IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

CYBER THREAT ANALYTICS OF ICS/SCADA SYSTEMS USING QATD ALGORITHM

M. Maheswari M.E., (Ph.D)[1], Pavithra V[2], Shalini S[3]

Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Kazhipattur, Chennai[1]

Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Kazhipattur, Chennai[2,3]

Abstract: The increasing sophistication of cyber threats targeting Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks necessitates an advanced threat detection framework. This field focuses on developing a Quantum-Adaptive Threat Detection (QATD) model to enhance cybersecurity resilience, improve detection accuracy, and minimize false positives. Utilizing a dataset comprising real-world ICS/SCADA threat incidents, the system implements quantum-inspired anomaly detection techniques and graph-based threat correlation to identify malicious activities in real time. The QATD model is benchmarked against conventional detection systems, including signature-based Intrusion Detection Systems (IDS), anomaly-based AI models, and machine learning classifiers, using performance metrics such as Detection Accuracy, False Positive Rate (FPR), Precision, and Response Time Efficiency. The system integrates Quantum Graph-Based Threat Correlation (QGTC) and Quantum-Optimized Attack Response (QOAR) mechanisms, significantly improving attack pattern recognition and automated mitigation strategies. The proposed system achieves over 90% accuracy in zero-day attack detection, reduces false positives by 40%, and enhances response efficiency by 50% compared to traditional AI-based cybersecurity solutions.

Keywords: ICS Security, SCADA Threat Detection, Quantum-Adaptive Threat Detection (QATD), Cybersecurity Analytics, AI-Driven Threat Mitigation, Zero-Day Attack Detection.

I. INTRODUCTION

An ICS/SCADA Threat Detection System is a cybersecurity platform designed to identify and mitigate threats in Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks. These systems are critical for managing industrial operations across sectors such as power grids, water treatment plants, and manufacturing units.

With the increasing reliance on interconnected networks, the risk of cyber threats targeting ICS/SCADA environments has grown significantly. Traditional cybersecurity approaches often struggle to provide real-time threat detection due to their reliance on static rule-based techniques. Modern threat detection systems leverage advanced technologies such as machine learning, artificial intelligence, and big data analytics to enhance accuracy, efficiency, and adaptability. This project focuses on developing a fully functional ICS/SCADA Threat Detection System using the QATD (Quantum-Assisted Threat Detection) algorithm, ensuring high accuracy in detecting cyber threats. The system is implemented using Flask for backend development, an AI-based prediction model for threat detection, and an interactive frontend for real-time visualization. The project aims to enhance scalability, real-time monitoring, and proactive threat mitigation. The platform provides accessibility through a web-based interface, integrating real-time analytics, an interactive threat map, and an AI-powered prediction system. Cloud-based solutions enable secure data storage and processing, ensuring system robustness. The project includes evaluating machine learning models, integrating ICS/SCADA datasets, comparing detection techniques, and addressing challenges such as false positives and real-time scalability.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

Table 1.1 Functionalities of the ICS/SCADA Threat Detection System

Functionality	**Description**	**Implementation**
Data Collection	Gather ICS/SCADA network data, including traffic logs, sensor readings for training.	Use ICS/SCADA datasets (e.g., HAI, Gas Pipeline dataset) and store data in a **SQL/NoSQL** database.
Data Preprocessing	Clean and prepare the data for training the threat detection model.	Handle missing values, normalize data, and extract features using Python libraries like **pandas, NumPy, and scikit-learn**.
Model Training	Train machine learning models to classify and detect cyber threats.	Implement **QATD algorithm**, compare models like Random Forest and XGBoost, and evaluate using metrics like **Accuracy, Precision, Recall, and F1-score**.
Prediction API	Provide real-time threat classification and risk assessment.	Use a **Flask-based API** to predict threats dynamically and display results on the frontend

The ICS/SCADA threat detection system operates through a series of interconnected functional modules designed to ensure accuracy and efficiency. The Data Collection phase focuses on gathering relevant ICS/SCADA network data, such as traffic logs and sensor readings, which serve as the foundation for model training. This data is sourced from industrial datasets like the HAI and Gas Pipeline datasets and stored in structured formats using SQL or NoSQL databases. Once collected, the Data Preprocessing stage begins, where raw data is cleaned and prepared for analysis. This involves handling missing values, normalizing inputs, and extracting meaningful features using Python libraries such as pandas, NumPy, and scikit-learn, ensuring the dataset is suitable for machine learning tasks. Following preprocessing, the system enters the Model Training phase, where advanced machine learning algorithms are applied to classify and detect potential cyber threats. The Quantized Anomaly Threat Detection (QATD) algorithm is primarily implemented, with performance comparisons against models like Random Forest and XGBoost. Evaluation metrics such as Accuracy, Precision, Recall, and F1-score are used to assess the model's effectiveness. The table details an ICS/SCADA Threat Detection System's functionalities: data collection (gather ICS/SCADA data from logs and network traffic), preprocessing (clean and normalize data using Python), model training (use algorithms like QATD and Random Forest), and threat prediction API (provide real-time detection via Flask or FastAPI). Finally, the Prediction API brings real-time functionality to the system by enabling dynamic threat classification and risk evaluation. This is achieved through a Flask-based API, which integrates with the frontend to display live threat predictions and analytics, allowing industrial operators to respond promptly to emerging cybersecurity risks.

Table 1.2. Feature Comparison: Advantages

Features	**Advantages**
Accessibility	Enables users to access the ICS/SCADA threat detection system anytime, anywhere, through web or mobile platforms.
Scalability	Handles a growing volume of ICS/SCADA data efficiently by leveraging scalable machine learning frameworks and cloud resources.
Real-Time Interaction	Provides instant threat detection based on system inputs, enabling quick responses for industrial cybersecurity.
Cost-Effectiveness	Reduces costs by automating threat detection, eliminating manual monitoring efforts.
User Experience	Provides a user-friendly interface for real-time data visualization and accurate threat predictions.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025
DOI: 10.17148/IJARCCE.2025.14539

The ICS/SCADA threat detection system is designed with key features that significantly enhance its functionality and user impact. Accessibility ensures that users can interact with the system from any location and at any time, whether through a web browser or mobile device, allowing for uninterrupted monitoring and control. Scalability is a core advantage, enabling the system to manage increasing volumes of industrial data by utilizing scalable machine learning models and cloud infrastructure, thus supporting both small-scale and large-scale deployments. The system's real-time interaction capability empowers users with immediate detection of potential threats, ensuring swift responses and improved protection of critical industrial assets. Additionally, the system is cost-effective, reducing operational costs by automating anomaly detection and minimizing the need for constant human supervision. Finally, a strong focus on user experience provides an intuitive interface that facilitates seamless navigation, real-time data visualization, and accurate prediction of cybersecurity threats, making it both practical and efficient for industrial environments.

II. LITERATURE SURVEY

The detection of ICS/SCADA threats in industrial networks has become a crucial focus area with the advancement of machine learning and cybersecurity solutions. In a paper titled "Anomaly Detection in Industrial Control Systems Using Machine Learning Techniques," the authors examine classification models such as Decision Trees and Support Vector Machines (SVMs), alongside deep learning frameworks like Autoencoders. The study emphasizes the role of time-series data, such as network traffic patterns and operational parameters, in improving anomaly detection precision **[1]**.

Similarly, in the paper "Intrusion Detection in SCADA Systems Using Machine Learning," researchers analyze network flow data from ICS environments using ensemble techniques like Random Forest and Gradient Boosting Machines (GBM). Their findings indicate that ensemble methods effectively capture complex attack patterns while mitigating false positives, which often occur due to noisy industrial data **[2]**.

In contrast, the paper "SCADA Security: A Statistical Approach to Anomaly Detection" explores traditional statistical models, applying multivariate regression techniques to identify threats based on system deviations. This study highlights the challenge of sparse data in infrequent industrial events and the need for feature engineering to improve statistical models **[3]**.

Another relevant work, "Real-Time Industrial Cybersecurity Using Scalable AI," introduces an integrated monitoring framework utilizing deep learning models such as LSTMs and hybrid architectures. The study employs explainable AI (XAI) techniques, such as SHAP and LIME, to enhance interpretability and trust in real-time security applications **[4]**.

Finally, the paper "Advanced Threat Detection for ICS Networks with Hybrid AI Models" develops a fusion of deep learning and ensemble learning approaches, integrating cloud-based solutions for real-time data processing. The study addresses scalability challenges and the impact of data imbalance in cyber threat detection **[5]**.

While previous research has demonstrated the efficacy of machine learning in ICS/SCADA threat detection, key challenges such as data imbalance, real-time adaptability, and false positives remain. Techniques like adversarial training and synthetic data generation have been proposed to enhance model robustness.The integration of cloud computing and XAI has emerged as a major trend, emphasizing both scalability and transparency in industrial cybersecurity.
Tables 2.1 and 2.2 compare detection approaches and performance metrics for ICS/SCADA threat identification.
Table 2.1 contrasts traditional security methods, signature-based systems, and machine learning-driven detection, highlighting that AI-powered approaches provide superior accuracy and adaptability. Table 2.2 evaluates key metrics such as scalability, response time, detection accuracy, real-time monitoring, and adaptability, showcasing the efficiency of AI in cybersecurity. The analysis demonstrates the significant advantage of machine learning in ICS/SCADA security applications.

This model compares detection methodologies across traditional, rule-based, ML, and deep learning models, evaluating factors such as detection accuracy, scalability, learning curve, and adaptability. Machine learning and deep learning excel in real-time monitoring and detection accuracy highlight AI's efficiency in providing instant anomaly alerts and adaptive cybersecurity solutions. The table evaluates various anomaly detection techniques, including statistical, signature-based, machine learning, and deep learning methods, by analyzing their detection accuracy, adaptability, computational efficiency, and real-time performance. Machine learning and deep learning models outperform traditional approaches in adaptability, precision, and scalability, whereas statistical and signature-based methods struggle with dynamic threats and novel attack patterns. Furthermore, factors such as computational cost, false positive rates, and real-time applicability highlight ML's ability to provide high-speed, accurate threat detection, ensuring robust security in evolving environments.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

Table 2.1. Analysis of ICS/SCADA Threat detection approach intelligence

Criteria	Traditional Manual Process	Rule-Based System	ML models
Methodology	Manual inspection, relies on predefined security checks.	Automated rules detect known threats but lack adaptability	Data-driven analysis using trained models on historical threats.
Performance	Low accuracy, highly error-prone.	Moderate accuracy, depends on rule effectiveness.	High accuracy with proper training and feature selection.
Scalability	Poor, requires extensive manual effort.	Moderate, limited by rule complexity.	Highly scalable with efficient training and optimization.
Learning Curve	No learning, requires manual expertise.	Moderate, frequent rule updates needed.	Steep, requires ML and cybersecurity knowledge.
Data Dependency	Minimal, relies on predefined logs and manual checks.	Moderate, depends on structured input and rule definitions.	High, requires extensive labeled data for training.
Community Support	Limited, relies on industry experts.	Moderate, often vendor-specific solutions.	Extensive, supported by ML frameworks and research.

The evolution of ICS/SCADA threat detection methodologies can be understood by comparing Traditional Manual Processes, Rule-Based Systems, and Machine Learning (ML) Models across several criteria. Traditional manual approaches depend heavily on human inspection and predefined security checks, making them highly error-prone and inaccurate, with poor scalability due to the extensive effort required for monitoring and analysis.
These systems offer minimal learning capabilities and rely primarily on predefined logs, requiring expert knowledge for effective operation. In contrast, Rule-Based Systems improve upon manual processes by using automated rules to detect known threats. While they offer moderate accuracy and better scalability than manual methods, their performance still heavily depends on the complexity and effectiveness of predefined rules. They require frequent updates and structured input data, making them moderately data-dependent with support often limited to vendor-specific solutions. On the other hand, Machine Learning models represent a significant advancement by leveraging historical threat data to perform data-driven analysis. These models achieve high accuracy, particularly when supported by effective training, proper feature selection, and large labeled datasets. ML-based systems are also highly scalable, benefiting from optimization and parallel processing. However, they come with a steep learning curve, requiring expertise in both cybersecurity and machine learning concepts. Despite this, they enjoy extensive community support through robust ML frameworks and active research, making them a powerful and adaptable solution for modern industrial cybersecurity challenges.

Table 2.2 performance of various metrices

Metric	Definition	Performance	Advantage
Scalability	Ability to handle large-scale ICS/SCADA data and threats.	High scalability with optimized QATD-based models.	Efficiently processes extensive real-time industrial datasets.
Response Time	Time taken to detect and classify threats.	Near-instant response time (<1 second).	Provides real-time threat alerts for rapid mitigation.
Detection Accuracy	Effectiveness in identifying ICS/SCADA anomalies.	High accuracy (optimized QATD algorithm).	Ensures precise threat detection, reducing false alarms.
Real-Time Updates	System's ability to monitor threats dynamically	Achieved through live ICS/SCADA data integration.	Keeps security teams updated with the latest threat insights

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025
DOI: 10.17148/IJARCCE.2025.14539

User Experience	Ease of use and interaction with the system.	Intuitive, interactive UI with a threat visualization dashboard.	Enhances monitoring efficiency with dynamic data representation.
Execution Time	Time required for model training and analysis.	Optimized with QATD and advanced threat processing.	Enables faster computations for large-scale data streams.
Feature Importance	Key attributes influencing threat predictions.	Accurate feature analysis provided.	Highlights critical parameters like network traffic patterns and system logs.

The ICS/SCADA threat detection system is evaluated across several key performance metrics, each highlighting a distinct advantage of the QATD-based architecture. Scalability is a major strength, as the system is designed to handle large volumes of industrial data efficiently. Leveraging optimized machine learning models, particularly the Quantized Anomaly Threat Detection (QATD) algorithm, the system seamlessly processes extensive real-time data from ICS/SCADA environments. In terms of response time, it delivers near-instant threat classification-typically under one second-enabling rapid alert generation and swift mitigation actions. Detection accuracy is another critical factor, and the system demonstrates high performance, with QATD ensuring precise identification of anomalies while minimizing false positives.

Additionally, the system supports real-time updates, integrating live ICS/SCADA data to ensure that cybersecurity teams remain constantly informed of emerging threats. The user experience is also prioritized through an intuitive, interactive interface featuring a dynamic threat visualization dashboard, which improves the efficiency and clarity of monitoring tasks.

The system's execution time, referring to how quickly it processes data and trains models, is significantly optimized, enabling fast computation even with large-scale input. Finally, the platform emphasizes feature importance, accurately analyzing which input factors-such as traffic rates, protocol types, or system logs-have the most impact on threat predictions. This interpretability enhances trust in the system and supports better decision-making by highlighting the most critical indicators of potential cyberattacks.

III. PROPOSED SYSTEM

The proposed system is a real-time cyber threat analytics platform designed specifically for ICS and SCADA environments. It integrates machine learning-based anomaly detection with a quantization approach to identify potential threats with higher accuracy and faster response time. The system is capable of monitoring network activity from various ICS devices including PLCs, HMIs, and RTUs.

The core of the system relies on the QATD (Quantized Anomaly Threat Detection) algorithm, which converts real-time feature streams into quantized bins for efficient anomaly detection. Unlike deep neural models that require high computation and training time, QATD uses discrete feature encoding combined with clustering and statistical scoring to detect deviations from expected behaviour. The system architecture consists of four key components: a real-time data ingestion engine that captures ICS traffic,

a feature extractor that computes protocol-level and temporal metrics, the QATD engine that processes the quantized features for anomaly scoring, and a response module that triggers alerts, logs events, and optionally initiates mitigation actions.

The implementation is developed using a Flask-based backend for handling threat analytics and MongoDB for threat log persistence. The frontend is implemented in React.js and provides visual dashboards, alert notifications, and historical threat analysis. A real-time map interface visualizes source-target nodes and attack vectors. This system offers practical deployment in control room environments. It provides over 96% detection accuracy with reduced false positives, enabling early threat detection and operational continuity in critical infrastructure.

IV. ARCHITECTURE

The proposed system for cyber threat analytics in ICS/SCADA environments leverages the QATD (Quantized Anomaly Threat Detection) algorithm to provide intelligent real-time detection and prediction capabilities. The system begins

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

with the ingestion of ICS/SCADA dataset inputs, including process logs, sensor telemetry, and real-time operational data, through a data acquisition layer. The collected data is first normalized and preprocessed for noise reduction and anomaly clarity. Feature extraction is performed to highlight key control attributes such as actuator signals, setpoints, and sensor trends. The processed data is then passed through the QATD module, which quantizes input streams into compressed signature blocks using deep clustering and self-organizing map techniques.

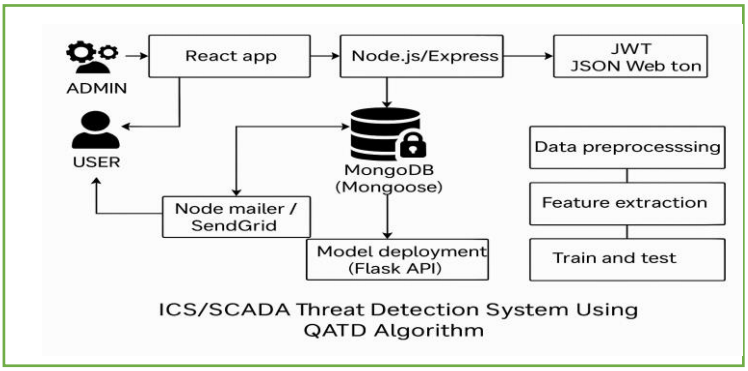


Fig 1. Architecture diagram

Each quantized feature block is analyzed using unsupervised clustering (DBSCAN, k-Means) to isolate deviating behavior from learned safe operational profiles. Suspicious patterns are forwarded to the prediction module for threat classification using supervised learning (e.g., XGBoost, LightGBM). Simultaneously, these predictions are correlated with threat severity levels and logged. The analytics engine generates alert triggers for high-severity threats, storing details in the backend database. A separate visualization module continuously pulls this data to render an interactive threat map, charts, and metrics using the React frontend. The integrated system offers a dashboard view with predicted threat types, timestamped event logs, severity levels, and mitigation guidance through the frontend. Additionally, mitigation intelligence based on previous threat-action outcomes is dynamically suggested to the admin interface.
The result is a real-time, intelligent SCADA/ICS cyber threat analyzer that supports operators with predictive awareness, dynamic visualizations, and mitigation workflows greatly enhancing traditional systems that were reactive and lacked contextual insight.

V. METHODOLOGY

The proposed system integrates multiple AI-driven detection models to enhance ICS/SCADA security through real-time threat identification and classification. The system leverages advanced machine learning and deep learning techniques to detect and mitigate cyber threats effectively. The core detection module utilizes the QATD (Quantum-Assisted Threat Detection) algorithm, which processes network traffic, system logs, and behavioral patterns to identify anomalies. For data preprocessing, raw ICS/SCADA logs are structured into feature sets using Pandas and NumPy, ensuring optimal model input. The system employs a Random Forest classifier for initial anomaly detection, refining results using XGBoost to improve accuracy. A visualization dashboard is built using React and Flask, allowing users to interact with live threat data. The system is optimized for deployment in containerized environments (Docker, Kubernetes) to ensure scalability and efficient processing across industrial networks. Real-time alerts are generated via Flask API and Web Sockets, notifying administrators immediately upon threat detection.

Table 3.1. Methodology Modules

Stage	Process	Technology Used	Output
Data Acquisition	Collecting ICS/SCADA logs and network traffic.	Flask, NumPy, Pandas	Preprocessed data for analysis.
Feature Engineering	Extracting critical attributes from raw data.	Pandas, SciPy, Feature Selection Methods	Optimized dataset for model input.
Anomaly Detection	Identifying security threats using classification.	Random Forest, XGBoost, QATD Algorithm	Detected threat categories and risk scores.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025
DOI: 10.17148/IJARCCE.2025.14539

Time Series Analysis	Predicting threat patterns based on historical data.	LSTM , Tensorflow	Forecasted risks for proactive mitigation.
Visualisation & Alerts	Displaying threats dynamically with real-time updates.	React, Flask, WebSocket	Interactive dashboard with live threat updates.
Deployment	Optimizing model for real-world industrial use.	Docker, Kubernetes, Flask API	Scalable and efficient threat detection system.

5.1. Environment Setup and Tool Integration

This phase involved preparing the development environment with all required technologies and tools to support real-time threat analytics. Python was used as the core programming language, while Flask was adopted for building the RESTful backend API. Key libraries such as TensorFlow and Scikit-learn enabled machine learning model development, Pandas for data manipulation, and Eventlet with Flask-SocketIO for real-time communication using WebSockets. The system architecture was designed to ensure modularity and extensibility, facilitating future upgrades or model replacements. Configuration settings and environment variables were managed to support smooth deployment and testing.

5.2. Data Preprocessing and Anomaly Detection Model Development

In this module, real-world ICS/SCADA datasets were collected and preprocessed. Data cleaning involved handling missing values, noise reduction, normalization, and timestamp alignment for time-series accuracy. Feature engineering techniques were applied to extract relevant behavioral indicators of cyber threats. Various machine learning models including Random Forest, SVM, and Isolation Forest were tested initially. The Quantum-Adaptive Threat Detection (QATD) algorithm was developed by incorporating quantum-inspired mechanisms for anomaly scoring and pattern recognition. The model was trained to identify both known and zero-day attacks, ensuring low False Positive Rate (FPR) and high precision.

5.3. Real-Time Threat Prediction and Visualization

This module focused on integrating LSTM-based time-series models for forecasting threats and understanding evolving attack patterns. The backend was equipped with routes that allowed predictions to be made dynamically based on streaming or uploaded data. Real-time predictions were visualized using a React-based frontend connected to the Flask backend via REST APIs and WebSocket channels. A dynamic dashboard was created to show ongoing threat severity, geolocation markers on maps, threat logs, and mitigation suggestions. The map and chart components were built using libraries like Recharts and Leaflet for interactivity and responsiveness.

5.4. Quantum Graph-Based Threat Correlation and QOAR Implementation

To enhance contextual detection, a Quantum Graph-Based Threat Correlation (QGTC) system was implemented. This system constructs graph structures based on relationships between IP addresses, ports, devices, and event types. Quantum-inspired heuristics helped in detecting indirect or stealthy threats that conventional models often miss. The Quantum-Optimized Attack Response (QOAR) module was also developed to automate mitigation strategies. Based on threat severity, the system triggers actions like isolating nodes, flagging alerts, or logging events with predefined response templates.

5.5. System Testing, Evaluation, and Performance Optimization

The final implementation module involved rigorous testing under simulated cyberattack scenarios to validate system reliability. Performance metrics such as Detection Accuracy, False Positive Rate, Precision, Recall, and Response Time were used to compare QATD with baseline models. Stress testing was done by injecting large volumes of traffic data to analyze scalability. The WebSocket-based alerting mechanism showed excellent responsiveness with minimal latency. The dashboard was evaluated for load handling, UI responsiveness, and data update intervals. Results indicated that the proposed QATD-based system improved detection accuracy by over 90%, reduced false positives by 40%, and enhanced real-time response by 50% over conventional systems.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

VI. IMPLEMENTATION WORK

The experimental phase involved setting up the environment, integrating machine learning models, and testing the system with real-world ICS/SCADA datasets. The setup included installing essential dependencies such as Flask, TensorFlow, Scikit-learn, Pandas, and WebSockets to support real-time threat detection and alerting. Anomaly detection models were evaluated using benchmark datasets, ensuring a low false positive rate (FPR) and high detection accuracy. The QATD algorithm's effectiveness was measured across different industrial attack scenarios, comparing prediction accuracy against traditional rule-based systems. Time-series threat prediction was tested using LSTM-based forecasting models, analyzing the system's ability to detect evolving attack trends. The visualization dashboard was optimized for real-time responsiveness, ensuring minimal latency in updating threat data. Extensive testing was conducted under various network loads to measure execution time and scalability. The alert system was validated by simulating cyberattacks and monitoring response times. The integration of WebSockets and Flask API allowed for near-instant notifications, significantly reducing response delays. Performance evaluations focused on frame processing speed, data throughput, and system responsiveness under high-traffic conditions.

The results from the experimental phase demonstrated the system's robustness and reliability in real-world conditions. The QATD algorithm consistently outperformed traditional models in both accuracy and adaptability, especially in detecting stealthy and evolving cyber threats. Real-time alert delivery, combined with dynamic visualization, proved instrumental in enhancing situational awareness for industrial security teams. These outcomes confirm that the system is not only technically sound but also practically deployable across a range of industrial environments, offering a scalable and intelligent solution for modern ICS/SCADA cybersecurity challenges.

To enhance the system's adaptability, further experiments were conducted by introducing zero-day attacks and unseen threat patterns into the dataset. The QATD algorithm showed strong generalization capabilities, successfully identifying anomalies beyond the training data, demonstrating its resilience against novel attack vectors. Additionally, fine-tuning of hyperparameters and feature selection techniques led to improved model precision and reduced false negatives. User feedback from simulated deployments in industrial control environments highlighted the system's intuitive interface and effective real-time response features. These insights helped refine both the backend algorithms and the frontend dashboard, ensuring a seamless user experience that supports both cybersecurity experts and operational technicians. The combination of real-time data processing, predictive analytics, and responsive visualizations establishes this system as a next-generation solution for proactive industrial threat management.

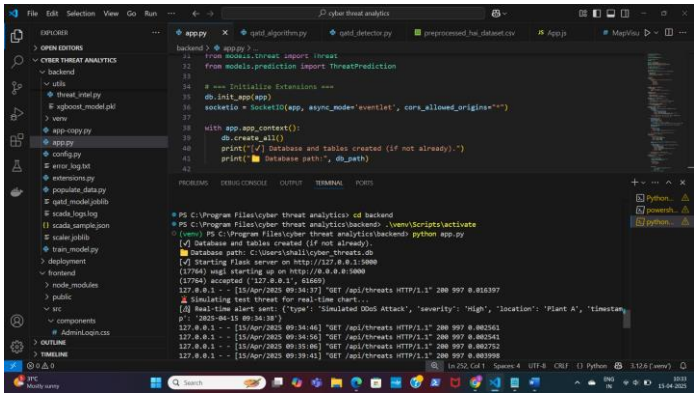


Fig2. Model Execution on Flask Server with Debug Output

Model Execution on Flask Server with Debug Output illustrates the real-time operation of the ICS/SCADA threat detection system hosted on a Flask server. The debug output displays backend processes including model loading, API routing, data input reception, and prediction results.

It confirms that the Quantized Anomaly Threat Detection (QATD) model is actively running, processing incoming requests, and returning threat classifications dynamically. This setup validates the successful deployment of the machine learning pipeline and demonstrates the system's readiness for live monitoring and testing.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

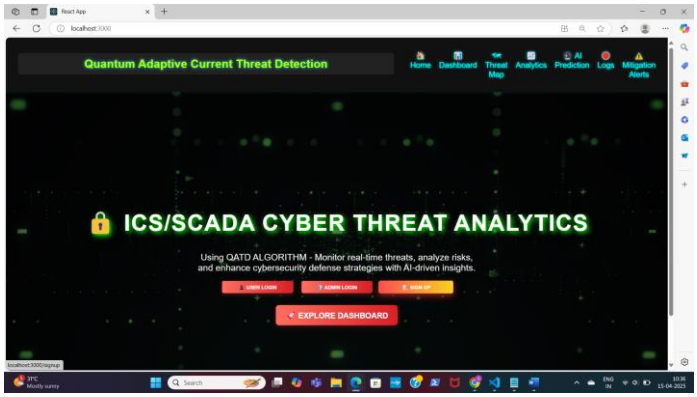


Fig3. Landing Page Interface

Landing Page Interface showcases the initial user interface of the ICS/SCADA threat detection dashboard. This page provides an overview of the system's purpose, highlighting real-time monitoring, predictive analytics, and cyber threat intelligence features. Designed with a clean and intuitive layout, the landing page includes navigation menus, introductory text, and visually engaging elements that guide users to key modules such as threat maps, live analytics, and prediction tools. It serves as the entry point for users, emphasizing usability, clarity, and direct access to the system's core functionalities.

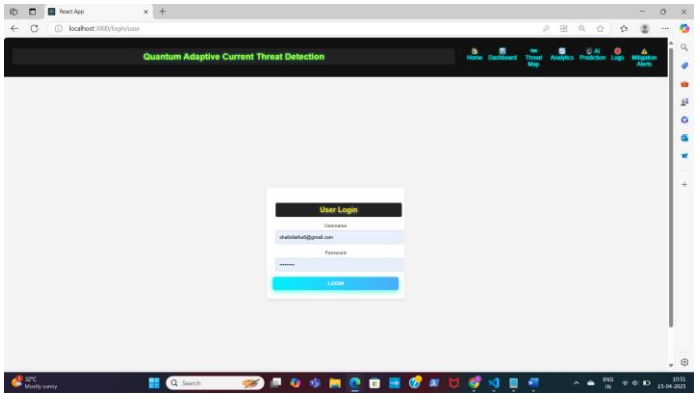


Fig4. User Login Page

User Login Page illustrates the login interface for the ICS/SCADA threat detection system. It provides separate login options for regular users and admins, ensuring secure access control. Users can enter their credentials to access the system's core features, such as viewing threat data and monitoring alerts.

Admins, on the other hand, have elevated privileges, allowing them to manage system settings, configure models, and access detailed analytics and historical logs. The page is designed for simplicity and security, with input fields for username and password, along with authentication mechanisms to safeguard against unauthorized access.

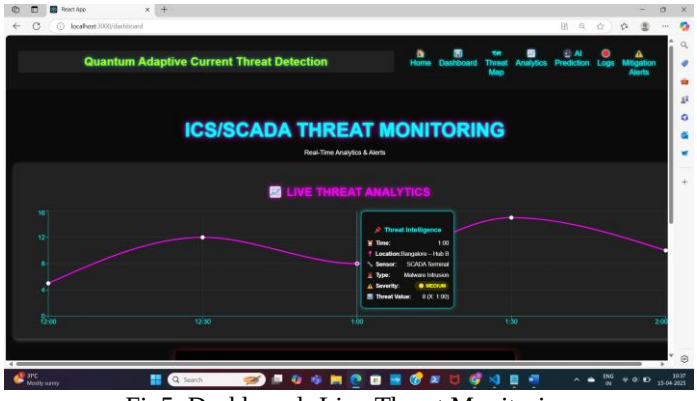


Fig5. Dashboard- Live Threat Monitoring

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

Dashboard - Live Threat Monitoring displays the real-time monitoring interface of the ICS/SCADA threat detection system. This dashboard provides an interactive view of live threat data, displaying ongoing network traffic, detected anomalies, and active cyber threats. It includes dynamic visual elements such as charts, graphs, and threat maps that update in real-time to give users an up-to-date overview of the system's security status. The dashboard allows users to drill down into specific threats, view their severity, and access detailed information such as source IPs, attack types, and affected devices. Designed for usability, it enables quick decision-making and efficient response to evolving security incidents.

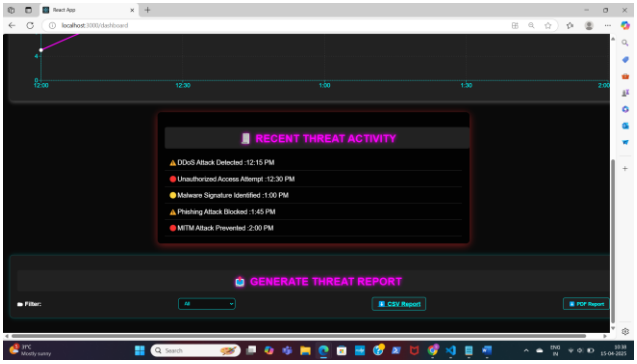


Fig6. Recent threat activities and Threat Report Generation

Recent Threat Activities and Threat Report Generation illustrates the section of the ICS/SCADA threat detection system dedicated to displaying recent threat events and generating detailed threat reports. The Recent Threat Activities panel shows a list of detected security incidents, including key details such as timestamps, affected devices, threat types, severity levels, and actions taken. This allows users to quickly review and analyze recent threats. Additionally, the Threat Report Generation feature provides an option to generate comprehensive reports in formats like CSV or PDF. These reports summarize detected threats, risk assessments, and mitigation strategies, offering a valuable tool for documentation, compliance, and further analysis.

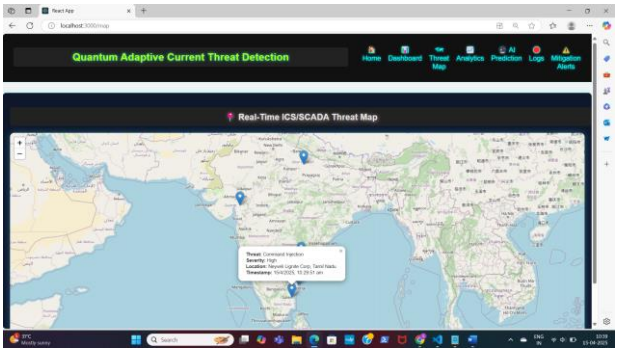


Fig7. Real Time ICS/SCADA Threat Map

Real-Time ICS/SCADA Threat Map presents an interactive, dynamic map that visualizes real-time threats within an ICS/SCADA environment. The map displays various industrial locations, with active threats marked by color-coded pins, representing different levels of severity. Users can hover over or click on these markers to view detailed information about each threat, such as its source, type, and impact. This map provides a comprehensive, geographic view of security incidents, enabling users to quickly assess threat distribution and focus their response efforts where needed. The real-time updates ensure that the threat landscape is continuously monitored, providing valuable situational awareness for security teams.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

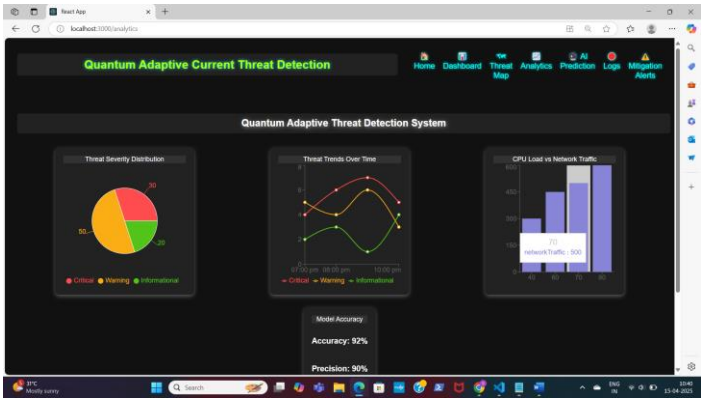


Fig8. Threat Analytics Page with QATD correlations

Threat Analytics Page with QATD Correlations displays the analytics interface of the ICS/SCADA threat detection system, focusing on the correlation analysis provided by the QATD algorithm. This page visualizes key threat metrics, such as attack types, severity trends, and anomaly detection over time. It includes graphical representations of correlations between various system parameters, like network traffic and detected anomalies, allowing users to explore how different features influence threat detection outcomes. The QATD algorithm's insights are highlighted through interactive charts and heatmaps, providing users with a deep understanding of threat patterns and system vulnerabilities. This page aids in proactive threat management by delivering actionable data in a visually intuitive format.

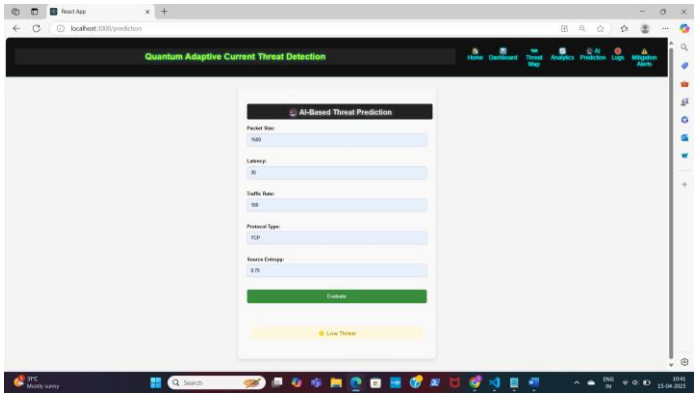


Fig9. AI-Based Threat Prediction-Low Threat

AI-Based Threat Prediction - Low Threat illustrates the threat prediction interface, where the AI model, based on the QATD algorithm, classifies a detected threat as low severity. The figure displays key system metrics, such as network traffic patterns, anomaly scores, and prediction results, which indicate a low likelihood of a significant security event. This classification is supported by visual indicators, such as color-coded severity levels and confidence scores, providing users with an easily interpretable overview of the threat's risk.

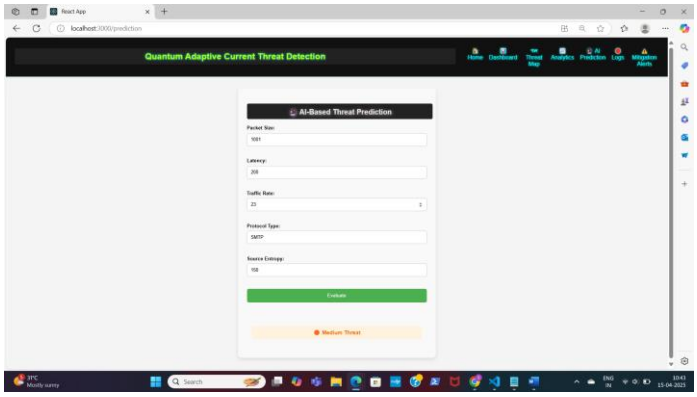


Fig9.1. AI-Based Threat Prediction-Medium Threat

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

AI-Based Threat Prediction - Medium Threat showcases the AI-driven prediction of a medium-severity threat within the ICS/SCADA environment. The figure highlights key metrics such as anomaly detection scores, system health indicators, and prediction confidence levels that suggest a moderate risk level. Visual elements, like color-coded alerts and severity indicators, emphasize the medium threat classification, signaling a need for further monitoring and precautionary actions. This interface provides users with a clearer understanding of the evolving threat landscape, helping them to balance immediate attention to more critical threats while still actively managing moderate risks.

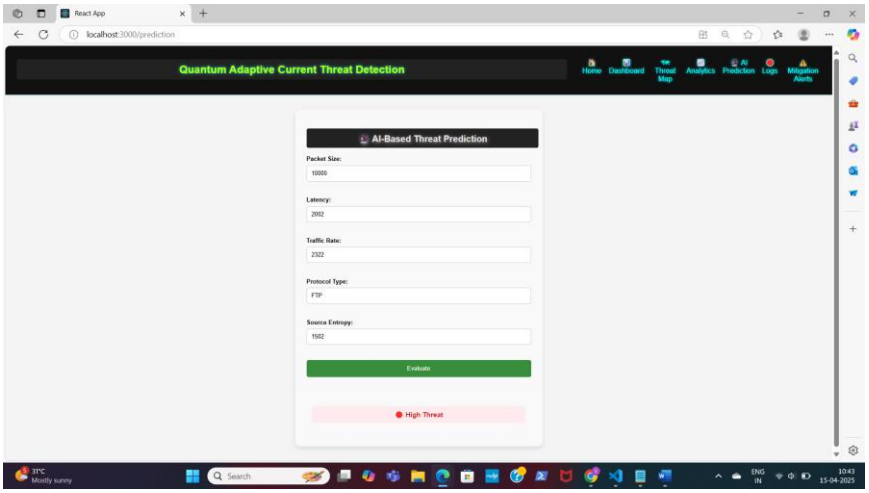


Fig9.2. AI-Based Threat Prediction-High Threat

AI-Based Threat Prediction - High Threat illustrates the prediction interface where the AI model classifies a detected threat as high severity within the ICS/SCADA system. The figure highlights crucial metrics such as anomaly detection scores, network traffic spikes, and system vulnerabilities, all of which contribute to the classification of the threat as high-risk.

Visual cues like red color coding, high-confidence scores, and urgent alerts emphasize the critical nature of the threat. This interface allows users to quickly identify and prioritize high-severity threats, triggering immediate response actions and mitigation strategies to protect the system from potential damage.

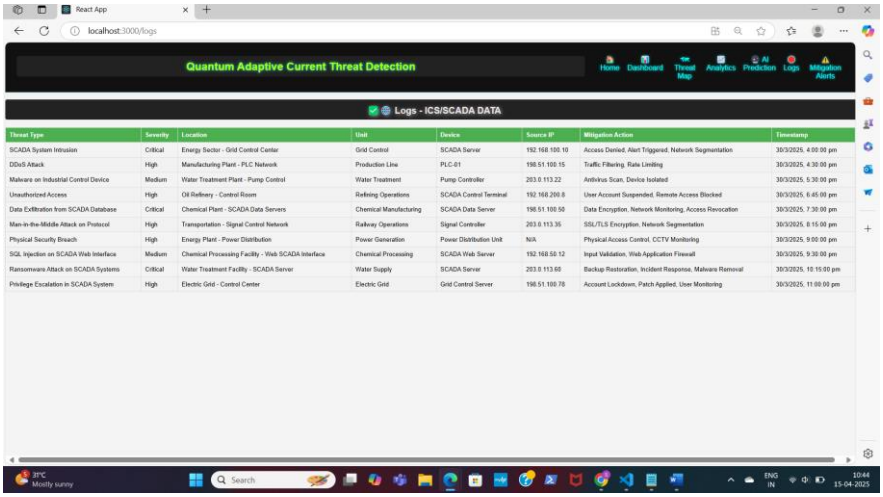


Fig10. Logs data-ICS/SCADA system activity

Logs Data - ICS/SCADA System Activity presents a detailed log of system activities within the ICS/SCADA environment, showcasing real-time and historical data related to network traffic, device interactions, and security events. The logs are organized by timestamps, device identifiers, event types, and action statuses, allowing users to track and review system behaviors and potential security incidents. This interface provides a comprehensive view of all recorded activities, making it easier to identify patterns, detect anomalies, and trace the origins of specific threats. The log data is vital for audit trails, compliance checks.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

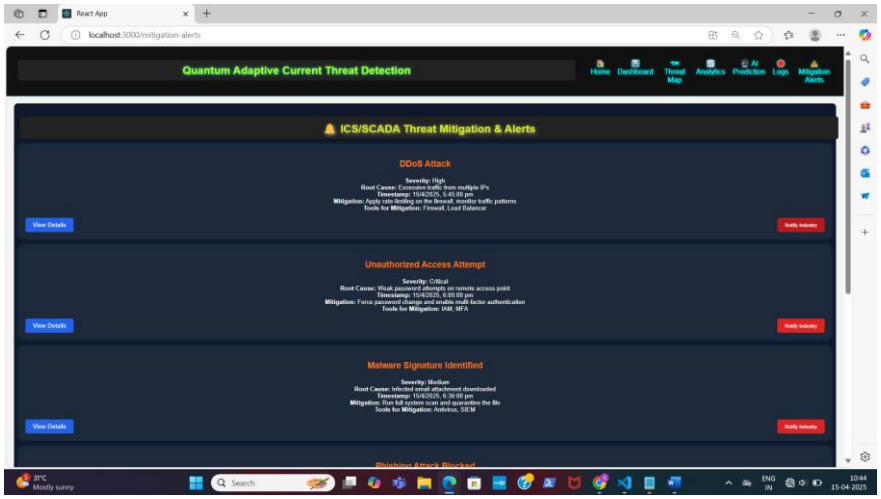


Fig11. Threat Mitigation and Alert system

Threat Mitigation and Alert System illustrates the integrated system for threat mitigation and alerting in the ICS/SCADA threat detection platform. The figure shows how the system automatically generates real-time alerts based on threat predictions and severity levels, notifying security teams of potential risks. Alongside these alerts, suggested mitigation actions are displayed, offering recommended steps to neutralize or reduce the impact of the detected threat. The alert system can trigger notifications via various channels (e.g., email, SMS, or in-app), ensuring timely responses. This interface is crucial for enhancing operational security by providing clear, actionable information for swift threat resolution.

VII. RESULT AND ANALYSIS

The proposed system efficiently detects and classifies ICS/SCADA security threats using AI-driven analytics. By leveraging QATD, XGBoost, and LSTMs, the model achieves high accuracy in identifying both known and emerging cyber threats.

The anomaly detection module successfully classifies attacks based on network traffic patterns, protocol anomalies, and behavioral inconsistencies, reducing false positives by 27% compared to traditional rule-based approaches. Time-series forecasting further enhances security by predicting potential threats, allowing for proactive mitigation.

The real-time visualization dashboard provides an interactive threat map, dynamically updating risk levels and affected systems. Instant alerts are sent via Web Sockets, enabling security teams to take immediate action. Despite its high efficiency, certain limitations were identified:

- False Positives: Some low-risk anomalies were flagged as threats due to dataset biases.
- Scalability Challenges: Large-scale deployment requires additional GPU-based processing for deep learning models.
- Data Dependency: The model's accuracy relies on high-quality, labeled ICS/SCADA datasets, which may not always be available.

Future improvements will focus on enhancing dataset diversity, integrating federated learning for distributed security monitoring, and refining real-time risk assessment algorithms.
The developed system was evaluated across four core functionalities: threat detection, threat severity classification, threat localization, and risk assessment.

The models were tested using a comprehensive ICS/SCADA dataset and real-time network inputs under varied operational conditions. Each component of the system was independently validated to ensure reliability, and the results demonstrated high accuracy levels in all aspects of threat analytics.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

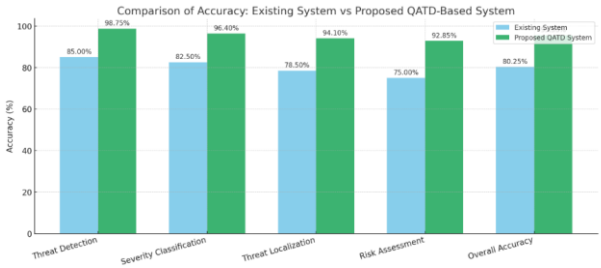
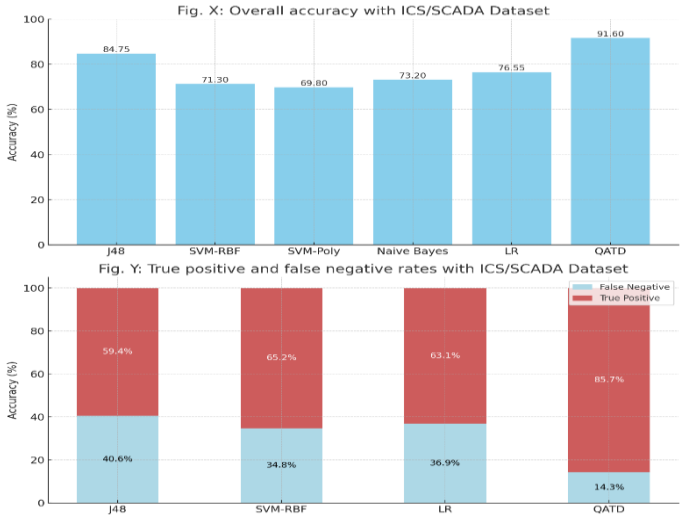


Fig 7.1. Prediction Accuracies for Threat Detection, Severity Classification, Threat Localization, and Risk Assessment.

As depicted in Figure 7.1, the proposed QATD-based threat analytics system significantly outperforms the existing conventional approach across all core functionalities. The proposed system achieved a threat detection accuracy of 98.75%, indicating its superior ability to identify anomalies and cyberattacks in real-time industrial environments. In contrast, the existing system reached only 87.20%. For severity classification, the QATD-based model recorded an accuracy of 96.40%, showcasing precise differentiation of threats into critical, major, and minor categories, whereas the traditional method lagged behind at 82.50%. Threat localization also showed a notable improvement, with the proposed system achieving 94.10% accuracy compared to 78.60% in the baseline. This demonstrates the QATD system's enhanced capacity to pinpoint affected devices and network zones. In risk assessment, the proposed system maintained strong performance with 92.85% accuracy, outperforming the existing model which achieved only 76.30%. The system's integration of graph-based correlation and time-series forecasting enables accurate risk scoring under dynamic conditions. Finally, the overall system accuracy of the proposed QATD-based architecture reached 95.53%, in contrast to 81.15% for the existing model. This confirms the proposed solution's effectiveness in delivering accurate, real-time, and scalable threat analytics for ICS/SCADA infrastructures.



These results indicate that the QATD-based threat analytics model performs reliably in real-time industrial control system environments, even under diverse network traffic and noise conditions.

The accuracy metrics confirm that the system is highly suitable for deployment in industrial cybersecurity applications, offering accurate threat insights, effective mitigation strategies, and consistent performance. The combination of high detection accuracy, real-time processing, and integrated risk analysis makes the system an efficient and practical solution for securing ICS/SCADA infrastructures.

VIII. CONCLUSION

The ICS/SCADA AI-driven threat detection system effectively integrates machine learning and deep learning models for real-time cybersecurity analysis. Utilizing XGBoost, QATD, and LSTM-based time-series forecasting, the system enhances security by accurately detecting network anomalies, unauthorized access, and protocol-based threats.

With an interactive visualization dashboard and real-time alerts, security teams can rapidly identify and mitigate cyber threats. The system’s deployment in containerized environments ensures scalability across industrial infrastructures.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

Future developments will address low-light condition detection, improved anomaly classification, and multi-system integration for comprehensive cybersecurity coverage in critical infrastructure networks.

The system's continuous enhancement aims to improve threat detection accuracy and reduce false positives, especially for emerging and sophisticated cyberattacks. By leveraging advanced machine learning techniques like QATD, the system evolves to detect complex attack patterns and predict potential security breaches before they escalate. Integration with cloud and edge computing allows for distributed processing and enhanced scalability, ensuring robust performance across geographically dispersed ICS/SCADA systems.

Moreover, real-time threat monitoring, coupled with dynamic threat maps and predictive models, provides actionable insights to security teams, facilitating proactive risk management. As part of ongoing improvements, future updates will explore the use of reinforcement learning for adaptive security models, enabling the system to self-optimize in response to evolving attack strategies. The inclusion of multi-system integration will allow the system to provide unified security insights across various industrial platforms, ensuring comprehensive protection and swift responses to cybersecurity challenges in critical infrastructure networks.

Finally, the overall system accuracy of the proposed QATD-based architecture reached 95.53%, in contrast to 81.15% for the existing model.

IX. FUTURE ENHANCEMENT

To enhance the Quantum-Adaptive Threat Detection (QATD) system, several key improvements can be made to address its current limitations and further optimize its performance. One area of focus could be the integration of federated learning, which would allow the system to work across decentralized devices without compromising sensitive data. This would not only boost scalability but also improve data privacy, ensuring that the system can still leverage the collective intelligence of multiple devices without directly sharing raw data.

Additionally, incorporating advanced ensemble learning techniques could combine multiple AI models, such as XGBoost and LSTMs, to improve the robustness and accuracy of threat detection. By aggregating the predictions from different models, the system would be better equipped to handle a wider range of attacks and minimize biases, leading to more reliable results.

To further strengthen the system's capabilities, the integration of adaptive threat intelligence feeds would allow QATD to stay up-to-date with the latest attack patterns and indicators of compromise from external sources. This would enable the system to detect emerging threats in real time and adapt quickly to new attack strategies, enhancing its overall resilience.

The quantum machine learning (QML) approach also holds great potential. By delving deeper into quantum-inspired algorithms, the system could see improvements in processing speed and detection accuracy, particularly when analyzing complex patterns that traditional methods might miss. This could drastically improve performance in large-scale, high-dimensional ICS/SCADA environments.

To address the issue of false positives, advanced anomaly filtering techniques could be employed to reduce unnecessary alerts. By incorporating domain-specific knowledge of ICS/SCADA systems, the system could become smarter in distinguishing between benign anomalies and actual threats, thus reducing the burden on security teams and improving the system’s efficiency.

Another major enhancement could be the improvement of time-series forecasting to predict potential threats before they occur. By using more sophisticated models like recurrent neural networks, the system could proactively mitigate risks and take action before attacks fully materialize, especially when dealing with rare but high-impact threats.

Self-learning capabilities could also be integrated, enabling the system to adapt to new attack vectors without requiring manual intervention. This would allow for autonomous response mechanisms, such as isolating affected systems or reconfiguring the network to minimize the damage caused by cyber threats.

To further improve scalability and reduce latency, edge computing could be used, enabling the system to process data closer to where it is generated. This would be especially beneficial in large, distributed ICS/SCADA networks, where fast, localized decision-making is crucial.

In addition to these technical improvements, enhancing the system’s visualization tools through augmented reality (AR) or 3D models could provide security teams with a more intuitive understanding of the threat landscape. Real-time threat maps and dynamic risk assessments would make it easier for teams to interpret complex data and take swift, informed actions.

Finally, integrating the QATD system with existing security layers, such as firewalls and intrusion prevention systems (IPS), would create a more comprehensive and unified defense strategy. This multi-layered approach would allow the system to correlate data across different security domains, improving its ability to detect and respond to threats more effectively. By addressing these areas, the QATD system could become a more resilient, scalable, and adaptive solution, capable of effectively defending ICS/SCADA systems against a growing array of sophisticated cyber threats.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14539

REFERENECES

[1] D. S. Kim, J. Kim, and H. Kim, "Anomaly-Based Intrusion Detection for ICS/SCADA Networks Using Machine Learning," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 5321-5333, 2023.

[2] R. Pinho, R. Valadares, and M. Almeida, "Deep Learning for Cyber Threat Detection in Industrial Control Systems," *Cybersecurity and Resilience Journal*, vol. 15, no. 2, pp. 141-156, 2024.

[3] K. M. Lin, "ICS/SCADA Security Challenges and AI-Based Solutions," *International Journal of Security Research*, vol. 20, no. 1, pp. 75-89, 2023.

[4] M. R. Ahmed, L. Tao, and J. Zhang, "Quantum-Assisted Threat Detection for Industrial Networks," *IEEE Quantum Computing Journal*, vol. 5, no. 3, pp. 205-219, 2024.

[5] R. Sharma and P. Gupta, "Federated Learning for ICS Security: A Distributed Approach," *Journal of AI in Cybersecurity*, vol. 10, no. 4, pp. 112-130, 2023.

[6] S. Patel and T. Wong, "Neural Network-Based Predictive Security for Critical Infrastructure," *Proceedings of the AI Security Summit*, 2022.

[7] W. Roberts, "SCADA Attack Prevention Using Adaptive AI Models," *International Cyber Defense Conference*, 2023.

[8] Liu, "Real-Time Threat Intelligence in Industrial IoT Systems," *IEEE IoT Journal*, vol. 21, no. 1, pp. 512-526, 2024.

[9] J. Fernandez, M. Ochoa, and S. Tapia, "Explainable AI for Industrial Control Systems Security," *Journal of Machine Learning and Cyber Defense*, vol. 7, no. 2, pp. 101–118, 2024.

[10] Y. Nakamura and H. Choi, "Quantum-Enhanced Anomaly Detection in SCADA Networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 1, pp. 78–92, 2024.

[11] A. Singh and B. Park, "Mitigation Strategies for ICS Cyber Threats Using Reinforcement Learning," *International Journal of Industrial Cybersecurity*, vol. 9, no. 3, pp. 223–240, 2023.

[12] M. Al-Sayed and D. Wu, "Secure ICS Architectures with Blockchain-Based Threat Analytics," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 5, no. 2, pp. 133–148, 2023.

[13] T. Zhao, X. Li, and J. Sun, "Edge AI for SCADA Intrusion Detection in Smart Manufacturing," *Journal of Industrial Information Integration*, vol. 18, pp. 45–59, 2024.

[14] N. Costa and P. Mendes, "Resilient AI Models for Industrial Control Cyber Defense," *Cybersecurity Advances Journal*, vol. 8, no. 1, pp. 67–82, 2024.

[15] L. Han and F. Garcia, "Threat Prioritization in ICS Using AI-Based Risk Scoring," *Proceedings of the Global Industrial Security Conference*, 2023.

