Applying Machine Learning Tools
to Detect Cyber Attacks in Financial Firms and Banks

Author: M A Islam Supervisor: Dr Kashinath Basu

OXFORD BROOKES UNIVERSITY
School of Engineering, Computing and Mathematics

Introduction

The use of machine learning in cybersecurity is becoming increasingly important for detecting cyber attacks in financial firms and banks. Machine learning offers improved scalability, efficiency, and actionability compared to traditional methods that rely on human interaction. Various machine learning techniques, including deep learning, support vector machines, and Bayesian classification, have shown promise in detecting cyber attacks. This study uses machine-learning techniques and tools to detect cyber attacks in financial firms and banks, and recommends the use of XGBoost due to its high performance. Ensuring cybersecurity in financial firms and banks is crucial for maintaining the integrity, confidentiality, and transparency of transactions in virtual and online banking systems.

Research Question

What is the best machine learning model financial companies (banks) have used to prevent information systems from online threats?

Research Aim

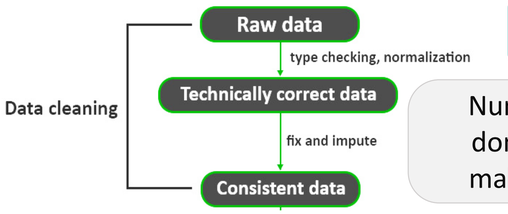
Analyzing cyberthreat challenges to banks is the primary objective of this research, which further proposes a method for identifying and preventing the cyberattacks.

Scope of Research

- To help company leaders implement effective protection measures against cybercrime for profitable business procedures and beneficial social reform.
- To help smaller financial companies and other enterprises guard against damaging cyber security incidents.
- Highlight the importance of ICT use for society, business as well as government in Bangladesh's Internet group.

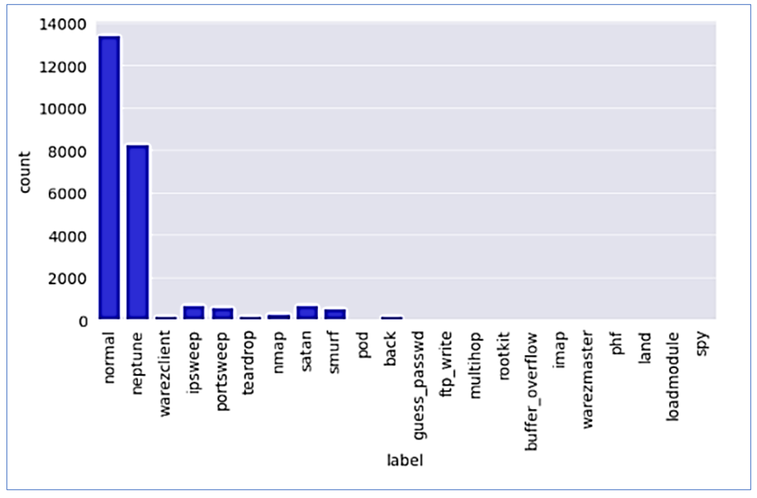
Methodology

1. Decision Making
2. Data Collection
3. Data Cleaning
4. Data Modelling
5. Data Visualization
6. Conclusion

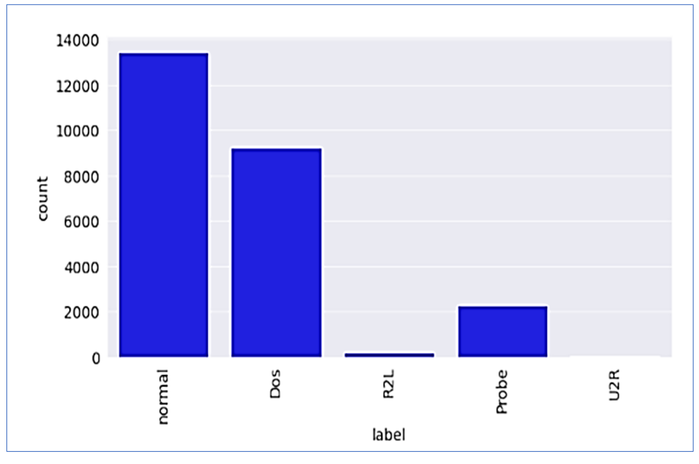


Outcomes

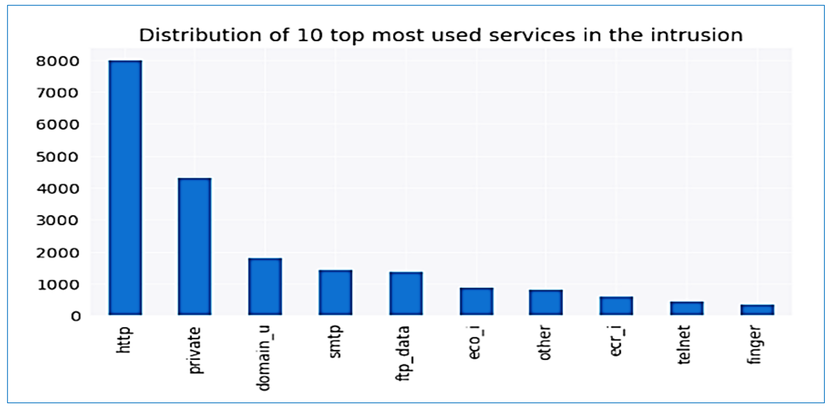
Number of different attacks done/attempted by several malwares are stated below:



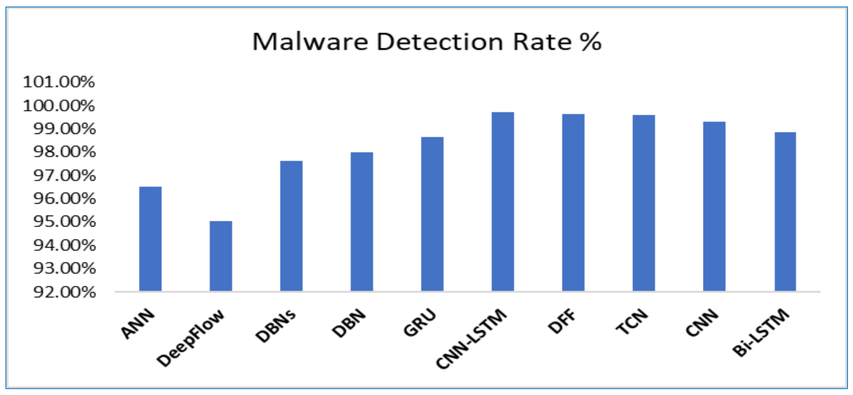
Different types of attacks and normal access:



Top 10 most used services used in the intrusion process are:



Malware detection rate by different approaches are as follows:



Conclusion and Recommendation

The study explored machine learning methods for detecting and combating cyber threats in the financial services industry. They suggest that implementing machine learning algorithms such as deep learning and XGBoost for fraud detection in banks can help to swiftly identify suspicious activity, confirm user identities, and respond to cyberattacks. Additionally, ML reduces the need for human intervention by scanning vast volumes of data in real-time and improves user experience by streamlining identity verification procedures.

References: Ali, L. (2019). Cybercrime is a growing menace to the commercial sectors that is constantly there (a study of the online banking sectors in GCC). Journal of Developing Areas, 53, 267-279. doi:10.1353/jda.2019.0016

Al-Hamar, A. K. (2016). enhancing Qatari organization's information security procedures. doi:10.5339/qfarc. 2016.ICTPP2531. Qatar Foundation Annual Research Conference Proceedings, 2016(1), p. ICTPP2531.

M. C. Cant and J. A. Wiid (2013). identifying the difficulties facing SMEs in South Africa. Journal of International Business and Economics, Volume 12, Pages 707–716. Obtainable at http://www.cluteinstitute.com