Chapter 59
Security and Privacy Challenges of Deep Learning: A Comprehensive Survey

J. Andrew Onesimu
https://orcid.org/0000-0003-3592-6543
Karunya Institute of Technology and Sciences, India & Vellore Institute of Technology, India

Karthikeyan J.
Vellore Institute of Technology, India

D. Samuel Joshua Viswas
https://orcid.org/0000-0002-6792-7391
Karunya Institute of Technology and Sciences, India

Robin D Sebastian
Karunya Institute of Technology and Sciences, India

ABSTRACT

Deep learning is the buzz word in recent times in the research field due to its various advantages in the fields of healthcare, medicine, automobiles, etc. A huge amount of data is required for deep learning to achieve better accuracy; thus, it is important to protect the data from security and privacy breaches. In this chapter, a comprehensive survey of security and privacy challenges in deep learning is presented. The security attacks such as poisoning attacks, evasion attacks, and black-box attacks are explored with its prevention and defence techniques. A comparative analysis is done on various techniques to prevent the data from such security attacks. Privacy is another major challenge in deep learning. In this chapter, the authors presented an in-depth survey on various privacy-preserving techniques for deep learning such as differential privacy, homomorphic encryption, secret sharing, and secure multi-party computation. A detailed comparison table to compare the various privacy-preserving techniques and approaches is also presented.

DOI: 10.4018/978-1-7998-8954-0.ch059

INTRODUCTION

In recent industry revolution, customer oriented services are getting popular every day. In order to provide customer oriented services huge amount of data is being collected from the users. The data collection is either done actively with the consent of the user or it is done passively without the knowledge of the user. However, such data contains personal information about individuals which is necessary to be protected. It is important to protect the collected data in the data storage, data processing and data transmission. Various security mechanisms are available to protect the data, nevertheless they differ based on the computational and time complexity.

Users generates the data through online and offline. Every electronic transaction is collected as data. This in turn helps the researchers to collect information about the various events and predict the future. Especially in the area of sciences and medicines a lot of research is being done to invent something new, to predict and treat diseases, to develop drugs and medicines, etc., So the researchers will always be looking for huge amount of data generated by the users. When such data is collected it is necessary to protect the personally identifiable information (PII) (Krishnamurthy & Wills, 2009) from the data. As the data are collected from the individuals it contains PII. Analyzing the data without removing PII could lead to privacy breach (J, Karthikeyan, & Jebastin, 2019). Thus it is essential to remove PII before publishing the data various researches.

There is a huge rise in artificial intelligence, (Russell & Norvig, 2016) machine learning, (Andrieu, De Freitas, Doucet, & Jordan, 2003) and deep learning (Arel, Rose, Karnowski, & others, 2010) in recent times because of the huge availability of the data and improved accuracy of the models. AI gives the decision making ability to the system based the previous records. Machine learning (ML) is a subset of AI, it can process large amount of data and provide accurate results than traditional approaches(Bhushan & Sahoo, 2018). Machine learning consists of supervised, unsupervised and reinforcement learning techniques. It can work with various types of data and can provide promising results in the field of stock market prediction, drug discovery, disease prediction, etc. (Andrew, Mathew, & Mohit, 2019) Deep learning is a subset of ML (Jindal, Gupta, & Bhushan, 2020), it is used when the dataset is huge and have complex structures. Deep learning mimics the human brain neurons to learn patterns from the data. Deep Learning gives promising results in the field of computer vision, audio processing, video processing, pattern recognition etc.

Contributions

Though the recent advancements provide greater advantages in terms of accuracy and processing time, it has considerable risks in securing the data during the model training and testing. Also, the private data has to be prevented from privacy leaks. These are the two challenges we have identified for this book chapter. In this book chapter, the various security and privacy challenges on deep learning models are presented. At first, the security challenges of training data and model data are presented. Then the various security attacks on deep learning models are analyzed. Secondly, the privacy issues of deep learning models presented along with various privacy attacks. Finally a comparative analysis is given on security and privacy attacks.