Chapter 4
Machine Learning (ML) Methods to Identify Data Breaches

Gururaj H. L.
https://orcid.org/0000-0003-2514-4812
Vidyavardhaka College of Engineering, India

Pooja M. R.
Vidyavardhaka College of Engineering, India

Pavan S. P. Kumar
Vidyavardhaka College of Engineering, India

ABSTRACT

In this digitized world, everything is changing from offline to online. Data plays a vital role in this digital network. The theft or loss of USB devices, computers, or mobile devices by an unauthorized person who gains access to your mobile or laptop devices, email account, or network is generally termed as a data breach. Securing data from theft and breaches is a challenging issue. It is very hard to identify data breaches in complex networks. Adding extra intelligence using machine learning (ML) approaches will be efficient in identifying such attackers. In this chapter, various ML techniques to identify data breaches such as malware attack, man in the middle (MIM), spear phishing attack, eavesdropping attack, password attack, cross-site scripting attack will be depicted with suitable case studies.

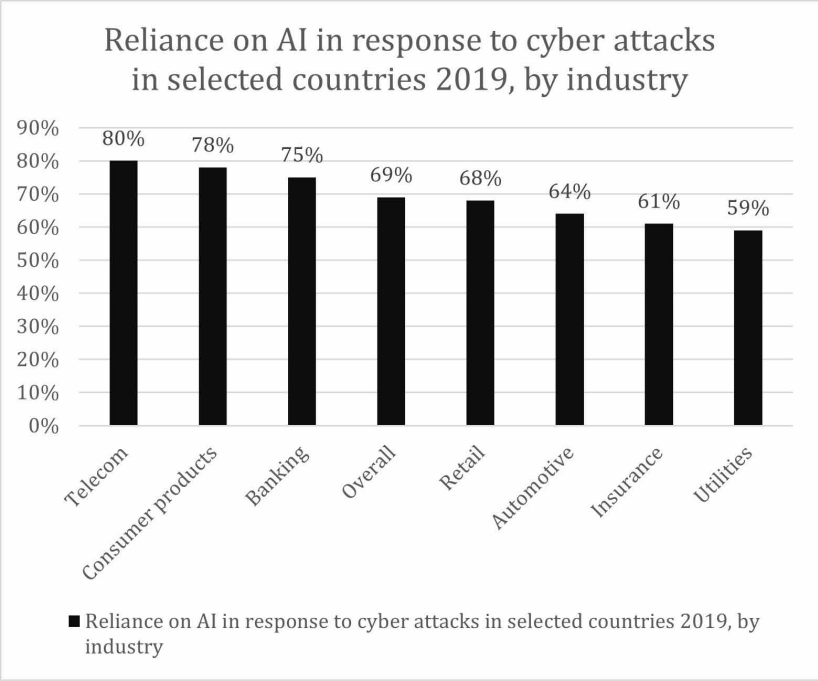
INTRODUCTION

The Indian scenario of communication completely changed from the recent past (E. Guven et al., 2016). Nowadays the importance of data is at its height. The users are trying very hard to secure the data in one or another way. Cyber Security is the protection of information, modification of data, data breaches from an unauthorized person (D. C. Le et al., 2019). A crime is conducted by criminals. A crime conducted in which the computer is directly or directly instrumental. The statistical survey according to Reliance on AI in response to cyber-attacks is depicted in Figure 1.

DOI: 10.4018/978-1-6684-3991-3.ch004

'Cyber' is a network that is vulnerable to the outside world. Cybercrime can be defined as any financial dishonesty that takes place in a computer environment or any threats to the computer itself, such as theft of the hardware or software for ransom.

Figure 1. Reliance on AI in response to cyber attacks



CYBER CRIMES

In this subsection, various cyber-attacks were introduced, and their details are explained. There are two kinds of attacks Techno-crime & Techno-vandalism. Techno-crime is an act against a system, with the intent of copying, steal or modifying the data. This type of attack is possible when the system is connected to the internet for 24x7 (Zincir-Heywood et al., 2019). Techno-Vandalism is a brainless defacement of the websites, such as publicizing someone else information. There are three types of Cybercriminals.

Cybercriminals – hungry for recognition, Cybercriminals – not interested in recognition and Cybercriminals – the insiders.

Some various types of cybercrimes are:

- IT Professionals
- Hobby hacker
- Politically motivators
- Terrorist