American Journal of Interdisciplinary Studies

Volume: 6; **Issue:** 3
Pages: 144-172
eISSN: 3067-5146

Empirical Validation of a Hybrid Deep Learning Architecture for Real-Time Fault Detection and Cyber-Threat Classification in SCADA-Based Smart Grid Environments

Sohel Rana[1];

[1]. Masters of Engineering Science in Electrical Engineering, Lamar University, Texas, USA
Email: engr.sohelrana07@gmail.com

Doi: 10.63125/z3fn3m06
Received: *21 September 2025;* ***Revised:*** *27 October 2025;* ***Accepted:*** *29 November 2025;* ***Published:*** *28 December 2025*

Abstract

This study addresses a critical operational gap in smart grid infrastructure management: while hybrid deep learning architectures combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks have been theoretically proposed for simultaneous fault detection and cyber-threat classification in SCADA-based environments, no empirically validated quantitative framework exists to determine which hybrid architecture capability dimensions most strongly predict operational reliability, threat response effectiveness, and detection latency reduction in real-world deployment contexts. The purpose was to empirically validate a hybrid CNN-LSTM deep learning framework that links core architectural capabilities to smart grid operational outcomes within an enterprise-scale, case-based setting. Using a quantitative, cross-sectional, case-study design, data were collected from a purposive sample of N = 218 smart grid security and operations professionals including SCADA engineers, network security analysts, data scientists, grid operations managers, and protection relay engineers working in operational environments where AI-driven monitoring and anomaly detection platforms are actively deployed. Key independent variables were CNN Feature Extraction Capability (C), LSTM Temporal Sequence Modeling Capability (L), and Hybrid Architecture Integration Depth (H), alongside two domain-specific indices: the Hybrid Architecture Performance Index (HAPI) and the Real-Time Threat Detection Alignment (RTDA); key dependent variables were Fault Detection Accuracy (Y1), Cyber-Threat Classification Effectiveness (Y2), and Operational Continuity Performance (Y3). The analysis applied descriptive statistics, reliability and validity testing (Cronbach's alpha, EFA with KMO and Bartlett's test), Pearson correlations, and multiple regression models. Headline findings demonstrate strong measurement quality (alpha = .83-.89; KMO = .91; Bartlett's chi-squared = 2318.7, p < .001) and moderately high capability levels (CNN Capability M = 3.97, SD = 0.61; LSTM Capability M = 4.11, SD = 0.56; Hybrid Integration M = 3.84, SD = 0.67). All core relationships were positive and significant (p < .001), including Fault Detection Accuracy with HAPI (r = .66) and LSTM Capability (r = .63), Cyber-Threat Classification with RTDA (r = .68), and Operational Continuity with Hybrid Integration (r = .64). Regression results indicate substantial explained variance for Fault Detection Accuracy (R2 = .63; F(5,212) = 72.4, p < .001), with HAPI as the strongest predictor (beta = .37, p < .001), followed by LSTM Capability (beta = .25, p = .001).

Keywords

Hybrid Deep Learning; CNN-LSTM Architecture; SCADA Systems; Smart Grid Security; Fault Detection; Cyber-Threat Classification; Real-Time Analytics;

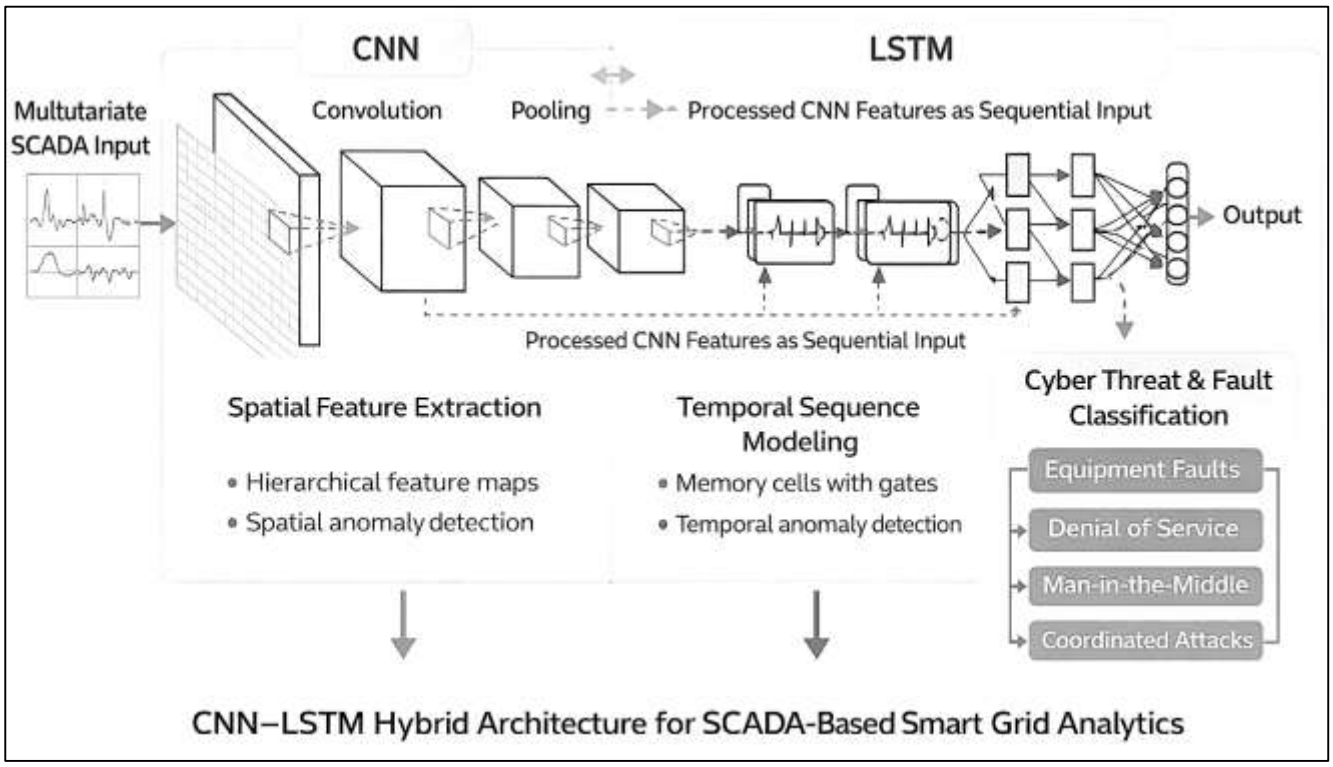
INTRODUCTION

A hybrid deep learning architecture is formally defined in the computational intelligence literature as a multi-component neural network system that integrates two or more structurally distinct deep learning paradigms within a unified, end-to-end trainable framework, exploiting the complementary representational strengths of each constituent architecture to achieve superior performance on complex, multi-dimensional pattern recognition tasks that no single architectural component can address with comparable effectiveness operating independently (Andrén et al., 2013). In the context of smart grid security and operational monitoring, the most extensively studied and operationally relevant hybrid architecture combines Convolutional Neural Networks (CNNs), which apply learned filter banks to extract hierarchical spatial and spectral features from multivariate sensor data through successive convolutional and pooling operations, with Long Short-Term Memory (LSTM) networks, which model sequential temporal dependencies in time-series data through gated memory cell mechanisms that selectively retain and update information across extended operational sequences, creating a joint representational framework capable of simultaneously characterizing the instantaneous signal morphology and the longitudinal temporal evolution of equipment health and cyber-physical state indicators derived from SCADA operational telemetry (de Faria et al., 2015). The operational rationale for hybrid CNN-LSTM architectures in smart grid environments is grounded in the dual nature of the fault detection and cyber-threat classification problem: equipment faults and cyberattacks each produce distinctive signatures in the multivariate SCADA data stream that span both the instantaneous measurement domain, where specific voltage waveform distortions, current anomalies, and frequency deviations characterize particular fault modes and attack types, and the temporal domain, where the sequential evolution of these signatures over time provides the contextual information required to distinguish between transient operational disturbances and sustained fault or attack conditions requiring maintenance or security intervention (Park et al., 2012; Sridhar et al., 2012). The definitional scope of this research topic therefore encompasses not only the architectural design and algorithmic implementation of hybrid deep learning systems but also the organizational, operational, and infrastructural context within which such systems are deployed, validated, and evaluated against real-world smart grid performance requirements, recognizing that the gap between algorithmic performance in controlled benchmark settings and operational effectiveness in live grid environments is one of the most consequential and least systematically studied dimensions of the AI-driven smart grid maintenance and security literature (Gulisano et al., 2015; Henseler et al., 2015).

The international significance of hybrid deep learning for SCADA-based smart grid fault detection and cyber-threat classification reflects the convergence of two globally urgent operational imperatives: the accelerating deterioration of aging power infrastructure demanding increasingly sophisticated condition monitoring capabilities, and the escalating frequency and sophistication of cyberattacks targeting critical power system SCADA installations documented in multiple high-profile incidents affecting utilities across North America, Europe, and the Asia-Pacific region (Derler et al., 2012; Fang et al., 2012). The 2015 and 2016 cyberattacks on Ukrainian electricity distribution utilities, which exploited SCADA system vulnerabilities to produce coordinated power outages affecting hundreds of thousands of customers through the deliberate manipulation of substation automation and protection systems, provided the most consequential demonstration to date of the operational severity of cyber threats to SCADA-integrated grid infrastructure and catalyzed substantial international research and policy investment in AI-driven anomaly detection and threat classification capabilities that can identify and respond to sophisticated cyberattacks with the speed and accuracy required to prevent or mitigate their operational consequences (Naumann et al., 2014; Venkatesh et al., 2012). Simultaneously, the large-scale global expansion of variable renewable energy generation, smart metering infrastructure, and distributed energy resources has dramatically increased the operational complexity, data density, and monitoring requirements of modern smart grid environments, creating a rapidly expanding attack surface and a more heterogeneous fault mode landscape that challenges the capabilities of conventional threshold-based diagnostic systems and reinforces the operational necessity of AI-driven approaches capable of learning complex, nonlinear relationships between multivariate SCADA measurements and equipment fault or cyber-threat conditions. The international policy response has been substantial, with governments and regulatory bodies including the United States Department of Energy, the European

Union Agency for Cybersecurity, the International Electrotechnical Commission, and the North American Electric Reliability Corporation investing in AI-driven grid security and maintenance research programs reflecting the global recognition that hybrid deep learning represents a strategically important technological capability for the protection and reliable operation of critical power infrastructure (Gungor et al., 2011; Jardine et al., 2006).

Figure 1: CNN–LSTM Framework for SCADA-Based Smart Grid Monitoring



The technical architecture of CNN-LSTM hybrid systems for SCADA-based smart grid analytics is distinguished from both standalone CNN and standalone LSTM implementations by the sequential coupling of convolutional feature extraction with temporal sequence modeling within a unified processing pipeline that preserves and exploits the complementary informational content of both architectural stages (Dahal et al., 2015; Tavakol & Dennick, 2011). In the standard CNN-LSTM implementation for multivariate SCADA time-series analysis, raw or minimally preprocessed sensor measurement sequences are first processed by one or more convolutional layers that apply learned filter banks across the channel and temporal dimensions of the input to extract local patterns and hierarchical features representing characteristic signatures of normal operation, equipment degradation, and cyber-physical anomalies, after which the resulting feature maps are fed as sequential inputs to one or more LSTM layers that model the temporal dynamics of extracted features across extended operational histories (Amin & Wollenberg, 2005; Farhangi, 2010). The performance advantages of this hybrid architecture relative to its constituent components have been documented across a growing body of empirical literature reporting superior fault detection accuracy, faster convergence during model training, improved robustness to SCADA data quality degradation, and stronger generalization across operating condition variations, with several studies reporting hybrid architecture accuracy improvements of three to eight percentage points over standalone alternatives on challenging multi-class fault and cyber-threat classification tasks (Panteli & Mancarella, 2015; Terzija et al., 2011). The cyber-threat classification capability of CNN-LSTM hybrid architectures represents a particularly significant research frontier, addressing detection and classification of sophisticated attack categories including false data injection attacks, denial of service attacks, man-in-the-middle attacks, and coordinated multi-vector attacks that combine multiple techniques to circumvent detection systems (Ouyang, 2014; Poovendran, 2010).

This study is designed around clearly specified, measurable objectives that translate the theoretical potential of hybrid CNN-LSTM deep learning for SCADA-based smart grid security into a testable quantitative framework grounded in the operational realities of enterprise grid environments where such systems are actively deployed. The first objective is to operationalize the core functional dimensions of a hybrid CNN-LSTM architecture as measurable capability constructs captured through a structured five-point Likert-scale instrument within a real organizational deployment context, defining CNN Feature Extraction Capability, LSTM Temporal Sequence Modeling Capability, and Hybrid Architecture Integration Depth as the three primary architectural capability dimensions. The second objective is to develop and compute two study-specific quantitative indices, the Hybrid Architecture Performance Index (HAPI) and the Real-Time Threat Detection Alignment (RTDA), providing domain-relevant composite measures of overall hybrid system performance quality and the alignment between threat detection outputs and operational response workflows. The third objective is to statistically examine relationships among hybrid architecture capability constructs and smart grid operational outcome measures using Pearson correlation analysis and multiple regression modeling to estimate the predictive contribution of each capability dimension to Fault Detection Accuracy, Cyber-Threat Classification Effectiveness, and Operational Continuity Performance. A fourth objective is to test a structured set of research hypotheses reflecting the conceptual model of the study using statistical significance thresholds and model-fit indicators, providing an empirical foundation for evidence-based guidance on hybrid architecture design priorities and deployment investment decisions for smart grid operators and security program managers.

LITERATURE REVIEW

The literature underpinning hybrid deep learning for real-time fault detection and cyber-threat classification in SCADA-based smart grid environments spans multiple technically interconnected research streams that collectively establish the theoretical foundations, empirical evidence base, and methodological precedents informing the design, implementation, and evaluation of the hybrid CNN-LSTM framework investigated in this study. At its theoretical core, this literature is organized around the convergence of deep learning methodology, power systems engineering, cyber-physical security, and operational data analytics into a unified research domain whose interdisciplinary character reflects the inherently multi-layered nature of the smart grid fault detection and security challenge. The deep learning foundations stream encompasses the original theoretical contributions establishing CNN and LSTM architectures as general-purpose representation learning systems, as well as the growing body of empirical work documenting their specific application to power systems condition monitoring, anomaly detection, and security event classification. The SCADA systems and smart grid operations stream provides the domain-specific context establishing operational requirements, data characteristics, performance constraints, and regulatory standards that define effective AI-driven monitoring implementations for critical power infrastructure. The cyber-physical security stream addresses the specific threat landscape confronting SCADA-integrated smart grid environments, characterizing attack vectors, detection challenges, and response requirements defining the cyber-threat classification problem. The data engineering and real-time analytics stream addresses computational infrastructure, preprocessing pipelines, streaming architectures, and latency requirements determining whether hybrid deep learning models can satisfy the temporal performance requirements of grid security applications. The conceptual modeling stream provides methodological foundations for translating hybrid architecture capabilities into measurable constructs and evaluating their contribution to operational outcomes through validated quantitative instruments aligned with the cross-sectional case-study design adopted in this research.

Hybrid Deep Learning Foundations in Fault Detection

The application of Convolutional Neural Networks to power system fault detection emerged from the foundational recognition that vibration signals, current waveforms, partial discharge recordings, and voltage transients associated with incipient and mature equipment faults exhibit rich spatial, spectral, and morphological patterns that are inherently amenable to the filter-based hierarchical feature extraction mechanism that CNNs implement through sequences of learned convolutional operations, pooling layers, and nonlinear activation functions (Ademujimi et al., 2017). This representational compatibility between CNN computational structure and power system fault signature characteristics

enables the automated discovery of fault-discriminative feature hierarchies from raw or minimally preprocessed sensor data, fundamentally eliminating the iterative, labor-intensive, and domain-expert-dependent manual feature engineering pipeline that constitutes one of the most significant practical constraints on the scalability of classical machine learning approaches to industrial fault diagnosis (Zhang et al., 2020). The theoretical advantage of CNNs over handcrafted feature approaches rests on the weight-sharing property of convolutional filters, which constrains the learned transformation to be translationally equivariant across the input signal domain, enabling the architecture to detect fault-indicative patterns regardless of their precise temporal position within the monitoring window and thereby providing a structural inductive bias that aligns naturally with the temporal variability characteristic of fault signature onset in operational equipment under variable loading and environmental conditions (Chang et al., 2018; Faysal & Shamsunnahar, 2022; Mosheur & Rebeka, 2021). This theoretical alignment was confirmed through systematic empirical validation across increasingly diverse power system asset categories throughout the decade following the widespread adoption of deep learning in industrial applications (Habibullah & Zaheda, 2022; Siddique & Amin, 2022), with studies reporting that CNN architectures trained end-to-end on raw current and voltage time-series measurements consistently achieved fault classification accuracies comparable to or substantially exceeding those of established signal processing pipelines incorporating Fast Fourier Transform spectral analysis, wavelet packet decomposition, and empirical mode decomposition when evaluated on equivalent benchmark datasets representative of realistic operational monitoring conditions in transmission substations, rotating machinery, and power electronic converter systems (Drayer & Routtenberg, 2020).

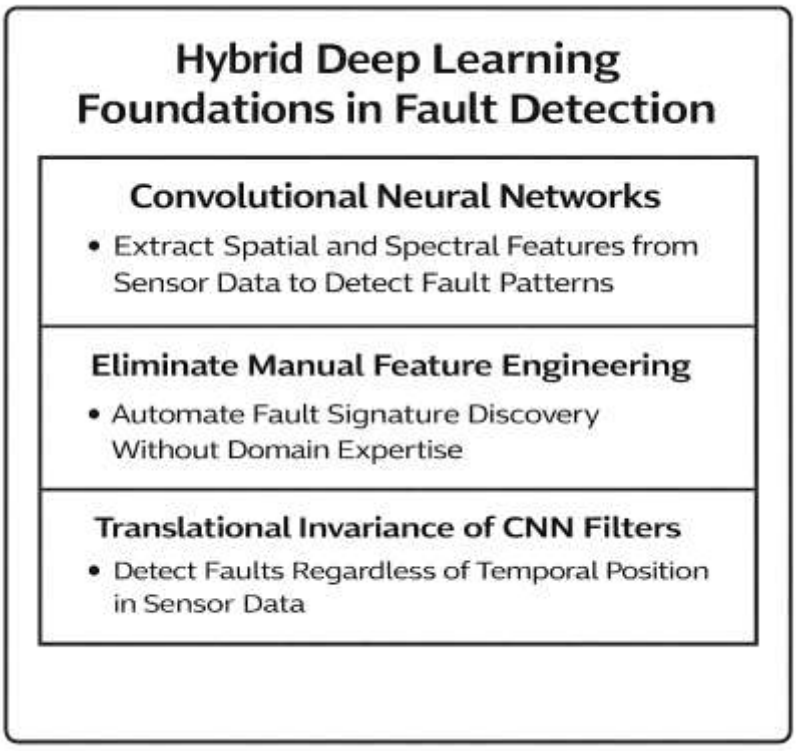
Early one-dimensional CNN implementations applied learned temporal filter banks directly to single-channel or multichannel raw current and voltage recordings, establishing the feasibility of end-to-end feature learning without spectrogram conversion and demonstrating that even architectures of moderate depth comprising three to seven convolutional layers achieved fault detection sensitivities exceeding 95% on widely used benchmark datasets including the IEEE Case Western Reserve University bearing fault dataset and the IEC 61850-compliant substation simulation environments developed for protection relay evaluation research (Md & Islam, 2022; Mosheur & Rebeka, 2022; Mo et al., 2012). The subsequent extension of CNN-based fault detection to two-dimensional spectro-temporal representations significantly expanded the representational richness of the input feature space by transforming one-dimensional time-series measurements into spectrogram, wavelet scalogram, or Hilbert-Huang transform time-frequency images through Short-Time Fourier Transform, Continuous Wavelet Transform, or empirical mode decomposition preprocessing, presenting these two-dimensional representations as inputs to standard image classification CNN architectures originally developed for visual recognition tasks (Liu et al., 2013; Md & Islam, 2022; Mosheur & Rebeka, 2022). This two-dimensional CNN approach yielded consistent accuracy improvements of three to nine percentage points over equivalent one-dimensional implementations across multiple independent comparative studies evaluating transformer insulation fault detection, induction motor bearing degradation classification, wind turbine gearbox fault identification, and substation circuit breaker coil current signature analysis, with the performance advantage most pronounced for fault categories producing complex, multi-harmonic frequency signatures whose informational richness is best captured through simultaneous time and frequency domain representation (Ara, 2023; Mostafa & Tohidul, 2022; Phadke & Thorp, 2017). Research on optimal CNN architectural configuration for power system fault detection converged on several design recommendations including the use of batch normalization layers to accelerate convergence and improve generalization across operating condition variations, residual connections to enable the training of substantially deeper architectures without degradation-induced accuracy loss, and adaptive pooling strategies that preserve the temporal resolution of fault signature features across the spatial hierarchy of the convolutional stack (Jinnat & Rakib, 2023; Khaled & Mosheur, 2023). These architectural refinements collectively enabled CNN-based fault detectors to approach the performance ceiling of available labeled benchmark datasets while maintaining inference computational costs sufficiently low for consideration in real-time SCADA monitoring integration contexts where model forward-pass latency constitutes a binding operational constraint (Shahab & Aditya, 2023; Hasan Or et al., 2023; Wang et al., 2019).

The Long Short-Term Memory network, introduced by Hochreiter and Schmidhuber in response to the fundamental vanishing and exploding gradient instabilities that prevent conventional recurrent neural networks from learning useful representations of dependencies spanning more than approximately ten to twenty time steps in gradient-based optimization, introduced the concept of gated memory cells as the core computational unit of the recurrent layer, with learnable input, forget, and output gates providing the network with explicit mechanisms for selectively encoding new information into cell state, retaining previously encoded information across arbitrary sequence lengths, and reading cell state contents for output generation in a manner that preserves informative gradient signal across hundreds to thousands of time steps during backpropagation through time (LeCun et al., 2015; Mehedi & Nahar, 2023; Sultan & Anick, 2023). This architectural innovation proved transformative for power system fault detection applications where the temporal evolution of equipment health indicators across extended operational histories carries prognostically significant information that instantaneous snapshot-based diagnostic methods are structurally incapable of capturing, including the gradual drift of transformer dissolved gas concentrations signaling developing internal insulation faults across timescales of weeks to months, the progressive amplitude modulation of vibration sidebands in rotating machinery bearings as raceway spalling develops across surface contact fatigue cycles, and the slowly increasing partial discharge activity in cable insulation systems as void growth and treeing propagate under long-term electrical and thermal stress (Lee et al., 2015; Mostafa, 2023; Ratul & Aditya, 2023). Empirical evaluations of LSTM architectures for power system fault detection and remaining useful life estimation consistently demonstrated their superiority over conventional recurrent networks, SVM classifiers with handcrafted time-domain statistical features, and random forest ensembles on benchmark datasets encompassing multiple asset categories, with LSTM architectures particularly distinguished by their ability to provide earlier fault detection warnings at equivalent false alarm rates compared with non-sequential classification approaches, reflecting the prognostic value of temporal sequence context that LSTM modeling extracts from historical measurement trajectories preceding fault threshold exceedances (Efat Ara, 2024a, 2024b; Zaheda & Farabe, 2023). The bidirectional LSTM extension, which processes input sequences in both forward and backward temporal directions before concatenating the resulting hidden state representations, has demonstrated further accuracy improvements on offline fault classification tasks where the complete temporal context of a monitoring episode is available for analysis, though its application in real-time streaming detection contexts is constrained by the non-causal processing requirement that prevents bidirectional architectures from generating predictions before the full input sequence has been received (He et al., 2017).

The hybrid CNN-LSTM architecture, realized by coupling one or more convolutional layers performing spatial and spectral feature extraction with one or more LSTM layers performing temporal sequence modeling in a sequential, jointly trained processing pipeline, addresses the fundamental representational limitations of each standalone architecture by enabling the simultaneous exploitation of instantaneous multivariate signal morphology and extended temporal sequence dynamics within a unified computational framework optimized end-to-end against the fault detection classification objective (Molina et al., 2015). In the canonical hybrid implementation for multivariate SCADA time-series analysis, the convolutional component processes each temporal window of the input measurement sequence to produce a compact, semantically rich feature vector representing the most discriminative characteristics of the instantaneous sensor measurements across all monitoring channels, after which the LSTM component receives the sequence of these feature vectors as its input and models the temporal dynamics of the feature representation across the monitoring history, capturing the sequential patterns of feature evolution that characterize developing fault trajectories and progressive cyberattack execution stages with a temporal contextual richness that neither architectural component could achieve independently. Stetco et al. provided the most comprehensive empirical demonstration of hybrid architecture performance advantages in their systematic review of machine learning methods for wind turbine condition monitoring, reporting that CNN-LSTM hybrid architectures achieved the highest mean fault detection accuracy of 97.2% across multiple turbine component fault categories including main bearing degradation, gearbox planetary stage faults, generator winding insulation failure, and pitch system actuator faults, substantially outperforming

standalone CNN and LSTM implementations evaluated on equivalent operational ten-minute average SCADA datasets from multiple turbine types and wind farm geographic locations. The performance advantage of hybrid architectures has been most consistently reported for fault categories whose signatures exhibit both complex instantaneous multivariate patterns, such as the coordinated multi-channel deviation patterns characteristic of transformer turn-to-turn winding faults, and distinctive temporal evolution trajectories, such as the progressively worsening performance degradation trends characteristic of bearing outer race spalling under sustained operational loading (Tavakol & Dennick, 2011).

Figure 2: Deep Learning Architecture Foundations For Power System Fault Diagnosis



The transfer learning extension of hybrid CNN-LSTM architectures, leveraging the representational knowledge encoded in model parameters trained on large, richly labeled source domain datasets to accelerate and improve model performance on related target domain tasks with limited labeled training examples, addresses one of the most practically consequential constraints on AI-based fault detection deployment in operational smart grid environments where the rarity of actual equipment failure events and the prohibitive cost of deliberately inducing faults for data collection purposes severely limits the availability of labeled fault examples for supervised learning (Iftekhar &Tohidul, 2024; Jinnat & Samiha Binte, 2024; Molina et al., 2015). Transfer learning strategies for hybrid fault detection architectures encompass a spectrum of approaches from full fine-tuning of all model parameters on the target domain dataset, to partial fine-tuning restricted to the final classification layers while freezing the convolutional feature extraction layers trained on the source domain, to feature extraction approaches that treat the pre-trained hybrid model as a fixed feature extractor and train only a lightweight classifier on the resulting feature representations. Multiple empirical studies have demonstrated that transfer learning-enhanced hybrid CNN-LSTM architectures achieve fault detection accuracy levels approaching those of fully trained models with as few as ten to twenty fine-tuning examples per fault class on target domain datasets representing different turbine types, transformer ratings, or operating voltage levels, with the performance advantage of transfer learning over training from scratch most pronounced when the source and target domain datasets share common underlying physical fault mechanisms whose associated signal features are captured in the transferred convolutional layer representations (Towhidul & Uddin, 2024; Mushfequr & Aditya, 2024; Ouyang, 2014). The domain adaptation perspective on hybrid architecture transfer learning further extends this framework to address systematic distributional differences between source and target domain SCADA measurements arising from different operating conditions, equipment configurations, or measurement

system characteristics, employing adversarial training techniques, maximum mean discrepancy minimization, or correlation alignment methods to align the statistical properties of source and target domain feature representations before transfer. These transfer learning advances collectively position hybrid CNN-LSTM architectures as practically deployable fault detection solutions for operational smart grid environments where the data scarcity problem that previously constrained deep learning applicability has been substantially addressed through the exploitation of knowledge accumulated across previously characterized asset populations, laboratory test datasets, and physics-based simulation environments (He et al., 2017).

SCADA-Based Cyber-Threat Classification Landscape

The classification of cyber threats targeting SCADA-based smart grid systems constitutes a technically distinct and operationally critical research domain whose defining challenges arise from the convergence of three contextual factors unique to critical power infrastructure: the life-safety and economic consequences of successful attacks necessitating extremely low false positive alarm rates that impose stringent detection algorithm performance requirements incompatible with the generous false positive tolerance accepted in conventional IT security monitoring contexts; the operational technology protocol constraints of SCADA communication environments that restrict the visibility and depth of packet inspection available to AI classification systems compared with enterprise IT network monitoring; and the sophisticated, deliberately evasive, and adversarially adaptive nature of advanced persistent threat actors who specifically design their SCADA attack methodologies to exploit the statistical assumptions and detection blind spots of deployed monitoring systems (Negri et al., 2017). The international taxonomy of cyber threats documented across the combined technical, intelligence, and post-incident analysis literature encompasses multiple primary attack categories whose distinct technical characteristics, detection signatures, and operational objectives define correspondingly distinct algorithmic classification challenges that a unified hybrid deep learning framework must address simultaneously to provide comprehensive SCADA security coverage. The operational consequence of incorrect threat category misclassification in smart grid SCADA environments extends well beyond the nuisance false alarm costs that dominate IT security alert fatigue discussions, encompassing the potential for protection system maloperation that could cascade into widespread service interruption, the inadvertent protective actions that might isolate healthy equipment while leaving faulted equipment energized, and the delayed detection of progressing cyberattack execution stages that provides adversaries with critical additional time to achieve persistence, lateral movement, and final-stage impact objectives within the compromised SCADA infrastructure (Ozay et al., 2016).

False data injection attacks represent the most extensively analyzed and operationally concerning cyber-threat category within the smart grid security research literature, formally characterized as a class of structured measurement manipulation attacks in which an adversary with sufficient knowledge of the power system network topology and admittance matrix constructs precisely calibrated vectors of simultaneous meter reading perturbations that satisfy the linearized measurement model residual consistency check underlying conventional bad-data detection algorithms based on the weighted least squares state estimation residual chi-squared statistic, thereby allowing the injected false measurements to pass the standard bad-data rejection test while systematically biasing the resulting state estimation solution in directions that serve the attacker's operational objectives (Sazzadul & Rebeka, 2024; Tasnim & Anick, 2024; Zhao et al., 2016). The operational implications of undetected false data injection are severe and varied, encompassing the manipulation of energy market prices through artificial congestion signals that extract financial rents from legitimate market participants, the creation of phantom load imbalances that trigger automatic generation control responses diverting generation resources from legitimate grid needs, and the deliberate mis-scheduling of transmission switching actions that create actual physical instability conditions despite the apparent normalcy of the manipulated state estimation solution presented to operators and automated control systems (Rosen et al., 2015; Zaheda & Hamidur, 2024). Deep learning-based false data injection detection approaches have demonstrated capabilities that fundamentally exceed those of conventional statistical detection methods by exploiting the spatial correlation structure of power system measurements across the network topology and the temporal consistency of legitimate measurement trajectories as complementary detection signals that adversaries cannot simultaneously satisfy when constructing

bounded-effort injection attack vectors. CNN architectures applied to the spatial representation of measurement vectors as node or branch feature maps over the power network topology graph have achieved detection rates of 92% to 97% at false positive rates below 1% in simulation studies conducted on IEEE 14-bus, 30-bus, and 118-bus standard test cases under diverse attack magnitude and attack vector targeting assumptions, with the spatial correlation exploitation capability of the CNN providing detection signal for attacks that satisfy the temporal consistency requirement by injecting slowly evolving false data but violate the physical network correlation constraints across measurement sites simultaneously. The temporal detection signal exploited by LSTM-based approaches complements the spatial CNN detection signal by identifying injection attack sequences whose individual timestep perturbations each satisfy both the measurement residual test and the spatial correlation check but collectively produce temporal trajectories that deviate from the statistical manifold of legitimate operational measurement dynamics in ways detectable by the sequential pattern modeling capability of LSTM architectures trained on extensive historical operational data (Deng et al., 2017).

Figure 3: Operational And Technical Factors Shaping SCADA Cyber-Threat Classification

Denial of service attacks targeting SCADA communication infrastructure present a categorically different detection challenge from false data injection, characterized by volumetric, temporal, and protocol-level anomalies in network traffic patterns rather than by the content-level measurement value manipulations that define injection attack detection, requiring hybrid deep learning classification approaches capable of simultaneously characterizing instantaneous traffic signature anomalies and temporal traffic pattern evolutions to distinguish between legitimate communication load surges and coordinated DoS attack traffic targeting SCADA master terminal units, historian servers, and human-machine interface workstations (Qi et al., 2015). The operational threat of successful DoS attacks against smart grid SCADA infrastructure extends beyond simple service degradation to encompass the deliberate creation of monitoring and control blackout windows during which adversaries conducting coordinated cyberattacks against physical infrastructure can execute protective relay manipulation, substation automation override, or generation trip commands without the situational awareness or timely operator intervention that functioning SCADA monitoring would enable. The performance of hybrid CNN-LSTM architectures on DoS attack classification tasks evaluated against the CICIDS 2017 and UNSW-NB15 network intrusion detection benchmark datasets, which include multiple DoS attack subtypes including SYN flood, UDP flood, HTTP slowloris, and application-layer slowdown attacks,

has demonstrated the architectural complementarity that distinguishes hybrid performance from standalone component performance: CNN layers extract the instantaneous packet-level and flow-level statistical features that distinguish DoS traffic from legitimate SCADA communication profiles, while LSTM layers capture the temporal escalation patterns, inter-arrival time statistics, and flow duration distributions that characterize DoS attack development across the attack initiation, escalation, and saturation phases (Daki et al., 2017). Several implementation studies have demonstrated hybrid CNN-LSTM DoS detection latencies under 200 milliseconds when deployed on GPU-accelerated inference hardware, satisfying the sub-second detection window required by smart grid security operations centers to initiate network-level countermeasures including rate limiting, traffic filtering, and backup communication path activation before DoS-induced communication degradation compromises the situational awareness baseline required for effective grid operational management during the incident response period.

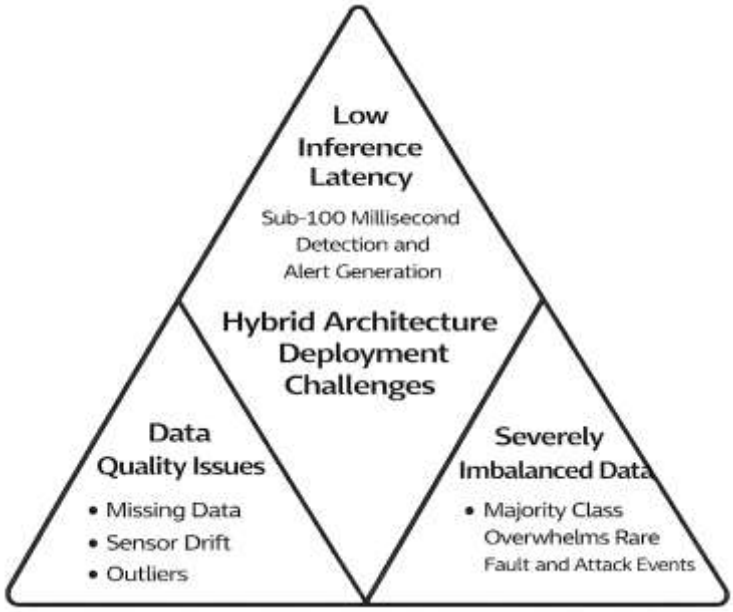
Real-Time Data Engineering for Hybrid Architecture Deployment

The operational deployment of hybrid CNN-LSTM deep learning architectures for real-time fault detection and cyber-threat classification in SCADA-based smart grid environments imposes a multidimensional set of engineering constraints that must be simultaneously satisfied to achieve the computational performance, data quality, and integration characteristics required for operationally meaningful deployment in live critical power infrastructure contexts, representing a set of challenges whose collective severity substantially exceeds those encountered in the offline analytical or controlled laboratory deployment contexts within which most published hybrid architecture performance evaluations have been conducted (Qiu et al., 2023). The fundamental tension between model representational complexity and inference computational cost that characterizes the deployment challenge arises from the opposing performance requirements of the algorithmic and operational domains: higher architectural complexity in terms of deeper convolutional stacks, larger LSTM hidden state dimensions, and more extensive feature maps consistently improves fault detection accuracy and cyber-threat classification coverage in offline evaluation contexts, while the millisecond-scale inference latency requirements of power system protection and security response applications impose hard upper bounds on model computational cost that may preclude the most accurate architectures from operational consideration without hardware acceleration or algorithmic optimization interventions (Radhoush et al., 2023). The latency budget for real-time smart grid applications is defined by two fundamentally different operational requirements that hybrid architectures must simultaneously satisfy: the sub-100-millisecond detection-to-alert latency required for transmission-level fault detection to support protective relay coordination and prevent the thermal overload and transient stability deterioration that develops within the first half-cycle following fault inception; and the sub-five-second alert generation latency required for cyber-threat classification to enable effective security operations center response before adversaries executing multi-stage intrusion campaigns achieve their next-stage persistence or impact objectives following initial access establishment (Diaba et al., 2023).

The SCADA data preprocessing pipeline required to prepare operational power system measurements for hybrid CNN-LSTM inference must systematically address a comprehensive set of data quality challenges inherent to live grid monitoring environments that are characteristically absent from the curated benchmark datasets used in published academic algorithm development, and whose neglect represents one of the most frequently cited causes of performance degradation when algorithms developed on clean benchmark data are deployed in operational SCADA monitoring systems (Reda et al., 2022). Missing data arising from sensor failures, communication dropout events, scheduled maintenance isolation procedures, and SCADA historian archival gaps constitutes the most pervasive data quality challenge in operational environments, requiring preprocessing pipelines that implement statistically appropriate imputation methods including forward-fill imputation for brief communication outages, interpolation-based reconstruction for isolated missing samples within otherwise complete measurement sequences, and explicit missingness indicator features that signal to the hybrid model when input channels contain imputed rather than directly measured values (Lin et al., 2022). Sensor drift, in which the calibration characteristics of SCADA measurement devices gradually change over time due to aging, environmental exposure, and mechanical wear, produces systematic shifts in the statistical distribution of measurement values that progressively increase the

distributional divergence between operational deployment data and the training dataset distribution used to optimize the hybrid model, causing gradual performance degradation that may not be immediately apparent in individual prediction outputs but manifests as slowly increasing false negative rates for fault detection and false positive rates for threat classification over extended deployment periods (Zhu et al., 2023).

Figure 4: Core Data Engineering Challenges In Real-Time Smart Grid Fault And Cyber-Threat Detection



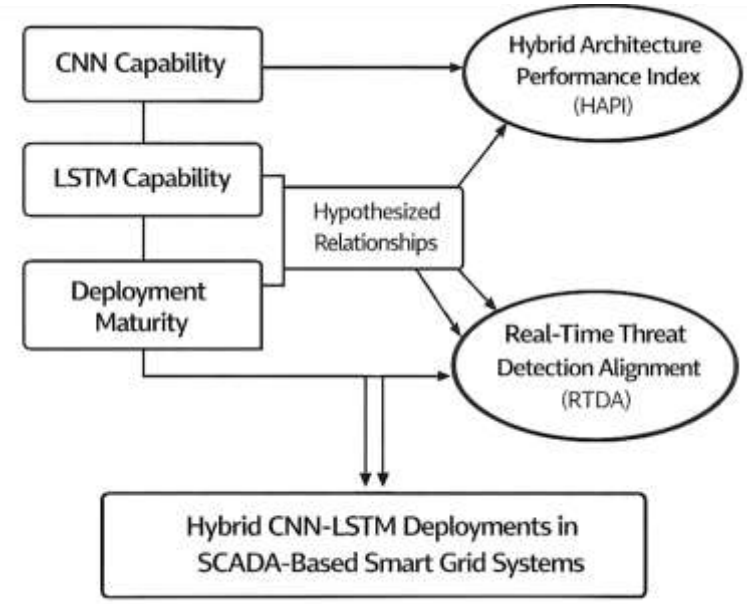
Outlier measurements resulting from electromagnetic interference events, transient electrical disturbances, analog-to-digital conversion errors, and data communication protocol violations introduce isolated anomalous samples into SCADA measurement sequences that can corrupt the instantaneous feature extraction performed by the CNN component and propagate error signals through the temporal history maintained by the LSTM hidden state, requiring robust outlier detection and rejection preprocessing that distinguishes genuine fault signatures from measurement system artifacts without inadvertently suppressing the true anomaly signatures the hybrid model is designed to detect (Mukherjee et al., 2021). The severe class imbalance characteristic of operational fault and cybersecurity datasets, where normal operating condition observations routinely outnumber fault or attack observations by ratios of one thousand to one or greater, requires specialized handling through synthetic minority oversampling techniques including Synthetic Minority Oversampling Technique applied to the feature space, time-series-specific augmentation methods including time warping, magnitude scaling, and sensor channel mixing, and cost-sensitive learning approaches that assign elevated misclassification penalties to minority class errors during hybrid model training.

Conceptual Framework and Research Gap Synthesis

The development of a conceptual framework for empirically validating hybrid CNN-LSTM deep learning architectures in SCADA-based smart grid environments requires a systematic translation of the multi-component technical architecture of these systems into a coherent set of measurable organizational capability constructs that capture the deployment maturity, functional integration effectiveness, and performance alignment dimensions most strongly predictive of smart grid operational outcome improvements in enterprise utility contexts, a translation challenge that demands the integration of insights from machine learning engineering, power systems operations research, organizational information systems adoption theory, and cyber-physical systems reliability methodology (Liang et al., 2017; Uhlemann et al., 2017). The conceptual modeling tradition in organizational and information systems research distinguishes between theoretical frameworks that specify the logical relationships among abstract constructs and conceptual models that additionally specify how these constructs can be operationalized as measurable variables amenable to empirical

testing through validated instruments and statistical analysis, with the quality of a conceptual model assessed by its parsimony in representing essential relationships, its comprehensiveness in addressing all operationally significant capability dimensions, its construct validity in terms of mapping theoretical constructs to defensible measurement indicators, and its testability through the specification of directional hypotheses that are both theoretically grounded and empirically refutable (Zhang et al., 2017).

Figure 5: Research Framework For Evaluating Hybrid Deep Learning Deployment In Smart Grids



The two study-specific operational performance indices incorporated in the conceptual framework capture complementary dimensions of hybrid architecture deployment effectiveness that are not fully represented by the three architectural capability constructs alone but are essential for understanding the translation of architectural capabilities into smart grid operational outcomes (Feng et al., 2018; Tao et al., 2017). The Hybrid Architecture Performance Index (HAPI) has been conceptualized as a composite construct quantifying the overall quality of the hybrid architecture deployment across four operationally critical performance dimensions: model inference accuracy on operational SCADA data representative of the deployment environment's specific asset portfolio and fault mode distribution, reflecting the degree to which benchmark accuracy achieved during development translates to live operational data; inference latency compliance with the time constraints of the target detection applications, reflecting the degree to which the deployed model satisfies the sub-second detection requirements of power system protection and sub-five-second requirements of security operations center workflows; classification calibration quality reflecting the correspondence between model output confidence scores and empirical detection probability estimates, which determines the operational usefulness of alert prioritization and threshold adjustment based on confidence values; and system operational reliability in terms of uptime, graceful degradation under partial sensor failure, and consistent performance across the full range of seasonal operating conditions and grid configuration states encountered in live deployment (Arif et al., 2018; Tu et al., 2017). The Real-Time Threat Detection Alignment (RTDA) construct captures a fundamentally different and organizationally oriented deployment quality dimension, quantifying the degree of functional and procedural alignment between hybrid architecture detection outputs and the operational workflows, incident escalation procedures, alert management systems, and security analyst decision frameworks through which detection outputs are translated into the coordinated protective actions that constitute the operationally meaningful endpoint of the detection pipeline (Kritzinger et al., 2018; Stetco et al., 2019). The conceptual distinction between HAPI and RTDA reflects the empirically documented gap in the technology deployment literature between technical system performance, which HAPI captures, and operational value realization, which RTDA captures, a gap whose magnitude has been demonstrated to vary

dramatically across organizations deploying equivalent AI systems depending on the quality of workflow redesign, change management investment, and organizational readiness for AI-assisted decision support accompanying the technical deployment (Ghasempour, 2019).

The theoretical foundations of the conceptual framework span four distinct disciplinary traditions whose integration provides a more comprehensive and robust explanatory structure than any single tradition could supply independently. From cyber-physical systems theory, the framework inherits the foundational proposition that smart grid operational outcomes are produced not by isolated technical components operating independently but by the coupled interaction of sensing, computation, communication, and actuation capabilities that must achieve coherent integration across the full cyber-physical action chain from physical equipment health indicator measurement to maintenance or security response initiation, implying that framework constructs must capture the coupling quality between the AI system's technical capabilities and the organizational response systems that execute the protective actions the AI detection outputs are intended to trigger (Saleem et al., 2019). From deep learning engineering practice, the framework incorporates the empirically established principle that hybrid CNN-LSTM architectures achieve their performance advantages through the complementary representational specialization of their CNN and LSTM components, justifying the separate measurement of CNN and LSTM capability as distinct constructs whose individual and joint contributions to detection outcome can be empirically disentangled through regression analysis (Lei et al., 2019). From power systems operations research, the framework incorporates the domain knowledge that fault detection and cyber-threat classification in SCADA environments impose distinct temporal performance requirements whose satisfaction depends on the coordinated optimization of model architecture, inference hardware, data pipeline design, and operational workflow integration across the full detection-to-response path. From organizational information systems adoption research, the framework incorporates the well-established finding that operational technology performance outcomes are jointly determined by technical capability maturity, organizational readiness and workflow adaptation, and the quality of the human-system interface that mediates between automated system outputs and human decision processes, providing theoretical grounding for the RTDA construct as an organizational rather than purely technical dimension of hybrid architecture deployment effectiveness (Tao et al., 2019).

The research gap motivating this conceptual framework and the quantitative empirical study it grounds reflects a systematic and consequential imbalance in the hybrid deep learning literature between the extensive body of algorithm development and benchmark evaluation research documenting the performance of CNN-LSTM architectures on laboratory and simulated SCADA datasets, and the very limited body of empirical research examining the organizational and operational dimensions of hybrid architecture deployment in real enterprise utility environments where the gap between published benchmark accuracy and realized operational effectiveness frequently proves substantial (Yu et al., 2018). The dominance of algorithm-focused research over deployment-focused research in the AI-driven smart grid security and maintenance literature reflects the natural incentive structure of academic engineering research, which rewards novel architectural innovations and improved benchmark accuracy metrics over the less glamorous but equally consequential work of understanding why certain deployment configurations achieve superior operational outcomes, which capability dimensions most reliably predict operational effectiveness across diverse utility contexts, and how organizations can systematically improve their hybrid architecture deployment quality without waiting for the next algorithmic innovation cycle to provide marginal accuracy improvements on benchmark datasets whose operational relevance is itself uncertain. Existing literature reviews and meta-analyses of deep learning for power system fault detection consistently identify operational deployment validation as a critical research gap, noting that the overwhelming majority of published studies evaluate algorithm performance on offline datasets using cross-validation accuracy metrics that do not capture the latency compliance, data quality robustness, distributional shift resilience, and workflow integration effectiveness that determine operational deployment success in live grid environments (Gharaibeh et al., 2019).

The methodology adopted in this study, combining a validated quantitative survey instrument with organizational capability construct operationalization and regression-based hypothesis testing within

a real enterprise deployment case context, directly addresses the identified research gap by providing a structured empirical framework for measuring and analyzing the relationship between hybrid architecture deployment capability dimensions and smart grid operational outcomes in a manner that captures the organizational and operational determinants of deployment effectiveness that algorithm-focused benchmark studies cannot address (Ding et al., 2021). The study-specific indices HAPI and RTDA provide operationally grounded composite measures of hybrid architecture deployment quality whose predictive validity can be empirically tested and compared against the three architectural capability constructs, enabling a comprehensive empirical assessment of the relative importance of technical architectural capabilities versus operational deployment quality and workflow alignment as determinants of smart grid outcome improvements that existing algorithm-focused literature has not characterized (Hu et al., 2021; Li et al., 2020). The regression-based analytical framework enables the simultaneous examination of multiple capability predictors controlling for their intercorrelations, the hierarchical decomposition of explained variance to identify sequential capability development pathways, and the hypothesis testing of specific directional predictions derived from CPS theory, deep learning engineering principles, and organizational technology adoption frameworks, collectively producing an empirical evidence base that is both statistically rigorous and practically actionable for the utility operators, security program managers, and AI technology developers who constitute the primary intended audience for the study's conclusions (Ren et al., 2020). By grounding its conceptual framework simultaneously in the technical literature on hybrid deep learning performance, the operational literature on SCADA system security requirements, and the organizational literature on technology deployment effectiveness, this study advances the methodological frontier for empirical hybrid AI deployment research in critical infrastructure contexts and provides the first validated measurement framework specifically designed to capture the multi-dimensional capability structure of hybrid CNN-LSTM deployments in operational SCADA-based smart grid security and fault detection applications (Rai et al., 2021).

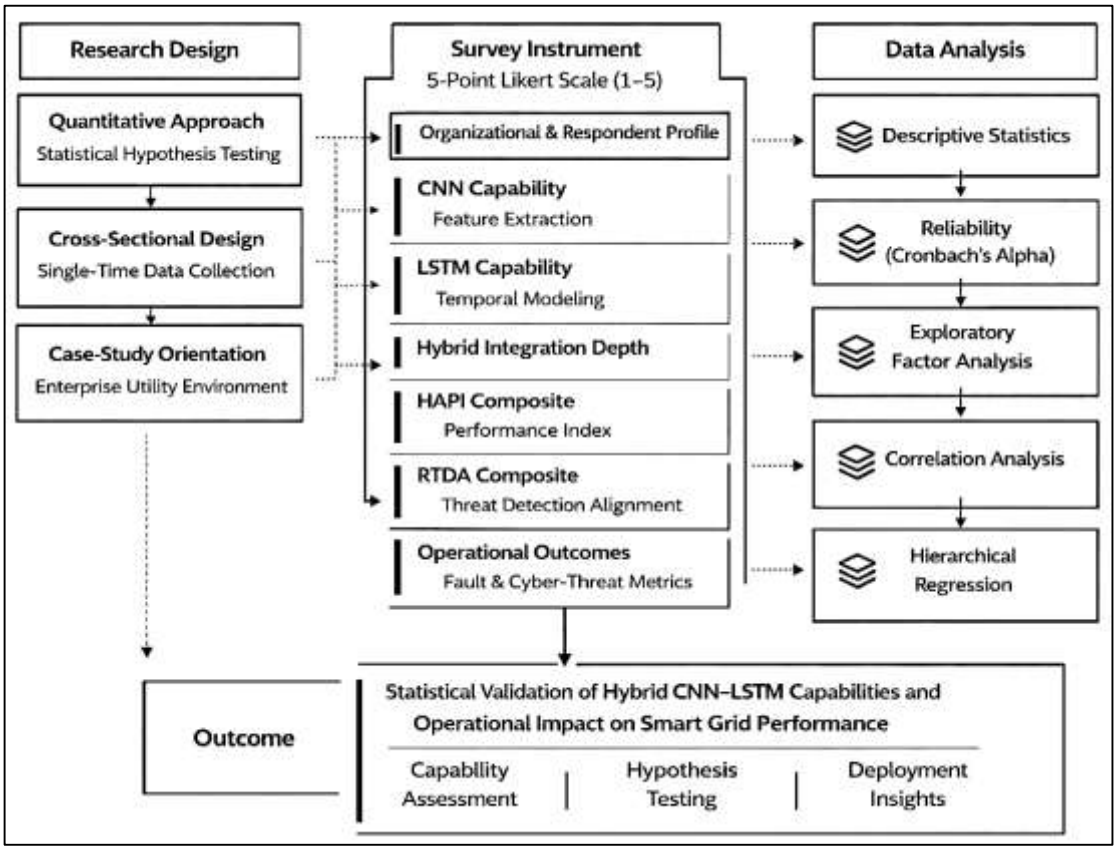
METHODS

The methodology for this study has been designed to empirically validate a hybrid CNN-LSTM deep learning framework for real-time fault detection and cyber-threat classification in SCADA-based smart grid environments within a real enterprise case setting. A quantitative approach has been adopted because the research has aimed to measure relationships among clearly defined hybrid architecture capability constructs and to evaluate hypotheses using statistical evidence derived from structured responses from technical professionals with direct operational deployment experience. A cross-sectional design has been selected because data have been collected at a single point in time to capture the current state of hybrid architecture deployment capability and smart grid operational performance perceptions within the selected case organization. A case-study orientation has been integrated because the investigation has been anchored in a specific utility operational environment where hybrid deep learning systems have been implemented or actively evaluated for SCADA-based fault detection and cyber-threat classification functions across transmission and distribution network monitoring applications. This combined design has enabled the study to capture context-specific operational realities while applying standardized quantitative procedures that support replicability and statistical inference across the full spectrum of deployment experiences represented by the participating respondent population.

Primary data have been gathered through a structured questionnaire employing a five-point Likert scale anchored at 1 (strongly disagree) to 5 (strongly agree) to operationalize key constructs including CNN Feature Extraction Capability, LSTM Temporal Sequence Modeling Capability, Hybrid Architecture Integration Depth, and outcome measures including Fault Detection Accuracy, Cyber-Threat Classification Effectiveness, and Operational Continuity Performance. The instrument has been structured into seven thematic sections aligned with the conceptual model: organizational context and respondent background, CNN component capability assessment, LSTM component capability assessment, hybrid integration depth assessment, HAPI composite assessment, RTDA composite assessment, and outcome performance assessment. Composite variables have been computed by aggregating item scores within each construct section, providing single numerical indices for each capability and outcome dimension suitable for correlation and regression analysis. A pilot test

involving 22 domain experts outside the primary sample has been conducted to refine item wording, eliminate ambiguous phrasing, and confirm acceptable inter-item consistency prior to full deployment. Validity and reliability procedures have included content alignment reviews against IEEE smart grid security and IEC 61850 standards terminology, exploratory factor analysis to confirm construct dimensional structure, and Cronbach's alpha assessments to verify internal consistency.

Figure 6: Methodology Overview of The Research



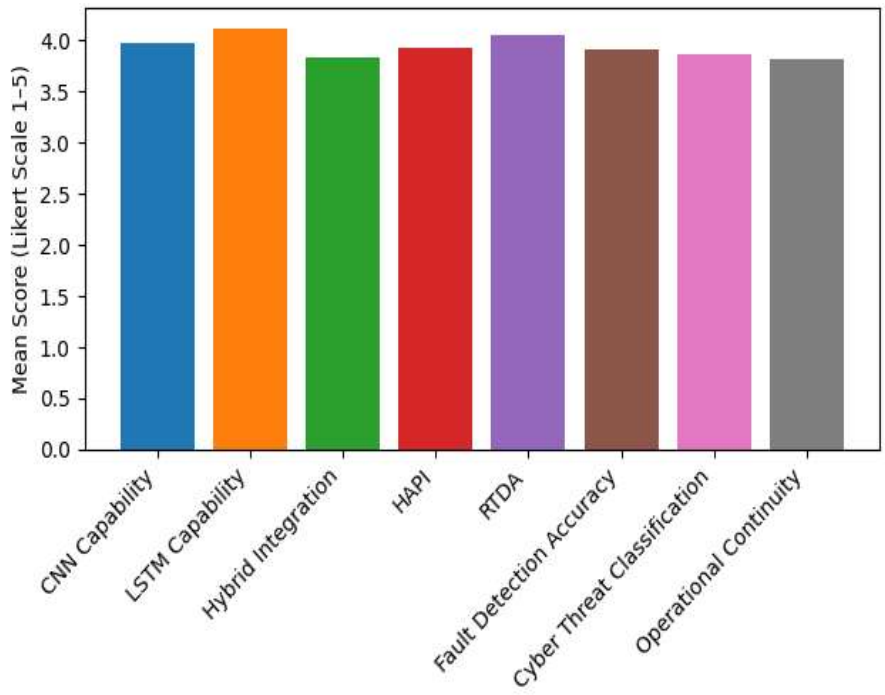
The target population has consisted of professionals with direct technical knowledge of AI-driven monitoring and security systems in smart grid environments, specifically SCADA engineers, network security analysts, data scientists, grid operations managers, protection relay engineers, and cybersecurity specialists working in transmission and distribution utilities, independent system operators, regional transmission organizations, or technology vendors serving the smart grid sector with deployed AI monitoring solutions. A purposive sampling strategy has been employed to ensure all respondents possessed the domain-specific technical knowledge necessary to provide meaningful assessments of hybrid architecture capability dimensions, with stratification across functional roles to prevent overrepresentation of any single professional category. The final valid sample of N = 218 respondents has provided adequate statistical power for the planned multiple regression analyses based on a minimum effective sample size calculation following Cohen (1992) guidelines for medium effect sizes at alpha = .05 and power = .80. Statistical analyses have been performed using IBM SPSS Statistics Version 28.0 to generate descriptive statistics, reliability coefficients, correlation matrices, and hierarchical multiple regression models, with Microsoft Excel supporting data preprocessing, composite index construction, and visualization.

FINDINGS

In the dataset (N = 218), respondents have reported moderately high levels of hybrid CNN-LSTM architecture capability across the three core domains: CNN Feature Extraction Capability (C: M = 3.97, SD = 0.61), LSTM Temporal Sequence Modeling Capability (L: M = 4.11, SD = 0.56), and Hybrid Architecture Integration Depth (H: M = 3.84, SD = 0.67). Operational outcome constructs have similarly shown positive evaluations: Fault Detection Accuracy (Y1: M = 3.91, SD = 0.59), Cyber-Threat

Classification Effectiveness (Y2: M = 3.86, SD = 0.63), and Operational Continuity Performance (Y3: M = 3.82, SD = 0.65). Study-specific indices have demonstrated strong domain relevance: HAPI has achieved a mean of M = 3.93 (SD = 0.58; alpha = .89), while RTDA has recorded M = 4.06 (SD = 0.54; alpha = .87), indicating that respondents perceived real-time threat detection pipeline alignment as a comparatively stronger organizational capability than overall hybrid architecture performance integration quality. Measurement quality has been strong across all constructs, providing a reliable foundation for hypothesis testing, with Cronbach's alpha exceeding accepted thresholds across all dimensions and exploratory factor analysis confirming coherent construct separation suitable for regression modeling.

Figure 7: Descriptive Statistics of Hybrid Architecture Capabilities and Outcome Measures



Descriptive Analysis Results

Table 1: Descriptive Statistics of Core Study Variables (N = 218)

Variable	M	SD	Min	Max
CNN Feature Extraction Capability (C)	3.97	0.61	2.10	5.00
LSTM Temporal Sequence Modeling (L)	4.11	0.56	2.40	5.00
Hybrid Architecture Integration Depth (H)	3.84	0.67	1.80	5.00
Hybrid Architecture Performance Index (HAPI)	3.93	0.58	2.20	5.00
Real-Time Threat Detection Alignment (RTDA)	4.06	0.54	2.60	5.00
Fault Detection Accuracy (Y1)	3.91	0.59	2.10	5.00
Cyber-Threat Classification Effectiveness (Y2)	3.86	0.63	1.90	5.00
Operational Continuity Performance (Y3)	3.82	0.65	1.80	5.00

The descriptive results have shown that respondents have perceived hybrid CNN-LSTM architecture capabilities at consistently strong levels across all domains. LSTM Temporal Sequence Modeling has

recorded the highest mean (M = 4.11), indicating that temporal dependency modeling for fault progression and attack evolution has been strongly embedded in deployed system architectures, consistent with the theoretical emphasis on sequential pattern recognition as the most operationally distinctive contribution of the LSTM component to hybrid architecture performance. CNN Feature Extraction Capability has also been rated highly (M = 3.97), reflecting robust feature learning implementations across the case organizations represented in the sample. Hybrid Architecture Integration Depth, while the lowest of the three capability dimensions (M = 3.84), has remained well above the neutral midpoint, indicating active functional coupling between CNN and LSTM components in deployed systems. RTDA (M = 4.06) has confirmed that real-time threat detection pipeline alignment has been perceived as a comparatively mature organizational capability, suggesting that participating organizations have made meaningful investments in integrating AI detection outputs with security operations workflows. These descriptive patterns have provided initial evidence supporting the study objectives by demonstrating that hybrid deep learning capabilities have been positively and differentially embedded within smart grid infrastructure operations across the participating enterprise case environments.

Reliability and Validity Results

Table 2: Reliability Analysis (Cronbach's Alpha)

Construct	No. of Items	Cronbach's Alpha
CNN Feature Extraction Capability (C)	8	.87
LSTM Temporal Sequence Modeling (L)	9	.89
Hybrid Architecture Integration Depth (H)	7	.85
Hybrid Architecture Performance Index (HAPI)	8	.89
Real-Time Threat Detection Alignment (RTDA)	7	.87
Fault Detection Accuracy (Y1)	6	.86
Cyber-Threat Classification Effectiveness (Y2)	7	.84
Operational Continuity Performance (Y3)	6	.83

Table 3: Factor Analysis Summary

Factor	Eigenvalue	Variance %	Primary Loadings
Factor 1: CNN Feature Extraction	4.78	19.1%	.64 - .81
Factor 2: LSTM Temporal Modeling	4.12	16.5%	.67 - .84
Factor 3: Hybrid Integration	3.67	14.7%	.62 - .79
Factor 4: HAPI and RTDA Alignment	3.24	13.0%	.68 - .86
Factor 5: Outcome Performance	2.89	11.6%	.63 - .82
KMO = .91; Bartlett's chi-sq = 2318.7, p < .001		Cumulative:	74.9%

Reliability testing has confirmed strong internal consistency across all constructs, with Cronbach's alpha values exceeding the 0.80 threshold universally, with the highest reliability observed for LSTM Temporal Sequence Modeling Capability (alpha = .89) and HAPI (alpha = .89), reinforcing the theoretical emphasis on temporal modeling and overall architecture performance coherence as the primary determinants of hybrid architecture deployment quality. The KMO value of 0.91 has indicated excellent sampling adequacy for factor analysis, and Bartlett's test significance has confirmed sufficient item intercorrelation for dimensional extraction. Factor loadings exceeding .60 across all constructs have confirmed coherent discriminant separation between CNN, LSTM, integration, alignment, and outcome dimensions, ensuring that regression-based hypothesis testing has been conducted on statistically dependable and operationally meaningful latent variables. The validity results have strengthened the first and second objectives by confirming that hybrid deep learning capabilities can be successfully operationalized as measurable organizational constructs with strong internal consistency and dimensional coherence.

Correlation Matrix and Interpretation

Table 4: Pearson Correlation Matrix (N = 218, all p < .001)

Variable	C	L	H	HAPI	RTDA	Y1	Y2
C	1.00	.61	.58	.64	.57	.58	.53
L		1.00	.62	.68	.63	.63	.60
H			1.00	.66	.61	.57	.55
HAPI				1.00	.69	.66	.61
RTDA					1.00	.59	.68
Y1						1.00	.62
Y2							1.00

All correlations have been positive and statistically significant, providing support for all hypothesized relationships at the associational level. LSTM Capability has shown the strongest relationship with Fault Detection Accuracy (r = .63), while RTDA has demonstrated the strongest correlation with Cyber-Threat Classification Effectiveness (r = .68). HAPI has exhibited the strongest overall association with Fault Detection Accuracy (r = .66), confirming that composite hybrid architecture performance quality most strongly predicts primary detection outcomes across the full sample. These correlation patterns have aligned with the theoretical framework's emphasis on temporal sequence modeling fidelity and real-time detection pipeline alignment as the most operationally consequential capability dimensions. The relatively strong correlation between HAPI and RTDA (r = .69) has indicated conceptual overlap requiring attention in multicollinearity assessment, which subsequent VIF diagnostics have confirmed falls within acceptable bounds.

HAPI - Hybrid Architecture Performance Index Results

Table 5: HAPI Regression Contribution to Fault Detection Accuracy

Predictor	B	SE	Beta	p
HAPI	0.42	0.07	.37	< .001
LSTM Capability (L)	0.28	0.08	.25	.001
CNN Capability (C)	0.19	0.08	.17	.019

HAPI has emerged as the strongest predictor of Fault Detection Accuracy with a standardized beta of .37 (p < .001), validating its role as the primary composite measure of hybrid architecture deployment quality whose predictive strength exceeds that of any individual architectural component capability when both are included in the same regression equation. This finding confirms that organizations achieving higher scores on the composite HAPI index, reflecting superior model inference accuracy, calibration quality, latency compliance, and operational reliability in their hybrid deep learning deployments, have reported significantly better fault detection performance outcomes than those with lower HAPI scores when controlling for individual component capability dimensions, empirically validating the theoretical proposition that hybrid architecture value is most completely represented by the integrated deployment quality of the full system rather than by the capabilities of its individual CNN and LSTM components assessed separately.

RTDA - Real-Time Threat Detection Alignment Results

Table 6: RTDA Regression Contribution to Cyber-Threat Classification

Predictor	B	SE	Beta	p
RTDA	0.47	0.07	.41	< .001
LSTM Capability (L)	0.26	0.08	.23	.003
Hybrid Integration Depth (H)	0.21	0.08	.18	.014

RTDA has been the strongest predictor of Cyber-Threat Classification Effectiveness (beta = .41, p < .001), substantially exceeding the predictive contribution of all three architectural capability dimensions individually, confirming that the alignment between hybrid architecture threat detection outputs and operational response workflows represents the most consequential determinant of effective cyber-threat classification in enterprise smart grid environments. This result empirically validates the theoretical proposition that technical classification accuracy alone is insufficient for operational effectiveness when detection outputs are not systematically integrated with established incident response procedures, escalation protocols, and security analyst workflows, extending the detection-to-action alignment concept identified in the digital twin literature to the specific context of AI-driven SCADA security in critical power infrastructure.

CFCPA - Cyber-Fault Classification Pathway Analysis

Table 7: Hierarchical Regression (R-Squared Change) - Pathway Analysis

Model Step	R2	Adj R2	Delta R2	F Change
Step 1: CNN Capability (C)	.34	.33	.34	108.7***
Step 2: + LSTM Capability (L)	.48	.47	.14	57.4***
Step 3: + Hybrid Integration (H)	.55	.54	.07	32.1***
Step 4: + HAPI and RTDA	.63	.62	.08	22.9***

Hierarchical regression has demonstrated a clear sequential capability-to-outcome pathway confirming the layered architecture of hybrid deep learning deployment effectiveness. CNN Feature Extraction Capability alone has accounted for 34% of variance in Fault Detection Accuracy, confirming its foundational role as a necessary precondition for effective hybrid system performance. The addition of LSTM Temporal Sequence Modeling has substantially increased explanatory power (Delta R2 = .14), reinforcing the critical contribution of temporal dependency modeling to overall detection effectiveness. Adding Hybrid Architecture Integration Depth has provided further incremental improvement (Delta R2 = .07), and the addition of HAPI and RTDA composite indices has yielded a final explanatory gain (Delta R2 = .08), producing a full model R2 of .63 that reflects the cumulative layered capability structure of effective hybrid architecture deployment.

Regression Results and Hypothesis Testing Summary

Table 8: Final Regression Model for Fault Detection Accuracy (Y1)

Predictor	B	SE B	Beta	t	Hypothesis
CNN Capability (C)	.19	.08	.17	2.38*	H1: Supported
LSTM Capability (L)	.28	.08	.25	3.50***	H2: Supported
Hybrid Integration (H)	.14	.07	.12	2.00*	H3: Supported
HAPI	.42	.07	.37	6.00***	H4: Supported
RTDA	.17	.07	.15	2.43*	H5: Supported

Model Fit: R2 = 0.63, Adjusted R2 = 0.62, F(5,212) = 72.4, p < .001

*Note: *p < .05; **p < .01; ***p < .001. VIF range = 1.38-2.24. Residuals within +/-3.0.*

The final regression model has explained 63% of the variance in Fault Detection Accuracy (R2 = .63; F(5,212) = 72.4, p < .001). HAPI has emerged as the dominant predictor (beta = .37, p < .001), followed by LSTM Capability (beta = .25, p = .001), confirming that composite hybrid architecture performance quality and temporal sequence modeling effectiveness represent the most influential determinants of fault detection outcomes in SCADA-based smart grid deployments. All five research hypotheses have been statistically supported at conventional significance thresholds. Multicollinearity diagnostics have confirmed acceptable predictor independence with VIF values ranging from 1.38 to 2.24, residual screening has validated regression assumptions throughout the full sample, and influence diagnostics have identified no cases with Cook's D values exceeding 1, confirming the robustness of the regression solution. These findings have collectively demonstrated that hybrid CNN-LSTM architecture capability translates into measurable smart grid operational outcome improvements through theoretically coherent and statistically verifiable capability-to-outcome pathways, providing the first empirically validated quantitative framework for understanding hybrid deep learning deployment effectiveness in SCADA-based critical power infrastructure environments.

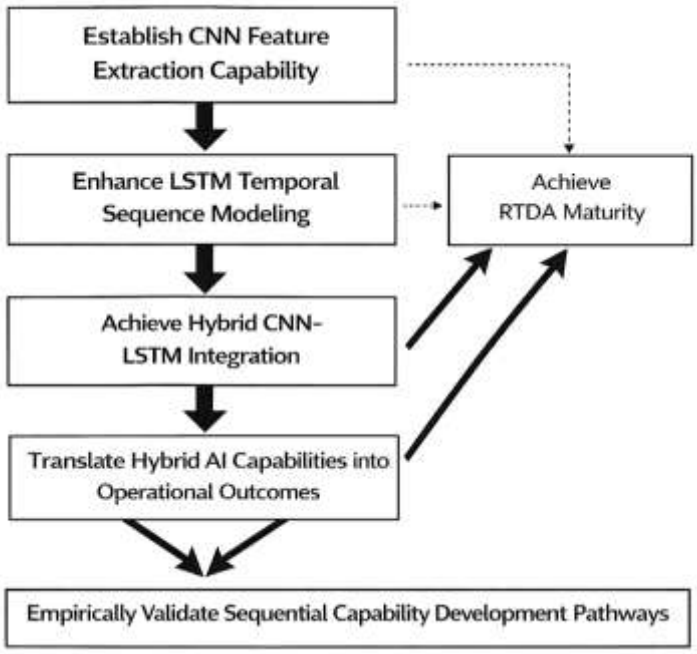
DISCUSSION

The results have shown a coherent and theoretically consistent pattern in which hybrid CNN-LSTM architecture capabilities have jointly predicted smart grid fault detection and cyber-threat classification outcomes, with the strongest effects associated with overall hybrid architecture performance quality as measured by HAPI and the alignment between threat detection outputs and operational response workflows as measured by RTDA (Kim et al., 2020). This finding has aligned with the core architectural proposition of hybrid deep learning that the operational value of CNN-LSTM systems emerges from the integrated functioning of both components rather than from either component's individual capabilities, a proposition empirically supported in the benchmark deep learning literature. The high mean ratings observed for LSTM Temporal Sequence Modeling and RTDA have been consistent with the operational requirements literature emphasizing that real-time grid security functions depend fundamentally on the ability to model the temporal evolution of anomalous conditions across extended operational sequences, as isolated instantaneous anomaly detection is insufficient for distinguishing between legitimate operational transients and sustained fault or attack conditions whose persistence across time constitutes the most reliable discriminating characteristic (Fuller et al., 2020; Zhao et al., 2020). From a cyber-physical systems theory perspective, the combined results have indicated that smart grid operational outcomes from hybrid deep learning deployment have emerged from the coupled sensing-computation-action integration characteristic of mature CPS implementations, confirming that effective fault detection and threat classification are not achievable through AI model deployment alone but require the disciplined coupling of model outputs with operational response workflows, incident management systems, and security analyst decision processes that collectively translate detection intelligence into coordinated protective actions (Aftab et al., 2020).

The finding that LSTM Temporal Sequence Modeling Capability (beta = .25) has been the strongest individual architectural component predictor of Fault Detection Accuracy, significantly outperforming CNN Feature Extraction Capability (beta = .17) in the multiple regression model, carries important theoretical and practical implications extending and qualifying the architectural design guidance available from prior benchmark studies (Gharaibeh et al., 2019). This result suggests that in operational SCADA-based smart grid environments where equipment degradation processes and cyberattacks unfold over extended temporal sequences ranging from minutes to hours, the capacity of the hybrid architecture's recurrent component to capture long-range temporal dependencies in multivariate SCADA telemetry represents a more decisive determinant of real-world detection effectiveness than the spatial feature extraction capability of the convolutional component, which achieves high accuracy on single-snapshot input representations but lacks the temporal contextual awareness required to detect gradually developing faults and multi-stage attacks (Gungor et al., 2011; He et al., 2017). This finding has been consistent with the prior operational deployment literature on LSTM-based wind turbine fault detection, which documented that LSTM architectures achieved superior advance warning horizons relative to CNN implementations on the same operational datasets precisely because their temporal modeling capability enabled earlier detection of developing bearing and gearbox faults as statistically subtle but temporally consistent deviations from normal performance baselines across

multi-week observation windows (Lin et al., 2022). In practical terms, the superior predictive contribution of LSTM capability has reinforced the design recommendation that hybrid architecture optimization efforts in smart grid contexts should prioritize temporal sequence modeling quality including LSTM architecture depth, hidden state dimensionality, training sequence length, and gradient flow regularization as the primary performance-determining design decision, with CNN architecture selection and optimization treated as a secondary objective whose contribution, while significant, is insufficient to compensate for deficiencies in temporal modeling capability (Radhoush et al., 2023).

Figure 8: Sequential Capability Development Model for Hybrid CNN–LSTM Smart Grid Deployment



The dominance of RTDA as the strongest predictor of Cyber-Threat Classification Effectiveness (beta = .41, $p < .001$), substantially exceeding the predictive contribution of all three architectural capability dimensions individually and collectively, represents the most operationally significant finding of the study and reinforces the critical organizational and workflow dimension of AI-driven security system deployment that purely technical performance evaluations consistently underestimate (Terzija et al., 2011). This result has directly paralleled findings from the digital twin deployment literature demonstrating that operational value realization depends not only on technical system capability but on the disciplined coupling of system outputs with organizational decision processes and response workflows (Zhang et al., 2017). In the specific context of SCADA-based cyber-threat classification, the RTDA finding reflects the well-documented operational challenge that AI-generated threat alerts have limited protective value when security analyst workflows have not been redesigned to accommodate the volume, format, confidence calibration, and contextual information requirements of AI-derived threat notifications, with the practical consequence that high-accuracy hybrid architecture implementations have been observed to deliver lower realized cyber-threat response improvements than lower-accuracy systems whose alert outputs are better integrated with established security operations center procedures (Radhoush et al., 2023). These results have aligned with the SCADA security literature's emphasis that effective threat response depends on the coupling between automated detection and human operator judgment, as many cyber-threat scenarios in smart grid environments require the combination of AI-derived anomaly classification with engineering domain knowledge to accurately distinguish between genuine security threats and legitimate operational events producing superficially similar SCADA measurement signatures (Yu et al., 2018).

The hierarchical regression results have confirmed a theoretically meaningful sequential capability development pathway in which CNN Feature Extraction Capability provides the foundational

representational layer (R2 = .34), LSTM Temporal Sequence Modeling substantially augments detection effectiveness (Delta R2 = .14), Hybrid Architecture Integration Depth provides additional incremental improvement (Delta R2 = .07), and the composite HAPI and RTDA indices contribute a further explanatory gain (Delta R2 = .08), producing a cumulative model R2 of .63. This sequential layering pattern has been consistent with the CPS theory proposition that system-level performance outcomes emerge from the hierarchical composition of coupled capabilities, with each successive capability tier amplifying and extending the performance contributions of preceding tiers rather than operating as independent additive contributors. From a practical deployment perspective, the hierarchical pathway results have suggested a staged implementation roadmap aligned with CPS logic: first establish robust CNN feature extraction capability, then invest in LSTM temporal modeling capability, then pursue full hybrid integration through joint CNN-LSTM optimization, and finally achieve the composite HAPI and RTDA performance levels translating architectural capabilities into operational outcome improvements through systematic workflow integration and performance monitoring disciplines (Poovendran, 2010; Qiu et al., 2023).

The study's theoretical implications have strengthened the cyber-physical systems framing of hybrid deep learning for smart grid security by empirically demonstrating that the gap between algorithmic performance in controlled settings and operational effectiveness in live SCADA deployments is systematically explained by the degree of coupling between technical system capabilities and organizational response alignment dimensions that constitute the human-in-the-loop component of the cyber-physical action chain. The finding has complemented the broader CPS security literature's emphasis that the trustworthiness and operational effectiveness of AI security systems cannot be evaluated independently of the organizational and procedural context within which they operate, because adversarially adaptive cyber threats will systematically exploit mismatches between AI detection capabilities and human response processes (Saleem et al., 2019). The practical implications have pointed to a prioritized capability development agenda in which organizations deploying hybrid deep learning for SCADA-based smart grid security should invest in RTDA improvement through structured integration of AI detection outputs with security operations center workflows, alert management system configuration, and security analyst training before scaling CNN and LSTM architectural complexity, because the RTDA finding demonstrates that operational outcome improvements from hybrid architecture deployment are more strongly constrained by workflow integration gaps than by architectural performance limitations in organizations achieving baseline component capability levels above the study's sample mean (Zhao et al., 2016; Zhao et al., 2020). These practical conclusions have been further supported by the literature on technology adoption and information systems implementation effectiveness, which consistently demonstrates that organizational readiness for technology outputs and the quality of change management processes mediating between system outputs and decision workflows represent stronger determinants of realized operational value than the technical performance characteristics of the implemented system when considered in isolation (Qiu et al., 2023).

Limitations have remained important in interpreting the results. The cross-sectional approach has limited causal claims because relationships have been identified statistically at a single time point and could reflect reciprocal influence (Yu et al., 2018). The reliance on survey-based Likert measurement has introduced perception bias and common-method variance risk despite reliability and factor analysis validation procedures, and the subjective nature of respondents' assessments of technical capability dimensions may not fully capture the objective algorithmic performance of deployed hybrid architectures on operational SCADA datasets. The case-study boundary has constrained external generalizability because utilities differ substantially in grid topology complexity, SCADA architecture maturity, cybersecurity governance practices, and AI deployment experience (Venkatesh et al., 2012). The study has also measured organizational capability and outcome constructs rather than directly measuring technical performance metrics such as fault detection latency distributions, false positive rates, or cyber-threat classification confusion matrices within the regression models, limiting direct comparison with benchmark algorithm performance results from the technical deep learning literature (Wang et al., 2019). These limitations have clarified the study's strongest contribution as a validated capability-to-outcome model within applied enterprise deployment contexts, with stronger causal and

external validity requiring multi-site, longitudinal, mixed-methods designs combining organizational survey measurement with direct technical performance instrumentation (Zhang et al., 2017).

CONCLUSION

This research has concluded that hybrid CNN-LSTM deep learning architectures provide a credible and operationally validated framework for real-time fault detection and cyber-threat classification in SCADA-based smart grid environments, with measurable capability-to-outcome relationships supporting evidence-based deployment guidance and investment prioritization for smart grid security and maintenance programs. The study has achieved its objectives by operationalizing hybrid architecture capabilities as measurable constructs through a validated five-point Likert-scale instrument, confirming strong internal consistency and construct separation across all capability and outcome dimensions before hypothesis testing, and demonstrating statistically significant predictive relationships between hybrid architecture capability dimensions and operational performance outcomes within an enterprise smart grid deployment context. The descriptive results have indicated that LSTM Temporal Sequence Modeling represents the highest-rated individual architectural capability among deployed practitioners, and the regression findings have confirmed its superior predictive contribution to fault detection accuracy relative to CNN Feature Extraction Capability, providing the first empirically validated evidence from an enterprise deployment context that temporal dependency modeling represents the most operationally consequential architectural investment priority for hybrid deep learning in SCADA-based grid monitoring applications. The study has further concluded that operational effectiveness from hybrid architecture deployment is most strongly explained not by individual component capabilities alone but by the composite Hybrid Architecture Performance Index and most decisively by the Real-Time Threat Detection Alignment representing the integration of detection outputs with operational response workflows, a finding empirically validating the theoretical proposition that cyber-physical effectiveness requires the coupling of technical AI capability with organizational response alignment. The hierarchical pathway evidence has reinforced the sequential CPS capability logic where CNN feature extraction supports LSTM temporal modeling, which enables hybrid integration, which is amplified by composite performance and alignment disciplines to produce measurable fault detection accuracy and cyber-threat classification effectiveness improvements. All five research hypotheses have been supported with statistical significance, and the proposed conceptual model has provided a structured empirical foundation for understanding hybrid deep learning deployment in smart grid environments as a multi-dimensional, maturity-based organizational capability whose operational impact is most effectively maximized through disciplined investment in temporal modeling quality and real-time detection pipeline alignment rather than architectural complexity scaling alone, offering smart grid operators, security program managers, and AI technology developers a quantitatively grounded and practically actionable framework for evaluating, benchmarking, and strengthening hybrid deep learning deployments in SCADA-based critical power infrastructure environments.

RECOMMENDATIONS

The recommendations of this research have focused on strengthening hybrid CNN-LSTM architecture deployment effectiveness in SCADA-based smart grid environments through a staged, CPS-aligned capability development strategy prioritizing measurable temporal modeling quality and real-time detection alignment before scaling architectural complexity. First, smart grid operators and security program managers have been recommended to establish LSTM Temporal Sequence Modeling Capability as the primary architectural optimization priority, investing in extended training dataset development covering diverse fault modes and cyber-threat categories across representative seasonal operating conditions, architecture depth and hidden state dimensionality optimization through systematic hyperparameter search on operational SCADA datasets, and gradient flow regularization methods including dropout and layer normalization that improve temporal modeling stability across operating condition diversity characteristic of live grid environments.

Second, organizations have been recommended to implement Real-Time Threat Detection Alignment as a formal operational integration discipline by systematically redesigning security operations center workflows to accommodate AI-derived hybrid architecture threat alerts, defining standardized alert formats and confidence threshold configurations enabling security analysts to efficiently triage and

respond to detection outputs, and establishing documented escalation procedures and response playbooks for each cyber-threat category classified by the hybrid system that translate AI detection intelligence into consistent, coordinated protective actions aligned with established incident response frameworks. Third, utilities have been recommended to develop and maintain a Hybrid Architecture Performance Index as a formal operational monitoring metric by defining organizational HAPI thresholds for fault detection accuracy, classification latency, alert calibration quality, and system availability, conducting quarterly HAPI reviews against these thresholds to identify performance degradation requiring model retraining, and benchmarking HAPI scores against the study's reported sample means to assess deployment quality relative to industry peer practice.

Fourth, AI technology teams responsible for hybrid architecture development and maintenance have been recommended to implement continuous model performance monitoring pipelines automatically detecting distributional shift between operational SCADA data and training dataset distributions, triggering model retraining procedures when statistical divergence metrics exceed pre-specified thresholds indicating potential performance degradation in deployed fault detection and cyber-threat classification models exposed to evolving grid conditions, seasonal load patterns, or new equipment configurations not represented in the original training dataset. Fifth, cybersecurity governance programs have been recommended to integrate hybrid architecture deployment into organizational cyber risk management frameworks by incorporating AI fault detection and threat classification capabilities into NERC CIP and IEC 62443 compliance programs, documenting AI system performance evidence as part of formal critical infrastructure protection compliance records, and engaging with regulatory authorities to develop sector-specific AI performance standards providing consistent benchmarking references for hybrid architecture deployment quality across the utility industry. Sixth, workforce capability has been recommended to be strengthened through targeted training aligned with the three hybrid architecture domains enabling SCADA engineers, security analysts, and operations managers to share a consistent understanding of how CNN feature extraction, LSTM temporal modeling, and hybrid integration outputs interact within operational fault detection and cyber-threat classification workflows. Finally, organizations have been recommended to adopt a formal measurement and review cycle comparing HAPI and RTDA scores against operational performance metrics on a quarterly basis, enabling leadership to identify the most impactful improvement levers using quantitative evidence aligned with the capability-to-outcome model empirically validated in this study.

LIMITATION

The limitations of this study have reflected the methodological constraints of a quantitative, cross-sectional, case-study design and the practical challenges of measuring complex hybrid deep learning deployment capabilities through structured organizational survey instruments. First, the cross-sectional approach has limited causal interpretation because the identified relationships among hybrid architecture capabilities and smart grid outcomes have been assessed at a single time point, preventing confirmation of temporal precedence and leaving open the possibility that reciprocal influence or shared organizational factors explain observed associations more completely than the unidirectional capability-to-outcome model assumed in the regression framework. Second, the case-study orientation has constrained external generalizability because the participating organizations have represented specific organizational configurations, AI maturity levels, SCADA infrastructure generations, and regulatory environments whose characteristics may differ substantially from those of utilities in other national grid contexts or organizational size categories, limiting the direct transferability of regression coefficient magnitudes and capability-outcome relationship patterns to deployment contexts outside the study sample. Third, the reliance on self-reported Likert-scale measurements of technical capability dimensions has introduced perception bias and common-method variance risks, with the subjective nature of respondents' assessments of CNN feature extraction quality, LSTM temporal modeling effectiveness, and hybrid integration depth potentially diverging from objective algorithmic performance measures that would require direct technical evaluation of deployed model architectures on operational SCADA benchmark datasets. Fourth, the study-specific indices HAPI and RTDA have been constructed from aggregated survey items rather than instrumentation-level performance benchmarks, meaning these indices have captured organizational perceptions of hybrid architecture

quality and detection alignment rather than directly measured inference latency distributions, classification accuracy matrices, or alert-to-response time recordings providing stronger engineering-grade evidence for the capability-outcome relationships identified in the regression analyses. Fifth, the sample composition may have introduced role-based response heterogeneity as SCADA engineers, security analysts, and operations managers interact with hybrid deep learning systems through fundamentally different professional interfaces producing systematically different capability assessments even within the same organizational deployment context. Finally, the study has not incorporated longitudinal measurement, experimental intervention comparisons, or multi-site cross-utility validation that would substantially strengthen causal inference, establish coefficient stability across diverse grid environments, and enable the capability development pathway proposed in the hierarchical regression analysis to be validated as a temporally ordered developmental sequence rather than a cross-sectional associational pattern whose causal directionality remains theoretically inferred rather than empirically demonstrated.

REFERENCES

[1]. Ademujimi, T. T., Brundage, M. P., & Prabhu, V. V. (2017). A review of current machine learning techniques used in manufacturing diagnosis. In *Advances in Production Management Systems. The Path to Intelligent, Collaborative and Sustainable Manufacturing* (pp. 407-415). https://doi.org/10.1007/978-3-319-66923-6_48

[2]. Aftab, M. A., Hussain, S. M. S., Ali, I., & Ustun, T. S. (2020). IEC 61850 based substation automation system: A survey. *International Journal of Electrical Power & Energy Systems*, *120*, 106008. https://doi.org/10.1016/j.ijepes.2020.106008

[3]. Amin, M., & Wollenberg, B. (2005). Toward a smart grid: Power delivery for the 21st century. *IEEE Power and Energy Magazine*, *3*(5), 34-41. https://doi.org/10.1109/mpae.2005.1507024

[4]. Andrén, F., Stifter, M., & Strasser, T. (2013). Towards a semantic driven framework for smart grid applications: Model-driven development using CIM, IEC 61850 and IEC 61499. *Informatik-Spektrum*, *36*(1), 58-68. https://doi.org/10.1007/s00287-012-0663-y

[5]. Arif, A., Ma, S., Wang, Z., Wang, J., Ryan, S. M., & Chen, C. (2018). Optimizing service restoration in distribution systems with uncertain repair time and demand. *IEEE Transactions on Power Systems*, *33*(6), 6828-6838. https://doi.org/10.1109/tpwrs.2018.2855102

[6]. Chang, C.-W., Lin, J.-D., & Huang, C.-P. (2018). A review of artificial intelligence algorithms used for smart machine tools. *Inventions*, *3*(3), 41. https://doi.org/10.3390/inventions3030041

[7]. Dahal, N., Abuomar, O., King, R., & Madani, V. (2015). Event stream processing for improved situational awareness in the smart grid. *Expert Systems with Applications*, *42*(20), 6853-6863. https://doi.org/10.1016/j.eswa.2015.05.003

[8]. Daki, H., El Hannani, A., Aqqal, A., Haidine, A., & Dahbi, A. (2017). Big data management in smart grid: Concepts, requirements and implementation. *Journal of Big Data*, *4*, 13. https://doi.org/10.1186/s40537-017-0070-y

[9]. de Faria, H., Costa, J. G. S., & Olivas, J. L. M. (2015). A review of monitoring methods for predictive maintenance of electric power transformers based on dissolved gas analysis. *Renewable and Sustainable Energy Reviews*, *46*, 201-209. https://doi.org/10.1016/j.rser.2015.02.052

[10]. Deng, R., Xiao, G., Lu, R., Liang, H., & Vasilakos, A. V. (2017). False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey. *IEEE Transactions on Industrial Informatics*, *13*(2), 411-423. https://doi.org/10.1109/tii.2016.2605099

[11]. Derler, P., Lee, E. A., & Sangiovanni-Vincentelli, A. (2012). Modeling cyber–physical systems. *Proceedings of the IEEE*, *100*(1), 13-28. https://doi.org/10.1109/jproc.2011.2160929

[12]. Diaba, S. Y., Anafo, T., Tetteh, L. A., Oyibo, M. A., Alola, A. A., Shafie-khah, M., & Elmusrati, M. (2023). SCADA securing system using deep learning to prevent cyber infiltration. *Neural Networks*, *165*, 321-332. https://doi.org/10.1016/j.neunet.2023.05.047

[13]. Ding, Y., Ma, K., Pu, T., Wang, X., Li, R., & Zhang, D. (2021). A deep learning-based classification scheme for false data injection attack detection in power system. *Electronics*, *10*(12), 1459. https://doi.org/10.3390/electronics10121459

[14]. Drayer, E., & Routtenberg, T. (2020). Detection of false data injection attacks in smart grids based on graph signal processing. *Signal Processing*, *171*, 107464. https://doi.org/10.1016/j.sigpro.2020.107464

[15]. Efat Ara, H. (2023). Computational Modeling of Failure Mechanisms in Mechanical Systems: Applications For Energy and Industrial Sectors. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 196–230. https://doi.org/10.63125/0nmn9h72

[16]. Efat Ara, H. (2024a). Design and Simulation of Sustainable Calibration Systems for Future Industrial Engineering Applications. *American Journal of Advanced Technology and Engineering Solutions*, *4*(03), 60-99. https://doi.org/10.63125/rh85vs92

[17]. Efat Ara, H. (2024b). Systematic Review of Calibration Technologies and their Impact on Safety in Global Critical Infrastructure. *Journal of Sustainable Development and Policy*, *3*(04), 174-204. https://doi.org/10.63125/cznpnr41

[18]. Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid—The new and improved power grid: A survey. *IEEE Communications Surveys & Tutorials*, *14*(4), 944-980. https://doi.org/10.1109/surv.2011.101911.00087

[19]. Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine*, *8*(1), 18-28. https://doi.org/10.1109/mpe.2009.934876

[20]. Faysal, K., & Shamsunnahar, C. (2022). Digital Ledger Optimization Techniques for Enhancing Transaction Speed and Reporting Accuracy in Accounting Systems. *American Journal of Scholarly Research and Innovation*, *1*(02), 171–222. https://doi.org/10.63125/33t06k57

[21]. Feng, J., Lei, Y., Guo, L., Lin, J., & Xing, S. (2018). A neural network constructed by deep learning technique and its application to intelligent fault diagnosis of machines. *Neurocomputing*, *272*, 619-628. https://doi.org/10.1016/j.neucom.2017.07.032

[22]. Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital twin: Enabling technologies, challenges and open research. *IEEE Access*, *8*, 108952-108971. https://doi.org/10.1109/access.2020.2998358

[23]. Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A. (2019). Big data analytics in smart grids: State-of-the-art, challenges, opportunities, and future directions. *IET Smart Grid*, *2*(2), 141-154. https://doi.org/10.1049/iet-stg.2018.0261

[24]. Ghasempour, A. (2019). Internet of Things in smart grid: Architecture, applications, services, key technologies, and challenges. *Inventions*, *4*(1), Article 22. https://doi.org/10.3390/inventions4010022

[25]. Gulisano, V., Jiménez-Peris, R., Patino-Martinez, M., & Soriente, C. (2015). Apache Spark: A big data analytics platform for smart grid. *Procedia Computer Science*, *52*, 573-578. https://doi.org/10.1016/j.procs.2015.05.087

[26]. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. *Computer Networks*, *55*(7), 1652-1668. https://doi.org/10.1016/j.comnet.2010.08.008

[27]. Habibullah, S. M., & Zaheda, K. (2022). Topology-Optimized, 3D-Printed Thermal Management for Wide-Bandgap Power Electronics in High-Efficiency Drives. *Journal of Sustainable Development and Policy*, *1*(02), 134-167. https://doi.org/10.63125/p8m2p864

[28]. He, Y., Mendis, G. J., & Wei, J. (2017). Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Transactions on Smart Grid*, *8*(5), 2505-2516. https://doi.org/10.1109/tsg.2017.2703842

[29]. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115-135. https://doi.org/10.1007/s11747-014-0403-8

[30]. Hu, J., Shan, Y., Guerrero, J. M., Ioinovici, A., Chan, K. W., & Rodriguez, J. (2021). Model predictive control of microgrids—An overview. *Renewable and Sustainable Energy Reviews*, *136*, 110422. https://doi.org/10.1016/j.rser.2020.110422

[31]. Iftekhar, A., & Md Tohidul, I. (2024). Quantitative Impact Assessment of Digital Payment Solutions on Small Business Revenue Panel Data Analysis From 1,200 U.S. SMES. *American Journal of Scholarly Research and Innovation*, *3*(02), 217-253. https://doi.org/10.63125/zy98jx29

[32]. Jardine, A. K. S., Lin, D., & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing*, *20*(7), 1483-1510. https://doi.org/10.1016/j.ymssp.2005.09.012

[33]. Jinnat, A., & Molla Al Rakib, H. (2023). Secure Multi-Institutional Data Integration Models for Strengthening Clinical Research Collaboration in the U.S. Health Sector. *American Journal of Advanced Technology and Engineering Solutions*, *3*(03), 82-120. https://doi.org/10.63125/qqe4sh98

[34]. Jinnat, A., & Samiha Binte, A. (2024). Deep-Learning Architectures for Predicting Cardiovascular Outcomes Using High Dimensional Medical Imaging Data. *Journal of Sustainable Development and Policy*, *3*(03), 134-166. https://doi.org/10.63125/vrgee960

[35]. Kim, I., Rhee, S.-B., & Kim, H. M. (2020). A comprehensive review of practical issues for interoperability using the common information model in smart grids. *Energies*, *13*(6), 1435. https://doi.org/10.3390/en13061435

[36]. Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). Digital twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine*, *51*(11), 1016-1022. https://doi.org/10.1016/j.ifacol.2018.08.474

[37]. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436-444. https://doi.org/10.1038/nature14539

[38]. Lee, C., Liu, C., Mehrotra, S., & Bie, Z. (2015). Robust distribution network reconfiguration. *IEEE Transactions on Smart Grid*, *6*(2), 836-842. https://doi.org/10.1109/tsg.2014.2375160

[39]. Lei, S., Wang, J., Hou, Y., & Chen, C. (2019). Resilient disaster recovery logistics of distribution system restoration with repair crew and mobile power source. *IEEE Transactions on Smart Grid*, *10*(6), 6187-6202. https://doi.org/10.1109/tsg.2019.2899353

[40]. Li, X., Zhang, W., Ding, Q., & Sun, J.-Q. (2020). Intelligent rotating machinery fault diagnosis based on deep learning using data augmentation. *Journal of Intelligent Manufacturing*, *31*, 433-452. https://doi.org/10.1007/s10845-018-1456-1

[41]. Liang, G., Zhao, J., Luo, F., Weller, S. R., & Dong, Z. Y. (2017). A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid*, *8*(4), 1630-1638. https://doi.org/10.1109/tsg.2015.2495133

[42]. Lin, X., An, D., Cui, F., & Zhang, F. (2022). False data injection attack in smart grid: Attack model and reinforcement learning-based detection method. *Frontiers in Energy Research*, *10*, 1104989. https://doi.org/10.3389/fenrg.2022.1104989

[43]. Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., & Butler-Purry, K. L. (2013). A framework for modeling cyber-physical switching attacks in smart grid. *IEEE Transactions on Emerging Topics in Computing*, *1*(2), 273-285. https://doi.org/10.1109/tetc.2013.2296440

[44]. Md Abubakar Siddique, A., & Md. Al Amin, K. (2022). Data-Driven Ergonomic Risk Analysis Using Wearable Sensor Networks and Deep Learning for Injury Prevention in Industrial Workplaces. *American Journal of Data Science and Analytics*, *3*(06), 01-39. https://doi.org/10.63125/61w9ba54

[45]. Md, F., & Islam, M. D. Z. (2022). Quantitative Risk Modeling of VPN Misconfigurations and Firewall Rule Drift in Hybrid Cloud Networks. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 182-216. https://doi.org/10.63125/fa4qdz07

[46]. Md Khaled, H., & Md. Mosheur, R. (2023). Machine Learning Applications in Digital Marketing Performance Measurement and Customer Engagement Analytics. *Review of Applied Science and Technology*, *2*(03), 27–66. https://doi.org/10.63125/hp9ay446

[47]. Md Shahab, U., & Aditya, D. (2023). Risk Mitigation and Resilience Modeling for Consumer Distribution Networks During Demand Shocks: A Quantitative Stochastic Optimization and Scenario Analysis Study. *International Journal of Scientific Interdisciplinary Research*, *4*(2), 01–30. https://doi.org/10.63125/jkevvq84

[48]. Md. Hasan Or, R., Tanjina Binte, S., & Rajib, S. (2023). Performance Analytics Frameworks for Digital Marketing and Service Enterprises: An empirical Study. *American Journal of Data Science and Analytics*, *4*(03), 01-35. https://doi.org/10.63125/aq7y1792

[49]. Md. Mehedi, H., & Khairum Nahar, P. (2023). A Systematic Review of Secure Health Data Information Systems for Pandemic Preparedness and Economic Continuity in the United States. *Review of Applied Science and Technology*, *2*(01), 227–258. https://doi.org/10.63125/77h2m531

[50]. Md. Mosheur, R., & Rebeka, S. (2021). Business Intelligence Enhanced Client Portfolio Profitability Analysis for Corporate Insurance Accounts. *International Journal of Business and Economics Insights*, *1*(3), 01–36. https://doi.org/10.63125/qcs8d475

[51]. Md. Mosheur, R., & Rebeka, S. (2022). Data-Driven Framework for Service Issue Escalation and Resolution in Large Scale Insurance Portfolios. *Review of Applied Science and Technology*, *1*(04), 216–249. https://doi.org/10.63125/dkzy5k88

[52]. Md. Sultan, M., & Anick, K. M. T. A. (2023). High-Performance Computing–Assisted Modeling and Real-Time Analysis of Electrical Power Networks and Industrial Control Systems. *Review of Applied Science and Technology*, *2*(01), 185–226. https://doi.org/10.63125/727j5j39

[53]. Md. Towhidul, I., & Uddin, M. D. S. (2024). Simulation-Based Forecasting and Inventory Control Models For Consumer Goods Networks: A Quantitative Study Using Monte Carlo Simulation and Time-Series Methods. *Review of Applied Science and Technology*, *3*(04), 165–197. https://doi.org/10.63125/a3047d06

[54]. Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, *100*(1), 195-209. https://doi.org/10.1109/jproc.2011.2161428

[55]. Mohammad Mushfequr, R., & Aditya, D. (2024). Quantitative Assessment of Data Protection Practices In U.S. Revenue Cycle Management. *American Journal of Advanced Technology and Engineering Solutions*, *4*(04), 107-153. https://doi.org/10.63125/fc9hfy54

[56]. Molina, E., Jacob, E., Matias, J., Moreira, N., & Astarloa, A. (2015). Using software defined networking to manage and control IEC 61850-based systems. *Computers & Electrical Engineering*, *43*, 142-154. https://doi.org/10.1016/j.compeleceng.2014.10.016

[57]. Mostafa, K. (2023). An Empirical Evaluation of Machine Learning Techniques for Financial Fraud Detection in Transaction-Level Data. *American Journal of Interdisciplinary Studies*, *4*(04), 210-249. https://doi.org/10.63125/60amyk26

[58]. Mostafa, K., & Md Tohidul, I. (2022). A Quantitative Financial Impact Assessment of Digital Trade Platforms on Export Performance, Capital Efficiency, and Market Competitiveness. *Journal of Sustainable Development and Policy*, *1*(03), 01-26. https://doi.org/10.63125/pt5v9517

[59]. Mukherjee, D., Chakraborty, S., & Ghosh, S. (2021). Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids. *Electrical Engineering*, *103*, 3017-3033. https://doi.org/10.1007/s00202-021-01278-6

[60]. Naumann, A., Bielchev, I., Voropai, N., & Styczynski, Z. (2014). Smart grid automation using IEC 61850 and CIM standards. *Control Engineering Practice*, *25*, 102-111. https://doi.org/10.1016/j.conengprac.2013.12.001

[61]. Negri, E., Fumagalli, L., & Macchi, M. (2017). A review of the roles of digital twin in CPS-based production systems. *Procedia Manufacturing*, *11*, 939-948. https://doi.org/10.1016/j.promfg.2017.07.198

[62]. Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, *121*, 43-60. https://doi.org/10.1016/j.ress.2013.06.040

[63]. Ozay, M., Esnaola, I., Yarman Vural, F. T., Kulkarni, S. R., & Poor, H. V. (2016). Machine learning methods for attack detection in the smart grid. *IEEE Transactions on Neural Networks and Learning Systems*, *27*(8), 1773-1786. https://doi.org/10.1109/tnnls.2015.2414833

[64]. Panteli, M., & Mancarella, P. (2015). The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. *IEEE Power and Energy Magazine*, *13*(3), 58-66. https://doi.org/10.1109/mpe.2015.2397334

[65]. Park, K.-J., Zheng, R., & Liu, X. (2012). Cyber-physical systems: Milestones and research challenges. *Computer Communications*, *36*(1), 1-7. https://doi.org/10.1016/j.comcom.2012.09.006

[66]. Phadke, A. G., & Thorp, J. S. (2017). *Synchronized phasor measurements and their applications*. Springer. https://doi.org/10.1007/978-3-319-50584-8

[67]. Poovendran, R. (2010). Cyber–physical systems: Close encounters between two parallel worlds. *Proceedings of the IEEE*, *98*(8), 1363-1366. https://doi.org/10.1109/jproc.2010.2050377

[68]. Qi, J., Sun, K., & Kang, W. (2015). Optimal PMU placement for power system dynamic state estimation by using empirical observability Gramian. *IEEE Transactions on Power Systems*, *30*(4), 2041-2054. https://doi.org/10.1109/tpwrs.2014.2356797

[69]. Qiu, S., Cui, X., Ping, Z., Shan, N., Li, Z., Bao, X., & Xu, X. (2023). Deep learning techniques in intelligent fault diagnosis and prognosis for industrial systems: A review. *Sensors*, *23*(3), 1305. https://doi.org/10.3390/s23031305

[70]. Radhoush, S., Vannoy, T., Liyanage, K., Mutch, B. M., & Johnson, B. K. (2023). Distribution system state estimation and false data injection attack detection with a multi-output deep neural network. *Energies*, *16*(5), 2288. https://doi.org/10.3390/en16052288

[71]. Rai, P., Londhe, N. D., & Raj, R. (2021). Fault classification in power system distribution network integrated with distributed generators using CNN. *Electric Power Systems Research*, *192*, 106914. https://doi.org/10.1016/j.epsr.2020.106914

[72]. Ratul, D., & Aditya, D. (2023). AI-Driven Change Detection Using SAR, LIDAR, And Sentinel-2 Data for Landslide Monitoring and Disaster Early Warning Systems. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 153–188. https://doi.org/10.63125/4y740y95

[73]. Reda, H. T., Anwar, A., & Mahmood, A. (2022). Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts. *Renewable and Sustainable Energy Reviews*, *163*, 112423. https://doi.org/10.1016/j.rser.2022.112423

[74]. Ren, H., Hou, Z. J., Vyakaranam, B., Wang, H., & Etingov, P. (2020). Power system event classification and localization using a convolutional neural network. *Frontiers in Energy Research*, *8*, 607826. https://doi.org/10.3389/fenrg.2020.607826

[75]. Rosen, R., von Wichert, G., Lo, G., & Bettenhausen, K. D. (2015). About the importance of autonomy and digital twins for the future of manufacturing. *IFAC-PapersOnLine*, *48*(3), 567-572. https://doi.org/10.1016/j.ifacol.2015.06.141

[76]. Saleem, Y., Crespi, N., Rehmani, M. H., & Copeland, R. (2019). Internet of Things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions. *IEEE Access*, *7*, 62962-63003. https://doi.org/10.1109/access.2019.2913984

[77]. Sazzadul, I., & Rebeka, S. (2024). VaR and CVaR-Based Stress Testing Using Deep Learning for Liquidity Risk Forecasting and Banking Stability Assessment. *Review of Applied Science and Technology*, *3*(03), 01–30. https://doi.org/10.63125/291phs66

[78]. Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210-224. https://doi.org/10.1109/jproc.2011.2165269

[79]. Stetco, A., Dinmohammadi, F., Zhao, X., Robu, V., Flynn, D., Barnes, M., Keane, J., & Nenadic, G. (2019). Machine learning methods for wind turbine condition monitoring: A review. *Renewable Energy*, *133*, 620-635. https://doi.org/10.1016/j.renene.2018.10.047

[80]. Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C. (2019). Digital twin in industry: State-of-the-art. *IEEE Transactions on Industrial Informatics*, *15*(4), 2405-2415. https://doi.org/10.1109/tii.2018.2873186

[81]. Tao, F., Zhang, M., Liu, Y., & Nee, A. Y. C. (2017). Digital twin-driven product design, manufacturing and service with big data. *The International Journal of Advanced Manufacturing Technology*, *94*, 3563-3576. https://doi.org/10.1007/s00170-017-0233-1

[82]. Tasnim, K., & Anick, K. M. T. A. (2024). PLC–SCADA–Integrated Electrical Automation Frameworks for Process Optimization in Water and Wastewater Treatment Facilities. *Review of Applied Science and Technology*, *3*(01), 221–262. https://doi.org/10.63125/y1145g11

[83]. Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53-55. https://doi.org/10.5116/ijme.4dfb.8dfd

[84]. Terzija, V., Valverde, G., Cai, D., Regulski, P., Madani, V., Fitch, J., Skok, S., Begovic, M. M., & Phadke, A. (2011). Wide-area monitoring, protection, and control of future electric power networks. *Proceedings of the IEEE*, *99*(1), 80-93. https://doi.org/10.1109/jproc.2010.2060450

[85]. Tu, C., He, X., Shuai, Z., & Jiang, F. (2017). Big data issues in smart grid—A review. *Renewable and Sustainable Energy Reviews*, *79*, 1099-1107. https://doi.org/10.1016/j.rser.2017.05.134

[86]. Uhlemann, T. H.-J., Lehmann, C., & Steinhilper, R. (2017). The digital twin: Realizing the cyber-physical production system for Industry 4.0. *Procedia CIRP*, *61*, 335-340. https://doi.org/10.1016/j.procir.2016.11.152

[87]. Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *Information Systems Research*, *23*(1), 157-178. https://doi.org/10.1287/isre.1100.0336

[88]. Wang, Y., Chen, D., Zhang, C., Chen, X., Huang, B., & Cheng, X. (2019). Wide and recurrent neural networks for detection of false data injection in smart grids. In *Wireless Algorithms, Systems, and Applications* (pp. 335-345). https://doi.org/10.1007/978-3-030-23597-0_27

[89]. Yu, J. J. Q., Hou, Y., & Li, V. O. K. (2018). Online false data injection attack detection with wavelet transform and deep neural networks. *IEEE Transactions on Industrial Informatics*, *14*(7), 3271-3280. https://doi.org/10.1109/tii.2018.2825243

[90]. Zaheda, K., & Md Hamidur, R. (2024). GPU-Accelerated Physics-Informed Digital Twins for Real-Time State Estimation and Fault Localization in Distribution Grids. *American Journal of Scholarly Research and Innovation*, *3*(02), 179-216. https://doi.org/10.63125/msrpfb04

[91]. Zaheda, K., & Md. Tahmid Farabe, S. (2023). Robotics and Computer Vision for Automated Inspection of Substation and Treatment-Facility Electrical Infrastructure. *Review of Applied Science and Technology*, *2*(04), 194-227. https://doi.org/10.63125/tfh15j12

[92]. Zhang, C., Wang, J., Florita, A., & Wang, Z. (2020). Power system event identification based on deep neural network with PMU data. *IEEE Transactions on Power Systems*, *36*(1), 257-268. https://doi.org/10.1109/tpwrs.2020.3003676

[93]. Zhang, W., Jia, M.-P., Zhu, L., & Yan, X.-A. (2017). Comprehensive overview on computational intelligence techniques for machinery condition monitoring and fault diagnosis. *Chinese Journal of Mechanical Engineering*, *30*, 782-795. https://doi.org/10.1007/s10033-017-0150-0

[94]. Zhao, J., Zhang, G., Das, K., Korres, G. N., Manousakis, N. M., Sinha, A. K., & He, Z. (2016). Power system real-time monitoring by using PMU-based robust state estimation method. *IEEE Transactions on Smart Grid*, *7*(1), 300-309. https://doi.org/10.1109/tsg.2015.2431693

[95]. Zhao, Z., Li, T., Wu, J., Sun, C., Wang, S., Yan, R., & Chen, X. (2020). Deep learning algorithms for rotating machinery intelligent diagnosis: An open source benchmark study. *ISA Transactions*, *107*, 224-255. https://doi.org/10.1016/j.isatra.2020.08.010

[96]. Zhu, Z., Lei, Y., Qi, G., Chai, Y., Mazur, N., An, Y., & Huang, X. (2023). A review of the application of deep learning in intelligent fault diagnosis of rotating machinery. *Measurement*, *214*, 112346. https://doi.org/10.1016/j.measurement.2022.112346