International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET229633

Modelling Data Privacy and Security with Respect to Machine Learning

K S Dhruva Teja, K. Vamshivardhan, K. Partha Sai, D. Hemanth
Department of Artificial Intelligence and Machine Learning, New Horizon College of Engineering, Bangalore, India

Article Info
Volume 9, Issue 6
Page Number : 235-238

Publication Issue :
November-December-2022

Article History
Accepted : 10 Nov 2022
Published: 28 Nov 2022

ABSTRACT

Organizations are collecting larger amounts of data to build complex data analytics, machine learning and AI models. Furthermore, the data needed for building such models may be unstructured (e.g., text, image, and video). Hence such data may be stored in different data management systems ranging from relational databases to newer NoSQL databases tailored for storing unstructured data. In some cases, the developed code will be automatically executed by the NoSQL system on the stored data. These developments indicate the need for a data security and privacy solution that can uniformly protect data stored in many different data management systems and enforce security policies even if sensitive data is processed using a data scientist submitted complex program.

Keywords : Big Data, Security, Privacy, Machine Learning, Artificial Intelligence.

I. INTRODUCTION

In this paper, we introduce our vision for building such a solution for protecting big data. Specifically, our proposed SECUREDL system allows organizations to:
1) enforce policies that control access to sensitive data
2) keep necessary audit logs automatically for data governance and regulatory compliance
3) sanitize and redact sensitive data on-the-fly based on the data sensitivity and AI model needs
4) detect potentially unauthorized or anomalous access to sensitive data
5) automatically create attribute-based access control policies based on data sensitivity and data type.[1]
Artificial Intelligence (AI) is one of the most prevalent topics of research today across almost every scientific field. For example, multi-agent systems can be applied to distributed control systems, while distributed machine learning has been adopted by Google for mobile users. However, as AI becomes more and more reliant on data, several new problems have emerged, such as privacy violations, security issues, model instability, model fairness and communication overheads.[2] As just a few of the tactics used to derail AI, adversarial samples can fool machine learning models, leading to incorrect results. Multi-agent systems may receive false information from malicious agents. As a result, many researchers have been exploring new and existing security and privacy tools to tackle these new emerging problems. Differential privacy is one of these tools. Differential privacy is a prevalent privacy preservation model which guarantees whether an individual's information is included in a dataset has little impact on the aggregate output.[3] Consider two datasets that are almost identical but differ in only one record and that, access

to the datasets is provided via a query function. If we can find a mechanism that can query both datasets and obtain the same outputs, we can claim that differential privacy is satisfied. In that scenario, an adversary cannot associate the query outputs with either of the two neighboring datasets, so the one different record is safe. Hence, the differential privacy guarantees that, even if an adversary knows all the other records in a dataset except for one unknown individual, they still cannot infer the generated by various sources, from connected devices to social media, termed as big data, is a valuable asset. The availability and widespread applications of big data significantly impacts the growth of Machine Learning (ML) and Artificial Intelligence (AI) with the goals of increasing the efficiency and the accuracy of prediction and decision making and also minimizing their computational cost. Statistics depict the interest of the world market in AI systems that, only between 2-018 and 2019, has increased by 154%, reached a $14.7 billion market size and will reach almost $37 billion by 2025. Stakeholders such as governments and industry sectors are attracted to benefit from AI to acquire insights from the data for customized services depend on customer's needs.[4]

II. EXISTING SYSTEM

In computer science, AI is associated with the accomplishments of tasks or problems by computers for which human intelligence is assumed to be required. AI is designed such that the input is the information acquired from the environment and takes actions to maximize success in achieving particular goals. The most dominant way of achieving AI nowadays is by Machine Learning (ML) techniques which are build based on the concept of "without being explicitly programmed". In principle, ML consists of a set of algorithms and statistical models for computer systems to efficiently perform a particular task without relying on rule-based programming or human interaction. Developing the mathematical model is strongly dependent on the dataset, referred to as training data, which allows the program to gradually improve through the experiences and learning process from the data for predicting, detecting or making decisions. A standard terminology of AI and Big data is also described in a standard document.[5]

III.PROPOSED SYSTEM

After examining the protection and security assaults of huge information in Artificial intelligence frameworks that are demonstrated in light of ML procedures. Each step in the work process of the artificial intelligence framework can be the objective of the particular attack(s). The phases are illustrated. The defined AI workflow system. The first phase, Training phase, is the step where the trained data is fed into the ML model for the learning process. The data in this stage is a labeled or unlabeled.

Significantly valuable source for the AI system that can be the aim of many attackers to violate the privacy and security. The next phase is the Model phase where the ML algorithm learns from the trained data set and develops a model, which is the other valuable intellectual property of AI systems and hence is the target of various attacks. The novel data is then fed into the trained model, named as Apply phase, where an adversary can penetrate the system and modify the results in his favor. Finally, the valuable outcomes of the system, determined as the Inference phase, may host attacks that disclose sensitive information.

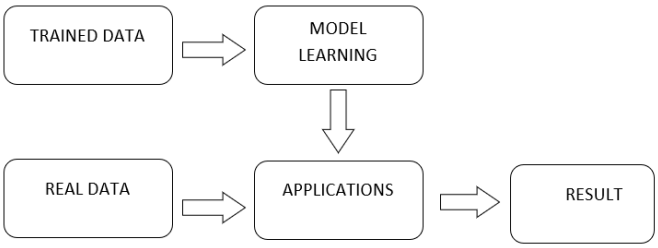

FIG 1.1 Workflow and different phases of AI systems developed based on ML algorithms

Algorithms

In computer science, AI is associated with the accomplishments of tasks or problems by computers for which human intelligence is assumed to be required. AI is designed such that the input is the information acquired from the environment and takes actions to maximize success in achieving particular goals. The most dominant way of achieving AI nowadays is by Machine Learning (ML) techniques which are build based on the concept of "without being explicitly programmed". In principle, ML consists of a set of algorithms and statistical models for computer systems to efficiently perform a particular task without relying on rule-based programming or human interaction.[6] Developing the mathematical model is strongly dependent on the dataset, referred to as training data, which allows the program to gradually improve through the experiences and learning process from the data for predicting, detecting or making decisions. A standard terminology of AI and Big data is also described in a standard document. Machine learning techniques can be classified in different ways. In an underdevelopment standard a set of ML approaches are defined as follows: 1) Supervised learning, 2) Unsupervised learning, 3) Semi-supervised learning, 4) Reinforcement learning, 5) Transfer learning.[7]

IV.RESULTS AND CONCLUSION

The huge volume, variety, and velocity of big data have empowered Machine Learning (ML) techniques and Artificial Intelligence (AI) systems. As privacy and security threats evolve, so too will the technology need to adapt – as well as the rules and regulations that govern the use of such technologies. The two perspectives of the research outcomes and standards development are considered in this study. We focus on challenges and threats of big data in the AI workflow by providing a review of the recent research literature, standard documents, and ongoing projects on this topic. Several projects are initiated by SDOs to investigate different aspects of big data privacy aspects and security issues. Even though most of the standards mentioned in this study are ongoing projects, they are expected to be published in the near future. One of the advantages standards can bring into research is a more coherent terminology, which is defined once and used later in subsequent projects. In contrast, researchers often use different terminologies for the same or similar concepts. Besides, according to the rapid growth of AI, developed road maps in standards can provide insights according to the demands and requirements of the market. Hence, it may provide opportunities for new research activities to address line with market needs.

V. REFERENCES

[1] Zhang, P. Porambage et al., "Sec-EdgeAI: AI for Edge Security Vs Security for Edge AI," 1st 6G Wireless Summit, 2019.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council, General Data Protection Regulation (GDPR).

[3] California Consumer Privacy Act of 2018 (CCPA).

[4] European Commission White Paper "On Artificial Intelligence – A European approach to excellence and trust", Brussels, 19.2.2020 COM(2020) 65 Final, Available from: https://ec.europa.eu/info/sites/info/files/commiss commission-white-paper-artificialintelligence-feb2020_en.pdf, last accessed March 2020.

[5] Charter of Fundamental Rights of the European Union 2012/C 326/02.

[6] C. Fennessy, "US sens. Unveil new federal provacy legislation", Nov 26, 2019, International Association of Privacy Professionals (IAPP), Available from: https://iapp.org/news/a/u-s-senators-unveil-new-federal-privacylegislation/, last accessed March 2020.

[7] 2019 Consumer Data Privacy Legislation, National Conference of State Legislatures, 2019 available https://www.ncsl.org/research/telecommunicatio

ns-and-informationtechnology/consumer-data-privacy.aspx, last accessed March 2022

Cite this article as :

K S Dhruva Teja, K. Vamshivardhan, K. Partha Sai, D. Hemanth, "Modelling Data Privacy and Security with Respect to Machine Learning", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 6, pp. 235-238, November-December 2022. Available at doi : https://doi.org/10.32628/IJSRSET229633
Journal URL : https://ijsrset.com/IJSRSET229633