# OKECHUKWU UDE

STUDENT, MASTER OF INFORMATION SYSTEMS ASSURANCE MANAGEMENT


## SECURING REMOTE ACCESS NETWORKS USING MALWARE DETECTION TOOLS FOR INDUSTRIAL CONTROL SYSTEMS


With their role as an integral part of its infrastructure, Industrial Control Systems (ICS) are a vital part of every nation's industrial development drive. Like every other facet of life, ICS have witnessed the integration of Information Systems (IS) into their processes, connecting them to the much larger Internet of Things (IoT). Despite several significant advancements--such as controlled-environment agriculture, automated train systems, and smart homes, achieved in critical infrastructure sectors through the integration of IS and remote capabilities with ICS, the fact remains that these advancements have also introduced vulnerabilities that were previously either non-existent or negligible, one being Remote Access Trojans (RATs). RATs are a crucial tool for every advanced persistent threat (APT) attack mounted against any organization, and as such attackers put a lot of effort into making them as undetectable as possible. Present RAT detection methods either focus on monitoring network traffic or studying event logs on host systems. This research's objective is the detection of RATs by comparing actual utilized system capacity to reported utilized system capacity. To achieve the research objective, open-source RAT detection methods were identified and analyzed, a GAP-analysis approach was used to identify the deficiencies of each method, after which control algorithms were developed into source code used in developing the solution.


***Research Advisor: Dr. Bobby Swar***