|  |  |  |  |
| --- | --- | --- | --- |
| **Title:** | Enhancing Industrial Control System Security: An Isolation Forest-based Anomaly Detection Model for Mitigating Cyber Threats | | |
| **Author(s) Name:** | Mahmud, Md Saif & Islam, Md Ashikul & Rahman, Md & Chakraborty, Debashon & Kabir, Shaharier & Shufian, Abu & Sheikh, Protik | | |
| **Contact Email(s):** | protik@aiub.edu | | |
| **Published Journal Name:** | Journal of Engineering Research and Reports (JERR) | | |
| **Type of Publication:** | Journal | | |
| **Volume:** | 26 | Issue | 3 |
| **Publisher:** | Journal of Engineering Research and Reports | | |
| **Publication Date:** | 6th March 2024 | | |
| **ISSN:** | 2582-2926 | | |
| **DOI:** | https://doi.org/10.9734/jerr/2024/v26i31102 | | |
| **URL:** | https://journaljerr.com/index.php/JERR/article/view/1102 | | |
| **Other Related Info.:** | Page 161-173 | | |
|  | | | |

|  |  |
| --- | --- |
| **Abstract:** |  |
| In the evolving landscape of industrial control systems (ICS), the sophistication of cyber threats has necessitated the development of advanced anomaly detection mechanisms to safeguard critical infrastructure. This study introduces a novel anomaly detection model based on the Isolation Forest algorithm, tailored for the complex environment of ICS. Unlike traditional detection methods that often rely on predefined thresholds or patterns, our model capitalizes on the Isolation Forest's ability to efficiently isolate anomalies in high-dimensional datasets, making it particularly suited for the dynamic and intricate data generated by ICS. Leveraging the HAI dataset, which encompasses operational data from a realistic ICS testbed augmented with a Hardware-In-the-Loop (HIL) simulator, this research demonstrates the model's effectiveness in identifying both known and novel cyber threats across various ICS components. Our findings reveal that the Isolation Forest-based model outperforms traditional anomaly detection techniques in terms of detection accuracy, false positive rate, and computational efficiency. Furthermore, the model exhibits a remarkable ability to adapt to the evolving nature of cyber threats, underscoring its potential as a robust tool for enhancing the security posture of ICS. Through a detailed analysis of its application in detecting sophisticated attacks represented in the HAI dataset, this study contributes to the ongoing discourse on improving ICS security and presents a compelling case for the adoption of machine learning-based anomaly detection solutions in industrial settings. | |