Blurb

By Prachi Gulihar

The book is targeting to cater to the needs of IT professionals, researchers, faculty members, scientists, graduate students, research scholars and software developers who seek to carry out research and develop combating softwares in the field of information and cyber security using machine learning based approaches. It gives an overview of principles, algorithm and applications of machine learning based solutions, it also discusses prominent future directions. The coming few years are going to be very eventful for cyber security professionals in this research area because these machine learning architectures will be used for doing large-scale analysis of the huge amounts of data being generated on Internet.

The Internet has come under the attack of malwares and hackers and the strain cyber security professionals to ensure the security of Internet is constantly increasing. Before the era of emergence of commercial internet there was not much need for protocols to be secure, it used to be an add-on feature, not a necessary feature but now times have changed. Rapid expansion of Internet have brought many secure protocols into existence rather there exist a lot of security protocols, a lot of security layers to understand. Ironically, the instances of cyber attacks are still prevalent today. The recent breakthrough solutions include extensive use of machine learning, data mining and artificial intelligence techniques. These methods have aided in building proactive defense mechanisms especially in the detection phase of the attacks. Many machine learning approaches for detection mechanism are described extensively. Privacy-preserving data mining mechanisms for profiling of anomalies and intrusions are also discussed at length. To solve certain problems direct application of these techniques is sufficient but for some other contemporary problems new approaches and algorithms are needed to be designed, this is where this book becomes of interest to researchers and security practitioners as it discusses the research conducted by academia and industry in this critical area. The papers selected have been strategically picked in a way that they complement one another to cover a broader area.