by E-healthcare. It even helps its users avoid unknowingly clicking on spurious links or on bogus websites. It can even help monitor employee network activity. The autonomous system is an AI-based cybersecurity system. They have a faster response time and can stop an active attack from even happening. While a passive attack can be detected and removed. The flexible nature of cyberattacks makes them more adaptable in case the attack strategy changes. In the future, an AI-driven model could be formulated that can help identify attacks and even defend against them for a small organization.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Divya Sharma: Conceptualization, Methodology, Software, Formal analysis, Resources, Data curation, Writing – original draft, Visualization. **Chander Prabha:** Conceptualization, Methodology, Validation, Formal analysis, Investigation, Writing – review & editing, Supervision, Project administration. **Amna Bamaqa:** Software, Investigation, Resources, Data curation. **Wedad O. Alahamade:** Formal analysis, Investigation, Resources, Data curation, Writing – review & editing, Visualization. **Mohammad Zubair Khan:** Validation, Supervision, Project administration.

References

[1] Neoaz, N. (2025). Harnessing artificial intelligence for cybersecurity in healthcare and food processing: A review of emerging trends and the role of generative models like ChatGPT. *Global Trends in Science and Technology*, *1*(3), 144–162. https://doi.org/10.70445/gtst.1.3.2025.144-162

[2] Nemec Zlatolas, L., Welzer, T., & Lhotska, L. (2024). Data breaches in healthcare: Security mechanisms for attack mitigation. *Cluster Computing*, *27*(7), 8639–8654. https://doi.org/10.1007/s10586-024-04507-2

[3] Ahmad, N., Saleem Rana, A., Jalil Hadi, H., Bashir Hussain, F., Chakrabarti, P., Alshara, M. A., & Chakrabarti, T. (2025). GEAAD: Generating evasive adversarial attacks against Android malware defense. *Scientific Reports*, *15*(1), 11867. https://doi.org/10.1038/s41598-025-96392-x

[4] Bhosale, K. S., Nenova, M., & Iliev, G. (2021). A study of cyber attacks: In the healthcare sector. In *2021 Sixth Junior Conference on Lighting*, 1–6. https://doi.org/10.1109/Lighting49406.2021.9598947

[5] Menzel, V., Hurink, J., & Remke, A. (2025). Real-world case studies for a process-aware IDS. *Energy Informatics*, *8*(1), 86. https://doi.org/10.1186/s42162-025-00545-1

[6] Nadhir, A. M., Mounir, B., Abdelkader, L., & Hammoudeh, M. (2025). Enhancing cybersecurity in healthcare IoT systems using reinforcement learning. *Transportation Research Procedia*, *84*, 113–120. https://doi.org/10.1016/j.trpro.2025.03.053

[7] Ruambo, F. A., Masanga, E. E., Lufyagila, B., Ateya, A. A., Abd El-Latif, A. A., Almousa, M., & Abd-El-Atty, B. (2025). Brute-force attack mitigation on remote access services via software-defined perimeter. *Scientific Reports*, *15*(1), 18599. https://doi.org/10.1038/s41598-025-01080-5

[8] Ali, M., Mushtaq, M. F., Akram, U., Aray, D. G., Vergara, M. M., Karamti, H., & Ashraf, I. (2025). Botnet detection in internet of things using stacked ensemble learning model. *Scientific Reports*, *15*(1), 21012. https://doi.org/10.1038/s41598-025-02008-9

[9] Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*, 862221. https://doi.org/10.3389/fdgth.2022.862221

[10] Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109. https://doi.org/10.3390/s22031109

[11] Chen, G., & Jin, G. (2024). Insights from evidence-based medicine method for building security systems against terrorist attacks in hospitals. *Journal of Multidisciplinary Healthcare*, *16*, 4133–4137. https://doi.org/10.2147/JMDH.S426166

[12] Svandova, K., & Smutny, Z. (2024). Internet of medical things security frameworks for risk assessment and management: A scoping review. *Journal of Multidisciplinary Healthcare*, *2024*(17), 2281–2301. https://doi.org/10.2147/JMDH.S459987

[13] El-Shafai, W., Khallaf, F., El-Rabaie, E. S. M., & Abd El-Samie, F. E. (2022). Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. *Neural Computing and Applications*, *34*(13), 10629–10653. https://doi.org/10.1007/s00521-022-06994-z

[14] Abiramasundari, S., & Ramaswamy, V. (2025). Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms. *Scientific Reports*, *15*(1), 13098. https://doi.org/10.1038/s41598-024-84879-y

[15] Verma, A., & Shri, C. (2025). Cyber security: A review of cyber crimes, security challenges and measures to control. *Vision: The Journal of Business Perspective*, *29*(4), 478–492. https://doi.org/10.1177/09722629221074760

[16] Kaiser, F. K., Wiens, M., & Schultmann, F. (2021). Use of digital healthcare solutions for care delivery during a pandemic-chances and (cyber) risks referring to the example of the COVID-19 pandemic. *Health and Technology*, *11*(5), 1125–1137. https://doi.org/10.1007/s12553-021-00541-x

[17] Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

[18] Virk, A., Alasmari, S., Patel, D., & Allison, K. (2025). Digital health policy and cybersecurity regulations regarding artificial intelligence (AI) implementation in healthcare. *Cureus*, *17*(3), e80676. https://doi.org/10.7759/cureus.80676

[19] Brohi, S., & Mastoi, Q. U. A. (2025). AI under attack: Metric-driven analysis of cybersecurity threats in deep learning models for healthcare applications. *Algorithms*, *18*(3), 157. https://doi.org/10.3390/a18030157

[20] Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyber-attacks and sociotechnical solutions for health care systems: Systematic review. *Journal of Medical Internet Research*, *26*, e46904. https://doi.org/10.2196/46904

[21] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, *11*(2), 198. https://doi.org/10.3390/electronics11020198

[22] Li, H., Ji, L., Li, Y., & Liu, S. (2024). Robustness analysis of multilayer infrastructure networks based on incomplete information Stackelberg game: Considering cascading failures. *Entropy*, *26*(11), 976. https://doi.org/10.3390/e26110976

[23] Kore, A., & Patil, S. (2022). Cross layered cryptography based secure routing for IoT-enabled smart healthcare system. *Wireless Networks*, *28*(1), 287–301. https://doi.org/10.1007/s11276-021-02850-5

[24] Jawad, L. A. (2024). Security and privacy in digital healthcare systems: Challenges and mitigation strategies. *Abhigyan*, *42*(1), 23–31. https://doi.org/10.1177/09702385241233073

[25] Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., . . . , & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, *8*(3), 66–77. https://doi.org/10.1049/htl2.12008

[26] Jarkas, O., Ko, R., Dong, N., & Mahmud, R. (2025). A container security survey: Exploits, attacks, and defenses. *ACM Computing Surveys*, *57*(7), 170. https://doi.org/10.1145/3715001

[27] Li, S., Surineni, K., & Prabhakaran, N. (2025). Cyber-attacks on hospital systems: A narrative review. *The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice*, *7*, 30–39. https://doi.org/10.1016/j.osep.2025.03.002

[28] Aljuraid, R., & Justinia, T. (2022). Classification of challenges and threats in healthcare cybersecurity: A systematic review. *Studies in Health Technology and Informatics*, *29*(295), 362–365. https://doi.org/10.3233/SHTI220739

[29] Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1), 1–4. https://doi.org/10.1093/intqhc/mzaa117

[30] Giansanti, D. (2021). Cybersecurity and the digital-health: The challenge of this millennium. *Healthcare*, *9*(1), 62. https://doi.org/10.3390/healthcare9010062

[31] Qiu, J., Li, L., Sun, J., Wei, H., Xu, Z., Lam, K., & Yuan, W. (2025). Emerging cyber attack risks of medical AI agents. *arXiv*. https://doi.org/10.48550/arXiv.2504.03759

[32] Narayan, S. M., Kohli, N., & Martin, M. M. (2025). Addressing contemporary threats in anonymised healthcare data using privacy engineering. *npj Digital Medicine*, *8*(1), 145. https://doi.org/10.1038/s41746-025-01520-6

[33] Swati, Roy., Singh, S., J, & Mathew, J. (2025). Securing IIoT systems against DDoS attacks with adaptive moving target defense strategies. *Scientific Reports*, *15*(1), 9558. https://doi.org/10.1038/s41598-025-93138-7

[34] Reshmi, T. R. (2021). Information security breaches due to ransomware attacks—A systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

[35] Mohammed, N., Mohammed, A. F., & Balammagary, S. (2025). Ransomware in healthcare: Reducing threats to patient care. *Journal of Cognitive Computing and Cybernetic Innovations*, *1*(2), 27–33. https://doi.org/10.21276/jccci.2025.v1.i2.5

[36] Kalodanis, K., Feretzakis, G., Anastasiou, A., Rizomiliotis, P., Anagnostopoulos, D., & Koumpouros, Y. (2025). A privacy-preserving and attack-aware AI approach for high-risk healthcare systems under the EU AI act. *Electronics*, *14*(7), 1385. https://doi.org/10.3390/electronics14071385

[37] Kandasamy, V., & Roseline, A. A. (2025). Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks. *Scientific Reports*, *15*(1), 1697. https://doi.org/10.1038/s41598-025-85547-5

[38] Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. *International Journal of Educational Reform*, *33*(1), 101–121. https://doi.org/10.1177/10567879221082966

[39] le Dez, A. (2024). Cyber data sanitization: A cyber revival at the heart of the next data battle. *The Cyber Defense Review*, *9*(2), 17–26.

How to Cite: Sharma, D., Prabha, C., Bamaqa, A., Alahamade, W. O., & Khan, M. Z. (2026). Cyber Threats in E-healthcare and an Autonomous Cybersecurity Agent: A Comprehensive Review. *Artificial Intelligence and Applications*. https://doi.org/10.47852/bonviewAIA62029545