CHAPTER V
CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

Mobile Apps Validation Sysytem 2.0 was developed to assist users in determining the possibility that the application being used is safe by using permissions required by android applications.

5.2 Project Contribution

Mobile Apps Validation System 2.0 is developed to assist users in determining the likelihood that the application being used is safe or contains malware. It utilizes machine learning techniques to analyze the possibilities based on the permissions required by the Android application.

The system employs machine learning algorithms to process and interpret the permissions requested by an application. By training the algorithms with a comprehensive dataset that includes known malware samples and legitimate applications, the system learns to recognize patterns and indicators that can help assess the safety of an application.

By examining the permissions required by the application, the system can evaluate the potential risks and security implications associated with it. It considers the combinations and relationships between different permissions to estimate the likelihood of the application being safe or containing malware.

The machine learning aspect of the system allows it to continually improve its accuracy and detection capabilities. As it encounters new application samples and evolves with emerging malware trends, the system can adapt and update its models to provide more reliable assessments.

5.3 Result Discussion

The Mobile Apps Validation Sysytem 2.0 has been successfully completed and has achieved the objectives discussed in the previous chapter. The main objective of this project was to develop a system that allows users to assess the security of installed applications by utilizing machine learning techniques on the permissions requested by those applications.

By processing the access permissions of installed applications through machine learning algorithms, users will gain valuable insights into the security implications of those applications. The system analyses the permissions requested by each application and uses machine learning models to evaluate the potential risks associated with those permissions.

Through the implementation of this project, users can now make informed decisions about the security of the application they install. By considering the permissions required by each application and utilizing machine learning, users can gain a deeper understanding of the security implications and potential risks involved.

5.4 Future Work

The Mobile App Validation System 2.0 serves as a tool to assist users in their decision-making process, but additional security measures, such as regular updates, reputable application sources, and security software, should also be used for comprehensive protection. and it is expected that in the future developers will add security in addition to app access permissions.

5.5 Conclusion

In conclusion, the Mobile App Validation System 2.0 represents a significant advancement in assisting users in determining application security and identifying potential malware. By utilizing the power of machine learning, the system provides users with a comprehensive analysis of application permissions and associated risks.

The system's capability to analyze and interpret the permissions required by an application offers users valuable insight into its security implications. By

considering patterns, relationships, and combinations of permissions, the system can estimate the likelihood of an application being safe or containing malware.

One significant of the system is its machine learning capabilities, which enable continuous learning and adaptation. By utilizing diverse data sets and updating its models, the system can improve its accuracy in detecting and identifying potential threats. The Mobile App Validation System 2.0 serves as a reliable tool for users, helping them make informed decisions about the application they install. It enhances the overall security of the mobile application ecosystem by empowering users to identify and avoid potentially malicious applications.