ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 4, pp: (38-45), Month: October - December 2022, Available at: www.researchpublish.com

Advance Data-Privacy by Using Artificial Intelligence

Hassan Jamal[1], Nasir A. Algeelani[2], Najeeb Al-Sammarraie[3]

[1,2,3] Faculty of computer science and Information technology

AL-Madinah International University

Kuala Lumpur, Malaysia

DOI: https://doi.org/10.5281/zenodo.7398762

Published Date: 16-November-2022
Amendment Date: 05-December-2022

Abstract: **With the progression utilize of computers broadly, utilization of the information has moreover developed to a huge level. Nowadays information is collected without any reason, and each action of a machine or a human being is recorded, On the off chance that required in the future, at that point, the information will be dissected but here the address of believe emerges as the information will go through numerous stages for the investigation by distinctive parties. The information may contain a few touchy or private data which can be mutualized by the organizations included in the investigation stages. So, it is required for the hour to consider the information security issues exceptionally truly. Diverse sorts of strategies have been presented in this paper to guarantee information security conjointly diverse machine learning calculations have been talked about which have been utilized to plan the proposed strategies to guarantee information protection.**

Keywords: **Data Privacy, Privacy, Artificial Intelligence, Advanced Data Privacy.**

I. INTRODUCTION

In the modern economy, data represents a certain monetary value. From growing sets of unstructured, seemingly disconnected data, one can extract information that can identify a given person, but also determine their demographic, socio-geographical, behavioural, or mental characteristics. (Małagocka, 2019). Artificial intelligence (AI) has developed rapidly in recent years. The capabilities of AI now and in the foreseeable future promise widespread and substantial benefits for individuals, institutions, and society. At the same time, protecting data privacy is more important than ever given the speed, impact, and difficulty of assessing and explaining many AI tools. This conundrum heightens the importance of expanding the focus of the debate from mere compliance with existing laws to the need to enhance the quality of data protection and effective governance in the face of emerging digital tools. (Christopher Kuner, 2018).

II. VARIABLES DEFINITIONS

A. AI Is in Widespread Use Today

AI is not a novel or far-fetched concept. 'Artificial intelligence (AI) is already part of our lives—it is not science fiction,' according to the European Commission. AI is a reality, from utilizing a virtual personal assistant to organize our workdays to traveling in a self-driving vehicle to our phones suggesting tunes or places we might enjoy. AI is a technology that is already profoundly established in our lives,' writes the UK House of Lords in its recent AI study. This is a crucial point. We're not talking about anything speculative or futuristic when we talk about AI. We're basically constructing the boat while sailing on it. (Christopher Kuner, Expanding the artificial intelligence-data protection debate, 2018).

B. Big Data, Machine Learning, and AI

Enormous information supplies the premise for AI by providing the environment from which it is able to memorize. Whereas like AI, no single definition exists, companies and organizations commonly characterize "big data" as "high-volume, high-velocity and high-variety data resources that request cost-effective, imaginative shapes of data preparing for enhanced knowledge and choice making.

Beneath this development, its three conceptualize huge information, where "volume relates to the massive dataset, speed relates to real-time information and assortment relates to distinctive sources of data." This concentration of information incorporates a wealth of data, extending from PII to mysterious information collections, such as Web of things gadgets, machine logs, or company reference information collections. This supply of enormous information is instrumental to AI's machine learning. Intel, a driving company in AI advancement, characterizes machine learning as "the of strategies and apparatuses that permit computers to 'think' by making numerical calculations based on accumulated data. Whereas this can be a wide definition, machine learning functions through complex implies. For illustration, there are two wide categories of machine learning: directed and unsupervised. With directed learning, the AI forms and learns from labelled information sets to develop algorithms. The administered approach "trains" the calculations to make models that can precisely outline information inputs to yields, which permits the calculations to anticipate future occasions.

With administered learning, it is easier for software engineers and examiners to supervise and watch the AI's improvement. The extra control permits those supervising the AI - artificial intelligence advancement to more effortlessly take after its rationale and present modern information sets vital for its ceaseless handling. Alternately, unsupervised learning supplies the calculations with no names or earlier input-output relationships, and instep takes off the algorithms on its possess to memorize. Machine learning is additionally categorized based on the profundity of its learning.

The profundity of machine learning is either shallow or profound. Regularly, shallow learning is less utilized since it as it were includes one layer of information, which limits the sum of information that AI can utilize to grow its information. (Humerick, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy &Artificial Intelligence, 2018).

C. Advance

Firstly, that the wide extended definition of "advance" as "to move forward" varies in relation to the kind of lexical items that compound its argument structure. Such a variation depends on four different conditions: "advance" behaving as a verb of self-motion; the use of time objects and subjects in a sentence that includes "advance" as a verb of movement; the use of a physical item as the direct object of the verb under study; and the understanding of movement as a metaphor associated to progression. Secondly, the verb "advance" still presents features related to verbs that express a movement upward, even though they are not explicitly mentioned in dictionaries. Thirdly, that "advance" is a verb of giving, against what Levin states in her classification of verbs of change of possession. (González, 2015).

Secondly. Lesson structure has three components: preparation, guidance, and evaluation; and each of these has sub-components. Preparation may take the form of an advance organizer, questions, or a structured overview; it also includes "vocabulary improvement," which requires the selection, teaching, and reinforcement of the technical language of the subject. (Herber).

D. Data

The data in such settings often contain sensitive information about individuals, corporations, or governments. (Laxman, 2011) Data can be broadly defined as information collected or generated from the world from which inferences about various phenomena can be made. Data also serve the role of evidence for preferring certain explanations of the world over others and can act as a source of innovation to change that world, with the distinction between descriptions of phenomena (matters of "fact") and ways of looking at them (matters of "theory") not nearly so clearly distinguishable as some would like (Bogen & Woodward, 1988; Leonelli, 2019a). (Wise, 2019).

In computing, data is information that has been translated into a form that is efficient for movement or processing. Relative to today's computers and transmission media, data is information converted into binary digital form. It is acceptable for data to be used as a singular subject or a plural subject. (Vaughan, n.d.).

E. Privacy

General privacy as a philosophical, psychological, sociological, and legal concept has been researched for more than100 years in almost all spheres of the social sciences. And yet, it is widely recognized that, as a concept, privacy "is in disarray [and n] nobody can articulate what it means" (Solove2006, p. 477). Numerous attempts have been made by social and legal scholars to bring together the different perspectives found in different fields. However, the picture that emerges is fragmented with concepts, definitions, and relationships that are inconsistent and neither fully developed nor empirically validated. (Smith ,Dinev, 2011).

Privacy can mean many things to many people. In the context of our research and this paper, we define privacy as the right of an individual to control information about themselves rather than as the right to individual isolation. The OECD principles provide high level privacy standards for dealing with personal information and have widespread consensus. These have provided input to legislation in many parts of the world that requires organizations to have privacy policies and constraints on the organizational collection and use of personal information to differing degrees. This legislation varies by both geography and domain. These variations as well as the inherent differences between domains and between the business practices of different organizations mean that it is not likely that a single privacy policy can be created to cover all personal information. The research reported in this paper has focused on how technology can be used by organizations to create and enforce the range of privacy policies needed to meet the varied requirements. (Brodie, Marie, & Feng, 2005).

Privacy can ensure that the data can only be controlled by the corresponding user and that no other user can access or process the data. Unlike confidentiality, which aims to encrypt the data without being eavesdropped on and interfered with by no authorized users, privacy ensures that the user can only have some specific controls based on received data and cannot infer other valuable information from the received data. Privacy is considered one of the important security principles due to many devices, services, and people sharing the same communication network in IoT. (Jie Lin, 2017).

Privacy can be considered a very vague concept and can be defined in different forms depending on the purpose. A generic way of defining privacy aligned with the purpose of this paper is the right that someone must keep their personal life or personal information secret or known only to a small group of people. The nature of privacy is an interesting and complex question that has been addressed in several disciplines.

Privacy is a broad topic that has attracted increasing attention as rapid technological advances have made it easier to share personal information intentionally and unintentionally. Privacy is essential to society, at so many levels: privacy is at the root of both freedom and prosperity. Internet users assert a strong interest in privacy while simultaneously disclosing substantial personal information for meagre rewards. We refer to Big Data Privacy when the data for which privacy is desired is that under the environment of the big data era. (Yang Yuxuan, 2020)

The general meaning of privacy is preventing the disclosure of sensitive information. (Krishna Mohan Pd Shrivastva, 2014).

F. Data Privacy

Data privacy refers to the protection of each sensor's raw private observation from the fusion centre, i.e., upon receiving information from all the sensors, it is difficult for the fusion centre to infer the original sensor observations. Protecting data privacy alone is not sufficient to prevent privacy leakage. A data privacy mechanism obfuscates the raw data while still allowing statistical information to be extracted from the data. Given multiple information sources, each with its local data privacy mechanism, it is possible to perform a correlation attack leading to de-anonymization and other types of privacy leakage. (Meng Sun, 2020).

Data privacy is an expanding sub-field of data management whose goal is to answer queries over sensitive datasets without compromising the privacy of the individuals whose records are contained in these databases. (Daniel Kifer , 2011)

Data privacy, sometimes also referred to as information privacy, is an area of data protection that concerns the proper handling of sensitive data including, notably, personal data but also other confidential data, such as certain financial data and intellectual property data, to meet regulatory requirements as well as protecting the confidentiality and immutability of the data. (SNIA, n.d.).

G. Output

To achieve such adaptive, algorithms must be developed to find the optimized operation bias voltages set which maximizes the spectral context inside the output data while reducing the data redundancy. (Zhipeng Wang, 2008)

The real value of the final goods and services produced in the nation's economy—the scope and movement of the measure will depend on the precise operational meaning given to such key words of the definition as "final," "nation," and "economy." (Kendrick, 1961).

We are all familiar with the fact that output is measured to equal input for some important subsectors (important both in terms of shares and in terms of employment trends), a procedure that effectively precludes measurement of technical structure. We are all aware of the problem of "quality"; we know that failure to adjust for changes in it leads to biases in conventional measures of productivity trends and we would probably agree that output measures for services are generally sorely by this problem. Many service outputs are highly intangible or qualitative in nature. (Production and Productivity in the Service Industries, 1969).

H. Big Data

The general term big data refers to a huge collection of information (the dataset), typically stemming from more than one data source, and being processed by a data analyst or data processor. (Meiko Jensen, 2013)

Big Data is defined as aggregations of data in applications of bigness and complexity demanding advanced analytic approaches. The approaches to Big Data are described as descriptive analytics, analysing data from the past; predictive analytics, analysing data for prediction; and prescriptive analytics, analysing data for pro-action (Camm, Cochran, Fry, Ohlmann, Anderson, Sweeney, & Williams, 2015). (James Lawler, 2017).

According to Gartner- "big data is high volume high velocity and high variety (structure, unstructured, semi-structure) information assets that require a new form of processing to enable enhanced decision making, insight discovery, and process optimization. Big data is too big, too fast, and too hard for existing technology. Too big means data base of size more than Peta Byte (1000 Terabyte). Too fast means quick processing of its requests, too hard means there is no existing tool that can fulfil all the types of requirements (storage and processing) of big data. (Krishna Mohan Pd Shrivastva, 2014).

III. INTRODUCTION TO ARTIFICIAL INTELLIGENCE

A. Critical Progresses Within the Expository Capacity of Cutting Edge Computers Are Progressively Challenging Information Security Laws and Standards

Those propel are regularly portrayed as "artificial intelligence", a term that depicts the wide objective of enabling "computer frameworks to perform assignments that ordinarily require human insights, such as visual recognition, discourse acknowledgment, decision-making, and interpretation between languages". This one term envelops a wide assortment of innovative advancements, each of which may show challenges to existing information security prerequisites. Most AI in utilize nowadays includes computer frameworks that perform discrete tasks—for example, playing recreations, recognizing pictures, or confirming identity by distinguishing designs in large amounts of information. The numerical concept of AI dates, back to the 1950s but has found genuine world applications in later a long time due to progress in handling control and the endless sums of advanced information accessible for examination.

As a result, AI nearly continuously is related to "big data". However, later applications of AI, such as the utilization of AI to overcome CAPTCHA and Google's Alpha Go Zero that instructed itself to play Go at the championship level; has happened with minimal preparation information demonstrating that enormous information may not continuously relate to AI. All the illustrations are "narrow" AI—AI outlined to perform one errand or set of tasks. Narrow AI is still complicated. AI and related innovations are quickly progressing. "Like the steam motor or power in the past, AI is changing our world, our society, and our industry". Hence, as the term is used below, AI envelops contract AI, which is broadly utilized nowadays and has been utilized for many years, as well as other advanced advances that are introduced in a future of computers so integrated into our way of life that we do not think of them as computers at all. (Bellamy, 2018).

B. Artificial Intelligence

Artificial intelligence, also known as AI, is an organizational principle. Artificial intelligence can be divided into two stages: strong artificial intelligence and weak artificial intelligence. Strong artificial intelligence refers to intelligent technology that has perception and self-awareness and can truly think. Strong artificial intelligence that can adaptively respond to the challenges of the external environment. Weak artificial intelligence refers to intelligent technology that can't really realize reasoning and problem-solving. Weak artificial intelligence does not really have autonomy. (Ma, 2021).

Artificial intelligence (AI) is the study of making computers simulate certain thought processes and intelligent behaviours of people, involving disciplines such as computer science, psychology, philosophy, and pedagogy. In recent years, many fields have been exploring innovative applications of artificial intelligence, especially in the field of education. (Jiong Du, 2021)

Artificial intelligence is to make things done by machines more "human", transfer people's thinking mode to the computer (brain), and realize information sharing. Then, using the sensor system and big data technology, the machine can complete people's daily simple calculations and analyses. (Zheng Zhenzhou, 2021).

IV. DEFENITION OF THE RELATION AMONG VARIABLES

A. Definition of The Relation Between Data Privacy and AI (Artificial Intelligence)

First, differential privacy has been proven to be good at minimizing risk in joining statistical databases. We considered advanced differential privacy preservation techniques in deep learning that have shown remarkable results in a wide variety of domains. Second, while data are in the public domain already, AI intelligence should be protected by differential access via a registration process. (Duy H. Ho, 2021).

AI has made the challenge both more addressable and more of a risk. The ability to train deep learning (DL) systems on large amounts of data has increased the speed of analysis and results, but the need for more and more data increases the risk of a lack of privacy. To provide processes to handle that challenge in a reasonable time frame, the software can again help. (Teich, 2020).

The impression we are left with is that most sectors have adopted AI in a relatively restrictive manner and that the techniques frequently used are limited. This corresponds well with the limited case portfolio of the Data Protection Authority and the requests for guidance received about AI and privacy. We are still in the early phase of AI development, and this is the right time to ensure that AI technologies comply with the rules society lays down. It is both possible and necessary to safeguard fundamental personal data protection rights. (Curzon, Ann Kosa, & Akalu, 2021).

Definition of the relation between Big Data and AI (Artificial Intelligence) Big Data for all intents and purposes constitutes all our actions, both on and offline, anything that leaves a digital trace contributes to the accumulation of Big Data, and therefore the infinite growth of our digital universe. AI, Algorithms, and modelling programs can then use individual data for predicted personality profiling, location status and history, personal health records, facial recognition, consumer purchasing activity, education, and virtually every part of your private life. (Gary Smith, 2019).

Big Data is no fad. The world is growing at an exponential rate, and so is the size of data collected across the globe. The data is becoming more meaningful and contextually relevant, breaking new ground for machine learning and artificial intelligence (AI), and even moving them from research labs to production. That is, the problem has shifted from collecting massive amounts of data to understanding it, i.e., turning data into knowledge, conclusions, and actions. This Big AI, however, often faces poor scale-up behaviour from algorithms that have been designed based on models of computation that are no longer realistic for Big Data.

The special issue constitutes an attempt to highlight the algorithmic challenges and opportunities but also the social and ethical issues of Big Data. Of specific interest and focus have been computation- and resource-efficient algorithms when searching through data to find and mine relevant or pertinent information. (Qlik, n.d.).

Big Data, in turn, which as an academic term is typically more loosely defined than AI, can mean a large volume of structured, semi-structured, or unstructured data, and a way to collect/produce, process, and analyse these datasets using non-traditional methods (e.g., AI methods). Such data are the fuel, “the new oil” (Agrawal et al. 2018) for AI and intelligent machines. Hence, Big Data and AI are often intertwined and go hand in hand as drivers of the current digital transformation in society (Brynjolfsson and McAfee 2014; Zomaya and Sakr 2017).

B. Theoretical Basis

The Concept and Fundamentals Substances of Enormous Information with the fast advancement and wide utilization of data innovation, the organized data information created by individuals within the process of way of life proceeds to extend. Hence, the advancement of data innovation moreover advances all mankind to enter a period of huge information. The so-called big data is the number of information that is colossal. In any case, enormous information

innovation isn't fair to gather information, its centre connect is to prepare and handle the collected data, to supply profitable information for human creatures at the display, the complete society is full of different sorts of information, a few of which are futile or indeed off-base. In this manner, how to select adjust and profitable information is the most work carried out by huge information innovation. (Yi Feng, 2020).

C. Challenges in Development

In bequest applications that have been ported to Apache Start, several challenges exist in information arrangement among profoundly normalized information structures. On such occasions, a level of pre-processing in which a deformalized database is executed, imitating the Kimball-influenced plan of deformalized information stockrooms. In such cases, by supporting this as a level of ETL, operations requiring holding on to the information inside an application due to intemperate joins inside a dispersed design are dodged hence permitting effective implementation.

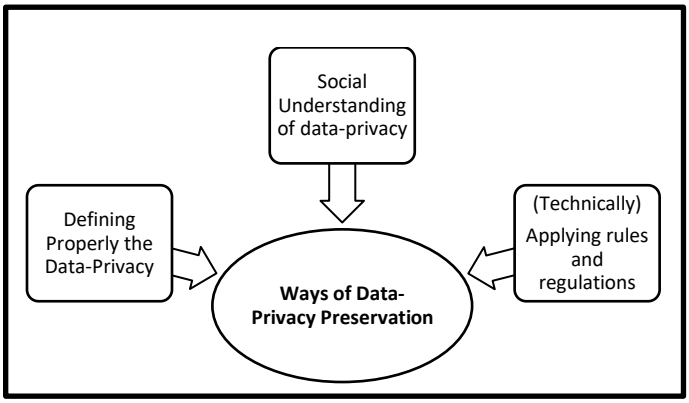
Additional issues exist within the setting of working with Start Windowing where performance can quickly decay within the occurrences where windows that are characterized inside the dispersed system are not competent of fittingly containing the action within a specific hub. In such cases, it may be a work of information engineering, volume, and window of time arrangement. (Ostrowski, 2018).

V. METHODOLOGY

A. Definition

The usage of individuals' data without permission could impact violating data privacy. The current methodology for analysis is based on (1) Scanning databases and the internet, looking for all recent articles that have a relation between data privacy and AI. (2) Gets the available definitions of data privacy and has a clear vision of its boundaries, and ways of violating data privacy. (3) Collect ways of protecting data from internal and external hacking and reformulating data before it is been exposed.

B. Relation Among Parties



VI. RESULTS

There is a consensus on concepts and some of the definitions of the term, like data privacy which is defined as the official rights given to the organization, that has the data, to deal with data and the way data are handled in accordance with the laws of the state. The application of the ethics of the profession in dealing with data, from leakage or even accessing it or making abuse of it morally or legally in an inappropriate usage for individuals' data without permission, which could impact in violating data privacy.

Data sensitivity is defined as the data may be detrimental if it is shared, either by giving the owner's authority or not, but in the end, it has been misused with or without intent. The data privacy concept may have the same understanding for different generations. However, there may be some minor differences in application, due to the openness that some members of the old generation have toward others. For policies that could be applied while data extraction, some techniques could be used like data-masking, encoding-decoding, and specific persons could be allowed to access data with different privileges.

AI could help in finding the sensitive data from within the text, audio, video, and pictures, then treat it as per the desired way, by building a model for that, and applying some techniques or methods. Ways for protecting data from external hacking and reformulating data before exposing it vary, and have two categories, both "Protecting data from external hacking", which cover different points like avoiding storing important and sensitive information in external storage, adding monitoring technology, and log monitoring information.

As a result, the hackers will be recorded and added permission, so those people who without permission cannot access into user's data, Monitoring and log all external data storage access activities with logical and relevant API event handlers. With monitoring and logging all suspicious actions will be recorded, add permission to read and write external data, so those people without physical permission cannot access SD card storage, Data Integrity – only authorized users are allowed to modify system data, and Authentication – the identity of the creator of a message or document is verified. And the other category is "Reformulating data before it is exposed", which covers, encrypting the data so that hackers can't easily get the user's information even if they have access to it, encrypting the data at rest in external data storage, and amount of personal data stored can be minimized or appropriate privacy policies are enforced.

Data privacy protection ways, other than technical ways, like, there should be awareness sessions for what is acceptable to be disclosed and what is not, and rules should be set by the government or company, like not disclosing the ID card.

VII. CONCLUSION

AI could create good opportunities for organizations to mitigate the risks of data processing. Can this technology actually help protect customer privacy and data and contribute to compliance with privacy laws?

Large-scale data analysis, such as that done by AI systems, is good at predicting patterns. This is not just limited to the world of customer-related behaviours, for example. AI could also be used for analysis to find patterns or trends relating to consent and its management, anomalies in user access to data, or data security from collection through processing and storage.

AI could also be used to consistently and thoroughly perform anonymization activities on data sets to ensure identifiers are removed from the aggregate sets and the data cannot be de-anonymized.

REFERENCES

[1] (1969). In Victor R. Fuchs, *Production and Productivity in the Service Industries* (p. 53). National Bureau of Economic Research.

[2] Bellamy, B. (2018). *Artificial Intelligence and Data Protection in Tension.* centre for information policy leadership-hunton andrews kurth.

[3] Brodie , C., Marie, C., & Feng, J. (2005). *Usable Security and Privacy: A Case Study of Developing.*

[4] Christopher Kuner, *. F. (2018). Expanding the artificial intelligence-data protection debate. *International Data Privacy Law*, 1.

[5] Curzon , J., Ann Kosa , T., & Akalu, R. (2021). *Privacy and Artificial Intelligence.*

[6] Daniel Kifer . (2011). *No Free Lunch in Data Privacy.* Athens, Greece.

[7] Duy H. Ho. (2021). *Big Data Analytics Framework for Predictive Analytics using Public Data with Privacy Preserving.* Kansas City, USA: Computer Science and Electrical Engineering University of Missouri - Kansas City.

[8] Gary Smith . (2019). *Artificial Intelligence and the Privacy Paradox of Opportunity, Big Data and The Digital Universe* . Dubai, United Arab Emirates: Amity University Dubai .

[9] González, J. C. (2015). *'Advance': Meaning, Syntax and the Influence of Metaphors in a Verb of Movement.* La Laguna.

[10] Herber, H. L. (n.d.). *Research in Reading in the Content Areas: First YearReport.* Washington, D.C. Bureau: Syracuse Univ., N.Y. Reading and Language Arts.

[11] Humerick, M. (2018). Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy &Artificial Intelligence. *The Santa Clara High Technology Law Journal*, 6-7.

[12] James Lawler. (2017). *Big Data Analytics Methodology in the Financial Industry.* New York, New York 10038 USA: Pace University.

[13] Jie Lin. (2017). A Survey on Internet of Things: Architecture,Enabling Technologies, Security and Privacy, and Applications. *IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 5*.

[14] Jiong Du. (2021). *Artificial Intelligence Aided Innovation Education Based on Multiple Intelligence.* Zhangzhou, Fujian, China: IEEE International Conference on Artificial Intelligence, Robotics, and Communication.

[15] Kendrick, J. W. (1961). The Concepts and Measurement of Output and Input. In M. R. Pech, *Productivity Trends in the United States* (p. 20). United States: Princeton University Press.

[16] Krishna Mohan Pd Shrivastva. (2014). *Big Data Privacy Based On Differential Privacy a Hope for Big Data.* Bhopal: National Institute of Technical Teachers' Training & Research.

[17] Laxman, S. (2011). *Tutorial on the state of data privacy.*

[18] Ma, J. (2021). *Research on the Application of Financial Intelligence Based on Artificial Intelligence Technology.* philippines : University of van carlos .

[19] Małagocka, G. M. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, 2-3.

[20] Meiko Jensen. (2013). *Challenges of Privacy Protection in Big Data Analytics.* Kiel, Germany: Independent Centre for Privacy Protection Schleswig-Holstein (ULD).

[21] Meng Sun . (2020). *On the Relationship Between Inference and Data Privacy in Decentralized IoT Networks.* IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 15.

[22] Millena Debaprada Jena, Sunil Samanta Singhar,Bhabendu Kumar Mohanta, and Somula Ramasubbareddy. (2020). *Ensuring Data Privacy Using Machine.* Sunil Samanta Singhar.

[23] Ostrowski, D. (2018). *Artificial Intelligence with Big Data.* Dearborn, MI: Ford Motor Company.

[24] *Qlik*. (n.d.). Retrieved from https://www.qlik.com/us/augmented-analytics/big-data-ai

[25] Smith, H., & Dinev, T. (2011). *Information Privacy Research: An Interdisciplinary Review.* Pennsylvania State University.

[26] *SNIA*. (n.d.). Retrieved from https://www.snia.org/education/what-is-data-privacy

[27] Teich, D. A. (2020, 4 10). *Forbes*. Retrieved from https://www.forbes.com/sites/davidteich/2020/08/10/artificial-intelligence-and-data-privacy--turning-a-risk-into-a-benefit/?sh=59661e4a6a95

[28] Vaughan, J. (n.d.). Retrieved from TechTarget: https://www.techtarget.com/searchdatamanagement/definition/data

[29] Wise, A. F. (2019). Educating Data Scientists and Data Literate Citizens for a New Generation of Data. *JOURNAL OF THE LEARNING SCIENCES*.

[30] Yang Yuxuan. (2020). Sociological Aspects of Big Data Privacy. *The School of Business* .

[31] Yi Feng. (2020). *Research on the Application of Big Data and Artificial Intelligence Technology in Computer Network Technology.*

[32] Zheng Zhenzhou. (2021). *Analysis of Systematic Reform of Future Teaching in the Age of Artificial Intelligence* . Qingzhou, Korea: 2nd International Conference on Artificial Intelligence and Education (ICAIE).

[33] Zhipeng Wang, J. S. (2008). *SIGNAL TO NOISE RATIO FOR SPECTRAL SENSORS WITH OVERLAPPING BANDS.* Tucson, AZ 85721, USA: College of Optical Sciences-University of Arizona.