**INTRODUCTION**

Phishing is the most common type of cybercrime that involves persuading victims to submit sensitive information such as account numbers, passwords, and bank account numbers. Cyber-attacks are commonly launched using email, instant messages, and phone calls[1, 2].

Despite continual updates to the procedures for preventing such cyber-attacks, the result is insufficient. On the other hand, phishing emails have expanded tremendously in recent years, indicating the need for more effective and modern measures to combat them.[3, 4]

Several approaches for filtering phishing emails have been developed. However, the problem still requires a comprehensive solution. This is the first poll we're aware of that focuses on applying Machine Learning (ML) approaches to detect phishing emails[4]. This research examines the various state-of-the-art machine learning (ML) algorithms currently used to detect phishing emails at different stages of the attack[5]. A comparative assessment and analysis of these methodologies are performed. This provides an overview of the topic, its immediate solution space, and potential future research possibilities[6-8].

The rapid advancement of internet technologies has changed the way people interact online while also posing new security risks. Newly growing global dangers attack the user's computer and have the potential to steal their identity and

money[9].

Phishing is a term with thousands of references in scientific papers, a lot of press coverage, and scrutiny from banks and law enforcement agencies. However, this raises the question of what phishing is[10].

In some publications, the phenomenon of phishing is expressly described; in others, it is presented with an illustration, while others assume that the reader already understands what phishing is. Many academics have offered their definitions of phishing, resulting in a wide range of interpretations in the scholarly literature. Because the phishing issue is broad and covers a multitude of circumstances, the literature does not provide a detailed description of phishing attacks[11, 12].

The term phishing was coined in 1996 as a result of social engineering attacks by web scammers against America Online (AOL) accounts, according to the APWG. Detecting phished email in the proposed system can be regarded as a classification problem with two types, ham and phished. Machine learning is a branch of artificial intelligence. When a system is given the ability to learn, it is intelligent. Without explicitly programmed, supervised learning is a concept that we use in our model. For classification, machine learning techniques are utilized.[13, 14]