A Survey on Supervised Machine Learning in Intrusion Detection Systems for Internet of Things

Shakirah Binti Saidin
Faculty of Computing
Universiti Malaysia Pahang Al-Sultan Abdullah
Kuantan, Pahang, Malaysia
shakirah.saidin90@gmail.com

Dr Syifak Binti Izhar Hisham*
Faculty of Computing
Universiti Malaysia Pahang Al-Sultan Abdullah
Kuantan, Pahang, Malaysia
syifak@ump.edu.my

2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS) | 979-8-3503-1093-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSECS58457.2023.10256275

***Abstract*—The Internet of Things (IoT) is expanding exponentially, increasing network traffic flow. This trend causes network security vulnerabilities and draws the attention of cybercriminals. Consequently, an intrusion detection system is designed to identify various network attacks and provide network resource protection. On the other hand, building a steadfast intrusion detection system is difficult since there are numerous flaws to address, such as the presence of supernumerary and irrelevant features in the dataset, leading to low detection accuracy and a high false alarm rate. To address these flaws, researchers are attempting to research on applying supervised machine learning techniques in intrusion detection systems for IoT. Therefore, this paper explores the prevailing machine learning techniques utilized in the intrusion detection system research area to provide better insight in this field.**

Keywords—supervised machine learning, intrusion detection system, security, Internet of Things

I. INTRODUCTION

Intrusion Detection System (IDS) is prominent as one of the solutions for system security alongside firewalls and anti-virus. However, as researchers continue their search for an intrusion detection technology with high detection accuracy, the performance of an IDS has become a fundamental issue[1]. IDSs are critical components of security as they will try to protect the systems from intruders. It works by monitoring systems or networks for anomalous and malicious behaviors [2]. An IDS's purpose is to identify any security breaches in a network [3]. It will gather and analyze data about a network's important notes to determine whether any security policies have been breached or if there are indicators of an attack.

Incorporating IDSs is crucial in conjunction with preventive security tools like firewalls because they identify and expose attacks that exploit vulnerabilities or glitches within the systems. Furthermore, they offer valuable forensic evidence that aids system administrators in effectively responding to cyber-attacks [4].

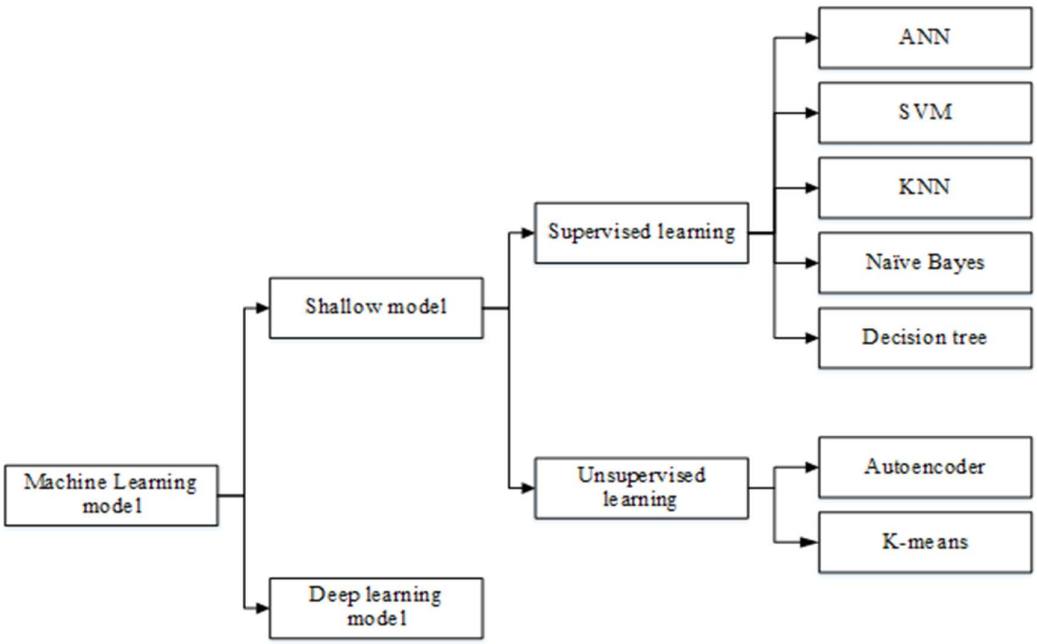

Fig. 1. Taxonomy of Machine Learning Model[15]