Project Proposal Report
What advanced intrusion detection techniques can be implemented in SCADA systems to identify and mitigate unauthorized access or anomalies in real-time?

Savali Sandip Deshmukh
sdeshmukh@ucdavis.edu

Shivani Suryawanshi
ssuryawanshi@ucdavis.edu

Tanvi Mehta
tanmehta@ucdavis.edu

October 15, 2024

1 Introduction

Supervisory Control and Data Acquisition (SCADA) systems are essential tools for managing and controlling industrial operations like manufacturing, energy distribution, and water treatment[1]. These systems allow the operators to remotely monitor the industrial processes by giving them real-time data to make decisions. But their dependency on the internet makes them more vulnerable to cyberattacks [2]. They are prone to threats such as buffer overflows, cross-site scripting, and SQL injection attacks which cause a public safety issue as well as operational ineffectiveness [3].

Our goal in this research project is to investigate intrusion detection methods designed specifically for SCADA systems in order to detect and address abnormalities and unauthorized access. This research is vital in ensuring the resilience and integrity of essential services of society, ultimately contributing to improved safety and security in critical infrastructure sectors. We also want to focus our research on the three main components of computer security: availability, confidentiality, and integrity to provide secure services in industrial and infrastructural sectors.

References

[1] Abdun Mahmood Manar Alanazi. "SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues". In: *Computers Security* (2023). DOI: https://doi.org/10.1016/j.cose.2022.103028.

[2] Huan Yang, Liang Cheng, and Mooi Choo Chuah. "Deep-Learning-Based Network Intrusion Detection for SCADA Systems". In: *2019 IEEE Conference on Communications and Network Security (CNS)* (2019). DOI: https://doi.org/10.1109/CNS.2019.8802785.

[3] Slavica V. Boštjančič Rakas, Mirjana D. Stojanović, and Jasna D. Marković-Petrović. "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems". In: *Innovations in Systems and Software Engineering* (2020). DOI: https://doi.org/10.1109/ACCESS.2020.2994961.