Abstract

As the use of software systems permeate diverse areas of the society, there is a need to ensure that not only does the software provide the needed functionality but it is also of high security, providing confidentiality, integrity and availability of the underlying data. Software security testing is one among the approaches towards detecting vulnerabilities and flaws in software which contribute to software insecurity. As machine learning finds success in other areas of computing, it has also gained interest in the field of software security testing. A review of the application of various machine learning techniques, including current trends in software security testing is of high value both to research and practice. This research provides an overview of how machine learning has been applied in software security testing and especially in the different phases of the testing cycle. Basic and recent developments of machine learning application in static analysis testing, dynamic analysis testing, symbolic execution and fuzz testing are discussed. The research followed a literature survey approach where existing literature on the subject were reviewed. A comparative performance of various machine learning techniques in the different phases of security testing is provided.