Ministry of Higher Education and

Scientific research

University of Babylon

College of information Technology

Department of information security

Study: (morning)

Network anomalies detection

A Graduate Project Submitted to the Department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfilment of the Requirements for the Bachelor's degree in Information Security of Information Technology

STUDENT'S NAME

Ahmed Mohammed Jasim

Supervisor by

Dr. Khaldoon Hasan

2023-2024

ABSTRACT

Every day millions of people and hundreds of thousands of institutions communicate with each other over the Internet. In the past two decades, while the number of people using the Internet has increased very fast. Parallel to these developments, the number of attacks made on the Internet is increasing day by day. Although signature-based methods are used to prevent these attacks, they are abortive against zero-day attacks. On the other hand, the Anomaly-based approach is an alternative solution to the network attacks and has the ability to detect zero-day attacks as well. In this study, it is aimed to detect network anomaly using machine learning methods. In this context, the CICIDS2017 has been used as dataset because of its up-to datedness, and wide attack diversity. On this dataset, feature selection was made by using the Random Forest Regressor algorithm. Seven different machine learning algorithms have been used in the application step and achieved high performance. Machine learning algorithms and success rates are as follows: Naive Bayes 86%, Random Forest 94%, ID3 95%, and K Nearest Neighbours 97%.