D. K. Tripathi, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Privacy And Security In The World Of Artificial Intelligence

D. K. Tripathi, Anjali Sharma and S. Nandi,
, 1,2 Narula institute of technology, Kolkata, W.B. PIN-700109, India.
3, Harishchandrapur College Malda, W.B. PIN-732125, India

Abstract- Many technical companies and organization are relying to artificial intelligence (AI) for a variety of advantages - problem solving or making a decision. Not only in organizations, we can see the tremendous use of AI, but also in healthcare, education, electronics, e-commerce, software development, pharmacies, games, engineering, communication and development. AI makes our work more accurate and saves our time on the other hand there is always a possibility of leaking of personal data to third party with whom we are not associated by any means. In spite of much advancement in AI, the privacy and security are not addressed to appreciable extent. In this paper the privacy and security issues associated with artificial intelligence is critically examined. The challenges related to the privacy and security is investigated on the basis of available literature data. This paper not only discusses the problems in using AI but also suggests an optimized solution regarding user privacy and their personal data.

Keywords - Artificial intelligence, Technological abuse, Privacy and security, E-commerce, cloud computing.

Statements and Declarations:

I. INTRODUCTION

In Dartmouth Conference (Year 1956), the word "Artificial Intelligence" first used by American scientist John McCarthy [1-2]. In 1997 a supercomputer named "Deep Blue" was designed by IBM defeated the world champion chess player in a match. Over the past 30 years, remarkable invention has been achieved in this area. Artificial intelligence is the study and use of methods that enable computer systems to carry out tasks that would normally need human intelligence. Many disciplines, including philosophy, psychology, linguistics, mathematics and medicine, can be used to analyze

the study of intelligence. From few years, artificial intelligence has become embedded in our day-to-day existence. From humanoid robots like Sophia to home speaker assistants like Alexa, we can see the maturation of AI techniques [3-4]. The topic of artificial intelligence (AI) is controversial and frequently portrayed negatively; some would consider it a disguised blessing for businesses, while others believe it to be a technology that threatens the very existence of humanity because it has the potential to subjugate and dominate humans. However, in reality, AI has already an impact on our way of life, either directly or indirectly and is helping to shape the world of tomorrow [3-4]. Despite the necessity of using digital assistants on smart phones, driver assistance systems, bots, text and speech translators and systems that help propose goods and services and personalized learning, AI has already influenced our daily lives and drastically changed our way of existence. With day-by-day achievement there will likely be more robots or intelligent programs that can help us, such as reading email, cleaning room or even driving cars for us [2]. The Artificial intelligence is advancing day by day with high rate. Although there are many advantages of AI but beside that there are also some disadvantages related to our safety, privacy and security. If we fail to identify and prevent related threats due to use of AI, many uncontrolled consequences might arise [1].In our society, AI is becoming more and more significant. Even after decades of study and learning, it continues to be the most esoteric topic in computer science and a popular catchphrase. The benefits of use of AI are widely acknowledged in a variety of fields, including medicine, security, consumer applications and business. Till near past, it was the subject of discussion and work among science fiction writers; it was restricted to university research labs. The evolution of new technologies gives excitement as well as mistrust on its output. The benefits and limitations of AI are reported by many researchers [5-6]. Yet before we can fully utilize the enormous revolutionary potential and overcome some obstacles, this nascent technology has. Because most people are uninformed of the science, technology, and algorithms that go into AI, it is challenging for them to put their trust in it. In this paper, we will discuss the threats and potential risks of Artificial intelligence.

II. ANALYSES

1. Artificial intelligence and its applications

The requirement for lifelong learning is one of the key characteristic of our information economy [7-8]. The technology that imitates human intelligence process by machines, especially computer systems is known as Artificial intelligence. These intelligent processes include perception, learning and reasoning. Currently it is being broadly used in different fields like in agriculture, healthcare, finance, education. AI has benefited us and will benefit in long term.

AI application in healthcare: Using machine learning technique the structured data of the healthcare system like imaging, genetic and EP data are analyzed which can infer the probability of disease outcome [9-10]. The natural language processing extracts the information from unstructured data and contributes to structured data. With the help of AI techniques, we can quickly improve the efficiency of image analysis accurately. It is reported in research that analysis using AI could find and match specific lung modules between 62% to 97% faster than a panel of radiologists [11]. Diagnosis of cancer, neurological and cardiac diseases reaches to a new height using AI [9 -18]. The AI is used in the diagnosis of eye disease also [18]. Another application is AI-assisted robotic surgery. A type of robotics assisted by artificial intelligence can analyze the pre-op medical records in orthopaedic surgery and can guide the surgeon's instrument in real time. For new surgical techniques are informed using AI on the basis of actual surgical experiences

[11]. AI also played a role in improving administrative workflows and eliminates time consuming non-patient-care activities, such as writing chart notes, filling prescriptions and ordering tests.

AI application in education: Not only in healthcare but also in the education section, AI has played an important role. With the help of AI, a

student can learn more with ease using technology. They can improve their knowledge with more visualization AI is educating people and facilitating an environment devoid of judgement for learning worldwide. For learning outside the classroom, advanced technology is required. Even the experimentation of disciplines like physics, robotics and statistics can be seen as a new development in the web-based education. The teaching-learning of every subject is possible using AI. It is to be noted that use of artificial intelligence in the field of education will support the students who frequently feel excluded from the conventional educational system by enhancing their performance through computers and the internet [19-20].

AI application in agriculture: Agriculture is contributing a significant role in the economic sector. The demand of food and employment is increasing with the increasing population. These requirements are not sufficient enough to be fulfilled by the traditional methods. We can see an agricultural revolution due to this technology as it can protect crops from various factors like insects and climatic changes. AI is fundamentally changing agriculture and has enormous possibilities. It gives farmers access to cutting-edge technologies that will help them cultivate more effectively and produce more. Preparing for agriculture is a stressful process for rain-fed farmers because even a week's delay in rain might ruin the crop. To help farmers, using artificial intelligence, Microsoft has created an AI based Sowing App powered by Microsoft Cortana Intelligence Suite in collaboration with ICRISAT (International Crop Research Institute for Semi-Arid Tropics) [21-26].

AI application in automobile industry: AI is quickly becoming a crucial component of the automobile industry, affecting both the manufacturing process and the actual vehicles. The customer demand is increasing day by day; with increasing demand we need to add some more value to supply chains which can be only done with the help of artificial intelligence. For making automobile industry more flexible and stable, AI has played an important role. The necessity for AI deployment is driven by the rising client expectations for new features and technological integration (such as driverless cars) as well as the fierce industry competition. Even businesses that manufacture replacement components have started integrating AI into their supply chains. One such business is Continental, one of the major suppliers of components (mostly tyres) to the vehicle industry. The business develops a virtual simulator using AI to test driver assistance technologies and autonomous driving. The corporation can gather data from up to roughly 5,000 miles of test driving in one hour using the virtual simulator, compared to the 6,500 miles that can be driven for testing purposes in a real automobile in one month. This improves safety while saving the business a great deal of time, effort, and resources [27-32]. Without the need for human intervention, sensed, evaluated and rectified in real-time, AI can also be used in manufacturing and information processing.

AI in Travel & Transport: The use of AI in transportation industry is emerging. By making travel time more reliable to their customers and improve the economics and productivity of their vital assets, AI had made our life easier. AI has the ability to plan, design and control the Transportation Network Structure. AI can predict traffic information and can also be used as accident detector [33-38]. The traffic signal timing and optimization uses AI based on algorithms, fuzzy logic control, artificial neural networks and reinforcement learning algorithms. These algorithms are used for optimizing signal timing parameters. Some of these algorithms like hill climbing and GAs are successfully incorporated in commercial software tools and demonstrated very good performance [5].

E-commerce: In most fields of science, engineering, education, business, etc., AI approaches have been effectively created and put to use. Like other fields, artificial intelligence has played an important role in e-commerce. An e-commerce website may propose items that are especially suited to customers using AI and users can search for things using natural language or visual clues much like they would if they were speaking to a person. AI may significantly contribute to one's efforts to automate the repetitive processes necessary to run an online store.

Automating processes like product suggestions, loyality discounts, basic customer care and more is possible with AI. In the modern period, it can be argued that the e-commerce sector is one that makes the finest use of artificial intelligence by attracting a sizable client base, comprehending consumer wants, doing real-time research, providing comprehensive answers to issues, and doing much more [39-44]. AI is present in the e-commerce sector in a variety of ways, including chatbots, CRM, ERP, Product Content Management (PCM) and many more [45].

2. Relation between Privacy, Security and Artificial Intelligence

In the above section, we have discussed about the benefits of AI in various sectors, but due to increasing dependence on AI day-by-day, the privacy and security of the users threatened [46-48]. The impacts of privacy of user must be handled with extra care. Companies working with artificial intelligence are already facing disadvantages in the user's eye in terms of privacy and security. The potential threats should be addressed before forwarding an application of AI to keep the privacy of a user.

SECURITY PROBLEMS:

We often hear the beneficial aspects of artificial intelligence security- the way it can predict and give us result about what customers need through data but when we discuss the other aspects of AI, the conversation often points on data privacy. Smartphone's, internet and surveillance cameras provide ease in collecting personal data. For record and better visibility, people use to upload and share their private data on social media which is ultimately uploaded to the cloud computers, increases the risk of privacy. The private information may be tracked easily. The social media companies may sell the data to others and reveals one's privacy and it may become problem for security. Search engines become successful in gathering very personal information because people can't hide the search information [49-54]. Sometimes, it happens that if we are typing one word then search engines suggest the other word based on the maximum searched things by others which is irrelevant to us.

Some common types of security challenges [40]:

Client Level Security Challenges: Client- level security vulnerabilities and threats are those which affect specific user endpoints, including laptops, smart phones, tablets and other endpoints. These difficulties can

affect confidentiality, integrity and accessibility of the data and services. They are frequently related to the security of the hardware, software and client-side components.

Captured and Retransmitted Messages: Attackers have the ability to collect and retransmit messages sent back and exchange between servers and the clients, possibly compromising data integrity.
Eavesdropping: Interception of client-server communication by unauthorized parties can result in security and privacy violations and data disclosure.

Mobile Devices Pull Attacks: Mobile devices may be deceived into sending harmful requests, which might allow for unauthorized access or the theft of data.
Mobile Devices Push Attacks: The security and privacy of the device and its user are at risk because attackers can utilize mobile devices to send harmful material or commands.

Lost Device: If a mobile device is not properly secured and encrypted, losing it might result in data exposure and unauthorized access.

Buffer overflow: When the buffer's storage capacity is exceeded, a buffer overflow occurs. The additional data spills onto nearby memory regions, corrupting or replacing the data there. A program's buffer can become overrun by malicious input, which might let attackers to run arbitrary code and take over the application.

Software bugs/faults: Attackers may take advantages of flaw in software code to breach security and obtain unauthorized access.
Viruses and other malicious software: Hackers may infect client devices, causing data breaches, unauthorized access and system compromise.

Unauthorized Access: Unauthorized access to client devices or applications can lead to data breaches and security compromises.

Spying Attacks: Spying attack is a kind of threat which can steal sensitive information and internet usage data and then pass that to the other users. This data is generally passed to the data collectors and advertisers who can then use it to target the individual/organization with advertisement. Sometimes they can sell that information to other companies. Due to spying attack our financial and personal information can be stolen.

Some of the sources of security issues are:

Technology abuse: The future of AI depends on - using and managing it. Experiment shows that if it is abused by malicious people, the technique may impact on our privacy and security. Using AI methods, the attracts can access to our personal information illegally. Organizations are becoming increasingly conscious of the importance of information and related technology in practically every activity, especially when it comes to fostering innovation and gaining a competitive edge. Information and technology services are susceptible to a variety of security concerns, including the leaking of sensitive data and protracted interruptions in email and internet access, all of which have a negative impact on business continuity [55]. If criminals hack AI based machines like unnamed vehicles, self-driving cars then they can harm public for their purpose. It is scary to think but if AI assistants get hacked, then they can become a major problem for human rights.

Security problems induced by possible self-aware intelligence: As a developing technology, current artificial intelligence system is far away from strong AI stage. Strong AI stage is that where the artificial intelligence may develop self awareness and can self-evolve which can become a threat to human existence. Security concerns need to be taken into account before using AI, which is still far from being realized. There was significant consideration of the possibility that machines may eventually replace human cognition rather than just enhancing it when powerful mainframe computers were developed [56]. With development of modern science, the technology is improving day-by-day. Group of researchers and scientist are studying high level cognition intelligence like machine emotion and machine awareness. A group of researchers from Columbia University made a robotic arm that was able to work without human command.

Technical defects: AI is developing day by day but it is not too perfect to trust completely. It requires consistency and focus in programming, testing and maintenance. If any technical defect arises, it may convert into accident. According to a report of Russian media, the chess playing robot was confused by the opponent boy's quick responses and fractured his finger. During a test of self-driving car, car runs over a man. Not only this case but many case has been noticed like this. Lack of care and low maintenance is the reason behind security problem.

Data security: The main goal of data security is to secure data which may be particular data and is often storage. Therefore, the definition of data security is to prevent unauthorized access, use, alternation, disturbance or destruction of data storage. Data science system evaluates enormous amounts of data in order to uncover patterns and abnormalize the patterns that may indicate a security issue. The system analyses data from several sources, such as network traffic, system logs and user behavior, using machine learning methods. The technology employs AI algorithms to identify possible risk and weakness after receiving the data.

Denial of service (Dos) attacks: The existing state of computer networks is being threatened by denial of service (Dos) assaults. For instance, an attacker may attempt to take over an IRC channel by launching Dos attacks on the channel owner. Dos attacks can be used to target AI systems to bringing down well-known websites. Dos attacks can be used to target AI system to disable or inactive them. Applications like autonomous vehicles or crucial infrastructure may suffer as a result, which might be quite detrimental.

Lack of transparency: Deep learning in particular, which is a current advancement in AI, continues to

operate in a black box paradigm. There aren't many methods for these algorithms that can explain the outcome. As a result, when an artificial intelligent system does an unexpected behavior it's not always straightforward to determine what caused it.

Misuse of AI: A substantial security risk is posed by the emergence of artificially intelligent systems that are purposefully created for malicious purposes, such as creating deep fake content or launching automated cyber-attacks, poses a significant security threat. Artificial intelligence (AI) – enabled phishing scams and autonomous weapons systems are only two examples of how legitimate AI technology maybe abused by hackers.

Model tampering and attacks: Accessing AI models without authorization can lead to tampering with model's design or setting, which might damage performance or encourage malevolent behavior. To avoid being discovered by AI-based security systems, attackers might modify input data. For example, hackers may design malware to bypass AI driven antivirus software.

Privacy Problems:
Privacy problem is the main threat of data exploration. There are many AI applications which depend on data, so there are many privacy problems in the application of artificial intelligence [56-62]. The public access to the personal information was limited in spite of availability of it, but with the surge of internet technology; these are at one click away [53]. There are no legal guarantees of privacy on the websites [44-45]. Several studies revealed the privacy issues as the main cause for not purchasing online. Privacy issues should be addressed in

Cloud computing: The introduction of cloud computing has led to the migration of many companies and government organizations to the cloud because it is widely available, cheap, easy to use and convenient to get on-demand access to the data. Among the higher computation needs of artificial intelligence, cloud computing has been configured as the primary infrastructure for multiple artificial intelligence applications, so extra care should be taken while using such AI applications.

Information retrieval: In today's digital era, individuals tend to spend a substantial part of their lives on the internet, leading to a surge in the amount of personal data collected through their online activities. When browsing the internet, traces and shopping activity are recorded on visited websites, rephrase various forms of recorded data and procedures exist in the realm of data management. When these data combined, a map of a person's behavior can be outlined. They have the ability to examine their individual preferences and behavioral patterns which rephrase the tendencies and routines people develop can help anticipate their future requirements. Many times we have seen in social media advertisements our shopping-wish list recommendations. These behaviors are serious threat to our data privacy and need to be addressed.

Data collection: Variety of information about users and their family members is being used by technology companies for commercial purposes illegally. A larger population uses smart home devices, which is an example of AI machine. During use of them, we indirectly use to give all our personal data. Other data produced by electrical activities, such as mobile phone (like live locations, geographical coordinates, credit card information, etc.), pharmacy notes and many other information which may cause privacy invasion. Data aggregation can be used for balancing the data collection and individual privacy [61].

Re-identification: Large datasets are a foundational component of AI systems, and if they are not properly protected, they may be become threat to our privacy. Sensitive personal information, including names, addresses and financial information can be made public by a data collection. Even when personal data is anonymised, there is a chance that hackers may re-identify people by combining anonymous data with other available information. Attacks can involve making small and imperceptible changes to input data to deceive artificially intelligent models. For example, an image recognition system can be tricked into misclassifying an image by adding imperceptible noise.

Data profiling: Examining, analyzing and producing meaningful summaries of data constitute the process of data profiling. The procedure produces a high- level overview that assists in the identification of data quality, problems, dangers and broad patterns. Companies can then take use of the data profiling results by using them to their advantage. AI has the ability to invade privacy by profiling and analyzing people based on their data. Without the subject's consent, profiling can be used for discrimination, targeted advertising and other things.

Smartphone surveillance and tracking techniques: The owners of mobile networks and SIM cards have the power to intercept and record all information on website visited, who called or sent SMS to whom, when and what was said. Our Wi-Fi internet provider includes DNS as part of their service; therefore they may also monitor our DNS traffic, thereby keeping a record of all of our browsing activity. Any mobile network provider can accurately determine the location of specific subscriber's phone by continuously monitoring a person's actions, AI-powered surveillance system that use face recognition and location tracking may violate the right to privacy.

Inference attacks: An inference attack is a data mining approach that uses data analysis to get information about a subject or database for improper purposes. Sensitive information about a topic may have been disclosed if an opponent may confidently determine its true worth. By analyzing patterns and behavior from seemingly innocuous data attacks can infer sensitive information about individuals. For example, inferring health conditions from shopping habits.

Supply chain Vulnerabilities: The security of AI deployments may be endangered by exploiting supply chain flaws, particularly those in the hardware and software utilized in AI systems. Our entire system might be vulnerable to disastrous data breaches due to a single weakness. Because of this vulnerability management is most important for businesses that want to maintain a safe and reliable IT infrastructure. The use of AI in conjunction with conventional vulnerability management solutions will produce the best results. Thus it is important to notice that AI should not be viewed as a replacement for conventional vulnerability management solutions.

Biometric data: Biometric data is so private and may be exploited, if not properly secured, because of this, AI systems that utilize it, including facial recognition and fingerprint scanning can offer serious privacy risks. There are several ways to deceive or compromise these biometric identification systems. Although AI is assisting in performance improvement of biometric identification, malicious individuals can also utilize AI technologies to compromise the biometric systems. We have observed examples where artificial intelligence created fake fingerprints that can effortlessly access a fingerprint reader. Similar to the race between viruses and anti-virus software, this is an ongoing competition. Criminals and hackers may have an endless desire to discover new techniques and security system flaws.

III. SOLUTIONS PROPOSED AND DISCUSSIONS

Our life is depending on technology in different ways but at the same time we have the risk of security, privacy, ethics and other risks at the same time. An optimized solution must be found. Just because AI applications becoming a threat of security and privacy, we should not stop the uses of artificial intelligence - our main aim should be how to operate AI systems in controlled way and in harmony with human beings. Different researchers have proposed following solutions for safe use of AI. The complexity and potential power of AI, as well as how closely it interacts with users, make it crucial to investigate. Implementation of artificial intelligence in more sectors requires privacy and security problems to be sorted out. Academicians and researchers need to place a greater emphasis on security protection and make every effort to make it more secure.

1. Enhancing Privacy and Security by utilizing AI Technology

Ethic rule should be embedded in AI designs: Software engineers may unknowingly write codes that violate and/or break important human rights if they lack the training of human rights laws. It is essential to educate software engineers on human rights laws. Democracy and civic rights must be considered in AI ethics. The discrimination and invasion of privacy issues in AI can be eliminated or at least reduced with the help of designers and engineers who have a better understanding of human rights regulations.

Improvement of the clarity and comprehensibility of AI systems: Artificial intelligence is a brilliant tool, but because of its inner algorithm sometimes it becomes hard to understand, it usually works on "black box". The algorithms of black box make it mysterious. Humans cannot easily interpret the black box because of its complex algorithms but AI can evolve without human monitoring and permission. For instance, Face book shut down an AI engine in 2017 after discovering that the AI had developed a special language that humans could not understand. We must develop AI systems that are user-acceptable in terms of interpretation and understanding.

Modification of security and robustness of AI system: Several AI technologies, including machine learning, computer vision, reinforcement learning, etc., are used by AI robots under the supervision of AI programmes. It is essential to confirm that machines are not directly under the control of any other agents and to deal with unexpected conditions and it should be safe enough before deploying an artificial intelligence system across a variety of applications.

Enhance security and privacy of user's private data: The vast volume of data, particularly private and personal data is crucial for the creation of AI agents. Nearly all of the application areas where deep learning is successful such as Apple Siri and Google Home have access to vast amounts of data. There is a greater potential for data misuse as society and corporations produces more data. A need and concern for enhanced security has emerged as a result of computers' capacity to collect and analyze massive quantities of data and the internet's ability to offer and make such data available on a global scale [40]. Every action that is taken with regard to the data should be meticulously documented. Risks pertaining to privacy might be caused by both the data subject and the transaction records. Determining what should be documented, who should be in control of the recording process and who may access the data and records is consequently crucial.

Securing social life: Studies have demonstrated the effectiveness of AI as a support tool for law enforcement, criminal prevention and cybercrime detection. Our home security system may be fitted with biometric authentication sensors, including fingerprint, heartbeat, and other characteristics, in addition to facial recognition software.

heIn addition to the technology research itself, the management of the use of artificial intelligence is crucial for addressing its security, privacy and ethical issues. It is important to conduct research on standards, regulation and policy to ensure that the use of artificial intelligence is under control. The governments should create laws and associated rules to specify what artificial intelligence can accomplish or what is not permitted. Since the emergence, the artificial intelligence brought possible hazards and concerns. Due to its appreciable significance, we must monitor and manage the growth of artificial intelligence. Because AI industrialization is still in its early stages, there are no defined safety regulations for many types of AI technologies, particularly for robots that can move, run and routinely collaborate with people. The administration and regulations are both urgently required to ensure the security of AI applications. AI technology can also be utilized to safeguard our privacy and improve system security. With the use of AI, not only the security of our society and the internet may be considerably increased, but there will be also the protection of each individual's privacy. The promising trend of ubiquitous computing, including location-based services and radio frequency identification, may compromise people's privacy. The protection of individual privacy

must be addressed in order to ensure the information for the society's healthy development. By identifying privacy breach habits, numerous emerging AI approaches, including pattern recognition and machine learning could significantly improve privacy protection. Research on the use of AI technology in data desensitisation, disclosure restriction and privacy infringement detection is necessary for careful use of AI technology.

IV. CONCLUSIONS

We have examined t privacy issues and investigated current AI applications for their privacy and security provisions. We can admit that Artificial Intelligent Technology made our life easier and by coming future AI applications can provide more efficiency and convenience, but we should not totally depend on this technology. Although Artificial intelligence is still developing in an exciting speed, it is necessary to discuss the privacy corners raised by AI. AI technologies are very useful for us though there are some disadvantages too. We can use it more effectively to improve the security and privacy protection for our society and cyberspace. With the new development in the application of AI, the new technology is more likely to bring us benefit rather than letting us to questioning on its management. A successful balance is possible as better solution which can adapt all the security and privacy proposals for this promising technology.

Conflict of Interest Statement

On behalf of all authors, the corresponding author states that there is no conflict of interest.

REFERENCES

[1] Subramanian, R. (2017). Emergent AI, social robots and the law: Security, privacy and policy issues. Journal of International, Technology and Information Management. 26, 81-105

[2] Li, X. & Zhang, T. (2017). An exploration on artificial intelligence application: From security, privacy and ethic perspective. .IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). 2017, 416-420

[3] Parviainen, J. & Coeckelbergh, M. (2021). The political choreography of the Sophiarobot: beyond robot rights and citizenship to political performances for the social robotics market. AI & Soc., 36, 715–24

[4] Bartneck, C., Lütge, C., Wagner, A. & Welsh, S. (2021). "An introduction to ethics in robotics And AI", "Springer; ed.1. Springer Cham", doi:

[5] Khanzode, K. C. A. & Sarode, R. D. (2020). Advantages and disadvantages of Artificial intelligence and machine learning: A literature review. International Journal of Library & Information Science (IJLIS). 9, 30-36

[6] Banerjee, M. S. (2022). Application, Advantage, and Disadvantage of Artificial Intelligence in Library Services. International Journal of creative research thoughts, 10, c723-29

[7] Harkut, D. G., Kasat, K.. (2019). Introductory Chapter: Artificial Intelligence - Scope and Limitations. In Harkut DG editor. Artificial Intelligence - Scope and Limitations. Intech Open, pp.1-5

[8] Kaplan, A. (2016). Lifelong learning: conclusions from a literature review. International Online Journal of Primary Education, 5, 43-50

[9] Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., et. al;(2017). Artificial intelligence in healthcare: past, present and future. Stroke and Vascular Neurology. 2, 230-43

[10] Azzi, S., Gagnon, S., Ramirez, A.,
., Rhee, K.., & Ramya, Y. Watson. (2018). 2018 for O& Richards, G. (2020). Healthcare Applications of Artificial Intelligence and Analytics: A Review and Proposed Framework. Appl. Sci.10,1-21

[11] Kalis, B., Collier, M., & Fu, R. (2018). 10 promising AI applications in health care. Harvard business review. Harvard Business School Publishing Corporation,

[12] Somashekhar, S. P., Sepúlveda, M. J., Puglielli, S., Norden, A. D., Shortliffe, E. H., Rohit Kumar, C., Rauthan, A., Arun Kumar, N., Patil, P ncology and breast cancer treatment recommendations: agreement with an expert multidisciplinary tumor board. Ann Oncol. 9, 418-23

[13] Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., et. al; (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature. 542, 115–18

[14] Bouton, C. E., Shaikhouni, A., Annetta, N. V., Bockbrader, M. A., Friedenberg, D. A., Nielson, D. M., et. al; (2016). Restoring cortical control of functional movement in a human with quadriplegia. Nature. 533, 247–50

[15] Farina, D., Vujaklija, I., Sartori, M., Kapelner, T., Negro, F., Jiang, N., et. al; (2017). Man/machine interface based on the discharge timings of spinal motor neurons after targeted muscle reinnervation. Nat Biomed Eng. 1, 0025. doi: 10.1038/s41551-016-0025

[16] Pandya, H., & Pandya, T. (2023). Application of artificial intelligence in medical care: review of current status. International Journal of Advances in Medicine. 10, 177-85

[17] Yu, K. H., Beam, A. L, & Kohane, I. S. (2018). Artificial intelligence in healthcare. Nat Biomed Eng, 2, 719–31

[18] Gulshan, V., Peng. L, Coram, M., Stumpe, M. C., Wu, D., Narayanaswamy, A., et. al; (2016). Development and Validation of a Deep Learning Algorithm for detection of Diabetic Retinopathy in retinal fundus photographs, JAMA, 316, 2402–10

[19] El-Khatib, K., Korba, L, Xu, Y., & Yee, G. (2003). Privacy and security in e learning. International Journal of Distance Education Technologies (IJDET), 1, 1-19.

[20] Awad, S. O. I., Mohamed, Y., Shaheen, R. (2022). Applications of Artificial Intelligence in Education. Al-Azkiyaa International Journal of Language and education, 1, 71-81

[21] Eli-Chukwu, N. C. (2019). Applications of Artificial Intelligence in Agriculture: A Review. Engineering, Technology &Applied Science Research, 9, 4377-83

[22] Dinrifo, R. R., Alonge, A. F., Audu, J., & Adegbenjo, A. O. (2022). A review of the applications of artificial intelligence in agriculture: prospects and challenges in Nigeria. Journal of Agricultural Engineering and Technology (JAET), 27, 1-23

[23] Kutyauripo, I., Rushambwa, M., & Chiwazi, L. (2023). Artificial intelligence applications in the agrifood sectors. Journal of Agriculture and Food research, 11, 1-8

[24] Sachithra, V., & Subhashini, L. D. C. S. (2023). How artificial intelligence uses to achieve the agriculture sustainability: Systemic review. Artificial intelligence in Agriculture, 8, 46-59

[25] Mavani, N. R., Ali, J. M., Othman, S., Hussain, M. A., Hashim, H., & Rahman, N. A. (2022). Application of ArtificialIntelligence in Food Industry—a Guideline. Food Eng Rev., 14, 134–175

[26] Marwaha, S., Deb, C. K., Haque, M. A. Naha, S., Maji, A. K.. (2023). Application of Artificial Intelligence and Machine Learning in Agriculture. In: H. M. Mamrutha et. al; editors. Translating Physiological Tools to Augment Crop Breeding. Springer Nature Singapore Pte Ltd. pp. 441-457

[27] Soegoto, E. S., Utami, R. D., Hermawan, Y. A. (2019). Influence of artificial intelligence in automotive industry. Journal of Physics: Conference Series, 1402, 1-5

[28] Xinran, Li. (2022). A sensor array-based control system design for the interior environment of driverless cars. Journal of Physics: Conference Series. 2386, 1-8

[29] Ajitha, P. V., & Nagra, A. (2021). An Overview of Artificial Intelligence in Automobile Industry–A Case

Study on Tesla Cars, Solid State Technology, 64, 503-512

[30] Abduljabbar, R., Dia, H., Liyanage, S., & Bagloee, S. A. (2019). Applications of artificial intelligence in transport: An overview. Sustainability. 11, 1-24

[31] Hadraoui, M. EL., & Ghaiti, F. (2020). An improved machine learning-based approach for predicting travelers mode choice in Morocco, Journal of Theoretical and applied approach Tech., 98, 1457-1465

[32] Ahmed, B. (2012). The traditional four steps transportation modeling using a simplified transport network: A case study of Dhaka city, Bangladesh. International Journal of Advanced Scientific Engineering and Technological Research, 1, 19–40

[33] Oladimeji, D., Gupta, K., Kose, N. A., Gundogan, K., Ge, L., & Liang, F. (2023). Smart Transportation: An Overview of Technologies and Applications, Sensors, 23, 1-32

[34] Iyer, L.S. (2021). AI enabled applications towards intelligent transportation. Transportation Engineering, 5,1-5

[35] Kalia,, P. (2021). "Artificial intelligence".1stEd. CRC Press. 2021

[36] Bawack, R. E., Wamba, S. F., Carillo, K. D. A., & Akter, S. (2022). Artificial intelligence in E Commerce: a bibliometric study and literature review, Electron Mark. 32, 297-338

[37] Kashyap, A. K., Sahu, I., & Kumar, A. (2022). Artificial intelligence and its applications in e commerce - a review analysis and research agenda, Journal of Theoretical and Applied Information Technology, 100, 7347-7365

[38] Singh,, A. (2018). E-Commerce interfering with Privacy: Perceived Risks and Security issues with Techno-policy outcomes. In: Singh A, Rai P, et. al; editors. Digital Transformation Strategies and trends in E-learning: Privacy, Preservation and Policy, New Delhi: Segment Books, 2018, 802-823

[39] Gupta, P., & Dubey A. (2016). E-Commerce Study of Privacy, Trust and Security from Consumer's Perspectiv,. International Journal of ComputerScience and Mobile Computing, 5, 224-232

[40] Ladan, M. I. A. (2016). E-Commerce Security Challenges: A Taxonomy. Journal of Economics, Business and Management, 4, 589-593

[41] Idris, A., & Esumeh, E.(2015). The Top Five Challenges of the Web to Achieve E commerce Success: A Literature Review, International Journal of Electronic Commerce, 3, 1-10

[42] Saeed, S. A. (2023). Customer-Centric View of E-Commerce Security and Privacy, Applied Sciences, 2023, 13, 1-22

[43] Soni, V. D. (2020). Emerging roles of artificial intelligence in E commerce, International Journal of trend in scientific research and development, 4, 223-225

[44] Yampolskiy, R. V. (2018). Artificial intelligence safety and security, 1STed.CRC Press, New York

[45] Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., Li, W., & Li, K. (2021). Artificial intelligence security: Threats and countermeasures, ACM Computing Surveys (CSUR), 55, 1-36

[46] Blauth, T. F., Gstrein, O. J., & Zwitter. A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI, IEEE Access, 10, 77110-77122

[47] Qammar, A., Wang, H., Ding, J., Naouri, A., Daneshmand, M., & Ning, H.(2021). Chatbots to ChatGPT in a Cybersecurity Space: Evolution, Vulnerabilities, Attacks, Challenges, and Future Recommendations, Journal of Latex class files, 14,1-17

[48] Gupta, C., Johri, I., Srinivasan, K., Hu, Y. C., Qaisar, S. M., & Huang, K.Y. (2022). A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks, Sensors (Basel). 22, 1-34

[49] Dolnicar, S., & Jordaan, Y. A. (2007). Market Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing, Journal of Advertising, 36, 123-149

[50] Kumar, S., & Singh, P. (2014). Empirical Analysis of Ethical issue of Privacy in E Marketing, International Journal ofBusiness Management, 1, 23-39

[51] Radulov, N. (2019). Artificial intelligence and security. Security 4.0. International Scientific Journal "Security & Future", 3, 3-5

[52] Hlávka, J. P. (2020). Security, privacy, and information-sharing aspects of healthcare artificial intelligence. Artificial Intelligence in Healthcare. Academic Press, 2020

[53] Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. American Journal of Science, Engineering and Technology, 3, 12-19

[54] Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). Taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cybersecurity, 4, 1-15

[55] Curzon, J., Kosa, T. A., Akalu, R., El-Khatib, K. (2021). Privacy and artificial intelligence, IEEE Transactions on Artificial Intelligence, 2, 96-108

[56] Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy, Yale JL & Tech., 21, 106-188

[57] Um, T-W., Kim, J., Lim, S., & Lee, G. M. (2022). Trust Management for Artificial Intelligence: A Standardization Perspective, Applied Sciences, 12, 1-14

[58] Bartneck, C., Lütge, C., Wagner, A., & Welsh, S. (2021). Privacy issues of AI. In: Bartneck C, Lütge C, Wagner A, Welsh S. editors. An introduction to ethics in robotics and AI, Springer Nature, 2021, 61-70

[59] Huang, C. (2022). An Overview of Artificial Intelligence Ethics, IEEE transactions on artificial intelligence, 4, 799-819

[60] Hunkenschroer, A. L, & Kriebitz, A. (2023). Is AI recruiting (un)ethical? A human rights perspective on the use of AI for hiring. AI Ethics, 3, 199-213

[61] Song, J., Han, Z., Wang, W., Chen, J., & Liu, Y. (2022). A new secure arrangement for privacy-preserving data collection, Computer Standards &Interfaces, 80, 103582,

[62] Qiwei, L.U., Caimei, W., Yan, X., Huihua, X., Wenchao, H., & Xudong, G. (2017). Personalized privacy-preserving trajectory data publishing, Chinese Journal of Electronics, 26, 285-291