**PROPOSAL DUE**

**Social Engineering attacks and counter measure using AI.**

Our research highlights the pressing necessity to deal with the threat of AI-enhanced social engineering attacks. It provides a path for people, businesses, and policymakers to better fight against these sophisticated and growing dangers by detailing the most recent attack strategies and suggesting proactive solutions. Protecting against AI-driven social engineering assaults is essential to maintaining trust and security in digital interactions in a future where AI is becoming more and more linked into our daily lives.

Cybersecurity is under unprecedented threat from AI-enhanced social engineering attacks because of their growing complexity. To combat these new risks, this study presents a cutting-edge countermeasure: behavioral authentication driven by AI.

Advanced algorithms are used in AI-enhanced social engineering assaults to mimic human behavior and trick targets into disclosing sensitive information or acting against their better judgment. Due to the increasingly convincing and individualized character of these assaults, traditional security measures frequently fall short in detecting them.

This study presents a thorough investigation of AI-powered behavioral authentication as a reliable countermeasure in response to the changing threat landscape. Utilizing machine learning algorithms, this state-of-the-art technology analyzes user behavior patterns across digital interactions to provide a behavioral biometric profile that is particular to each person.