Chapter 78
Privacy Preserving Machine Learning and Deep Learning Techniques: Application – E-Healthcare

Divya Asok
Thiagarajar College of Engineering, India

Chitra P.
Thiagarajar College of Engineering, India

Bharathiraja Muthurajan
Indian Institute of Technology Madras, India

ABSTRACT

In the past years, the usage of internet and quantity of digital data generated by large organizations, firms, and governments have paved the way for the researchers to focus on security issues of private data. This collected data is usually related to a definite necessity. For example, in the medical field, health record systems are used for the exchange of medical data. In addition to services based on users' current location, many potential services rely on users' location history or their spatial-temporal provenance. However, most of the collected data contain data identifying individual which is sensitive. With the increase of machine learning applications around every corner of the society, it could significantly contribute to the preservation of privacy of both individuals and institutions. This chapter gives a wider perspective on the current literature on privacy ML and deep learning techniques, along with the non-cryptographic differential privacy approach for ensuring sensitive data privacy.

DOI: 10.4018/978-1-7998-8954-0.ch078

INTRODUCTION

In today's digital world, we are progressively relying on the internet for numerous applications. Especially online storage of our data for backup purposes or for real-time use which gives an anywhere, anytime access. This has become a part of our routine day to day activity. Cloud Computing has recently achieved consistent growth in the field of computing. Consumers and businesses have started using the cloud as a platform or a service by virtue of its efficiency. Machine learning powers many of the products we use today, like social feeds, voice assistants, navigation maps, advertisements, and auto-complete.

Because machine learning is data famished, it can have a negative influence on data privacy. Accessing data for machine learning increases the outward area for attack. Data scientists are given access to data that may have been previously vaulted. Neural networks can memorize information from data sets that can be extracted through statistical inference attacks and GANs. Anonymized data is prone to re-identification attacks when they are de-anonymized.

The increasing utility of data from machine learning has a reverse effect on privacy too. Data that was seemingly safe through the eyes of a human suddenly produces perceptions and results that only a machine could deduce. The mosaic effect states "disparate pieces of information—although individually of limited utility—become significant when combined with other types of information". What happens when an E - company puts together your credit card transactions, location history, professional profile, and browser history?

These properties of machine learning seem adverse from the perception of privacy, but they are also mandatory fundamentals for deep learning that helps us to grow and transform our society. In healthcare, for example, this technology can save many lives, but this shouldn't have at our own risk of sensitive data.

The main concerns that come along with these practices are the security and privacy pitfalls as the user's data is stored out of his premises.

This chapter is divided into the following sections. Introduction, Privacy preservation approaches in Cloud environment, Privacy Preserving through Differential Privacy, Privacy Preserving Machine Learning, and Deep Learning Techniques. So, once we get a better picture of different privacy preservation methodologies, we explore how it is applicable in the e-healthcare system. In the next sections, we have briefed the introduction to the E-Healthcare architecture, Privacy preservation Approaches in the e-Healthcare environment, Privacy-Preserving Approach using Deep Learning: Differential Privacy for e-Health care data, and finally Concluded with the overall picture

BACKGROUND

Privacy Preservation Approaches in Cloud Environment

Privacy is when a person's information is fully secured and is free from all interference. Today, we have cloud playing a key role in providing services across various domains, e.g., - health care, online banking, social networking, etc., these utilize user's personal information. These privacy- sensitive data are residing out of user's premises, so privacy preservation of these data against leaks and attacks is of concern. According to the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Charted Accountants (CICA), the definition is "Privacy is the right and obligation of individuals and organizations concerning the collection, use, retention, and disclosure of personal information." Hence,