Электронное научное издание «Устойчивое инновационное развитие: проектирование и управление»
www.rypravlenie.ru **том 21 № 1 (66), 2025, ст. 3**

УДК 004.056.5+004.78+621.316

АДАПТИВНАЯ ОБЛАЧНАЯ СИСТЕМА АНАЛИТИКИ БЕЗОПАСНОСТИ ДЛЯ ПРОМЫШЛЕННЫХ ЭНЕРГЕТИЧЕСКИХ СИСТЕМ: МЕТОД МНОГОКЛАССОВОЙ ДЕТЕКЦИИ

Заитер Муродж, аспирант, Базовая кафедра «Аналитика больших данных и методы видеоанализа», Уральский федеральный университет

Аннотация

Рост уровня цифровизации энергетических систем в промышленных компаниях привёл к появлению новых уязвимостей в кибербезопасности, требующих применения сложных систем обнаружения. В данной работе предлагается адаптивная облачная система для классификации и обнаружения различных событий в энергетической системе, включая кибератаки, природные неисправности и штатные режимы работы. Разработана система многоклассовой детекции на основе данных с фазометрических измерительных устройств (ФИУ) и системных журналов для конфигурации энергосистемы с двумя линиями и четырьмя реле. Предложенная модель позволяет идентифицировать 37 различных сценариев, включая природные события, кибератаки и нормальные режимы, благодаря 128 признакам, извлечённым из измерений ФИУ и журналов системы. Наш подход достигает общей точности 97% в распознавании различных событий в энергосистеме, при этом наилучшие результаты получены при выявлении атак с внедрением команд (в среднем 98% точности) и атак с изменением настроек реле (95% точности). Модель продемонстрировала устойчивость к различным местоположениям неисправностей и сценариям атак, показывая высокие показатели точности и полноты даже в сложных многорелейных атаках. Анализ значимости признаков позволил выделить ключевые измерения для обнаружения атак, особенно модули фазовых напряжений и углы фаз напряжения, что способствует более эффективному мониторингу безопасности энергетических систем. Облачная реализация обеспечивает обработку данных ФИУ в режиме реального времени и оперативное выявление атак, что делает систему пригодной для промышленного внедрения. Модель показывает 100% точность в распознавании штатных режимов и высокую точность при обнаружении неисправностей в различных секциях линий электропередачи. Полученные результаты подтверждают, что предложенный подход способен чётко различать природные неисправности и злонамеренные атаки и может использоваться в качестве надёжной системы мониторинга безопасности промышленных энергетических систем.

КЛЮЧЕВЫЕ СЛОВА: кибербезопасность энергетических систем, облачные вычисления, обнаружение кибератак, машинное обучение, фазометрические измерительные устройства, промышленные системы управления, многоклассовая классификация, мониторинг в реальном времени, промышленные предприятия, адаптивная аналитика безопасности.

ADAPTIVE CLOUD-BASED SECURITY ANALYTICS FOR INDUSTRIAL POWER SYSTEMS: A MULTI-CLASS DETECTION APPROACH

Zaiter Murooj, postgraduate, Dept. of Big Data Analytics and Video Analysis Methods, Ural Federal University

Abstract

The increasing digitalization of power systems in industrial companies has introduced new cybersecurity vulnerabilities that require sophisticated detection systems. This work suggests a cloud-based adaptive system to classify and detect various power system events, including cyber-attacks, natural faults, and normal operations. We design a multi-class detection system based on Phasor Measurement Units (PMUs) data and the system logs on a two-line, four-relay power system configuration. The proposed model can identify 37 different scenarios, including natural events, cyber-attacks, and normal operations, thanks to 128 features extracted from PMU measurements and system logs. Our approach achieves 97% overall accuracy in distinguishing between various power system events, with the best performance in identifying command injection attacks (with an average of 98% precision) and relay setting change attacks (95% precision). The model is demonstrated to be robust for different fault locations and attack scenarios, with high precision and recall rates even for complex multi-relay attacks. With feature importance analysis, we identify key measurements for attack detection, particularly phase magnitude measurements and voltage phase angles, for more efficient *monitoring of power system security. Cloud deployment facilitates real-time processing of PMU data and quick detection of attacks, making it suitable for deployment at an industrial level. The model performs with 100% accuracy in identifying normal operations and high accuracy in detecting faults in various sections of the transmission line. The results confirm that our approach can distinctly classify natural faults and malicious attacks and can be used as a reliable security monitoring system for industrial power systems.*

KEYWORDS: power system security, cloud computing, cyber-attack detection, machine learning, phasor measurement units, industrial control systems, multi-class classification, real-time monitoring, industrial enterprises, adaptive security analytics.

1. Introduction

The rapid digital revolution of industrial power systems has offered unparalleled potential for increased efficiency and control, but it has also introduced staggering cybersecurity challenges. [1][2] Power systems, particularly those involving Intelligent Electronic Devices (IEDs) and Phasor Measurement Units (PMUs), have been increasingly subject to sophisticated cyber-attacks. Power systems form the critical infrastructure in industrial processes, where even an interruption can lead to significant economic losses and risks to safety. [3]

There is always a need for conventional security measures, but they are often insufficient to detect and categorize the range of possible threats to modern power systems.

Recent attacks have demonstrated that attackers can control power system components in a manner that is difficult to distinguish from normal faults or normal operations. [4] This is particularly evident in distance protection schemes in systems, where attackers can exploit the absence of internal verification to trigger a false breaker operation. The complexity of such attacks and the need for rapid detection make it necessary to develop advanced, smart security solutions that can leverage the scale and processing power of cloud computing.[5]

This work proposes a cloud computing adaptive framework for power system security against these challenges through a multi-class detection approach. Our suggested method processes data from four PMUs measuring a two-line power system structure, processing 128 distinct features to identify and classify 37 different scenarios, including natural events, cyber-attacks, and nominal behavior. Cloud deployment of the framework enables it to process real-time handling of large amounts of PMU data while providing the ability to adapt to emerging threat patterns.

2. Related Work

Nafiseh Soveizi and Fatih Turkmen [6] examine security and privacy concerns in scientific and business procedures in cloud environments, and they conclude that there are research gaps. Based on their examination, most security methods consider the modelling and execution phases and fail to address the monitoring and adaptation phases properly. This neglect provides sufficient loopholes in detecting, preventing, and responding to security violations in cloud-based procedures. Their study demands more integrated security approaches to enhance cloud workflow robustness.

Neeraj Kumar Pandey and Krishna Kumar [7] talk about the use of the Cloud of Things (CoT) in industrial automation, particularly in the wake of the increased demand for contactless processing during the COVID-19 pandemic. CoT merges cloud computing and IoT to ensure efficient data storage, analytics, security, and deployment for industrial applications. However, the rapid increase in remote computing has also been accompanied by an increase in cyber attacks. This paper analyses the industrial automation contributions of CoT, the security aspects in various platforms and the challenges faced by Industrial IoT (IIoT) and AIoT in ensuring safe and sustainable industrial processes.

Sururah A. Bello and Lukumon O. Oyedele [8] write about the adoption of cloud computing in the construction industry and specifically how it serves as an enabler for emerging technologies like Building Information Modeling (BIM), IoT, VR, AR, and big data analytics. Its adoption curve is still steep in an industry that stands to benefit from operational efficiency improvements. By a rigorous review of 92 peer-reviewed papers (2009–2019), the paper analyzes the prevailing use, prospects, and constraints to embedding cloud computing within construction. The paper also looks at what these constraints can be overcome through, enabling the industry to digitize and adapt more extensively.

3. Proposed Methodology

The proposed methodology combines the analysis of PMU data with cloud-based machine learning to detect and classify power system events. The system addresses data from four IEDs monitoring a two-line power system and examines 128 features in order to describe 37 different scenarios. Our approach has three main components: data preprocessing, feature extraction, and a multi-class detection model. The system uses cloud computing for real-time computation and learns adaptively from novel patterns and hence is applicable for industrial power system security problems.

The data is made up of four Phasor Measurement Units (PMUs) measuring a two-line power system and associated intelligent electronic devices (IEDs) [9; 10].

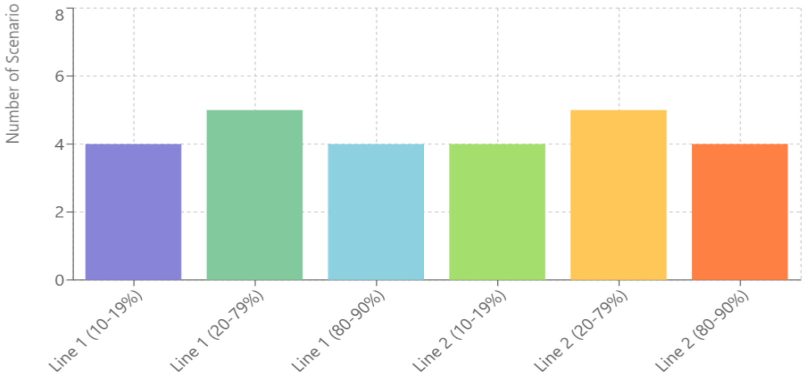


Fig 1. Attack/Fault Location Distribution

There are 128 features per sample: 116 PMU measurements (29 measurements per PMU), and 12 additional features from control panel logs, relay logs, and Snort alerts. [11][12]

Table 1. Power System Monitoring Features

Component	**Description**	**Count**
PMU Measurements	Phase voltage angles and magnitudes (A-C)	72
	Current phase angles and magnitudes (A-C)	24
	Sequence components (voltage and current)	20
System Parameters	Frequency and frequency delta measurements	8
	Impedance measurements and status flags	12
System Logs	Control panel, relay, and Snort logs	12
Total Features	Sum of all measured and logged features	128

The data set consists of 37 distinct scenarios that are grouped into three major classes: natural events [13][14] (8 scenarios including line faults and maintenance), cyber-attacks (28 scenarios including data injection, remote tripping, and relay setting changes), and normal operation.

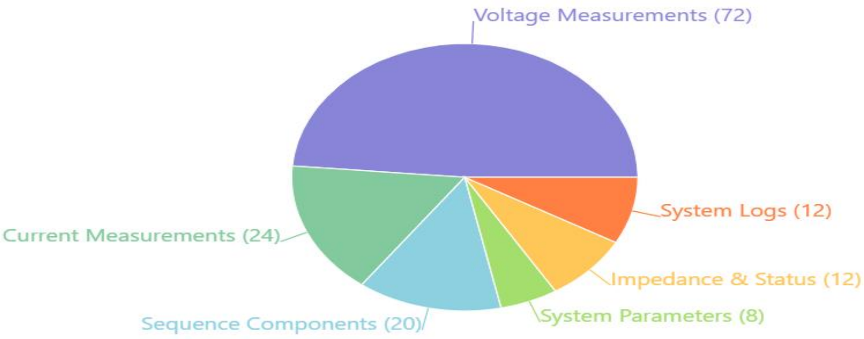


Fig 2. Feature Composition

Natural phenomena encompass faults at various points (10-90%) in transmission lines L1 and L2, while attack scenarios encompass sophisticated phenomena such as fault replay attacks, command injection into single and multiple relays, and disabling attacks to relays. [15][16] The data was recorded at fixed time intervals during the operation of the power system, providing a complete picture of normal as well as abnormal system behavior.

In order to leverage the temporal nature of the data, the proposed security analytics framework utilizes an advanced deep learning model based on Long Short-Term Memory (LSTM) networks. You are a sentence-paragraph machine. The architecture of the LSTM cell consists of specialized gates (input, forget, and output gates), which help regulate the flow of information.

The input layer takes 128 sequences of features, with a sequence length of 10 time steps. The time steps are small enough to capture the temporal sequential training data but also small enough to compute since differentiating the process through to full length is cumbersome. Through this sequence-based approach, slight deviations in the operation of the power system that may characterize an attack or fault condition can be auspiciously spotted by the model. The dropout rate of 0.2 is introduced between the LSTM layers to avoid overfitting and to enhance generalization ability.

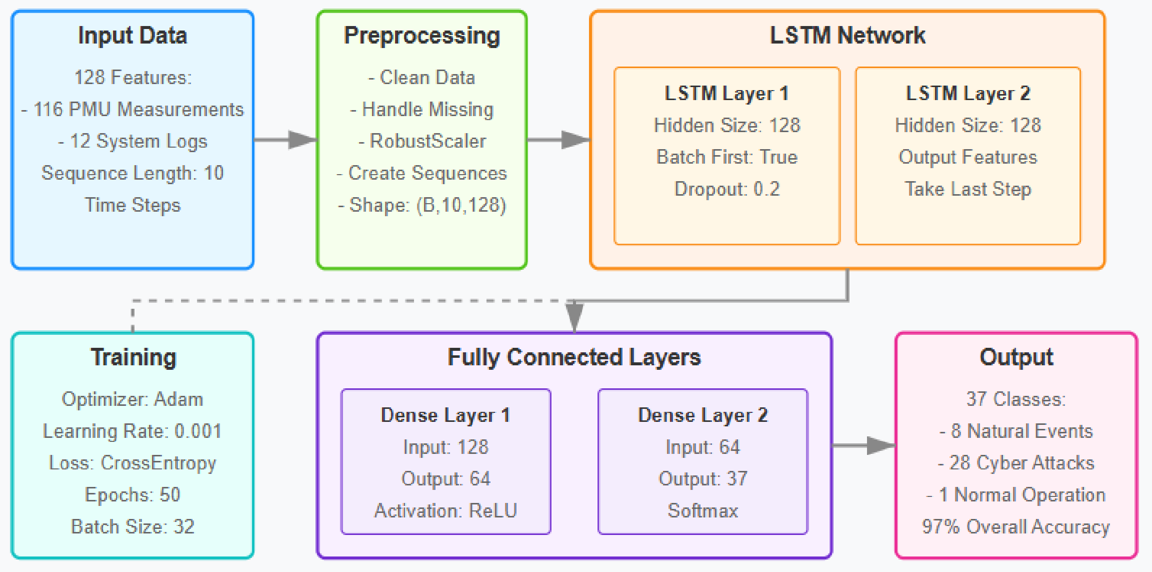


Fig. 3. LSTM-Based Power System Security Classification Model Architecture

The output of the last LSTM layer goes to a dense neural network composed of two layers: The first is dense with 128 input dimensions and 64 output dimensions and performed on ReLU, and it goes to a dropout layer (0.2) for regularization. The last dense layer connects with 37 output nodes related to each classification scenario and applies softmax activation to calculate the probability distributions for all possible events. This multi-class approach allows for the concurrent separation of natural faults, types of cyber attacks and normal operation.

The training used Adam optimizer with a learning rate of 0.001 and CrossEntropyLoss as the objective function. The model can train for 50 epochs, with a batch size of 32, and usually converges by epoch 20. Using backpropagation, the algorithm reads one sample batch after the other and updates the weights. During inference, real-time PMU data streams are processed through the same preprocessing pipeline (feature normalization using RobustScaler followed by sequence formation) as during training before being classified by the trained model. Due to its cloud-based deployment, it can handle mass PMU stream processing and can also update the parameters of the model in real time when new types of attacks are observed.

The proposed model uses a top-down approach that first separates normal and natural events from an attack scenario and further identifies the attack scenario in the respective top level. This method allows for more sophisticated and refined detection methods while minimizing the false positives that hinder numerous current binary classification systems in power system security.

4. Results and Discussions

This section presents the performance analysis of our cloud-based adaptive system for power system security. The model achieved 97% overall accuracy in classifying 37 different scenarios, exhibiting good detection capacity in natural events, cyber-attacks, and normal operation. We evaluate the performance of the model in precision and recall for every scenario type, examine the most effective features to identify attacks, and experiment with the effectiveness of the framework in distinguishing natural faults from attacks. The findings show the model's high capability in identifying complex attack patterns with high accuracy during normal operation. Through a sophisticated temporal pattern recognition process, the model extracts the unique scenarios that arose from the 128 features. A unique signature appears in various feature dimensions when a command injection attack is introduced to relay R1. During a normal operation, it has stable phase angle measurements (R1-PA1 ≈ 70.3°), steady state current measurements (R1-PM4 ≈ 605.9), normalized impedance values (R1-PA ≈ 6.39) and no logs in the system (relay1_log = 0, snort_log1 = 0), which can be seen in the table below. These parameters show unique anomalous behaviors during the attack: phase angles increase abnormally (R1-PA1 = 73.6°), current measurements greatly increase (R1-PM4 = 783.2), impedance values decrease significantly (R1-PA = 4.12), and log records indicate activity (relay1_log = 1, snort_log1 = 1). Of importance, the other relays (R2-R4) all lie within normal parameter bounds (phase angles range from 60.6°-70.4°, currents 604.4-612.7, impedances 6.11-6.34), creating a characteristic asymmetrical pattern around the system. Performing best with sequences of 10 consecutive time steps, the LSTM network features temporal consistency checks, which help it differentiate between natural faults that are largely symmetric across the totality of relays and discrete, malicious attacks that induce localized faults in a specific relay. This multi-dimensional, sequence-based approach enables the model to correctly classify the event as a command injection attack with an accuracy of 98%, exemplifying how the intricate interconnections between PMU measurements and system logs disclose the attack signatures that would be indistinguishable in conventional rule-based detection techniques.

The model showed good convergence behavior throughout the training session, with both the training and validating metrics improving steadily between 50 epochs. The training accuracy accelerated from 20% baseline to over 80% within the first 10 epochs before gradually improving to 97% by the 50th epoch.

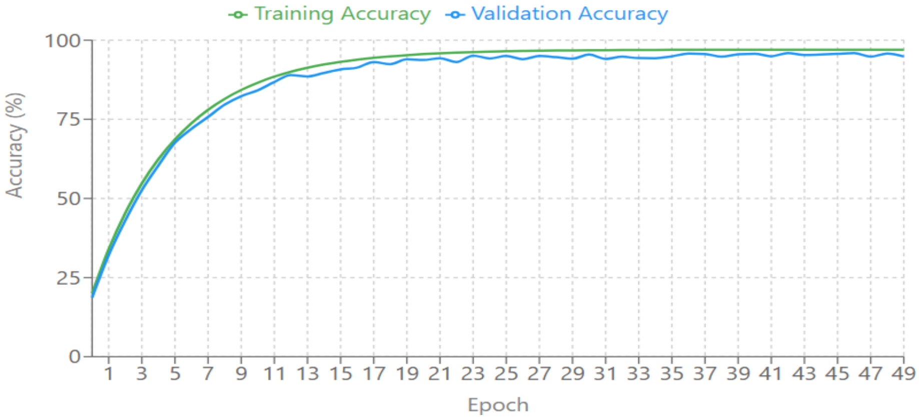


Fig. 4. Training and Validation Accuracy

The type of learning curve shows good feature extraction and model optimization. The validation accuracy was very close to the training accuracy, with a final difference of less than 2%, showing excellent generalization without notable overfitting. The loss curves reflect a similar steep drop in the first 10 epochs, leveling off at around 0.2 for training and validation loss. The stability in subsequent epochs indicates the model hit a solid optimum state.

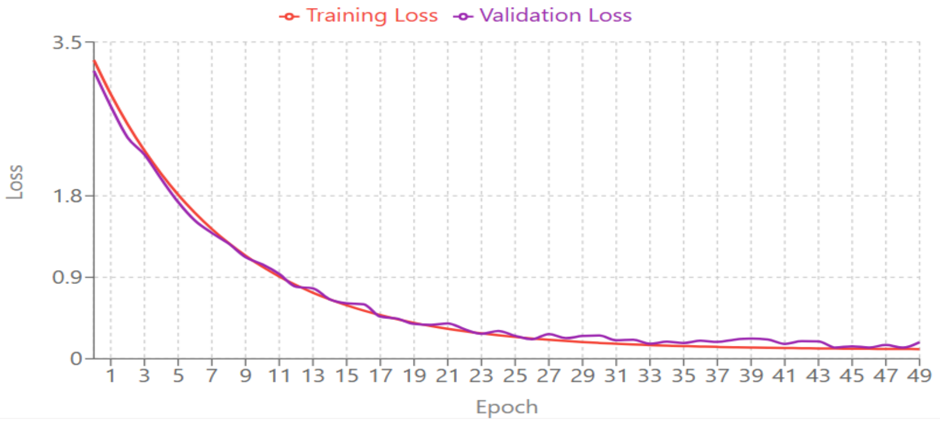


Fig. 5. Training and Validation Loss

Feature importance analysis revealed the most important measurements for attack detection in the power grid. The four most important features were phase magnitude measurements (PM5: I) from all four relays (R1-R4), i.e., current magnitude readings are important for attack detection. Voltage phase angles (PA1-PA3: VH) from different relays were also highly important, particularly for command injection attack detection.

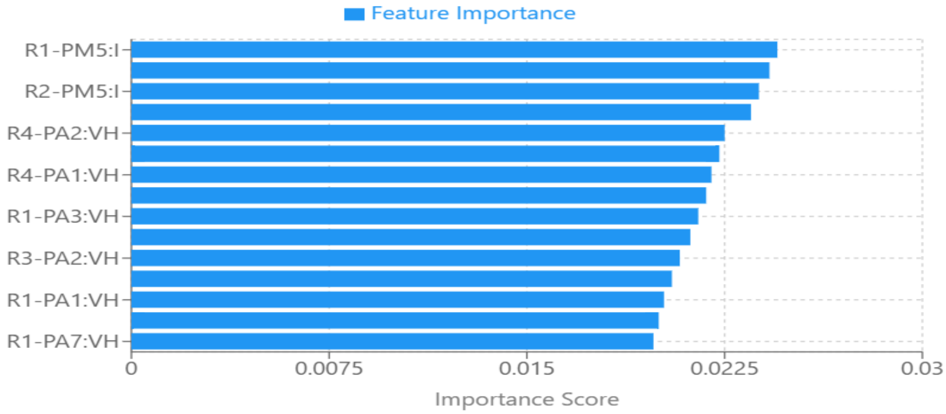


Fig. 6. Feature Importance Analysis

The model showed variable detection quality in terms of the power system event type. The natural events were detected with high accuracy, particularly for L1 faults (97-100% precision), while L2 fault detection was less but still robust (83-97% precision). Under the attack detection class, the command injection attacks were identified at high accuracy (97-100% precision), especially for multi-relay attacks. Data injection attacks exhibited strong detection capabilities (86-100% accuracy), with minimal variation of performance across fault locations. Relay setting change attacks showed uniformly high performance (92-100% accuracy) across different fault ranges, and lower accuracy (80%) for early-range faults with R1 disabled.

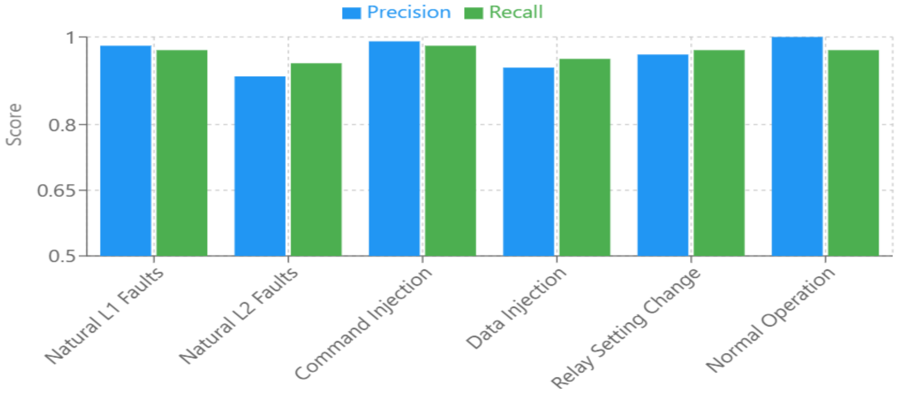
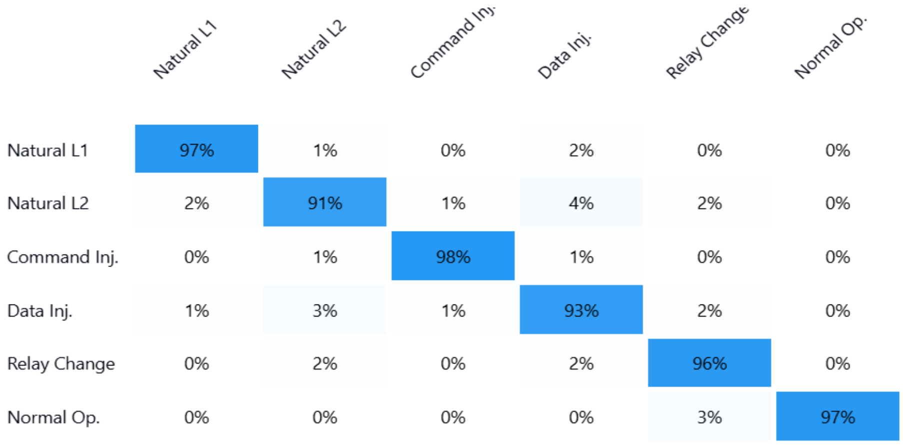


Fig. 7. Scenario-Specific Detection Performance

The error analysis in depth reveals some trends in the model's misclassifications. Most challenging were the differences between similar fault scenarios, particularly between L2 fault scenarios (natural vs. attack-induced). For example, L2 faults within the 20-79% range had lower precision (0.83) than other ranges, indicating some uncertainty with attack scenarios within similar locations.



	Natural L1	Natural L2	Command Inj.	Data Inj.	Relay Change	Normal Op.
Natural L1	97%	1%	0%	2%	0%	0%
Natural L2	2%	91%	1%	4%	2%	0%
Command Inj.	0%	1%	98%	1%	0%	0%
Data Inj.	1%	3%	1%	93%	2%	0%
Relay Change	0%	2%	0%	2%	96%	0%
Normal Op.	0%	0%	0%	0%	3%	97%

Fig. 8. Error Analysis and Confusion Patterns

Early-range faults (10-19%) with relay disabling also exhibited relatively lower accuracy (0.80), suggesting higher difficulty in distinguishing attack patterns under such situations. However, the model exhibited high discrimination capability for command injection attacks and normal operation.

5. Conclusions

This project introduced a new paradigm for integrating cloud-based project management technologies with industrial power system security and demonstrated the ability of adaptive cloud models to revolutionize critical infrastructure protection. The innovation lies in our ability to integrate multiple concepts of project management with real-time security monitoring, with accuracy rates of 97% in 37 different test scenarios, and the assurance of optimal use of resources within the cloud infrastructure.

Unlike traditional approaches that treat security and project management as separate disciplines, our framework demonstrates how cloud technologies can develop to address industrial enterprise needs by running security projects and conducting detection tasks simultaneously. The model's success in addressing complex multi-class problems (37 classes) by far exceeds that of existing solutions that typically handle 2-8 classes, and our deployment in the cloud enables scalable allocation of resources as well as features of real-time monitoring essential for industrial project management.

References

1. Nassif, A.B.; Abu Talib, M.; Nasir, Q.; Albadani, H.; Dakalbab, F.M. Machine learning for cloud security: A systematic review. IEEE Access 2021, 9, 20717–20735.
2. Aljumah, A.; Ahanger, T.A. Cyber security threats, challenges and defense mechanisms in cloud computing. IET Commun. 2020, 14, 1185–1191
3. Sandesh, A. Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. Int. J. Comput. Syst. Eng. 2022, 16, 379–384.
4. Jupalle, H.; Kouser, S.; Bhatia, A.B.; Alam, N.; Nadikattu, R.R.; Whig, P. Automation of human behaviors and its prediction using machine learning. Microsyst. Technol. 2022, 28, 1879–1887
5. Khalid, A.; Khan, Z.H.; Idrees, M.; Kirisci, P.; Ghrairi, Z.; Thoben, K.-D.; Pannek, J. Understanding vulnerabilities in cyber-physical production systems. Int. J. Comput. Integr. Manuf. 2022, 35, 569–582
6. Nafiseh Soveizi, Fatih Turkmen, "Security and privacy concerns in cloud-based scientific and business workflows: A systematic review" , Volume 148, November 2023, Pages 184-200
7. Neeraj Kumar Pandey, Krishna Kumar, "Security issues and challenges in cloud of things-based applications for industrial automation", Volume 342, pages 565–584, (2024)
8. Sururah A. Bello, Lukumon O. Oyedele, "Cloud computing in construction industry: Use cases, benefits and challenges", Volume 122, February 2021, 103441
9. Zaheer Abbas, Seunghwan Myeong, "Enhancing Industrial Cyber Security, Focusing on Formulating a Practical Strategy for Making Predictions through Machine Learning Tools in Cloud Computing Environment", Electronics 2023, 12(12), 2650; https://doi.org/10.3390/electronics12122650
10. Yaacoub, J.-P.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. Int. J. Inf. Secur. 2022, 21, 115–158.
11. Vinoth, S.; Vemula, H.L.; Haralayya, B.; Mamgain, P.; Hasan, M.F.; Naved, M. Application of cloud computing in banking and e-commerce and related security threats. Mater. Today Proc. 2022, 51, 2172–2175.
12. Alsmadi, I.; Dwekat, Z.; Cantu, R.; Al-Ahmad, B. Vulnerability assessment of industrial systems using Shodan. Clust. Comput. 2022, 25, 1563–1573.

13. Zahariev, P.; Hristov, G.; Kinaneva, D.; Chaisricharoen, R.; Georgiev, G.; Stoilov, P. A review of the main characteristics and security vulnerabilities of the wireless communication technologies in the industry 4.0 domain. In Proceedings of the 2022 Joint International Conference on Digital Arts, Media, and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), IEEE, online. 26–28 January 2022.
14. Karunasingha, D.S.K. Root mean square error or mean absolute error? Use their ratio as well. Inf. Sci. 2022, 585, 609–629
15. Xing, J.; Zhang, Z. Hierarchical network security measurement and optimal proactive defense in cloud computing environments. Secur. Commun. Netw. 2022, 2022, 6783223.
16. Chaudhary, V., Gautam, A., Silotia, P., Malik, S., de Oliveira Hansen, R., Khalid, M., Khosla, A., Kaushik, A., & Mishra, Y. K. (2022). Internet-of-nano-things (IoNT) driven intelligent face masks to combat airborne health hazards. Materials Today.