ABSTRACT

Information Security is a critical aspect to consider because information for some parties becomes a valuable asset. Currently, the processing of information or data involves a lot of technology. However, in the implementation of real cases, there are many problems that cause the integrity and confidentiality of the processed information or data to be under risks. There are many aspects of technology that can be applied in information processing, the more aspects involved, the greater the threat to information processed with technology. To minimize these problems, one solution that can be applied is to detect and classify the data to be processed. One platform of technology used to serve data exchange is a *web* application. The *web* application is currently one of the platforms that is widely used by the public, therefore any data that comes to the the *web* application will be analyzed first, to detect indications of impending danger. The analysis process is carried out with Ensemble Machine Learning with the aim that the classification is more specific to the form of a pattern that becomes the identity of the data which is identical to the threat and does not need to apply the classification process programmatically or manualy. Ensemble Machine Learning performs classification by combining the classification process from several Machine Learning models. Currently the use of *Android*-based devices is so popular because of its flexible use and easy to carry anywhere. This is a consideration that *Android* devices will interact a lot with users. This condition can be used to speed up the process of detecting threats to *web* applications by utilizing *Android* devices as alarms that are connected to an integrated data classification system without having to always interact with the *server* interface.

Keywords :Machine Learning, Infomation Security, *Web* Application, *Android*