



A comprehensive survey and taxonomy of the SVM-based intrusion detection systems

Mokhtar Mohammadi ^a✉, Tarik A. Rashid ^b✉, Sarkhel H.Taher Karim ^{c d}✉,
Adil Hussain Mohammed Aldalwie ^e✉, Quan Thanh Tho ^f✉, Moazam Bidaki ^g✉,
Amir Masoud Rahmani ^{h i}✉, Mehdi Hosseinzadeh ^{j k}✉

Show more ▾

+ Add to Mendeley Share Cite

<https://doi.org/10.1016/j.jnca.2021.102983>

[Get rights and content](#) ➔

Abstract

The increasing number of security attacks have inspired researchers to employ various classifiers, such as support vector machines (SVMs), to deal with them in Intrusion detection systems (IDSs). This paper presents a comprehensive study and investigation of the SVM-based intrusion detection and feature selection systems proposed in the literature. It first presents the essential concepts and background knowledge about security attacks, IDS, and SVM classifiers. It then provides a taxonomy of the SVM-based IDS schemes and describes how they have adapted numerous types of SVM classifiers in detecting various types of anomalies and intrusions. Moreover, it discusses the main contributions of the investigated schemes and highlights the algorithms and techniques combined with the SVM to enhance its detection rate and accuracy. Finally, different properties and limitations of the SVM-based IDS schemes are discussed.