Machine Learning for Security and Security for Machine Learning: A Literature Review

Nuruddin Wiranda
Computer Education
Lambung Mangkurat University
Banjarmasin, Kalimantan Selatan, Indonesia
nuruddin.wd@ulm.ac.id

Fal Sadikin
PJJ Teknik Informatika
Universitas Amikom Yogyakarta
Yogyakarta, Indonesia
fal_sadikin@yahoo.com

***Abstract*—**This manuscript is a literature survey and review of the topic of machine learning for security and security for machine learning. The work was carried out covering 36 previous research studies on this issue. It also presents solutions to three research questions (RQ) through delivering graphs, charts, and facts to summarize data. In addition, it provides readers with summaries of the paper on the concern**.**

Keywords—security, machine learning, literature review

I. INTRODUCTION

The internet was initially designed to connect administration, army, and educational investigators. As such, there is little essential for secure protocols, encoded packets, and wired servers. The invention of the www escorted in the Internet into the profitable Internet era, making it impossible to implement secure mechanisms retroactively. The Internet designers not ever invented words like spam, phishing, zombies, and spyware [1], but this term we now encounter constantly.

The function of confidence in the storage, processing, and broadcast process is to secure the confidentiality, integrity, and availability of data with the aid of technology, policy, and education. In general, for data security, the following three activities can be carried out: prevention [2]–[4], detection [5]–[9], and recovery [10], [11]. In the field of artificial intelligence, data security can be done using ML. ML can adapt quickly to the environment so it is suitable for prevention, detection and restoration of security. However, this ML adaptability can also backfire on computer systems, as they are vulnerable to exploitation by attackers of ML systems.

In previous investigation, a methodical literature survey and review has been showed on AI in Cybersecurity Education (Massive Open Online Courses) by Laato etc [12] using samples from four major scientific databases ACM, IEEE, Springer, and DBLP. Wiafe et al [13] have carried out a methodical mapping of the literature on AI for cybersecurity using a sample from the two main scientific databases of ACM and IEEE Xplore. Nassif et al [14] provide a methodical literature analysis of ML and Cloud security methods and practices.

The main purpose of this research is to manage a machine learning review for security and security for machine learning. While there have been many research studies on machine learning for security, to our knowledge, there have been very few systematic reviews on this topic. Through this study, we contributed by providing a comprehensive and up-to-date review related to the previous research conducted in machine learning and confidence, in particular the problems, methods, and challenges on machine learning for security, and security for machine learning.

For our research, research papers published in 2011 to 2020 from Science Direct and IEEE Xplore databases were warily saved and chosen with interest to (I) machine learning for security, (II) security for machine learning systems, and (III) security solutions for machine learning.

II. METHOD

This study adopted and combined the method used by Kitchenham etc.[15], Liao etc. [16], Mutai [17], and Nassif etc [14] that have been presented on Fig 1. There were six stages conducted in this study, containing the preparation of investigation problems, the process of searching articles, the strategy of documenting search results, the selection process of articles, conducting quality assessment, and the procedure of data abstraction.

Fig. 1. Literature Review Design.

A. Formulating Research Qeustions

The main purpose of this methodical literature review is to determine the questions that machine learning can cover for security and security for machine learning, and provide concrete answers to these questions. The Research Question (RQ) aims to keep the focus of the reviews. Descriptive and motivation details about the questions in this study are recorded in Table I.

TABLE I. RQ. MOTIVATION AND DESCRIPTION

Research Question	Motivation/ Description
RQ1 What are the problems, methods, and challenges of implementing ML for security?	The question focuses on identifying problems, methods and challenges in implementing ML for security
RQ2 What are the problems, methods and security challenges for ML systems?	The question focuses on identifying problems, methods and challenges in security for ML systems
RQ3 What is the security solution for ML?	The question focuses on knowing security solutions for ML

B. Search Proses

The search process for articles is carried out in four stages, namely: