Chapter 10
Data-Driven Mathematical Modeling for AI-Based Security Applications

Sini Anna Alex
Ramaiah Institute of Technology, India

Parkavi A.
Ramaiah Institute of Technology, India

Sangeetha V.
Ramaiah Institute of Technology, India

ABSTRACT

Artificial intelligence (A.I.) is defined as the ability of a machine to perform cognitive functions that we associate with human minds, such as perceiving, reasoning, learning, interacting with the environment, problem solving, decision-making, and even demonstrating creativity. This field of artificial intelligence finds itself indispensable across various domains like shopping, fraud prevention, personalized learning, autonomous vehicles, voice assistants, etc. It is widely used in the field of cyber security. There are numerous AI based security models to delay security threats. Such algorithms could be classified under three heads – rule-based, shallow machine learning and deep learning algorithms. Fuzzy logic and fuzzy neural networks fall under rule-based algorithm. support vector machine (SVM), naïve bayes, decision tree, random forest, k-nearest neighbour and ensemble learning are some shallow ML algorithms that could be employed for cyber security.

INTRODUCTION

Artificial intelligence represents the human capacity accomplish cognitive functions that relate with human minds, like discerning, reasoning, understanding, interrelating with the environment, problem solving, decision making, and exemplifying creativity (Zaman et al., 2021). This field of Artificial Intelligence

DOI: 10.4018/978-1-6684-6408-3.ch010

finds itself indispensable across various domains like shopping, fraud prevention, personalized learning, autonomous vehicles, voice assistants, etc., It is widely used in the field of cyber security (Bansal et al., 2022; Zaman et al., 2021). There are numerous AI based security models to delay security threats. Such algorithms could be classified under three heads – Rule-based, shallow Machine Learning and Deep Learning algorithms. Fuzzy Logic and Fuzzy Neural Networks fall under Rule-based algorithm. Support vector machine (SVM), naïve bayes, decision tree, random forest, k-nearest neighbour and ensemble learning are some shallow ML algorithms that could be employed for cyber security. Multi-layer perceptron, auto-encoder, long short term memory, recurrent neural network and convolutional neural network are the deep learning algorithms that could be used for cyber security.

The above-mentioned Machine Learning (Dushyant et al., 2022) algorithms could be used for network traffic management. Different elements of computational, network devices and humans get connected through the applications of emerging fields like Internet of things. Security threats (Pramanik and Raja, 2019) are more in such heterogeneous environments. Various traditional encryption methods can be used to secure the data and the network in such heterogeneous systems. Using trendy encryption methods in applications of internet of things is trivial. Because resources are less in such applications security provisions for individual elements in networking applications of internet of things are critical. Determining the security solutions for such environments can be provided using rule-based mechanisms. They can be provided using deep learning mechanisms. We know that deep learning mechanisms are part of artificial intelligence domain.

Nowadays all organizations started using digital models for promoting their businesses. This helps them to maintain the interactions between their production team and clients. The model can be built using layered approach which helps to combine various functionalities through different modules. This approach helps them in managing the systems efficiently, addition of benefits like security and achieving scalable modules. The new generation digital environments are implemented using artificial intelligence. Artificial intelligence is used to enable machine to conduct cognitive operations similar to human. Hence it is inducing the machine to perform reasoning, knowledge gaining, interaction with the systems and human, providing solutions to the problems. Artificial intelligence-based applications are helpful in vigilant applications to monitor systems and their performances (Rai et al., 2019).

Nowadays we hear and see about more threats towards artificial intelligence systems. AI systems help in determining the future requirements of customers by using their history of behaviours. The problem with respect to artificial intelligence is maintaining the secrecy of the customer data. Researchers in cyber security are focusing on the threats towards artificial intelligence systems. Slowly the raise of offensive artificial intelligence scenario is happening to AI applications. In future this threat and attack increases towards AI systems. The only solution to defeat the offensive AI is using AI to deal with it. Hence the cyber-attacks can be dealt using defensive AI. AI provides smarter solutions towards both offensive AI and defensive AI (Gregory, 2021).

Anomaly Detection

Anomaly detection is very essential as it could provide knowledge transformation for network security management and protect user's information and integrity. For anomaly detection in networks, the resultant feature vectors from feature extraction of traffic data could be used for training and testing traffic classification model. Later, the information related to traffic is categorized as normal or abnormal. The network traffic can be analysed to identify the threats and attacks through SQL, scripts and directories.