1. INTRODUCTION

1.1 Project Overview

Phishing attacks have become a major cybersecurity threat, especially in the financial and banking sectors. Cybercriminals use phishing emails to trick users into providing sensitive information such as login credentials, credit card details, and personal identification numbers. These attacks often lead to financial losses and identity theft.

The primary objective of this project is to develop a **machine learning-based phishing email detection system** that can classify emails as either phishing or legitimate. By analyzing email content, metadata, and other distinguishing features, the system aims to enhance cybersecurity and prevent fraud in financial institutions.

1.2 Purpose

The purpose of this project is to design an **efficient and automated system** that can detect phishing emails based on various textual and metadata features. Financial institutions often struggle with identifying sophisticated phishing attempts, as traditional security measures may not be sufficient. The proposed solution will assist banks and financial organizations in:

- Reducing fraudulent activities caused by phishing attacks.
- Improving customer trust by preventing security breaches.
- Enhancing the accuracy of phishing email detection with machine learning models.