# IMPLEMENTING HONEYPOT AND ARTIFICIAL INTELLIGENCE IN NETWORK SECURITY ANALYSIS TO DETECT CYBER ATTACKS ON SOCIAL MEDIA

**CARLOS SUSANTO**
*Program Studi Informatika, Fakultas Sains & Teknologi*
*Universitas Teknologi Yogyakarta*
*Jl. Ringroad Utara Jombor Sleman Yogyakarta*
*Email: carlossusanto89@gmail.com*

## ABSTRACT

Social media platforms have evolved into essential ecosystems for global digital interaction. However, their widespread popularity and inherently open nature make them prime targets for a variety of increasingly sophisticated and destructive cyber threats, including large-scale disinformation campaigns, social engineering-based fraud schemes, user identity theft, and malware distribution. Traditional security approaches, which are often reactive and rely on signature-based pattern matching, are proving increasingly inadequate to keep pace with the rapid evolution and adaptability of attacker tactics in the highly dynamic and high-volume social media environment. To address this critical security gap, this research proposes an initiative to develop and implement a proactive cyberattack detection model by integrating state-of-the-art artificial intelligence (AI) with a cyber-trap mechanism adapted for social media, known as a social honeypot. The methodology involves the strategic creation and deployment of decoy accounts carefully crafted to resemble authentic users, aiming to attract and trap malicious human actors, automated bot networks, or content propagators. These honeypots serve as intelligence-gathering sensors on the front lines, tasked with recording detailed interaction data, such as linguistic patterns in messages, frequency and anomalies in friend requests, and various social engineering tactics employed by attackers.

**Keywords**: Social Media, Cyber Security, Proactive Detection, Artificial Intelligence, Social Honeypot, Behavioral Analysis, Disinformation.