NJESR/ April-2023/Volume-5/Issue-4 E-ISSN-2582-5836
DOI-10.53571/NJESR.2023.5.4.14-26

Artificial Intelligence-Based Security And Data Protection

Jessy.K.Mathew*, Nimmi George**

Lecturer

Department Of Computer Hardware Engineering*

Department Of Computer Engineering**

Government Polytechnic College

Kaduthuruthy*

Kalamassery**

(Received:10March2023/Revised:25March2023/Accepted:1April2023/Published:5April2023)

Abstract

In recent years, artificial intelligence (AI) has grown rapidly. Organizations in both the public and private sectors use AI tools more and more these days. Individuals, institutions, and society stand to gain significantly from AI's capabilities now and in the not-too-distant future. However, the very same technological advancements bring up significant issues, such as the conflict between AI and data protection laws. As a result, in light of the technological realities of the 21st century, we have the opportunity and obligation to investigate the efficacy of existing data protection laws. While adhering to the laws governing data protection is important, a more long-term strategy would be to view the difficulties posed by AI as yet another signal that our current data protection strategy is becoming increasingly out of date and ineffective. When viewed in this way, the law governing data protection needs to be improved if it is to effectively address AI's challenges, protect privacy, and prevent the creation of unnecessary bureaucratic barriers to AI's benefits. Five changes seem vital:

A Framework of Harms, Transparency, and Redress, a Greater Focus on Data Uses and Impacts, a More Systematic and Well-Developed Use of Risk Management, and a Shifting from Individual Consent to Data Stewardship

Introduction

In recent years, artificial intelligence (AI) has grown rapidly. Organizations in both the public and private sectors use AI tools more and more these days. Individuals, institutions, and society stand to gain significantly from AI's capabilities now and in the not-too-distant future. However,

the very same technological advancements bring up significant issues, such as the conflict between AI and data protection laws. As a result, in light of the technological realities of the 21st century, we have the opportunity and obligation to investigate the efficacy of existing data protection laws. In the age of AI and the big data that it frequently depends on, we need data protection laws and practices that not only effectively protect privacy but also do not impose unnecessary roadblocks on the development of these innovative technologies in the future. It cannot be a choice between the already common benefits of AI and the protection of personal data, as has been emphasized in numerous reports from the government and regulators: We must discover practical means to guarantee both. This article discusses AI and some of its applications, as well as some of the difficulties and conflicts that AI poses with current data protection laws and principles. It aims to provide a more nuanced comprehension of those applications and argues that their interaction with data protection laws calls for and welcomes the revision of those laws to reflect technological realities of the 21st century. Data security and artificial intelligence (AI) are two crucial fields that are increasingly intertwining. The use of personal data and the possibility of bias in AI systems are important ethical issues that are being raised as AI technology continues to advance.

Organizations must first and foremost ensure that they are open and honest about how AI is used and that individuals are given clear and concise information about how their personal data is collected, used, and processed. This includes describing the purposes for which the data are being collected, the kinds of data being collected, and the legal basis for the collection and processing of the data.

In addition, businesses must ensure that individuals have given their consent to the processing of their personal information for the particular purposes for which it is being collected. This necessitates giving individuals the opportunity to explicitly consent to the processing of their data.

The issue of automated decision-making is another important consideration for businesses in relation to AI and the General Data Protection Regulation (GDPR). In 2018, the European Union implemented the GDPR. It grants individuals the right to avoid having their decisions affected solely by automated processing, such as profiling. This implies that associations should think about the likely effect of their computer based intelligence frameworks on people and guarantee

that they are not pursuing choices that altogether influence people without satisfactory human oversight.

Transparency, consent, and the potential impact of automated decision-making on individuals are, all things considered, the most important considerations for businesses in relation to AI and the GDPR. Companies can guarantee that their use of AI is in accordance with the General Data Protection Regulation (GDPR) and that individuals' rights regarding their personal data are respected by taking into account these aspects and taking the necessary precautions.

Information security is more prominent than simply the GDPR so here is a rundown of key contemplations for man-made intelligence regarding information insurance.

1.Ensuring that personal information is collected, processed, and stored in accordance with applicable data protection regulations.

2.Putting in place appropriate security measures to prevent unauthorized access, disclosure, or use of personal data.

3.Monitoring and auditing the use of personal data on a regular basis to make sure it is being used legitimately and in accordance with any permissions or consents that have been granted.

4.Providing individuals with clear and transparent information regarding the AI system's use of their personal data, including their rights to access, rectify, erase, or limit its processing.

5.Establishing procedures for handling complaints and other data protection-related issues, as well as responding to requests from individuals for access to or correction of their personal data.

6.Putting together robust governance frameworks to guarantee that the AI system is being used in an ethical and responsible manner, as well as conducting regular assessments of the system's potential risks and effects on people and society.

Therefore, it is essential for businesses to strike a balance between the requirement to adhere to data protection regulations and laws and the requirement to make use of artificial intelligence and technological advancements.

Introduction To Artificial Intelligence

A. Defining Artificial Intelligence

The broad objective of empowering “computer systems to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages” is referred to as “artificial intelligence” (AI). This single term encompasses a wide range of technological advancements, each of which may pose their own

unique difficulties to current data protection tools. The majority of AI systems currently in use are computer systems that find patterns in large amounts of data to perform discrete tasks like playing games, recognizing images, or verifying identity. Although the mathematical idea of AI dates back to the 1950s, it has only recently found use in the real world as a result of advancements in processing power and the vast amount of digital data that can be analyzed. Consequently, AI is frequently associated with "big data." Numerous instances of "narrow" AI—AI designed to perform a single task or set of tasks—have been observed. Narrow AI is still hard to understand. As the New York Times noted, even restricted man-made intelligence devices can be "bafflingly obscure" and "sidestep understanding since they include a torrential slide of likelihood." Concerns regarding "artificial general intelligence" present a greater challenge. "Notional future AI system[s] that exhibit apparently intelligent behavior at least as advanced as a person across the full range of cognitive tasks" are what we mean when we talk about these systems. At the point when a framework can act so that a spectator couldn't recognize it from that of a human, it is said to pass the supposed "Turing Test," set out by Alan Turing in 1950. These technologies describe the reality of modern computing more and more, and nations around the world have pledged to be at the forefront of AI by announcing ambitious plans to advance AI technology development. In its most recent report, Artificial Intelligence for Europe, the European Commission noted the following: Artificial intelligence (AI) is not science fiction; it is already a part of our lives. AI is a reality, and we can use it to organize our days with a virtual assistant, drive a self-driving car, and have our phones suggest good restaurants or songs. “[b]eyond making our lives easier, AI is helping us to solve some of the world's biggest challenges,” the report continues. from combating climate change to anticipating cybersecurity threats, from treating chronic diseases to lowering traffic accident fatality rates. The development of AI and related technologies is accelerating. Like the steam motor or power previously, simulated intelligence is changing our reality, our general public and our industry. “7 As a result, the term "AI" as used below encompasses both narrow AI, which is widely used today and has been used for a long time, and other digital technologies that are ushering in a future in which computers are so ingrained in everyday life that we no longer consider them to be computers at all.

Public And Private Uses Of Artificial Intelligence

The momentous advancements in man-made intelligence applications have prompted impressive utilization of artificial intelligence openly and confidential areas. "AI is a tool that is already deeply embedded in our lives," the UK House of Lords stated in its most recent AI report. Artificial intelligence (AI) enables subject matter experts in every industry to provide improved services and achieve unprecedented breakthroughs as a computational tool that can enhance any decision-making process. A trend that is highly demanded by consumers and citizens is the facilitation of commercial interactions and personalized services and products by AI technologies. Personalization happens in the confidential area through movement the board, customer suggestions, and designated publicizing, as well with respect to cultural progressions in clinical analysis and treatment, customized training, and productive utilization of assets. The following are just a few of the many areas where AI can benefit you.

• AI in Health and Medicine: AI is assisting in patient diagnosis and treatment as well as in disease research and prevention. The purpose of Intel's Collaborative Cancer Cloud is to assist researchers in locating new biomarkers associated with the diagnosis and progression of cancer. AI is increasingly being used in medical applications, such as assisting surgeons in locating the best place to operate during surgeries or scanning images for early disease detection. “Robots can analyze data from pre-op medical records to guide a surgeon's instrument during surgery, which can lead to a 21 percent reduction in a patient's hospital stay,” according to AI-equipped machines. IBM's Watson is used in a partnership between the Cleveland Clinic and IBM to mine big data and assist physicians in developing treatment plans that are more tailored to each patient's needs. "By transforming mosquitoes into devices that collect data from animals in the environment, Microsoft's Project Premonition seeks to detect pathogens before they cause outbreaks," states the company. Microsoft is developing autonomous drones that can locate mosquito breeding grounds; using robots to gather them; and by "searching for pathogens using cloud-scale genomics and machine learning algorithms."

• AI in Transportation: Artificial intelligence (AI) technology is present in a lot of modern automobiles, assisting drivers with backing up or changing lanes. These tools can also be found on airplanes, ships, trains, and almost any moving object. Fully autonomous vehicles are also increasingly becoming a reality, with driverless vehicles designed to respond to shifting traffic patterns and road conditions logging more than 10 million miles on public roads. These sensor-

empowered vehicles are changing transportation and promising sensational changes in vehicle wellbeing, confidential vehicle possession, and public transportation.

• AI in Marketing: AI has proven useful in making marketing more efficient and effective by assisting businesses in creating targeted advertisements for customers who are most likely to be interested in particular products (and, conversely, by sparing customers from being bombarded with advertisements for products in which they have no interest). AI is used by well-known technology companies like Amazon, Netflix, and Spotify, as well as traditional retailers like Starbucks, to tailor customer experiences and advertisements.

• AI in Agriculture: The agricultural industry was one of the first industrial users of AI, utilizing AI for a variety of purposes. For instance, a group of researchers worked with Microsoft to create algorithms that help cattle farmers identify and analyze patterns for each animal.26 Other recent advancements in artificial intelligence in agriculture focus on crop monitoring, irrigation, and upkeep. Based on sensor data, IBM's Watson, for instance, can automatically detect and water small sections of vineyards. This technology is currently being adapted to other crop systems as well. Predicting fertilizer efficacy and hybrid seed performance based on genomic information and parent line identifiers are two other agricultural applications of AI.

The Challenge for Data Protection

AI has both advantages and disadvantages. AI is already assisting workers in many fields, but it is likely to reduce the need for workers in other fields. Particularly if the data used in the development of AI only represents partial segments of the population or reflects societal bias, it may introduce bias and new forms of discrimination. Traditional notions of urban and residential planning, which allocate large areas to parking lots and garages, will likely be challenged by AI. If the data necessary for its development is concentrated in the hands of a few entities, AI may also raise significant antitrust concerns. Each of these significant issues requires careful consideration, but they are beyond the scope of this article and typically fall under other legal bodies. This article centers only around information assurance challenges introduced by simulated intelligence involved today and a work in progress for use sooner rather than later.

A. The Scope Of Data Protection Regulation In The AI Context: Personal Data

Information assurance regulations apply when individual information is involved. Sadly, the correlations and inferences that can be drawn from aggregated data sets have significantly blurred the distinction between what is "personal" and what is not. Data users and regulators

alike face the difficult task of deciding which data should be subject to regulation because information that appeared to be non-personal may now be personal data. Personal data are defined as follows by the EU's General Data Protection Regulation (GDPR): any data about a known or identifiable natural person (a "data subject"); a recognizable normal individual is one who can be distinguished, straightforwardly or by implication, specifically by reference to an identifier, for example, a name, an ID number, area information, a web-based identifier or to at least one elements well defined for the physical, physiological, hereditary, mental, monetary, social or social character of that regular individual.

Personal data are also broadly defined in other nations. Personal information, for instance, is defined as "information pertaining to any living person that makes it possible to identify such individual by their name and resident registration number, image, etc." in South Korea's Personal Information Protection Act. and specifically includes "information that, if combined with other information, makes it possible to identify any specific individual if not by itself." By expanding the capability of linking data or recognizing patterns of data that may render non-personal data identifiable, AI, and the variety of data sets on which it frequently relies, only exacerbates the difficulty of determining when data protection laws apply. This is not a novel finding. Professor Latanya Sweeney demonstrated that just three data elements can uniquely identify 87% of the US population: birth date, gender, and a ZIP Code with five digits. There are well-publicized instances of Google, Netflix, AOL, and other companies releasing identified data sets only to have the data reidentified by researchers within days by comparing them to other data sets. "The ability to compare databases threatens to make a mockery of data protections," The Economist wrote in 2015.

Data Protection

A lot of academics, businesses, lawyers, and regulators are trying hard to figure out how to deal with the problems AI has with data protection laws. Given the urgent need for data users to adhere to existing data protection laws, these are significant initiatives that are obviously required. However, as we have seen, efforts to reconcile these laws and AI run the risk of weakening data protection or interfering with AI's benefits. This is because the tension between the two is so great and fundamental. Neither one of the outcomes is helpful given the significance of simulated intelligence and of individual security. A superior long haul approach is to see the difficulties introduced by simulated intelligence as another reminder that our

ongoing way to deal with information insurance is progressively obsolete and inadequate. When viewed in this way, the law governing data protection needs to be improved if it is to effectively address AI's challenges, protect privacy, and prevent the creation of unnecessary bureaucratic barriers to AI's benefits. Data protection law has received a lot of attention over the past ten years, with the goal of making it more effective in the face of AI, big data, the Internet of Things, social media, and other developments that were not anticipated when the OECD Guidelines were published in 1980. A lot of this work is pertinent to the difficulties introduced by man-made intelligence. Particularly, it appears that five reforms are required.

AI-powered Tools Meet A Variety Of Cyber Security Needs

1. Biometric confirmation. Passwords can be broken, putting a user, business, or government agency's sensitive data at risk. The system is able to reliably scan fingerprints and palm prints, making AI-based authentication much safer here. When biometric logins are related with passwords, the probability of client information being compromised is altogether lower.
2. Increase in the rate of threat detection. Multiple varieties of malware cannot be handled concurrently by conventional cybersecurity systems. In addition, hackers have raised not only the cybersecurity standard but also the bar. You need to use advanced security tools that can address these issues in order to quickly identify advanced threats. Companies are adopting AI-driven systems that can quickly and easily identify threats through pattern recognition by utilizing cutting-edge, constantly-updated codes and algorithms. Simulated intelligence joined with AI is compelling in examining site creep ways, miniature way of behaving of malware, and any noxious action that further aides direction.
3. Rapid reaction to attacks. Essentially distinguishing dangers continuously is unimportant assuming that the framework can't battle and forestall dangers before they make minor harm the framework. The AI automatically suggests strategies to prevent an attack when a group of hackers attacks a system from a variety of angles. Attacks can be detected and dealt with more quickly and simply through AI's use of intelligent analytics. For instance, when the artificial intelligence system locates a malicious file on the system, it primarily disconnects the file from the system.
4. Establishing a dynamic authentication environment. On networks, data can also be intercepted. Traditional authentication methods are no longer secure because of this alarming situation for employees who gain remote access to systems. AI steps in to save the day here.

Using multi-factor authentication, AI systems create a global real-time authentication environment that adjusts access privileges based on network or location. When accessing data remotely, this includes collecting data and analyzing user behavior in the application, device, and network.

5. reducing human involvement. No machine can outperform the innovativeness, creative mind and considering skill people. However, engineers' decisions are also supported by the appropriate collection of data, opinions, and current trends. It takes a lot of time to look at and use meaningful data, and it is impossible to solve a problem with a high risk right away. Security personnel will get a break by automating the detection and prevention of security threats without human intervention when businesses develop a secure application using AI technology. Engineer intervention to shield systems from a series of attacks is reduced by continuous user behavior analysis and predictive analytics. You can put the time saved to use on creative and satisfying endeavors. Nonetheless, computerized reasoning frameworks are prepared and worked by people, and in certain spots the requirement for human specialists is obligatory, as they can go past abnormalities that machines can't distinguish and affirm that the supposed assault is veritable.

How Artificial Intelligence Can Improve Data Security

Trade, banking, and healthcare are just a few of the industries that have benefited greatly from digitization, but it has also made businesses more susceptible to cyberattacks. As a result, in the digital age, data security has emerged as one of the top priorities for businesses. Cyberthreats affect every sector. Throughout the long term, the world has seen a sensational expansion in web-based assaults. These threats are not only becoming more numerous, but they are also becoming more sophisticated.

It is more important than ever to have data-protection systems and procedures in place as more businesses embrace digital technologies and the Cloud. Be that as it may, the inquiry is, the manner by which computerized reasoning further develops information security.

Artificial intelligence (AI) and machine learning (ML) are regarded as the solution by numerous business leaders and experts.

How Artificial Intelligence Improves Data Security

Experts acknowledged AI's potential to reshape the business world at the 2018 Oracle OpenWorld, an annual conference on cutting-edge cloud technology. One of them was Mark

Hurd, CEO of Oracle. He predicted that AI and cybersecurity would alter business models by 2025.

Larry Ellison, the founder of Oracle, also stated that AI will aid businesses in identifying, evaluating, and even resolving online threats. He confirmed that Oracle is working on AI and will use it to improve the security of business data.

Additionally, Ellison spoke about how Oracle's next-generation cloud will turn data into a valuable corporate asset. He claims that the autonomous cloud, which enables greater dependability and shorter development times, has increased developer productivity.

Oracle also revealed at the conference that nine new locations will be used to host their cloud services. By the end of the year, they anticipate these data centers to be operational.

The Global State Of Information Security

At the Open World conference, AT&T CEO Thaddeus Arroyo also provided valuable insights. He says that businesses should use AI and the Cloud to talk to their customers. In addition to improving customer service, this will improve data security.

Businesses will be able to protect their systems and networks from organized cyber-attack groups and predict attacks before they occur by utilizing AI and machine learning capabilities.

As business activities become progressively digitized, organizations should embrace information security best practices or chance losing their important information — and clients.

Organizations and their data may still be vulnerable to online attacks due to growing political imbalances, even though AI-driven apps and the Cloud will help improve productivity and customer experience.

Ian Bremmer, President of Eurasia Group, claims that the global economy is steadily expanding at 4%, but the geopolitical situation does not appear to be as favorable. First and foremost, the politics and economics of the United States and China are at odds.

For instance, when a company enters China, the Chinese government is in charge of all strategy-related decisions. They also influence other governments around the world to follow in their footsteps because they are an economic superpower.

Examination and warning organization Gartner states that worldwide data security will undoubtedly go more than $124 billion of every 2019. In terms of global spending on data security software and services in 2018, it is anticipated to exceed $114 billion. This is an increase of 12.4% from the previous year.

Keep in mind that security breaches are also costing a lot more money.

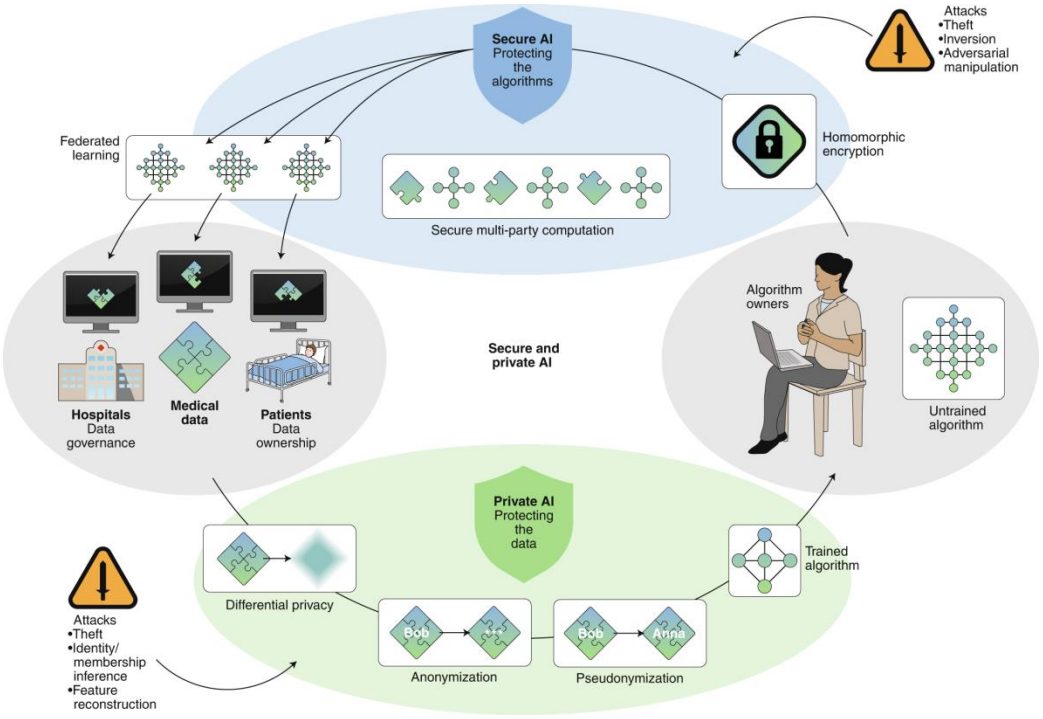
All governments and businesses must respond to the growing risk of cyberattacks, regardless of their political situations. Additionally, the revolutionary concept we require for data security is intelligent systems. It ought to assist us in protecting IT environments from constantly evolving threats.

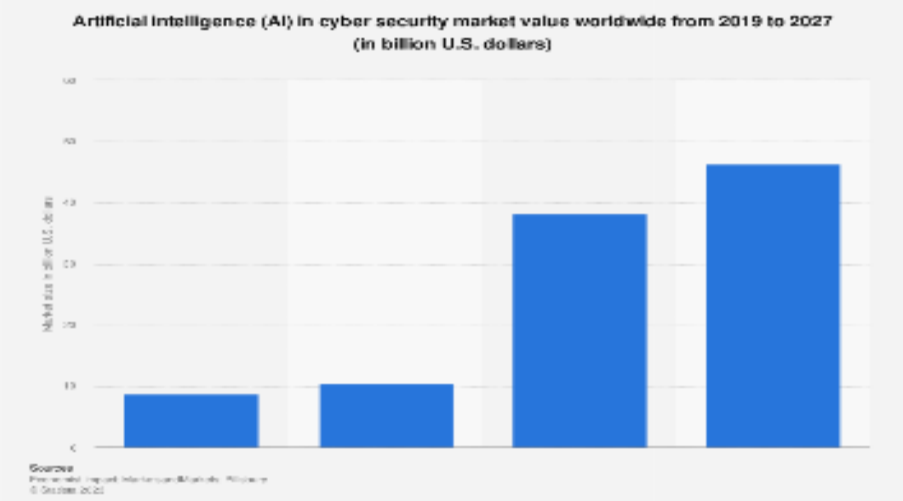
Takeaway On How Artificial Intelligence Improves Data Security

Leaders in business, like you, ought to be aware of the new dangers posed by new technologies. These threats have the potential to disrupt your operations and compromise your confidential data.

You should also be aware that, despite the numerous cyber threats facing the security industry, there is a shortage of skilled workers who can assist you in protecting your business from these threats.

However, with AI and machine learning automating cyber threat detection and response, businesses like yours can reduce employee workload and deal with attacks more effectively.





Conclusion

The widespread use of AI is already bringing about significant advantages, but it is also bringing up significant issues. In an economy that is becoming increasingly dependent on data, efforts to address these issues within the frameworks for data protection are increasingly demonstrating the limitations of those frameworks and their inadequacy for both privacy protection and innovation facilitation. As new man-made intelligence applications are created and conveyed, we have an open door and an undeniably undeniable need to look at the adequacy of current information security regulations and to reexamine them considering 21st-century real factors.

References

[1]. Attkan, A. and Ranga, V., 2022. Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, 8(4), pp.3559-3591.

[2]. Alrayes, F.S., Alotaibi, S.S., Alissa, K.A., Maashi, M., Alhogail, A., Alotaibi, N., Mohsen, H. and Motwakel, A., 2022. Artificial Intelligence-Based Secure Communication and Classification for Drone-Enabled Emergency Monitoring Systems. Drones, 6(9), p.222.

[3]. Awotunde, J.B. and Misra, S., 2022. Feature extraction and artificial intelligence-based intrusion detection model for a secure internet of things networks. In Illumination of Artificial Intelligence in Cybersecurity and Forensics (pp. 21-44). Cham: Springer International Publishing.

[4]. Lehner, O.M., Ittonen, K., Silvola, H., Ström, E. and Wührleitner, A., 2022. Artificial intelligence based decision-making in accounting and auditing: ethical challenges and normative thinking. Accounting, Auditing & Accountability Journal, 35(9), pp.109-135.

[5]. Rana, S.K., Rana, S.K., Nisar, K., Ag Ibrahim, A.A., Rana, A.K., Goyal, N. and Chawla, P., 2022. Blockchain technology and Artificial Intelligence based decentralized access control model to enable secure interoperability for healthcare. Sustainability, 14(15), p.9471.

[6]. Saura, J.R., Ribeiro-Soriano, D. and Palacios-Marqués, D., 2022. Assessing behavioral data science privacy issues in government artificial intelligence deployment. Government Information Quarterly, 39(4), p.101679.

[7]. Mann, S., Balyan, A., Rohilla, V., Gupta, D., Gupta, Z. and Rahmani, A.W., 2022. Artificial Intelligence-based Blockchain Technology for Skin Cancer Investigation Complemented with Dietary Assessment and Recommendation using Correlation Analysis in Elder Individuals. Journal of Food Quality, 2022.

[8]. Kamradt, M., Poß-Doering, R. and Szecsenyi, J., 2022. Exploring Physician Perspectives on Using Real-world Care Data for the Development of Artificial Intelligence–Based Technologies in Health Care: Qualitative Study. JMIR Formative Research, 6(5), p.e35367.

[9]. Martin, C., DeStefano, K., Haran, H., Zink, S., Dai, J., Ahmed, D., Razzak, A., Lin, K., Kogler, A., Waller, J. and Kazmi, K., 2022. The ethical considerations including inclusion and biases, data protection, and proper implementation among AI in radiology and potential implications. Intelligence-Based Medicine, p.100073.

[10]. Murdoch, B., 2021. Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Medical Ethics, 22(1), pp.1-5.

[11]. Jabarulla, M.Y. and Lee, H.N., 2021, August. A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. In Healthcare (Vol. 9, No. 8, p. 1019). MDPI.

[12]. Davahli, M.R., Karwowski, W., Fiok, K., Wan, T. and Parsaei, H.R., 2021. Controlling safety of artificial intelligence-based systems in healthcare. Symmetry, 13(1), p.102.