Artificial Intelligence and the Field of Robotics: A Systematic Approach to Cybersecurity and Healthcare Systems

Usman Ibrahim Musa[1], Aminu Ibrahim Musa[2], Sakshi Dua[3]

[1]School of Computer Applications, Lovely Professional University, Punjab, India.
[2]Depertment of Information Technology, Ecole De Superieure De Gestion Et De Technologie, Benin.
[3]School of Computer Applications, Lovely Professional University, Punjab, India.

---***---

Abstract - *A systematic review of cybersecurity and healthcare systems from the Artificial Intelligence (AI) and robotics perspective for the past 6 years is presented in this research. Cybercriminals nowadays are always researching new ways to break into corporate networks and steal sensitive data. People frequently adhere to the same fundamental security precautions on a daily basis, and as they use more devices at work, for security experts, maintaining the data and keeping them current is becoming more and more challenging. AI in cybersecurity is gaining importance as it contributes to overcoming the aforementioned difficulties. Additionally, the advances brought about by AI and the field of robotics have proved advantageous for the healthcare sector. With the use of AI techniques like deep learning and machine learning, a number of healthcare systems have been developed that autonomously diagnose various diseases from medical images and further generate reports based on the findings. This research focuses on the role of AI and the field of robotics in enhancing the cybersecurity and healthcare sector. The research's literature demonstrates that AI in healthcare and cybersecurity is still a new and innovative field that needs to be studied further in the future. Researchers may utilize this study to get helpful tips and knowledge for their next work.*

Key Words: AI, Robotics, Cybersecurity, Healthcare.

1. INTRODUCTION

Robotics and artificial intelligence are two major fields of science and engineering research. These terms are often used interchangeably to describe the development of technologies that help make machines intelligent. However, there is a significant difference between the two. AI is what enables robots to function like humans, while robotics is the study of how to make them do so. Together, these technologies hold great promise for the future.

A topic that in recent years has become familiar to just about everyone. Hardly a day goes by without news media reporting on the latest cyber-attack, whether it's conducted by criminal or government organizations. The study of strategies we may employ to lessen the possibility of such assaults, wherever they come and for whatever reason, is known as cyber security. A paper surveys the field of robot learning from demonstration, which is a key aspect of AI in robotics. The authors provide an overview of the different techniques used for robot learning from demonstration, including inverse reinforcement learning, apprenticeship learning, and behavioural cloning. They also discuss the challenges and future directions of this field [1].

A surveys the field of AI-based intrusion detection systems, which are a key aspect of using AI for cybersecurity. The authors provide an overview of the different techniques used for AI-based intrusion detection, including rule-based systems, signature-based systems, and anomaly-based systems. They also discuss the challenges and future directions of this field [2]. This research's goal is to provide an overview of AI from the perspective of cybersecurity, including what it is, how we may define it, and how we can use it to try to enhance the security features of both businesses and our own personal life. We may conceive of it as attempting to counteract any threat resulting from our reliance on and usage of information and communication technology. A paper surveys the field of robotic security systems, which is the intersection of robotics and cybersecurity. The authors provide an overview of the different types of robotic security systems, including those used for surveillance, reconnaissance, and search and rescue. They also discuss the challenges and future directions of this field [3]. If you think about it for a moment, this not only includes using the smartphones tablets, and desktop computers that we use for work, personal, business, or leisure, but all the aspects of everyday life that depend on the use of information technology. A research discusses the challenges and future directions of cybersecurity for industrial control systems, which are a key aspect of the intersection of AI, robotics, and cybersecurity. The authors highlight the unique challenges of securing industrial control systems and the importance of developing new security technologies and standards to address these challenges [4] Because information technology is so prevalent, problems with cyber security affect all of our systems and gadgets that are connected to the Internet. Almost every part of our working life, including the functioning of factories, transit, and offices globally are included in this, as well as cars for private and public transportation, the infrastructure bringing power and water to our houses, and many other areas. Since practically every part of our life now depends on information and communications technology, cyber security has evolved into a basic requirement for everyone. At the same time, we are aware of the numerous ways in which modern information processing systems are susceptible to assault. One more research discusses the techniques and challenges of AI-based malware detection, which is another key aspect of using AI for cybersecurity [5]. It is easy to argue that our increasingly linked world is the issue and that we should change how we interact with it. However, in most cases, going back is impossible, and in truth, we almost likely don't want to. Modern information and communication technologies have a significant positive impact on our ability to work from home, increase productivity, and engage in a variety of previously unimagined kinds of communication and social contact. If we accept that information and communications is here to stay, what are we going to do about the major security threats we all face? In this study, we will introduce some of the techniques that can be used to reduce these threats, especially from the AI and Robotics perspective. It is important to realize that providing security is not just about more and better technology.

A contemporary healthcare system is made up of several components, each of which gathers and analyses data. Massive volumes of data are produced by healthcare providers, intermediaries, and government programmes like Medicare and Medicaid. Patients can provide information on the care they get, their health state, the results of their treatment, and related expenditures. Nearly all of these data are now digitised, and some of them may be used for artificial intelligence research. Artificial intelligence has a wide range of applications in the medical field, including improving diagnostic accuracy, performing robotic procedures, discovering potential drug candidates, and choosing the most effective therapies for particular patients However, much like any technology or breakthrough, artificial intelligence creates ethical questions that its creators, users, and significant stakeholders like patients may want to take into consideration [26]. We will call attention to the ethical ramifications of some components of the healthcare system that, in our opinion, users and developers of AI systems should consider. Here, we'll concentrate on a specific subset of artificial intelligence applications that are most closely associated with the provision of healthcare services. What are the moral dilemmas, though? They are many. AI model systematic mistake is particularly detrimental to the healthcare industry. Considering that the results of these models may have an impact on crucial and even life-and-death choices [27]. Sometimes these deliberate mistakes can result in discriminatory judgments, especially if they target entire groups of socially disadvantaged individuals, such as women, children, persons of colour, or those with poor incomes. With that being said, we will be discussing some points to take care of when it comes to robots in healthcare. The lack of transparency in AI models is one sort of ethical issue that is particularly pertinent to this technology. It's sometimes challenging or impossible to determine how AI derives its judgments [28]. Particularly if the AI makes use of machine learning techniques, which implies that the models are always evolving depending on the data they are using. Because physicians and healthcare institutions depend on AI developers to produce tools and technologies that are reliable and efficient to employ on their patients, this is a particularly serious issue in the context of healthcare [29]. However, there are currently few guidelines or rules for assessing the efficacy and safety of many AI-based medical solutions. However, doctors and other healthcare workers are responsible ethically and legally for the choices that AI is increasingly guiding. Physicians and health care facilities who use AI in ways that may have an impact on healthcare choices must be aware of the limitations of the techniques, data, and models when they are applied to their specific patient populations. In this research, we'll concentrate on the ethical problem of competing or conflicting interests. This issue arises particularly in the area of healthcare. Robots are being employed for a variety of minimally invasive surgeries. Many modern hospitals feature robots that function occasionally in lieu of surgeons and others that help doctors. This is where artificial intelligence, specifically the field of robotics came in and had a big influence on healthcare. Some of the algorithms that were linked to those robots aided them in doing activities depending on the instructions given and trained to them with very good and high precision.

RESEARCH QUESTIONS

1. What are the general problems in Cybersecurity?
2. What are the general problems in Healthcare?
3. What is the significance of AI and the field of robotics?
4. What are the various characteristics of AI.
5. What are the challenges of AI in Healthcare and Cybersecurity and how to overcome it?
6. What is the research gap existing in AI in Cybersecurity and Healthcare?
7. What is the future of AI from a Cybersecurity and Healthcare perspective?

We have compiled the research questions listed above, and the information from studies on Artificial Intelligence and robotics, Cybersecurity, and Healthcare is used to further answer the questions.

WHAT ARE THE GENERAL PROBLEMS IN CYBERSECURITY?

Cybersecurity is a field that deals with protecting information, communication, and networks from malicious attacks. Attackers use cyberspace to carry out their crimes; thus, it's crucial to secure them. Governments and corporations need to look after their systems and data since anyone can access the internet without permission. However, not all security measures are good when protecting the internet.

The worldwide web has become a haven for cybercrime in recent years. Hackers have found many new ways to exploit systems and data. Many attacks target government systems. This is because our system of government is involved in much of our politics. Other targets are corporations that handle our country's financial wealth. Many cybercrimes are committed by state agencies or other high-profile organizations. They're capable of carrying out dangerous plans in secrecy. Fortunately, there's a lot of work being done to secure cyberspace. A few of the most important general problems include:

1. Increase in Cyberattacks: The number of cybercrimes continues to grow annually as criminal organizations try to capitalize on their efforts, such as ransomware and crypto-jacking. However, in 2021, one of the biggest concerns was the rise of this type of crime. The number of cyberattacks in 2021 increased by 50% over the previous year. However, certain regions were hit harder by the attacks, such as education, healthcare, and research. This might indicate that cyber threat actors are concentrating their efforts in regions where they are most exposed. An attack rate that has risen so quickly bodes ill for 2022. Cyber threat actors' use of automation, deep learning, and automation to improve their techniques will only lead to a rise in the number and intensity of attacks.

2. Ransomware attacks are on the rise: Attacks involving ransomware are increasing. In 2017, the WannaCry epidemic brought ransomware to public attention. Ever since, a sizable number of ransomware businesses have emerged, posing a costly and visible threat to all businesses. In 2021, ransomware organisations shown their ability and willingness to impact businesses in addition to their immediate targets.. The most famous example is the imperial pipeline hack. One of the primary pipelines used by the ransomware gang Dark Side was shut down.

3. Mobile devices bring new risks: The implementation of Bring Your Own Device (BYOD) rules is another result of the transition to remote working. Organizations can increase employee productivity and retention by allowing them to work from their own devices, but this practise also offers important information about security and susceptibility to diseases that might endanger company systems and solutions. You become incapable of responding. Cybercriminals have modified their ways in 2021 to capitalise on the use of mohiles that rises. Triada, FlyTrap, and MasterFred malware, among other mobile malware trojans, have all recently surfaced. These mobile trojans approach the target device and request the required rights through lax app store security measures, social media, and other similar strategies.

WHAT ARE THE GENERAL PROBLEMS IN HEALTHCARE?

1. Concerns about health equity: The health sector has long acknowledged that different demographic groups experience varied levels of health care. These discrepancies go beyond only salaries and medical expenses. On the other hand, environmental influences have a significant effect on health and wellbeing. The zip code is one of these elements, also referred to as the social determinants of health. racial and cultural diversity, the quality of the air and water, and access to jobs, housing, education, transit, and wholesome food. In certain areas, enduring racial and social inequality has also put generations' worth of health at risk. All of these factors have an effect on a person's overall health and capacity to get healthcare. Health crises for the underserved sometimes include hospitalisation or emergency room visits and incur considerable medical expenses.

2. Opportunities (and pitfalls) of technology: The current health issue has numerous opportunities but also has the potential to cause a lot of issues if not properly addressed. Data are being used more and more in health. The difficulty is in managing this ocean of data. According to a Frontiers in ICT research, healthcare professionals and health systems were already producing about 80MB of data per patient year before the epidemic. In addition to information from electronic health records (EHRs), this data also contains information and details such addresses, demographics, claim and insurance information, payment history, and schedules.

3. Expensive medical bills: The exorbitant expense of healthcare is arguably the most serious issue facing our present healthcare system. More than 45% of American people say it is difficult to afford medical care, and more than 40% say they pay for treatment, according to a poll by the Kaiser Family Foundation. Healthcare costs are changing people's behaviour, with many avoiding a doctor when ill or skipping check-ups altogether. A quarter of Americans cannot afford the prescriptions they need and may skip doses or skip prescribed medications. Each of these behaviours can lead to serious health problems and, therefore, increased medical costs.

WHAT IS THE SIGNIFICANCE OF AI AND THE FIELD OF ROBOTICS?

Robots are becoming increasingly advanced both technologically and structurally. The primary focus of robotics today is on repairing and saving lives. For example, doctors use robot arms in hospitals to perform complicated surgeries without putting their patients at risk. AI is quickly becoming essential in many areas of life including healthcare and cybersecurity. This is due to the fact that it saves lives, reduces costs and makes life easier. However, there are still many unknown with AI, which is why it is significant to consider the positives and negatives before implementing this technology in both healthcare and cybersecurity. AI has a lot of potential in healthcare; it can perform complex tasks and can help doctors treat patients more effectively. For example, it can asset physicians in diagnosing and treating diseases and also assist them in performing triage and radiology procedures. Reinforcement learning programs help medical professionals save lives by performing life-saving surgeries on human beings. In addition, predictive models help medical professionals manage patients' records and identify issues with patient care systems. Additionally, AI helps with patient counselling by assisting with diagnosis and providing psychological support to patients and essentially has the potential to revolutionize our healthcare system

WHAT ARE THE CHALLENGES OF AI IN CYBERSECURITY AND HEALTHCARE AND HOW TO OVERCOME IT?

AI is the term given to describe the advancement of computers to perform tasks that were once reserved for humans. It has the potential to revolutionize many aspects of our lives- from health and education to military and commercial sectors. However, it is also a source of considerable concern as it raises questions regarding ethics, safety, and accountability.

AI is still in its infancy so there are still many challenges to overcome. For instance, AI is not very good at handling controversial or negative data, as it can have a conflictive effect on the system. It is also susceptible to adversarial behaviour since hackers can use AI for their own purposes by programming it against the systems they target. Many Cybersecurity experts believe that AI will be most beneficial in situations involving classified data, where security measures are necessary but impossible. The cybersecurity industry is getting bigger every year. As more and more people rely on technology in their daily lives, it's important to make sure these devices and computers are safe from hackers. There are some cybersecurity issues that are easy to fix. For example, many people use the same password for their social media accounts and email girlfriend accounts. This makes it easier for hackers to steal passwords and use them to break into those accounts. They can then steal your personal information and use it to commit identity theft. Another problem with cybersecurity is that ordinary people are not fully aware of how to protect themselves. They are also unaware of the dangers of opening emails or attachments that appear to come from people they know. These emails may contain viruses that can harm your device. It could also be a phishing scam that steals your personal information.

The fundamental healthcare issue has a few other remedies as well. Collaboration between local, state, and federal governments, as well as healthcare professionals, is necessary to find answers to the problem of excessive healthcare expenditures. To address environmental variables and enhance access to healthcare in marginalized neighbourhoods, it is possible to employ housing, transportation, and collaborations with churches and non-profit health groups. To satisfy the demands of patients, healthcare managers might put up a several kinds of programs. Example, telemedicine can help patients who do not have access to transportation, as is the case in many rural places, yet internet connectivity is still an issue. Elderly home care is one of the other initiatives. a healthcare team that prioritises community involvement and patient care.

WHAT IS THE RESEARCH GAP EXISTING IN AI IN CYBERSECURITY AND HEALTHCARE?

Artificial Intelligence and Cybersecurity are two of the most important technologies today. Cybersecurity and Healthcare are also two areas that are rapidly developing, expanding, and gaining more relevance in our daily lives. However, AI technologies have many flaws that need to be addressed-which is why more research is needed to make them more useful. Both areas are in a stage of development; therefore, they have many challenges to overcome before they can revolutionize our lives.

AI has a lot of potential in Cybersecurity and Healthcare since it can help detect and prevent cybercrime when we take the field of Cybersecurity. And in healthcare, it can help diagnose a disease from its very early stage and also reduce the workload on the doctors as well.

Currently, Cybercrime is mostly detected through human involvement, which is slow and error-prone. AI can also help with the investigation process by analysing data collected from various sources and identifying potential threads. It can also help with countermeasures by developing mechanisms that stop attacks before they happen. With that being said, AI has the potential to become an invaluable tool for Cybersecurity and Healthcare when applied practically.

WHAT IS THE FUTURE OF AI FROM A CYBERSECURITY AND HEALTHCARE PERSPECTIVE?

Robotics and artificial intelligence have many exciting applications that will become clear once they're ready for use by the public. For now, these technologies are primarily used in scientific research or in niche applications by professionals only. However, there's no shortage of interest from amateurs who want to create their own robot companions. It's clear that these technologies have a huge future.

AI has many applications- from natural language processing to pattern recognition and will change our lives in many years when we take a look at how it changes and is changing our daily lives from the perspective of cybersecurity and healthcare. It is very obvious that the AI has a very large and good future.

2. METHODOLOGY

Several research papers used in this research were explained in this part. Consequently, we provide and clarify the current surveys in all the areas of this research including AI and Robotics, Cybersecurity, and Healthcare.

A. APPLICATIONS OF AI IN CYBERSECURITY DEFENCE

The AI model provides highly powerful defensive capabilities for cybersecurity protection that will help defend various systems against cyberattacks and support digital forensic investigations. Having said that, we highlight a few of the uses of AI in cybersecurity defense. Additionally, we encourage the reader of this research to look at these publications for additional information on AI's role in cybersecurity protection.

i. AI for malware detection and classification: This term simply stands for “Malicious Software” which is actually dangerous in short. It is a document that contains programs or codes which is mostly delivered over a network [1] [2]. It is produced or planned to employ various methods, such as ransomware, spyware, viruses, trojans, and adware, to damage target computer systems, mobile devices, and online applications. [3] [4].

Several algorithms and techniques have been used to detect malware [5]. Detection of malware using AI techniques can be done when a model is trained using a dataset that can help in classifying the type of malware [6].

ii. AI for network intrusion detection: Many programmers created and suggested network intrusion detection solutions. Ding et al. [7] presented a real-time anomaly detection technique and was successful in achieving high accuracy. Additionally, after conducting K-means clustering, Alom and Taha [8] attained a respectable accuracy of 91.86%. Chen et al [9] provided an example of how deep convolutional neural networks (DCNNs) are used to identify DDoS assaults. Some other researchers who worked on the same topic include Mirsky et al. [10], Biswas [11], Clements, et al. [12], and Xia et al. [13].

iii. AI for traffic identification and classification: At a time, several applications are flowing in any network, and the one and single most important phase in identifying and recognizing multiple classes is the use of network traffic classification. A researcher [14] utilized a deep learning model to distinguish the flowing of traffic in a network after diving it into 25 protocols, he was successfully able to get 100% and 91.74%, depending on the type of protocol. Another research [15] used a Convolutional Neural Network (CNN) model to distinguish the classes of traffic and also try to recognize the application category.

iv. AI for spam detection: Spam emails, to put it simply, are any unwelcome or virus-containing emails. In addition to acting as a detector of all those viruses, spam detection systems also work as a preventer of emails by stopping them from introducing viruses into one's inbox. One of the techniques that developers have suggested is an auto-encoder that functions and further distinguishes spam mail by Mi et al. [16], with a 95% accuracy rate. A different researcher created a machine-learning approach and algorithmic phishing email detection system [17]. The reader of this paper can refer to the following works related to this by Aksu et al. [18], Yi et al. [19], and Benavides et al. [20].

v. AI for insider threat detection: A document that demonstrates and clearly explains how to examine and assess a user's system logs using a DNN or RNN model, as well as how to find abnormalities that might lead to an insider threat incident. Tuor et al. [21] described how to do this.

vi. AI for digital forensics: AI technology become most significant in investigations nowadays and also improves the methods and ways of detecting cybercrime. The specialists of forensics found this very useful as it helps them in effectively and quickly find the actual source and cause of the problem, on the other hand, the use of AI in digital forensic saves a lot of money and time. Some machine-learning techniques or algorithms have been utilized to classify file fragments. For example, papers are written by Beebe et al. [22], Axelsson et al. [23], and Calhoun & Coles [24]. Another researcher [25] proposed a technique that works based on deep learning for file fragment classification.

B. APPLICATIONS OF AI IN HEALTHCARE

i. Disease Detection systems: One of the most significant tasks in healthcare is the detection of various diseases. it lessens the stress on doctors, because those systems may be replaced to run automatically instead of manually for various other duties. . Researchers have suggested a method in 2019 that might assist physicians in identifying and categorizing skin conditions, such as melanoma and eczema [26]. A machine learning algorithm is used in detecting skin cancer where it differentiates healthy skin from diseased one and high accuracy was achieved [27]. Many systems for brain cancer classification have also been invented by developers which include an approach by Sha et al [28], they developed a system using deep Convolutional Neural Networks (DCNNs) to detect brain tumors after Magnetic Resonance Imaging (MRI) generated the high-quality images of the inside of the brain. The reader of this research can also go through these articles for disease detection systems: Ahmad et al. [29], Ahmad et al. [30], Shabbir et al [31], and Hussain et al [32].

ii. Test Analysis and Diagnosis: Because all those AI-based apps will have a huge influence on interpreting medical scans, including X-rays, MRI pictures, CT scans, and many more, it is getting simpler for physicians to simply comprehend the problem of their patients when there is an AI application. As the effort associated with scanning analysis is lessened, medical physicians feel more at ease [33]. The AI-based approach will assist in realizing and comprehending whether any gene might cause cancer while evaluating biological data such as DNA and RNA [34]. The AI can help identify any disease risk or existence. The characteristics depend on outside factors [35]. It further helps in alerting people about any disease-infected area [36].

iii. Chatbots: These days, hospitals and other clinics hold a number of websites, mobile applications, and web applications. These websites, mobile applications, and web applications feature chatbots that act to aid patients directly from where they are and try to learn more about their health issues [37]. Every time a patient enters a hospital, the first thing the medical staff does is screen the patient to learn about their beginning circumstances. In this situation, AI chatbots can take the role of these time-consuming procedures [38]. Additionally, chatbots may be used as interacting agents between language processing and speech recognition technology [39]. As a whole, majority of the modern healthcare institutions have these kinds of chatbots which help patients in different ways [40].

iv. Health Monitoring: When it comes to patient prevention through condition monitoring, this is crucial. The monitoring system may occasionally be able to keep a patient in their present state when an illness is caught early by informing the doctors. Algorithms and AI approaches are used to assist it. A smart health monitoring system has been proposed by some researchers [41], the system is capable of keeping track of patients' health and it also contains a feature that enables patients' families to access and check on their patient's health status. Anandh [42] created a system that uses AI algorithms to provide body temperature. Papers written by Soppimath et al [43] and Srinivasan et al. [44] can be checked to get more health monitoring systems that were trained based on AI algorithms and techniques.

v. Digital Consultation: The world is getting increasingly digital; thus, this is a fairly broad area. A digital consultation is just a video call between a doctor or other healthcare professional and a patient made possible through a smartphone or online application. Through these tools, the patient and the doctor will communicate. Examples of the evolution of digital healthcare include patients' engagement in the development and higher expectations for patient access to healthcare [45, 46, 47]. Most primary care doctors can now operate from home, and in this scenario, digital consultation will undoubtedly occur [48, 49]. This reader can check [50] and [51] to get more ideas about digital consultations and their cost-effectiveness.

C. DATA SOURCE

The literature in this paper is made up of several research publications and articles from different sources. Fig.1 shows the pictorial or graphical representation of the data sources used in this research and their respective percentages. Additionally, we have made a table of the databases and their respective URLs that were all used in this research which can be seen in fig. 2.

D. EXPLORATION CRITERIA

As mentioned in the abstract that this research will focus more on the area of AI and robotics in cybersecurity and healthcare for the past 6 years which is from 2017 to 2022. In light of the foregoing, we gathered all the references and brought out the percentage of the papers used in this research for each and every respective year. The pictorial representation of the same is shown in fig. 3 where all the percentages are clearly stated.

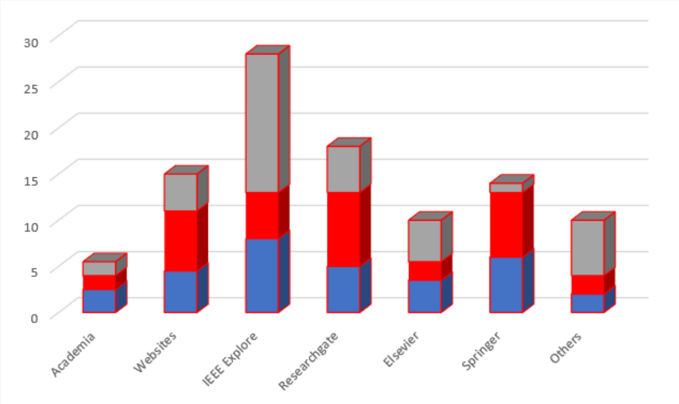
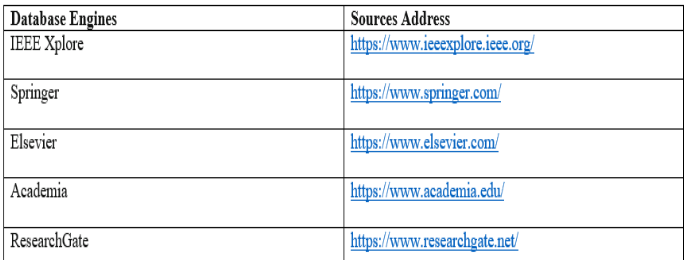


Fig.1. Research Papers from Data Sources.



Database Engines	Sources Address
IEEE Xplore	https://www.ieeexplore.ieee.org/
Springer	https://www.springer.com/
Elsevier	https://www.elsevier.com/
Academia	https://www.academia.edu/
ResearchGate	https://www.researchgate.net/

Fig.2. Database Engines and their URLs

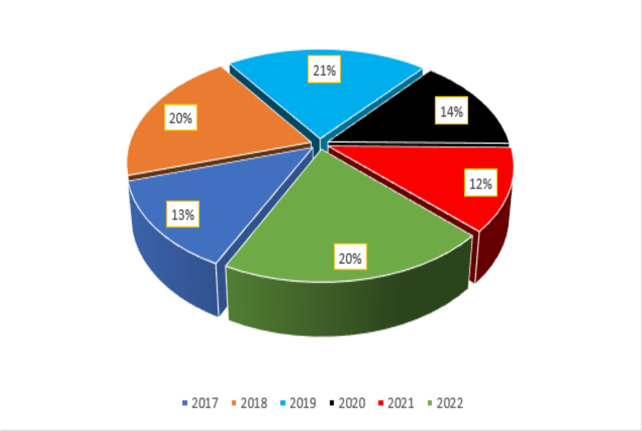


Fig.3. Percentage of Research Papers from 2017 to 2022.

Cybersecurity is an ever-evolving field, and the systems developed in the past five years have been instrumental in helping protect individuals and organizations from cyber threats. In this article, we will take a look at some of the most important cybersecurity systems developed in the past five years in Table.1. Let's first examine how machine learning (ML) and artificial intelligence (AI) have evolved in the field of cybersecurity. Systems that can identify and respond to cyber threats in real-time have been developed using AI and ML. These technologies are capable of analyzing vast volumes of data to spot trends and abnormalities that can point to an impending attack. Systems that can recognize and react to harmful code have also been created using AI and ML, as well as systems that can detect and respond to phishing attacks. These are just a few of the many cybersecurity systems developed in the past six years. As the field of cybersecurity continues to evolve, new and improved systems will be developed to protect individuals and organizations from cyber threats.

Table 1. Summary of AI-Based Cybersecurity Systems Developed in the past 6 years.

[8]	2017	Cybersecurity network intrusion detection with unsupervised deep learning	Attained a respectable accuracy of 91.86%	Usability issues
[53]	2017	Convolutional neural networks' ability to identify new assaults is evaluated.	The CNN model obtained an 81.57% of accuracy rate.	High dimensional data
[54]	2017	developed a recurrent neural network-based intrusion detection system (RNNs)	The RNN model has an 83.28% detection rate in the binary classification, according to the results.	Personal Integrity
[55]	2017	An innovative fuzziness-based semi-supervised learning strategy that uses unlabelled data with supervised learning algorithm assistance improves the classifier's performance for IDS.	Obtained very high accuracy on the proposed algorithm.	The accuracy of the J48, Naïve Bayes, NB tree, Random forests, Random tree, multi-layer perceptron, and Support Vector Machine (SVM) is lower than the proposed algorithm
[57]	2018	A safe malware detection system using encryption	Achieved 98.93%	Efficiency
[58]	2018	An Android malware family categorization has been proposed, along with a representative sample selection.	FalDroid – 94.2%	Usability
[59]	2018	for unsupervised feature learning, a non-symmetric deep autoencoder (NDAE) has been suggested.	a training time reduction of up to 98:81% and an improvement in accuracy of 5%.	Huge amount of complex
[60]	2019	a method to identify malware based on the incidence of opcodes	The suggested method can identify the virus with about 100% accuracy.	Less number of datasets.

[61]	2019	Using data and APIs, to identify malware	AUC 99.3%	Privacy
[56]	2019	examination of extracted characteristics from big-data sources in real time.	True Positive Ratio, Precision, Recall and F1 > 99%, FPR < 0.1%	Effectiveness
[63]	2019	It was showed how to find malware payloads in a number of file types, including Portal Document File.pdf and Microsoft Document File.doc.	The accuracy of finding ransomware was 91.7% and 94.1%, respectively.	Limited incremental rate
[64]	2019	Deep learning-based proposed method for virus detection using behaviour graphs	Accuracy of 98.60%	Unstructured
[66]	2020	proposed a dynamic technique for detecting and predicting Windows malware	Prediction – 0.997 FPR of 0.000 FNR of 0.007	Trust
[67]	2020	suggested using a method called SourceFinder to locate malware source code repositories.	According to the research, the suggested method locates malware repositories with 89% precision and 86% recall.	Poor understanding of safety
[68]	2021	They provide a novel approach for automatic hyperparameter optimization based on Bayesian optimization to produce the best possible DNN design.	BO-GP obtained the highest accuracy scores, with 82.95% for the KDDTest+ dataset and 54.99% for the KDDTest-21 dataset. accuracy.	Appropriateness
[86]	2022	ML-based malware classification for Android devices using repacked app detection and removal	Detection Accuracy of 98.2%	Efficiency
[87]	2022	Malware Threads Classification	98% Accuracy in detecting and classifying the malware threads	Trust
[62]	2022	Approaches in malware detection systems that rely on visualisation	The Approach Achieved 100% Accuracy	Poor and little amount of dataset to get high accuracy

Table 2. Summary of Datasets, Samples, and Methodology used in the Past AI-Based Cybersecurity Systems

Reference	Title of Paper	Methodology	Datasets and Samples Used
[86]	AndroMalPack: enhancing the ML-based malware classification by detection and removal of repacked apps for Android systems	Nature Inspired Algorithm	AndroZoo Dataset
[55]	Fuzziness-based semi-supervised learning approach for intrusion detection system	Random forests, NB tree, J48, Naive Bayes, random tree, multi-layer perceptrons, and SVM (SVM)	unlabelled samples assisted with a supervised learning algorithm.
[54]	Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks	Binary classification (Normal, Anomaly) and five category classifications using the RNN-IDS model (Normal, DoS, R2L, U2R, and Probe).	NSL-KDD dataset

[87]	Binary and Multi-Class Malware Threads Classification	Naïve Bayes (NB) and Gaussian Discriminant Analysis (GDA)	MaleVis Dataset
[60]	Detection of Advanced Malware by Machine Learning Techniques	Machine Learning Techniques	Kaggle Microsoft malware classification challenge dataset
[68]	Bayesian hyperparameter optimization for deep neural network-based network intrusion detection	Deep Neural Network Algorithms	NSL-KDD dataset
[57]	A secure encryption-based malware detection system	Privacy-Preserving Naïve Bayes Classifier (PP – NBC)	4-Gram API Fragment Sequence
[67]	Source finder: Finding malware source code from publicly available repositories	Machine Learning Techniques in detecting the Malware	Not Identified
[62]	Disarming Visualization-based Approaches in Malware Detection Systems	Visualization-based techniques	Mallmg Dataset
[8]	Network intrusion detection for cybersecurity using unsupervised deep learning approaches	K-means Clustering	NSL-KDD dataset
[61]	ASSCA: API sequence and statistics features combined architecture for malware detection	Dynamic behaviour	Malicious samples from virus Share and VirusTotal, as well as samples from Windows 7 and Windows XP system exe files
[63]	A novel malware detection system based on machine learning and binary visualization	Neural network and deep learning are used in the detection of the malware.	Not mentioned
[53]	Intrusion Detection Using Convolutional Neural Networks for Representation Learning	In testing the set, 17 extra attack kinds were added, and a new attack was also found.	NSL-KDD dataset
[66]	A dynamic Windows malware detection and prediction method based contextual understanding of API call sequence	Using Markov chain sequence to depict the link between API functions to represent malware and goodware	Intelligent and Security Informatics Data sets Brazilian-malware-dataset
[64]	Malware detection based on deep learning of behaviour graphs	Stacked AutoEncoders and the Behaviour-based Deep Learning Framework (BDLF)	Malware samples from VX heaven
[58]	Android malware familial classification and representative sample selection via frequent subgraph analysis	FallDroid	Genome Project Dataset, Drebin Dataset, FallDroid – I, FallDroid - II
[56]	An investigative study on motifs extracted features on real time big-data signals	Visualization and deep learning techniques were used	The Virus Share community has 9 virus families, each with 1000 variants
[59]	A deep learning approach to network intrusion detection.	By stacking the NDAEs, a layer-wise unsupervised representation learning method was produced.	KDD Cup'99 and NSL-KDD datasets

In the past six years, healthcare systems have undergone a dramatic transformation. Advances in technology, data analytics, and artificial intelligence have enabled the development of new and improved healthcare systems that are revolutionizing the way healthcare is delivered. These systems are designed to improve patient outcomes, reduce costs, and provide better access to care.

Table.3 below presents some of the most significant healthcare systems developed in the past six years. These systems are designed to address a variety of healthcare needs, from patient monitoring and diagnosis to population health management. Each system is designed to provide a unique set of features and benefits to healthcare providers and patients alike. These healthcare systems are just a few of the many that have been developed in the past five years. As technology continues to advance, healthcare providers will continue to develop new and improved systems to improve patient outcomes and reduce costs.

Table 3. Summary of AI-Based Healthcare Systems Developed in the past 6 years.

Reference	Year	Topic Addressed	Performance	Limitation
[69]	2017	Human Skin Cancer Detection System	84% Predictive Value and 75% Sensitivity	Unstructured Data
[70]	2017	Skin Cancer Classification Using Deep Learning	High performance achieved	Lack of Elaboration
[71]	2017	Review of Common AI Disease including, cancer, cardiology, and neurology	Perfect Analysis in the Review	Data Exchange and Safety
[72]	2018	Detection of Onychomycosis and normal nails	Sensitivity of 96.7% and a Specificity of 96.7%	Too Much Load of Different Dataset
[73]	2018	Skin Disease Identification	88% in detection	Efficiency
[74]	2018	Diagnosis of Skin Cancer	Detection accuracy of 90%	Less Flexible
[75]	2019	Approach on Melanoma and other skin cancer types	99% of Accuracy in Classifying Skin Cancer	Less amount of Data
[65]	2019	Device Application for Skin Cancer Detection	They Achieved an overall accuracy of 75.2% in detecting the Skin Cancer using the Application	Detection of Only two Disease
[76]	2019	Review of AI in Applications in India	Detailed Review of the Topic	Ethical Consideration
[77]	2020	Brain Tumour/Cancer Detection	CNN Architecture = 86% VGGNet = 97%	Very less number of the images used
[78]	2020	Skin Cancer Detection	97.9% Accuracy was achieved	Interoperability
[79]	2020	Classification of Skin Cancer	Achieved an Accuracy of 94.5%	Poor Documentation
[80]	2021	Detection of Brain Cancer	SVMs = 92.4% Five-layer Custom CNN = 97.2%	Less Amount of dataset
[81]	2021	Review of Common Healthcare Applications and Projects	Clearly explained about the algorithms and techniques	Poor Abstraction
[82]	2021	The model can identify photographs that don't fit into the eight classifications that are	94.9 Accuracy	Safety

		often utilised (Classified as unknown images)		
[83]	2022	Detection and Classification of Brain Tumour that are generated by MRI	Overall accuracy of 98.87% in classification and detection	Huge amount of complex
[84]	2022	Chatbot System for Women's Healthcare	96% for prediction of PCOS	Restrictions (Only for Women)
[85]	2022	Detection of Skin Cancer using different algorithms	Accuracy of the proposed ensemble is 93.5%	Trust
[52]	2022	Classification of Skin Lesion	Overall, of 98% Accuracy in Classifying Skin Lesion	Privacy

Table 4. Summary of Datasets, Samples, and Methodology used in the Past AI-Based Healthcare Systems

Reference	**Title of Paper**	**Methodology**	**Dataset and Samples Used**
[84]	Intelligent Medical Chatbot System for Women's Healthcare	Logistic Regression Algorithm, Machine Learning Algorithm, and KNN.	DialogFlow
[83]	A Robust Approach for Brain Tumour Detection in Magnetic Resonance Images using Finetuned EfficientNet	Deep Convolutional Neural Network	Brats2015 Brain Tumour Dataset
[76]	Artificial intelligence in healthcare in developing nations: The beginning of a transformative journey	SWOT Analysis	Review*
[85]	Skin Cancer Detection Using Combined Decision of Deep Learners	SVM, Naïve Bays, and K-Nearest Neighbour	ISIC Public Dataset
[71]	Artificial intelligence in healthcare: Past, present and future	Support Vector/ Neural Networks	Review*
[78]	Region-of-Interest Based Transfer Learning Assisted Framework for Skin Cancer Detection	Convolutional Neural Networks (CNNs)	DermIS
[70]	Dermatologist-level classification of skin cancer with deep neural networks	Deep Learning Algorithms	Not Specified
[80]	Brain Tumour Detection using Convolutional Neural Network	SVMs, K-NN, multi-layer perceptron, Naive Bayes, and random forest algorithms	HAM10000
[69]	A machine learning algorithm for identifying atopic der-mastitis in adults from electronic health records	Machine Learning Algorithms	ISIC Dataset
[52]	Skin Lesion Classification System using a K-Nearest Neighbour Algorithm	K-Nearest Neighbour Approach (KNN) and Convolutional Neural Network	ISIC Public Dataset
[81]	Unbox the black-box for the medical explainable AI via multi-modal and multi	Rule-based Decision Support System	Review*

	centre data fusion: A minireview, two showcases and beyond		
[72]	Deep neural networks show an equivalent and often superior performance to dermatologists in onychomycosis diagnosis: automatic construction of onychomycosis datasets by region-based convolutional deep neural network	Convolutional Neural Networks (CNNs)	Not Identified
[77]	Brain Tumour Detection using Deep Learning Models	Convolutional Neural Network and VGGNet	HM1000
[82]	Skin lesions classification into eight classes for ISIC 2019 using deep convolutional neural network and transfer learning	Deep Convolutional Neural Network in Addition to GoogleNet	ISIC Dataset
[79]	Analysis of basic neural network types for automated skin cancer classification using Firefly optimization method	Neural and Fuzzy Approach	ISIC Dataset
[75]	Integrated design of deep features fusion for localization and classification of skin cancer	Otsu Algorithm, Alex and VGG-16 Model	HAM10000
[65]	An on-device inference app for skin cancer detection	Convolutional Neural Network using Tensorflow	ISIC Dataset
[73]	Automated skin disease identification using deep learning algorithm	InceoptionV2, InceptionV3, MobileNet	ISIC Dataset
[74]	Diagnosis of skin diseases using convolutional neural networks	Convolutional Neural Networks	ISIC Dataset

The past six years have seen a dramatic shift in the way healthcare systems are developed and implemented. With the advent of new technologies and the increasing emphasis on patient-centered care, healthcare systems have become more efficient and effective. Table 4 highlighted some of the various healthcare systems developed in the past six years, their methodologies, and the datasets & samples used.

ARTIFICIAL INTELLIGENCE AND ROBOTICS

The goal of the computer science field of artificial intelligence (AI) is to develop intelligent machines that can think and behave like humans. AI is used to develop computer systems that can solve complex problems, recognize patterns, and learn from experience. AI systems can be used to automate tasks, such as scheduling, data analysis, and decision-making. AI is also used to develop robots that can interact with humans and the environment. AI has applications in many industries, including healthcare, finance, and transportation. AI can be used to improve customer service, automate manufacturing processes, and develop autonomous vehicles. AI is also used to develop virtual assistants, such as Amazon Alexa and Google Assistant, which can understand natural language and respond to voice commands. AI is an ever-evolving field of research, and its potential applications are limitless.

AI is significantly influencing cybersecurity and healthcare. AI is being utilized in cybersecurity to detect threats to the network more rapidly and accurately than ever before. AI-based systems are able to recognize harmful behavior, identify malicious actors, and respond to threats in real-time. This is helping to reduce the amount of time recognized takes to detect and respond to cyber threats, as well as reducing the cost of responding to them.

In healthcare, AI is being used to diagnose and treat diseases more accurately and quickly than ever before. Doctors may make more accurate diagnoses and administer better care when using AI-based systems, which can analyse vast volumes of data to find patterns and trends in patient health. In order to cut costs and increase efficiency, AI is now being utilized to automate administrative chores like appointment scheduling and insurance claim processing.

AI appears to have a bright future in both cybersecurity and healthcare. More rapidly and precisely than ever, AI may be used to detect and address cyber threats. AI may also assist healthcare businesses better secure patient data by identifying possible security flaws. Healthcare practitioners might concentrate on more crucial activities by using AI to automate menial chores. AI may also be used to examine vast volumes of data and find patterns and trends that can be utilized to enhance patient outcomes and treatment. Finally, AI can automate illness diagnosis and treatment, freeing up medical experts to work on more challenging situations.

Characteristics of Artificial Intelligence

1. Automation: Artificial intelligence (AI) is able to do things like recognize patterns, make judgements, and solve problems that would typically need human intelligence. Data analysis, natural language processing, and picture identification are a few examples of complicated jobs and processes that AI can automate.

2. Machine Learning: AI is capable of learning from its environment and experiences. Through machine learning algorithms, AI can learn from data and use it to improve its performance. On the other hand, Machine learning is a type of artificial intelligence (AI) that enables computers to learn without explicit programming. The goal of machine learning is to build computer programs that can access data and use it to learn for themselves. The learning procedure occurs with observations or data, such as examples, direct experience, or teaching, in order to uncover patterns within the information and enhance future judgements based on the examples we provide. The basic objective is to enable computers to learn independently of humans and adapt their behavior as a result.

i. Supervised Learning: This kind of machine learning algorithm makes predictions using labeled data. A labelled dataset with input data and the associated predicted output is used to train the algorithm. After that, the system makes predictions on fresh, unlabeled data using the labelled data.

ii. Unsupervised Learning: This is a kind of machine learning method that generates predictions from unlabeled data. An unlabeled dataset, which consists of input data without any corresponding predicted output, is used to train the algorithm. Afterward, the program makes predictions on fresh, unlabeled data using the unlabeled data.

iii. Reinforcement Learning: This is an algorithm that uses rewards and punishments to learn. The algorithm is trained on an environment, which contains input data and the corresponding rewards or punishments. The algorithm then uses rewards and punishments to make decisions and take actions in the environment.

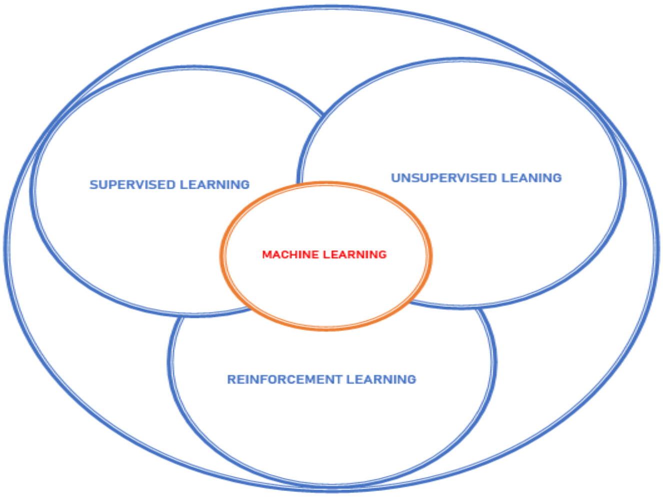


Fig. 4. Types of Machine Learning

3. Natural Language Processing: AI can understand and process natural language, such as spoken words and written text. This allows AI to interact with humans in a more natural way. Similarly, the goal of the artificial intelligence (AI) branch of natural language processing (NLP) is to give computers the ability to comprehend, analyze, and modify human language. To analyze text, NLP algorithms are employed, allowing computers to understand the structure and meaning of the language in order to extract insights from text data. NLP can be used to automate tasks such as sentiment analysis, text classification, and entity extraction.

4. Adaptability: AI is capable of adapting to changing environments and conditions. AI can learn from its mistakes and use the data to improve its performance. On the other hand, Adaptability in AI refers to the ability of an AI system to adjust its behavior in response to changes in the environment or the user’s preferences. This allows the AI system to remain effective and efficient over time, even as the environment or user preferences change. This is important for AI systems that are used in dynamic environments, such as self-driving cars, where the environment is constantly changing. Adaptability also allows AI systems to learn from their mistakes and improve their performance over time.

5. Automated Reasoning: AI can reason and draw conclusions from data. This allows AI to make decisions and solve problems without human intervention. On the other hand, automated reasoning is a subfield of artificial intelligence (AI) that focuses on using computers to reason logically about a given problem. Automated reasoning systems use algorithms to analyze a set of facts and rules to draw logical conclusions. Automated reasoning systems can be used to solve problems in many different areas, such as

mathematics, law, medicine, engineering, and philosophy. Automated reasoning can also be used to create new knowledge by combining existing facts and rules. Automated reasoning systems are becoming increasingly important in the development of AI systems, as they can help to reduce the amount of manual labor required in problem-solving.

6. Autonomous Agents: AI can act independently and autonomously. This allows AI to take action without human input or direction. On the other way, Autonomous agents in AI are computer programs that can act independently in a given environment. They are able to perceive their environment, make decisions, and take actions to achieve their goals. Autonomous agents are used in many areas of AI, consisting computer vision, NLP, and machine learning. Autonomous agents can be used to automate tasks, such as scheduling, planning, and decision-making. They can also be used to interact with humans, such as in virtual assistants, catbots, and autonomous vehicles. Autonomous agents can be used to improve the efficiency of existing systems, as well as to create entirely new systems.

The Robotics Field

Robotics is a field of engineering that focuses on the design, construction, and operation of robots. It involves the application of mechanical, electrical, and computer engineering principles to the design, manufacture, and operation of robots. Robotics is used in a variety of applications, including manufacturing, medical, military, and space exploration. Robotics engineering involves the design, construction, and operation of robots. This includes the development of robotic systems, sensors, and actuators, as well as the integration of these components into a functioning robotic system. Robotics engineers must also consider the safety and reliability of the robot, as well as its ability to interact with its environment. Robotics engineers must also consider the application of the robot. This includes the development of algorithms for robot control, navigation, and manipulation. Robotics engineers must also consider the ethical implications of their work, as robots are increasingly being used in a variety of applications, including those involving human interaction. Robotics engineering is a rapidly growing field, and the demand for qualified engineers is increasing. Robotics engineers are in high demand in a variety of industries, including manufacturing, medical, military, and space exploration. As the technology continues to advance, the demand for robotics engineers is expected to continue to grow.

Robotics is becoming increasingly important in many areas of our lives. Robotics can be used to automate processes, reduce labor costs, and increase efficiency. Robotics can also be used to improve safety, reduce human error, and increase accuracy. Robotics can also be used to explore new environments, such as space, and to perform dangerous tasks that would otherwise be too risky for humans. Additionally, robotics can be used to improve healthcare, such as through surgical robots and robotic prosthetics. Finally, robotics can be used to improve the quality of life for people with disabilities, by providing them with more independence and mobility.

The future of robotics is an exciting one. Robotics technology is advancing rapidly, and it is expected to continue to do so in the coming years. Robotics will continue to be used in a variety of industries, from manufacturing to healthcare, and even in the home. As robots become more capable and more intelligent, they will be able to take on more complex tasks and interact with humans in more meaningful ways. In the future, robots may be able to perform tasks that are currently too difficult or dangerous for humans to do. They may also be able to provide companionship, help with household chores, and provide assistance to the elderly and disabled. As robotics technology continues to evolve, it is likely that robots will become an integral part of our lives.

Different Types of Robotics

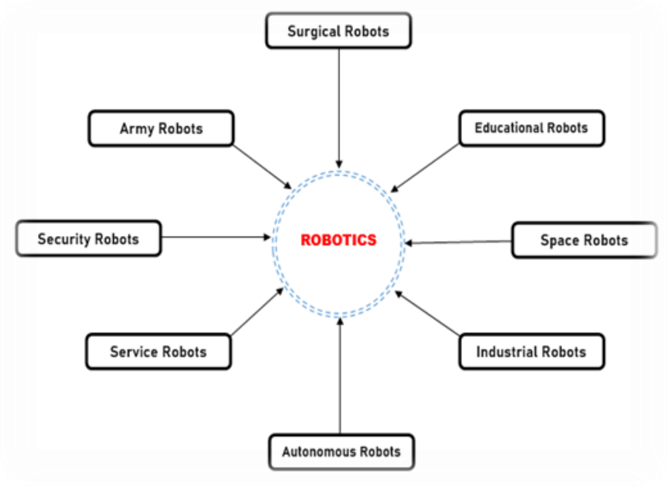


Fig.5 Few Types of Robotics

1. Surgical Robotics: These are robotic systems that are used to assist in surgical procedures. They are designed to improve the accuracy and precision of the surgeon, and to reduce the risk of complications and errors. Surgical robots typically consist of a robotic arm attached to a console, which is operated by the surgeon. The robotic arm is equipped with various tools and instruments, such as a camera, scalpel, and forceps, which are used to perform the surgery.

2. Army Robotics: This is the use of robots and robotic technology in military applications. This includes the use of unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), unmanned underwater vehicles (UUVs), and other robotic systems for reconnaissance, surveillance, target acquisition, and other military missions.

3. Security robotics is the use of robots to provide security services such as surveillance, access control, and perimeter protection. These robots are typically equipped with sensors, cameras, and other technologies to detect and respond to potential threats. They can be used to patrol areas, monitor access points, and detect intrusions. They can also be used to provide real-time information to security personnel, allowing them to quickly respond to any security incidents.

4. Service Robotics: Service robots are designed to interact with humans and provide assistance in a variety of tasks. Examples of service robots include vacuum cleaners, medical robots, and personal assistant robots.

5. Autonomous Robots: Autonomous robots are robots that are capable of making decisions and acting independently without any human input. Examples of autonomous robots include self-driving cars, unmanned aerial vehicles (UAVs), and search and rescue robots.

6. Industrial Robotics: Industrial robots are used in manufacturing and production processes to automate tasks such as welding, painting, assembly, and packaging. These robots are designed to be highly accurate and efficient, and are often used in hazardous environments.

7. Space Robotics: Space robots are designed to operate in space and are often used for exploration and research. Examples of space robots include the Mars rovers, space shuttles, and satellites.

8. Educational Robotics: Educational robots are designed to teach students about robotics and programming. These robots are often used in classrooms and can be used to teach students about robotics concepts such as sensors, motors, and programming languages.

When we talk about how Robotics will impact the cybersecurity and healthcare sector, we will consider the following;

Robotics is increasingly being used in the field of cybersecurity to help protect networks, systems, and data from malicious attacks. Robotics can be used to automate and streamline many of the tedious, manual tasks associated with cybersecurity, such as vulnerability scanning, malware detection, and patch management. Robotics can also be used to detect and respond to threats in real-time, allowing for faster and more effective responses to cyberattacks.

Robotics can also be used to help identify and mitigate potential threats before they become a problem. By using machine learning and artificial intelligence, robotics can analyze data and detect patterns that may indicate a potential threat. This can help organizations identify and address potential threats before they become a major problem.

Robotics can also be used to help organizations better understand their security posture. By using robotics to analyze data and identify potential vulnerabilities, Organizations may enhance their security posture by having a better understanding of it. In this case, it can be of help to organizations better protect their networks, systems, and data from malicious attacks.

Finally, robotics can be used to help organizations comply with security regulations and best practices. Robotics can help organizations automate the process of ensuring that their networks, systems, and data are compliant with security regulations and best practices. This can help organizations reduce the risk of non-compliance and ensure that their networks, systems, and data are secure.

Similarly, the impact of the robotics in the healthcare sector may include the following;

Robotics in healthcare is a rapidly growing field that has the potential to revolutionize the way healthcare is delivered. Robotics can be used to automate mundane tasks, reduce errors, and improve patient outcomes. Robotics can help in the accuracy improvement and speed of diagnosis and treatment. For example, Robotic systems can evaluate medical photos and find anomalies faster and more precisely than humans. This can help to reduce the time it takes to diagnose and treat patients.

Robotics can also help to reduce the risk of medical errors. Robotic systems can be programmed to follow protocols and procedures more accurately than humans, reducing the risk of mistakes. Robotics can also help to improve the safety of medical procedures. Robotic systems can be used to perform minimally invasive surgeries, reducing the risk of complications and improving patient outcomes.

Robotics can also help to improve the efficiency of healthcare delivery. Robotic systems can be used to automate mundane tasks such as dispensing medications, reducing the amount of time it takes to complete these tasks and freeing up healthcare professionals to focus on more important tasks.

Finally, robotics can help to improve access to healthcare. Robotic systems can be used to provide remote consultations and treatments, allowing patients to access healthcare from anywhere in the world. This can help to reduce the cost of healthcare and make it more accessible to people who may not have access to traditional healthcare services.

3. CONCLUSION

In conclusion, AI and robotics are revolutionizing the way we approach cybersecurity and healthcare systems. AI and robotics are providing us with more efficient and secure solutions for both industries, allowing us to better protect our data and improve healthcare outcomes. AI and robotics are also providing us with new opportunities for automation, which can help reduce costs and increase efficiency. The potential for AI and robotics to revolutionize cybersecurity and healthcare systems is immense, and it is important to continue to explore and develop these technologies in order to maximize their potential. The integration of AI and robotics in cybersecurity and healthcare systems is a promising development that could revolutionize the way we protect our data and provide medical care. AI and robotics have already been used to detect and respond to cyber threats, automate medical diagnosis, and assist with surgical procedures. As technology continues to evolve, it is likely that AI and robotics will become even more prevalent in the healthcare and cybersecurity industries. This could lead to improved security, increased efficiency, and better patient outcomes. Ultimately, the use of AI and robotics in healthcare and cybersecurity systems could have a positive impact on society as a whole.

4. FUTURE DIRECTION

AI in cybersecurity and healthcare is expected to continue to grow in the future. AI-based systems can be used to detect and respond to cyber threats, as well as to detect and prevent healthcare fraud. AI may be employed to automatically analyse massive volumes of data to find patterns and anomalies that may indicate a security breach or healthcare fraud. AI can also be used to create more secure and efficient healthcare systems, such as by automating the process of scheduling appointments and managing patient records. In addition, AI can increase the precision and efficiency of medical diagnosis and therapy, as well as to provide personalized healthcare services. Finally, AI can be used to create more secure and efficient healthcare systems, such as by automating the process of scheduling appointments and managing patient records.

5. REFERENCES

[1] M. Ahmad, "Malware in computer systems: Problems and solutions," IJID (International Journal on Informatics for Development), vol. 9, p. 1, 04 2020.

[2] N. Milosevic, "History of malware," Digital forensics magazine, vol. 1, no. 16, pp. 58–66, Aug. 2013.

[3] S. Gupta, "Types of malware and its analysis," International Journal of Scientific Engineering Research, vol. 4, 2013. [Online]. Available: https://www.ijser.org/researchpaper/Types-of-Malware-andits-Analysis.pdf

[4] Statista. A number of worldwide internet hosts in the domain name system (dns) from 1993 to 2019. [Online]. Available: https://www.statista.com/statistics/264473/number-ofinternet-hosts-in-the-domain-name-system/

[5] F. Kamoun, F. Iqbal, M. A. Esseghir, T. Baker, "AI and machine learning: A mixed blessing for cybersecurity".

[6] H.S. Anderson, A. Kharkar, B. Filar, B. Roth, "Evading machine learning malware detection," Black Hat USA 2017, July 22-27, 2017. https://www.blackhat.com/docs/us-17/thursday/us-17-Anderson-Bot-VsBot-Evading-Machine-Learning-Malware-Detection-wp.pdf, accessed November 6, 2018.

[7] N. Ding, H. Ma, H. Gao, Y. Ma, and G.Tan, "Real-time anomaly detection based on long short-term memory and Gaussian Mixture Model," Computers & Electrical Engineering, vol. 79, pp. 1-11, 2019.

[8] M.Z. Alom, and T.M. Taha, "Network intrusion detection for cybersecurity using unsupervised deep learning approaches," In Proceedings of the 2017 IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, pp. 63–69, 2017.

[9] J. Chen, Y. Yang, K. Hu, H. Zheng, and Z. Wang, "DAD-MCNN: DDoS attack detection via multi-channel CNN," In Proceedings of the 11th International Conference on Machine Learning and Computing: ICMLC '19, pp. 484-488, 2019.

[10] Y. Mirsky, T. Doitshman, Y. Elovici, A. Shabtai, and A. Kitsune, "An ensemble of autoencoders for online network intrusion detection," arXiv preprint arXiv:1802.09089, pp. 1-15, 2018.

[11] S.K. Biswas, S. K, "Intrusion detection using machine learning: A comparison study," International Journal of Pure and Applied Mathematics, vol. 118, no. 19, pp. 101-114, 2018.

[12] J. Clements, Y. Yangy, A.A. Sharma, H. Huy, and Y. Lao, "Rallying adversarial techniques against deep learning for network security, arXiv preprint arXiv:1903.11688v1, pp. 1-8, 2019

[13] S. Xia, M. Qiu, M. Liu, M. Zhong, and H. Zhao, "AI-enhanced automatic response system for resisting network threats," In M. Qiu (Ed.): SmartCom 2019, LNCS 11910, pp. 221–230, 2019.

[14] Z. Wang, "The Applications of Deep Learning on Traffic Identification", BlackHat, 2015, https://www.blackhat.com/docs/us15/materials/us-15-Wang-The-Applications-Of-Deep-Learning-OnTraffic-Identification-wp.pdf , accessed March 23, 2019.

[15] M. Lotfollahi, R. Shirali, M.J. Siavoshani, and M. Saberian, "Deep packet: A novel approach for

encrypted traffic classification using deep learning," arXiv preprint arXiv:1709.02656, pp. 1-13, 2017.

[16] G. Mi, Y. Gao, and Y. Tan, "Apply stacked auto-encoder to spam detection," In Proceedings of the International Conference in Swarm Intelligence, Beijing, China, pp. 3–15, 2015.

[17] M. Alauthman, M. Almomani, M. Alweshah, W. Omoush, and K. Alieyan, "Machine learning for phishing detection and mitigation," In: Machine Learning for Computer and Cyber Security, B. Gupta, and Q.Z. Sheng, (eds), pp. 1-27, Taylor & Francis, 2019.

[18] D. Aksu, Z. Turgut, S. Üstebay, and M.A. Aydin, "Phishing analysis of websites using classification techniques," pp. 251–258. Springer, Singapore, 2019.

[19] P. Yi, Y. Guan, F. Zou, Y. Yao, W. Wang, and T. Zhu, "Web phishing detection using a deep learning framework," Wirel. Commun. Mob. Comput, pp. 1–9, 2018.

[20] E. Benavides, W. Fuertes, S. Sanchez, and M. Sanchez, M." Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review," in Á. Rocha and R. P. Pereira (eds.), Developments and Advances in Defense and Security, Smart Innovation, Systems and Technologies vol. 152, pp. 51-64, 2020.

[21] A. Tuor, S. Kaplan, B. Hutchinson, N. Nicholsand, and S. Robinson, "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," arXiv preprint arXiv:1710.00811, pp. 1-9, 2017.

[22] N.L. Beebe, L.A. Maddox, L. Liu, and M. Sun, "Sceadan: Using concatenated n-gram vectors for improved file and data type classification," IEEE Transactions on Information Forensics and Security, vol. 8, no. 9, pp. 1519–1530, 2013.

[23] S. Axelsson, "The normalised compression distance as a file fragment classifier," Digital Investigation, vol. 7, no. 8, pp. S24–S31, 2010.

[24] W.C. Calhoun, and D. Coles, "Predicting the types of file fragments," Digital Investigation, vol. 5, pp. S14–S20, 2008.

[25] Q. Chen, Q. Liao, Z. Jiang, J. Fang, S. Yiu, G. Xi, et al, "File fragment classification using grayscale image conversion and deep learning," In Proceedings of the IEEE Symposium on Security and Privacy Workshops, pp. 140-147, 2018.

[26] N. Soliman A. ALEnezi. "A Method of Skin Disease Detection Using Image Processing and Machine Learning" Procedia Computer Science 163 (2019) 85–92.

[27] Kritika Sujay R, Pooja Suresh Y, Omkar Narayan P, Dr. Swapna B."Skin disease detection using machine learning" IJERT Vol. 9. Issue 3. 2021.

[28] H. A. Shah, F. Saeed, S. Yun, J. -H. Park, A. Paul and J. -M. Kang, "A Robust Approach for Brain Tumor Detection in Magnetic Resonance Images Using Finetuned EfficientNet," in IEEE Access, vol. 10, pp. 65426-65438, 2022, doi: 10.1109/ACCESS.2022.3184113.

[29] A. H. Abdel-Gawad, L. A. Said and A. G. Radwan, "Optimized Edge Detection Technique for Brain Tumor Detection in MR Images," in IEEE Access, vol. 8, pp. 136243-136259, 2020, doi: 10.1109/ACCESS.2020.3009898.

[30] A. S. Musallam, A. S. Sherif and M. K. Hussein, "A New Convolutional Neural Network Architecture for Automatic Detection of Brain Tumors in Magnetic Resonance Imaging Images," in IEEE Access, vol. 10, pp. 2775-2782, 2022, doi: 10.1109/ACCESS.2022.3140289.

[31] M. Rizwan, A. Shabbir, A. R. Javed, M. Shabbir, T. Baker and D. Al-Jumeily Obe, "Brain Tumor and Glioma Grade Classification Using Gaussian Convolutional Neural Network," in IEEE Access, vol. 10, pp. 29731-29740, 2022, doi: 10.1109/ACCESS.2022.3153108.

[32] Mahbub Hussain, Jordan J. Bird, and Diego R. Faria "A Study on CNN Transfer Learning for Image Classification" Contributions Presented at the 18th UK Workshop on Computational Intelligence, September 5-7, 2018, Nottingham, UK. January 2019 DOI: 10.1007/978-3-319-97982-3_1

[33] A. Kumar and S. Joshi "Applications of AI in Healthcare Sector for Enhancement of Medical Decision Making and Quality of Services," in 022 International Conference on Decision Aid Sciences and Applications (DASA) | 978-1-6654-9501-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ DASA54658.2022.9765041.

[34] "Understanding Cancer using Machine Learning | by Pier Paolo Ippolito | Towards Data Science." https://towardsdatascience.com/understanding-cancerusing-machine-learning-84087258ee18 (accessed Aug. 14, 2021).

[35] A. Maharana and E. O. Nsoesie, "Use of Deep Learning to Examine the Association of the Built Environment With Prevalence of Neighborhood Adult Obesity," JAMA

Netw. Open, vol. 1, no. 4, pp. e181535–e181535, Aug. 2018, doi: 10.1001/JAMANETWORKOPEN.2018.1535.

[36] P. Kostkova, "A roadmap to integrated digital public health surveillance," Proc. 22nd Int. Conf. World Wide Web - WWW '13 Companion, pp. 687–694, 2013, doi: 10.1145/2487788.2488024.

[37] M. Bryant, "Hospitals turn to chatbots, AI for care | Healthcare Dive," Healtcare Dive, 2018. https://www.healthcaredive.com/news/chatbots-aihealthcare/516047/ (accessed Aug. 14, 2021).

[38] A. Kumar and S. Joshi "Applications of AI in Healthcare Sector for Enhancement of Medical Decision Making and Quality of Services," in 022 International Conference on Decision Aid Sciences and Applications (DASA) | 978-1-6654-9501-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ DASA54658.2022.9765041.

[39] A. Jouman Hajjar, "6 Chatbot Applications / Use Cases in Healthcare in 2021," AI Multiple, 2021. https://research.aimultiple.com/chatbot-healthcare/ (accessed Aug. 14, 2021).

[40] K. Kalinin, "Healthcare Chatbots: Role of AI, Benefits, Future, Use Cases, Development." https://topflightapps.com/ideas/chatbots-in-healthcare/ (accessed Feb. 16, 2022).

[41] A. Mihat, N. Mohd Saad, E. Shair, A. Aslam and R. Abdul Rahim, "SMART HEALTH MONITORING SYSTEM UTILIZING INTERNET OF THINGS (IoT) AND ARDUINO", Asian Journal Of Medical Technology, vol. 2, no. 1, pp. 35-48, 2022. Available: 10.32896/ajmedtech.v2n1.35-48

[42] R. Anandh and G. Indirani, "Real Time Health Monitoring System Using Arduino with Cloud Technology", Asian Journal of Computer Science and Technology, vol. 7, no. 1, pp. 29-32, 2018. Available: 10.51983/ajcst-2018.7.s1.1810.

[43] V. Soppimath, A. Jogul, S. Kolachal and P. Baligar, "Human Health Monitoring System Using IoT and Cloud Technology - Review", International Journal of Advanced Science and Engineering, vol. 5, no. 2, p. 924, 2018. Available: 10.29294/ijase.5.2.2018.924-930.

[44] C. Srinivasan, G. Charan and P. Sai Babu, "An IoT based SMART patient health monitoring system", Indonesian Journal of Electrical Engineering and Computer Science, vol. 18, no. 3, p. 1657, 2020. Available: 10.11591/ijeecs.v18.i3.pp1657-1664.

[45] Regeringskansliet. Vision e-hälsa 2025 – gemensamma utgånspunkter för digitalisering i socialtjänst och hälso – och sjukvård. Socialdepartementet och SKL; 2016. https://www.regeringen.se/499354/contentassets/79df147f5 b194554bf401dd88e89b791/vision-e-halsa-2025-overenskommelse.pdf Accessed 12 June 2020.

[46] Baird B, Charles A, Honeyman M, Maguire D, Das P. Understanding pressures in general practice. London: King's Fund; 2016

[47] Greenhalgh T, Shaw S, Wherton J, Vijayaraghavan S, Morris J, Bhattacharya S, et al. Real-world implementation of video outpatient consultations at macro, meso, and micro levels: mixed-method study. J Med Internet Res. 2018;20:e150.

[48] Chen J, Lan YC, Chang YW, Chang PY. Exploring doctors' willingness to provide online counseling services: the roles of motivations and costs. Int J Environ Res Public Health. 2019;17:110.

[49] Allen TD, Golden TD, Shockley KM. How effective is telecommuting? Assessing the status of our scientific findings. Psychol Sci Public Interest. 2015;16:40–68

[50] SKR. Statistik om hälso – och sjukvård samt regional utveckling 2018; 2018. https://skr.se/ekonomijuridikstatistik/statistik/ekonomiochverksamhetsstatistik.1342.html Accessed 12 June 2020.

[51] Ekman B. Cost analysis of a digital health care model in Sweden. Pharmacoecon Open. 2018;2:347–54.

[52] M. Q. Hatem "Skin Lesion Classification System Using a K-Nearest Neighbour Algorithm", Hatem Visual Computing for Industry, Biomedicine, and Art (2022) https://doi.org/10.1186/s42492-022-00103-6

[53] Z. Li, et al. Intrusion Detection Using Convolutional Neural Networks for Representation Learning. In International Conference on Neural Information Processing (pp. 858-866). Springer, Cham, November 2017.

[54] C. Yin et al. Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, 21954-21961.

[55] R. Ashfaq, et al. Fuzziness based semi-supervised learning approach for intrusion detection system. Fuzziness based semi-supervised learning approach for intrusion detection system. Information Sciences, 378, 484-497, 2017.

[56] S. T. Ahmed and K.K Patil, "An Investigative study on motifs extracted features opn real-time big-data signals", in Proceedings of the 2016 International Conference on Emerging Technological Trends (ICETT), Kollam, India, IEEE, 2016, pp. 1-4. Doi: 10.1109/ICETT.2016.7873721

[57] Z. Lin, X. Fei, S. Yi, M. Yan, X. Cong-Cong and H. Jun, "A secure encryption-based malware detection system." KSII Transaction on Internet and Information Systems (TIIS), Vol. 12, no. 4, April 2018, pp.1799-1818. Doi: 10.3837/tiis.2018.04.022.

[58] M. Fan, J. Liu, X. Luo, K. Chen, Z. Tian, Q. Zheng, and T. Liu, "Android malware familial classification and representative sample selection via frequent analysis" IEEE Transaction on Information Forensics and Security, Vol. 13, No. 8 August 2018, pp. 1890-1905, doi: 10.1109/TIFS.2018.2806891.

[59] N. Shone et al. A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41-50, 2018.

[60] S. Sharma, R. Challa, and S. Sahay, Detection of Advanced Malware by Machine Learning Techniques: Proceedings of SoCTA 2017, 01 2019, pp. 333–342.

[61] L.Xiaofeng, J. Fangshuo, Z. Xiao, Y. Shengwei, S. Jing and P. Lio "ASSCA: API sequence and statistics features combined architecture for malware detection", Computer Networks, Vol. 157, July 2019, pp. 99-111, doi: 10.1016/j.comnet.2019.04.007.

[62] L. S. Fasci, M. Fisichelle, G. Lax, and C. Qian "Disarming Visualization-based Approaches in Malware Detection Systems" in Computers & Security · December 2022 DOI: 10.1016/j.cose.2022.103062

[63] I. Baptista, S. Shiaeles, and N. Kolokotronis, "A novel malware detection system based on machine learning and binary visualization," 05 2019, pp. 1–6.

[64] F. Xiao, Z. Lin, Y. Sun and Y. Ma, "Malware detection based on deep learning of behaviour graphs", Mathematical Problems in Engineering, Vol.2019, February 2019, pp. 1-10, doi: 10.1155/2019/8195395.

[65] Dai XF, Spasić I, Meyer B, Chapman S, Andres F (2019) Machine learning on mobile: An on-device inference app for skin cancer detection. In: Abstracts of the 4th international conference on fog and mobile edge computing, IEEE, Rome, 10-13 June 2019. https://doi.org/10.1109/FMEC.2019.8795362

[66] E. Amer and I. Zelinka, " A dynamic windows malware detection and prediction method based on contextual understanding of API call sequence", Computers and Security, Vol. 92, February 2020, pp. 1-5, doi: 10.1016/j.cose.2020.101760.

[67] M. O. F. Rokon, R. Islam, A. Darki, E. Papalexakis, and M. Faloutsos, "Sourcefinder: Finding malware source-code from publicly available repositories," in RAID, 2020.

[68] M. Mohammad, S. Hossain, H. Hisham, H. F. Md Jobair, V. Maria, K. Md Abdullah, A. R. Mohammad, A. Muhaiminul I., C. Alfredo, and W. Fan, "Bayesian hyperparameter optimization for deep neural network-based network intrusion detection," IEEE International Conference on Big Data, 2021.

[69] Gustafson E, Pacheco J, Wehbe F, Silverberg J, ThompsonW. A machine learning algorithm for identifying atopic der-matitis in adults from electronic health records. 2017 IEEEInternational Conference on Healthcare Informatics (ICHI).2017;2017:83---90.

[70] Esteva A, Kuprel B, Novoa RA, Ko J, Swetter SM, Blau HM,et al. Dermatologist-level classification of skin cancer withdeep neural networks. Nature. 2017;5427639:115---8

[71] F. Jiang, Y. Jiang, H. Zhi, Y. Dong, H. Li, S. Ma, Y. Wang, Q. Dong, H. Shen, and Y. Wang, ''Artificial intelligence in healthcare: Past, present and future,'' Stroke Vascular Neurol., vol. 2, no. 4, pp. 230–243, 2017, doi: 10.1136/svn-2017-000101.

[72] Han SS, Park GH, Lim W, Kim MS, Na JI, Park I, et al. Deep neuralnetworks show an equivalent and often superior performanceto dermatologists in onychomycosis diagnosis: automaticconstruction of onychomycosis datasets by region-based con-volutional deep neural network. PLoS One. 2018;13:e0191493

[73] Patnaik SK, Sidhu MS, Gehlot Y, Sharma B, Muthu P (2018) Automated skin disease identification using deep learning algorithm. Biomed Pharmacol J11(3):1429–1436. https://doi.org/10.13005/bpj/1507

[74] Rathod J, Waghmode V, Sodha A, Bhavathankar P (2018) Diagnosis of Skin diseases using convolutional neural networks. In: Abstracts of the 2nd International Iconference on electronics, communication and aerospace technology. Coimbatore: IEEE. https://doi.org/10.1109/ICECA.2018.8474593

[75] Amin J, Sharif A, Gul N, Anjum MA, Nisar MW, Azam F et al (2020) Integrated design of deep features fusion

for localization and classification of skin cancer. Pattern Recogn Lett 131:63–70. https://doi.org/10.1016/j.pa trec.2019.11.042

[76] A. Mahajan, T. Vaidya, A. Gupta, S. Rane, and S. Gupta, "Artificial intelligence in healthcare in developing nations: The beginning of a transformative journey," Cancer Res., Statist., Treatment, vol. 2, no. 2, p. 182, 2019, doi: 10.4103/crst.crst_50_19

[77] S. Grampurohit, V. Shalavadi, V. R. Dhotargavi, M. Kudari, and S. Jolad, ``Brain tumor detection using deep learning models,'' in *Proc. IEEE India Council Int. Subsections Conf. (INDISCON)*, Oct. 2020, pp. 129_134.

[78] R. Ashraf, S. Afzal, A. Rehman, S. Gul, J. Baber, M. Bakhtyar, I. Mehmood, O. Song, and M. Maqsood, "Region-of-Interest Based Transfer Learning Assisted Framework for Skin Cancer Detection", IEEE ACCESS, *Digital Object Identifier 10.1109/ACCESS.2020.3014701*

[79] Balaji MSP, Saravanan S, Chandrasekar M, Rajkumar G, Kamalraj S (2021) Analysis of basic neural network types for automated skin cancer classification using Firefly optimization method. J Ambient Intell Human Comput 12(7):7181–7194. https://doi.org/10.1007/s12652-020-02394-0

[80] G. Kumar, P. Kumar, and D. Kumar, ``Brain tumor detection using convolutional neural network,'' in *Proc. IEEE Int. Conf. Mobile Netw. Wireless Commun. (ICMNWC)*, Dec. 2021, pp. 1_6.

[81] G. Yang, Q. Ye, and J. Xia, ''Unbox the black-box for the medical explainable AI via multi-modal and multi-centre data fusion: A minireview, two showcases and beyond,'' 2021, arXiv:2102.01998.

[82] Kassem MA, Hosny KM, Fouad MM (2020) Skin lesions classification into eight classes for ISIC 2019 using deep convolutional neural network and transfer learning. IEEE Access 8:114822–114832. https://doi.org/10.1109/ACCESS.2020.3003890

[83] H. A. Shah, F. Saeed, S. Yun, J. Park, A. Paul, and J. Kang, "A Robust Approach for Brain Tumor Detection in Magnetic Resonance Images Using Finetuned EfficientNet", IEEE ACCESS *Digital Object Identifier 10.1109/ACCESS.2022.3184113*

[84] S. Polekar, S. Wakde, M. Pandare, P. Shingane, "Intelligent Medical Chatbot System For Women's Healthcare" ITM Web of Conference 44, 03020 920 (2022) https://doi.org/10.1051/itmconf/20224403020.

[85] A. Imran, A. Nasir, M. Bilal, G. Sun, A. Alzahrani, and A. Almuhameed, "Skin Cancer Detection Using Combined Decision of Deep Learners", IEEE ACCESS, *Digital Object Identifier 10.1109/ACCESS.2022.3220329.*

[86] H. Rafiq, N. Aslam, M. Aleem, B. Issac, and R. H. Randhawa "AndroMalPack: enhancing the ML-based malware classification by detection and removal of repacked apps for Android systems", Scientific Reports | (2022) 12:19534 | https://doi.org/10.1038/s41598-022-23766-w

[87] Ahmed, I.T. Jamil, N.; Din, M.M. Hammad, B.T. Binary and Multi-Class Malware Threads Classification. Appl. Sci. 2022, 12, 12528. https://doi.org/10.3390/app122412528