Abstract

In an increasingly advanced and complex digital era, cybersecurity has become a top priority for organizations worldwide. Cyber threats, such as malware, phishing, and network intrusions, continue to evolve and demand more innovative and effective solutions for detection and prevention. Therefore, this proposal proposes the development of a Non-Functiona l Requirements (NFR)-ba sed Fraud Deterrence Propeller V.2 Model to improve the effectiveness of cybersecurity systems. This model is designed to integra te va rious important aspects, such as security, performance, and scalability, enabling it to withstand various potential attacks while ensuring the system remains functionally optimal. This research methodology consists of several key stages, starting from model design based on NFRs to testing and evaluation. In the initia l stage, the model will be designed with releva nt NFR requirements in mind. After that, a system prototype will be developed and tested. Security testing is conducted through penetration testing to detect existing vulnerabilities, while performance testing will evaluate the system's ability to handle workloads under various conditions. This approach ensures that the model is not only designed theoretically but also measured for its performance in real-world situations. The results of this study are expected to provide in - depth insights into the effectiveness of the developed model, including potential improvements. Through data ana lysis from the test results, this resea rch will identify a reas for improvement and propose more robust solutions. Thus, this resea rch's contribution lies not only in developing more adaptive security systems but a lso in providing strategic guidance for organizations in addressing evolving cyber threats.

Keywords: Fraud Detterence Propeller, Penetra tion Testing, Non-Functiona l Requirements