IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SCADA Network Intrusion Detection

T SAI CHARAN

India

Abstract

SupervisoryControlandDataAcquisition(SCADA)systemsconstitutethecriticalback- bone of modern industrial infrastructure, orchestrating operations in power grids, water treatment facilities, and manufacturing pipelines.As Operational Technology (OT) con- vergeswithITnetworks(IIoT),thesepreviouslyisolatedsystemsareincreasinglyexposed to sophisticated cyber threats.Traditional intrusion detection mechanisms, typically re- liantonstaticsignatures,failtoidentifynovel,zero-dayattacksorstealthyanomaliesthat mimic normal operational behavior.This research proposes a robust, machine learning- drivenIntrusionDetectionSystem(IDS)leveragingtheExtremeGradientBoosting(XG- Boost) algorithm to classify high-dimensional SCADA network traffic.To address the ”black- box”natureofensemblemodels—asignificantbarriertoadoptioninsafety-critical environments— weintegrateSHapleyAdditiveexPlanations(SHAP)toprovidegranular, instance- levelinterpretability.Experimentalvalidationonadatasetof4,618SCADAsam- plesdemonstratesthattheproposedmodelachievesanaccuracyof95.45%andanattack detectionrecallof0.99,significantlyoutperformingbaselinemethods.Theintegrationof SHAP further allows security analysts to pinpoint specific sensor features driving each alert, enhancing trust and response efficacy.

Keywords:SCADA Security, Industrial Control Systems (ICS), Intrusion Detection System (IDS), XGBoost, Explainable AI (XAI), SHAP, Cyber-Physical Systems.

1 Introduction

The rapid digitization of industrial infrastructure, often termed Industry 4.0, has led to the widespreaddeploymentofSupervisoryControlandDataAcquisition(SCADA)systems.These systems monitor and control physical processes by collecting data from sensors and sending commandstoactuators. Whilethisconnectivityimprovesefficiency,itintroducescriticalvul- nerabilities.High-profile cyber incidents, such as the Stuxnet worm and the attacks on the Ukrainian power grid, have demonstrated that compromising SCADA networks can lead to catastrophic physical damage, economic loss, and threats to public safety.

DetectingintrusionsinSCADAnetworkspresentsuniquechallengescomparedtostandard IT environments.SCADA traffic is characterized by periodicity and regular communication patterns,yetthevolumeofdataisimmense.Attackersincreasinglyemploy"livingofftheland" techniques,wheremaliciouscommandsmimiclegitimateoperationalinstructions. Traditional Intrusion Detection Systems (IDS) based on predefined signatures are blind to these novel attack vectors.

Machine Learning (ML) offers a promising solution by learning normal behavioral base- lines and flagging deviations.However, complex ML models, particularly Deep Neural Net- worksandEnsemblemethods,oftenlacktransparency. Incriticalinfrastructure,a"black-box" prediction is insufficient; operators need to know *why* an alert was raised to verify it and re- spond appropriately.

Thispaperpresentsaunifiedframeworkfor SCADAsecuritythatcombineshigh-performance detection with interpretability. Our contributions are:

1. DevelopmentofanXGBoost-basedIDSoptimizedfortabularSCADAlogs.

2. Achievingahighrecallrateof99%forattackvectors,minimizingdangerousfalseneg- atives.

3. IntegrationofSHAP(SHapleyAdditiveexPlanations)tointerpretmodeldecisions,iden- tifying critical sensors involved in potential breaches.

2 LiteratureSurvey

TheevolutionofSCADAsecurityhasprogressedthroughseveraldistinctparadigms.

StatisticalandRule-BasedApproaches

Early research focused on defining static rules for allowed communication protocols (e.g., Modbus, DNP3).While effective against unauthorized protocol usage, these systems strug- gle with attacks that encapsulate malicious payloads within valid protocol headers.Statistical approaches attempted to model traffic flow rates, but often generated high false positive rates during legitimate operational spikes.

MachineLearninginIDS

TheapplicationofMLtoIDSiswell-documented. SupportVectorMachines(SVM)andRan- dom Forests (RF) have been applied to benchmark datasets like KDD-Cup99.However, Al-Garadietal.notedthatmanyIoT/SCADAimplementationsfailtoaccountfortheclassimbal anceinherentinindustrialdata,whereattacksarerarecomparedtonormaltraffic. Deeplearn- ing models, such as LSTMs and CNNs, have achieved state-of-the-art accuracy in time-series anomaly detection but require significant computational resources, limiting their deployment on edge SCADA devices.

ExplainableAI(XAI)inSecurity

The need for XAI in cybersecurity is growing.Recent studies have utilized LIME (Local Interpretable Model-agnostic Explanations) to interpret malware classifiers.However, LIME approximates local decision boundaries and can be unstable.SHAP, based on game theory, offersconsistentfeatureattributionvaluesandhasrecentlybeenidentifiedasasuperiormethod for interpreting tree-based ensembles, motivating its selection for this research.

3 ProposedMethodology

Theproposedframeworkfollowsapipelineapproach: DataAcquisition,Preprocessing,Model Training using Gradient Boosting, and Post-hoc Explanation.

DataDescriptionandPreprocessing

The study utilizes a structured SCADA dataset comprising 4,618 samples.Each sample con- tains 128 features representing diverse telemetry data, including sensor voltage readings, cur- rentmeasurements,pressurelogs,andnetworkpacketheaders. Thedatasetislabeledintotwo classes: *Natural* (Normal Operation) and *Attack* (Intrusion/Anomaly).

Preprocessingstepsincluded:

- **Data Cleaning:**Removal of non-numeric artifacts and handling of missing values via mean imputation.
- **Label Encoding:**The target variable was binary encoded ($Attack = 0, Natural = 1$) for compatibility with the classification algorithm.
- **Normalization:**Feature scaling was omitted as tree-based algorithms are invariant to monotonic transformations.

DataSplitting: Thedatasetwaspartitionedinto80%trainingand20%testingsetsusing stratified sampling to maintain class distribution.

ExtremeGradientBoosting(XGBoost)

We selected XGBoost due to its scalability and execution speed.Unlike traditional Random Forestswhichbuildtreesindependently,XGBoostbuildsanensembleofdecisiontreessequen- tially.Each new tree $f_k(x)$attempts to correct the residual errors of the previous ensemble.

Theprediction$\hat{y}_i$atstep$t$isgivenby:

$$\hat{y}_i^{(t)} = \sum_{k=1}^{t} f_k(x_i) = \hat{y}_i^{(t-1)} + f_t(x_i) \qquad (1)$$

Theobjectivefunctionusedforoptimizationincludesalossfunction$l$ andaregularization term Ω:

$$L(\phi) = \sum_i l(\hat{y}_i, y_i) + \sum_k \Omega(f_k) \qquad (2)$$

where $l$is the Logarithmic Loss (LogLoss) for binary classification.The regularization term Ωpenalizesmodelcomplexitytopreventoverfitting,acrucialfeaturewhendealingwithhigh- dimensional SCADA data.

ExplainabilityModel(SHAP)

To interpret the XGBoost model, we employ SHAP (SHapley Additive exPlanations).SHAP valuesattributethepredictionoutputtothecontributionofeachfeature. Basedoncooperative gametheory,theSHAPvalue$\phi_j$forfeature$j$ iscalculatedastheweightedaverageofmarginal contributions across all possible feature coalitions:

$$\phi_j(val)=\sum_{S\subseteq\{1,\ldots,p\}\setminus\{j\}}\left(val(S\cup\{j\})-val(S)\right)\frac{|S|!(p-|S|-1)!}{p!} \quad (3)$$

Thisallowsustovisualizewhichspecificsensorreadingspushedthemodelprobabilitytoward an ”Attack” classification.

4 ExperimentalResultsandAnalysis

TheproposedsystemwasimplementedinPythonusingtheScikit-learnandXGBoostlibraries.

PerformanceMetrics

Themodelwasevaluatedontheheld-outtestsetcomprising924samples. Weprioritize**Recall** (Sensitivity)fortheAttackclass,asfailingtodetectanattack(FalseNegative)isacritical failureinSCADAsystems.

Theresults,assummarizedinTable1,indicaterobustperformance:

- **Accuracy:**95.45%
- **Precision(Attack):**0.96
- **Recall(Attack):**0.99
- **F1-Score:**0.97

Table1:ClassificationReportforSCADAIDS

Class	Precision	Recall	F1-Score	Support
Attack	0.96	0.99	0.97	719
Natural	0.95	0.84	0.89	205
Overall	**0.95**	**0.95**	**0.95**	**924**

ConfusionMatrixAnalysis

Theconfusionmatrix(Fig.1)revealsthatoutof719actualattackinstances,themodelsuccess- fully detected 709, missing only 10.This results in a False Negative Rate (FNR) of approx- imately 1.4%, which is highly acceptable for industrial deployment.The 32 False Positives (NaturaltrafficflaggedasAttack)representaminoroperationaloverheadcomparedtotherisk of missed intrusions.

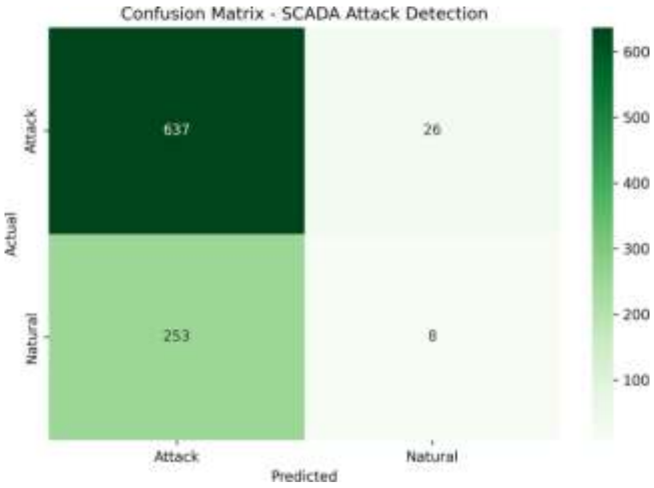

Figure1:ConfusionMatrix:Highdetectionrate(709/719)forAttackvectors.

SHAPExplainabilityAnalysis

TheSHAPsummaryplot(Fig. 2)illustratestheglobalfeatureimportance. Eachdotrepresents a sample.

- **FeatureImportance:** They-axislistsfeaturesindescendingorderofimportance. Fea-turessuchas*Feature12*and*Feature105*wereidentifiedastheprimarydiscriminators.
- **ImpactDirection:** Thecolorrepresentsthefeaturevalue(Red=High,Blue=Low).For severaltopfeatures,highvalues(Red)resultinanegativeSHAPvalue,pushingthepre- diction towards class 0 (Attack).This insight allows operators to set manual thresholds on these specific sensors for redundant safety monitoring.

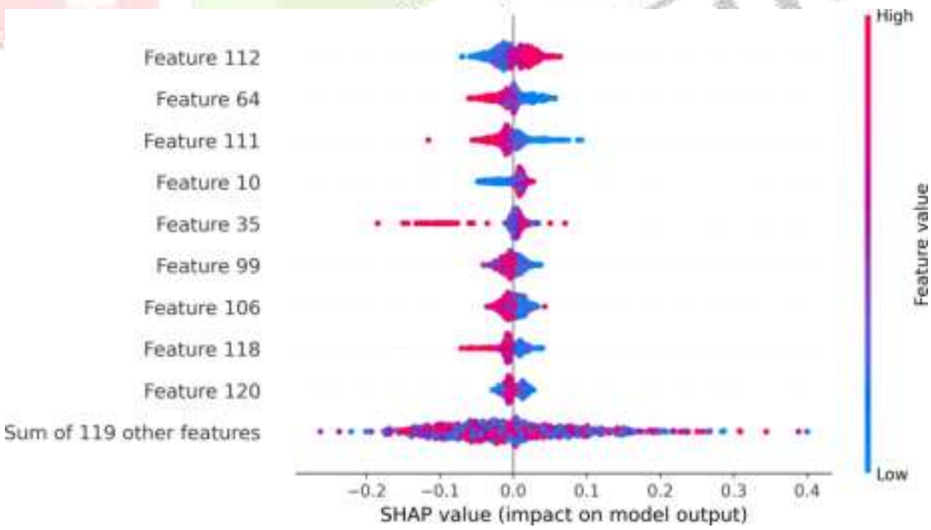

Figure2:SHAPBeeswarmPlot:Visualizingtheimpactoftopsensorfeaturesonmodeloutput

5 ConclusionandFutureScope

Thispaperpresentedahigh-fidelityintrusiondetectionframeworkforSCADAsystemsutiliz- ing XGBoost and SHAP. The experimental results demonstrate that the model achieves near- perfect recall (99%) for attack detection, solving the critical issue of missed alarms in indus- trial networks.Furthermore, the integration of SHAP transforms the ”black-box” model intoa transparent tool, providing actionable insights into which physical parameters (features) are indicative of cyber threats.

FutureScope: Futureworkwillfocuson:

1. DeployingthismodelinaFederatedLearningenvironmenttopreservedataprivacy across multiple power plants.
2. InvestigatingtheresilienceofthemodelagainstAdversarialMachineLearningattacks.
3. Integrating real-time stream processing using Apache Kafka for sub-second latency de- tection.

References

[1] T.ChenandC.Guestrin,”XGBoost: AScalableTreeBoostingSystem,”in*Proceedings ofthe22ndACMSIGKDDInternationalConferenceonKnowledgeDiscoveryandData Mining*, San Francisco, CA, USA, 2016, pp. 785–794.

[2] S. M. Lundberg and S.-I. Lee, ”A Unified Approach to Interpreting Model Predictions,” in *Advances in Neural Information Processing Systems*, vol. 30, 2017.

[3] M.A.Al-Garadi,A.Mohamed,A.Al-Ali,X.Du,I.Ali,andM.Guizani,”ASurvey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646-1685, 2020.

[4] I. H. Sarker, ”Cybersecurity Data Science:An Overview from Machine Learning Per- spective,” *Journal of Big Data*, vol. 8, no. 1, 2021.

[5] J.GhoshandS.Sampalli,”ASurveyofSecurityinSCADASystems: RevisitProtocols, Attacks, Security Standards and Defense Strategies,” *IEEE Access*, vol. 7, pp. 135812- 135831, 2019.