Chapter 1
AI-Powered Phishing Detection System

Mehaboob Mujawar
https://orcid.org/0000-0002-8260-7062
Mangalayatan University, India

Aasheesh Raizada
Mangalayatan University, India

Abdullah Gubbi
Bearys Institute of Technology, Mangalore, India

ABSTRACT

This research presents an AI-driven system to combat phishing attacks using machine learning and natural language processing. Key components include data collection, feature extraction, model training, and real-time detection. The system offers high accuracy, real-time protection, customizability, enhanced security, reduced financial and data breach risks, and improved efficiency through automation. This scalable, adaptive solution provides robust protection against phishing threats, improving security and productivity while optimizing resource allocation. The system's automation and adaptability make it valuable in addressing this persistent cybersecurity challenge

INTRODUCTION

In our increasingly digital era, phishing attacks have emerged as a sophisticated and widespread threat, targeting both individuals and organizations through deceptive strategies that mimic legitimate entities. These attacks exploit human vulnerabilities

DOI: 10.4018/979-8-3373-1832-5.ch001

and trust to obtain sensitive information, including login credentials, financial data, and personal details. Phishing attempts are conducted via various channels, such as emails, websites, and messages, each designed to trick users into believing they are interacting with a trusted source. The ramifications of successful phishing attacks are severe, often leading to substantial financial losses, compromised personal information, and significant reputational harm to both individuals and organizations. Phishing attacks have undergone significant evolution over time, employing advanced techniques to circumvent traditional security measures (Ogundairo & Broklyn, 2024). Cybercriminals continually refine their methods, utilizing social engineering tactics, creating highly convincing fake websites, and using tools to avoid detection. The growing sophistication of these attacks poses a formidable challenge to conventional security measures, which typically rely on static rule-based systems that struggle to keep up with the dynamic nature of phishing threats. As a result, there is a pressing need for innovative and adaptable solutions capable of effectively addressing the complexities of phishing attacks.

In response to this escalating threat, researchers and cybersecurity experts have turned to artificial intelligence (AI) as a potent weapon in the battle against phishing. AI-driven phishing detection systems harness advanced technologies, particularly machine learning (ML) algorithms and natural language processing (NLP) techniques, to identify and thwart phishing attempts in real-time. Unlike traditional approaches that depend on predefined rules and signatures, AI-based systems are designed to analyze intricate data patterns and comprehend the nuanced characteristics of phishing content. This enables them to detect suspicious activities with significantly greater accuracy and efficiency, providing a robust defense against phishing attacks.

The Evolution of Phishing Attacks

The landscape of phishing attacks has undergone a significant transformation, evolving from rudimentary email-based scams to intricate, targeted operations. In the early days, cybercriminals relied on a quantity-over-quality approach, disseminating generic messages to a vast number of recipients in hopes of ensnaring a few unsuspecting victims. However, contemporary phishing techniques have become far more refined and strategic. Modern phishing campaigns often employ sophisticated tactics such as spear phishing and whaling. These methods involve tailoring attacks to specific individuals or high-ranking executives within organizations. Unlike their predecessors, these advanced phishing attempts are meticulously crafted to appear authentic, often incorporating personal details about the target to establish credibility and trust. The scope of phishing has also expanded beyond the traditional email medium. Cybercriminals now exploit a diverse array of digital platforms to reach potential victims. Social media networks, instant messaging applications,