American Journal of Advanced Technology and Engineering Solutions

Volume: 1; **Issue:** 2
Pages: 95-134
eISSN: 3067-5146

open access

Crossref

An Empirical Evaluation of Anomaly Detection Techniques in Smart Grid Systems Using Real-Time Operational Data

S M Shakil[1]; Alamgir Hossain[2]; Md Mijanur Rahman[3];

[1]. *Department of Electrical and Computer Engineering; Florida Polytechnic University, FL, USA; Email: sshakil2152@floridapoly.edu*
[2]. *School of Engineering; University of Tasmania, Australia; Email: alamgir.hossain@utas.edu.au*
[3]. *Department of Electrical and Electronic Engineering; Dhaka University of Engineering and Technology, Bangladesh; Email: mijan.duet@duet.ac.bd*

Doi: 10.63125/2xcry064
Received: *09 May 2025;* ***Revised:*** *10 June 2025;* ***Accepted:*** *12 July 2025;* ***Published:*** *08 August 2025*

Abstract

This study addresses the problem that smart grid operators increasingly rely on enterprise and cloud enabled monitoring platforms, yet anomaly detection outputs are often difficult to trust due to data quality variability, limited alarm explainability, weak workflow integration, and false alarm overload. The purpose was to quantify which technical and organizational factors most strongly predict perceived detection effectiveness and adoption readiness for anomaly detection techniques in a real smart grid case. A quantitative cross sectional, case-based design was applied using a structured 5-point Likert survey administered to N = 182 stakeholders drawn from enterprise smart grid environments spanning AMI and smart metering, SCADA and EMS or DMS, PMU or WAMS, and supporting IT and cybersecurity functions (operations 28.6%, metering 20.3%, data and IT 20.9%, protection 15.9%, cybersecurity 14.3%). Key variables included Data Quality Adequacy (DQ), Robustness and Adaptability (RB), Explainability of Alarms (EX), System Integration Capability (SI), Perceived Detection Effectiveness (PDE), Adoption Readiness and Trust (ART), and False Alarm Burden and Operational Impact Index (FABOI). The analysis plan used descriptive statistics, scale reliability (Cronbach alpha .81 to .88), Pearson correlations, and multiple regression models. Headline findings showed moderately high perceptions of DQ (M = 3.92, SD = 0.61) and PDE (M = 3.81, SD = 0.62), while false alarm burden was nontrivial (FABOI M = 3.41, SD = 0.73). PDE correlated with DQ (r = .52) and RB (r = .48), while ART correlated most strongly with EX (r = .54) and PDE (r = .58), and decreased with FABOI (r = −.49), all p < .01. Regression confirmed PDE was predicted by DQ (β = .31, p < .001) and RB (β = .27, p < .001), R^2 = .39, whereas ART was driven by EX (β = .33, p < .001), PDE (β = .29, p < .001), SI (β = .21, p = .002) and reduced by FABOI (β = −.24, p < .001), R^2 = .47. Implications suggest utilities should prioritize data governance and robustness for effectiveness, but invest in explainable alarms, workflow integration, and alarm burden management to increase operational trust and sustained adoption.

Keywords

Smart grid, Anomaly detection, Explainability, False alarm burden, Technology Organization Environment (TOE);

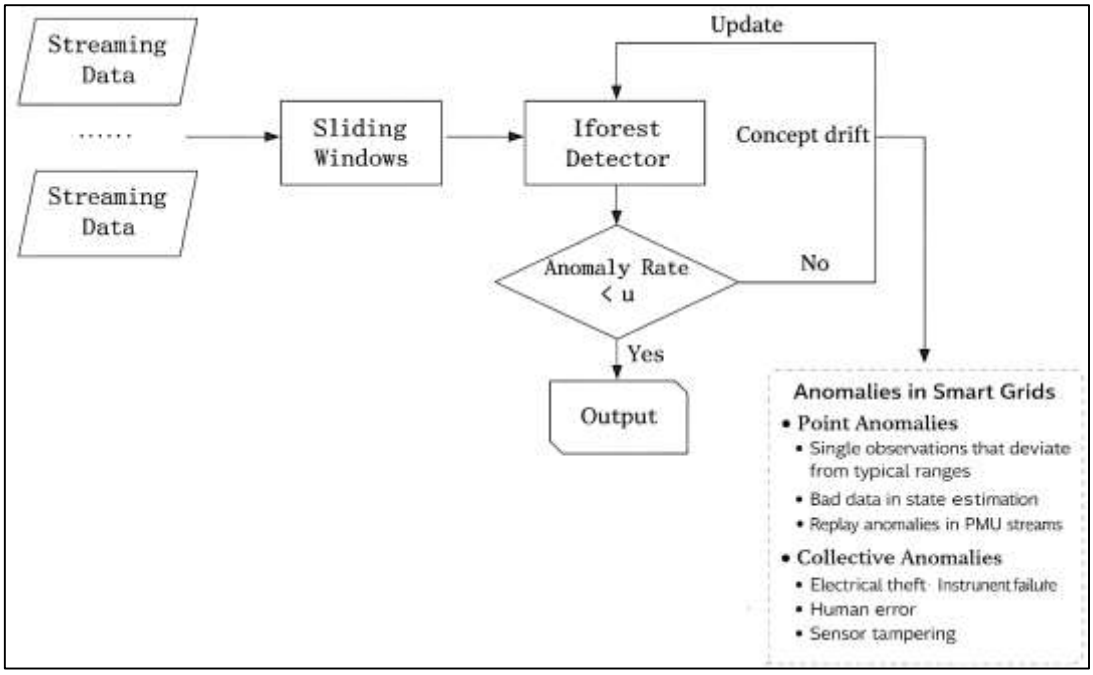
INTRODUCTION

Anomaly detection refers to the set of analytic processes used to identify observations, patterns, or sequences that deviate from an established notion of "normal" behavior in data streams or datasets. In electric power systems, and specifically in smart grid systems, the meaning of "anomaly" is anchored to grid physics, operational constraints, and cyber-physical interactions that link sensing, communication, control, and energy delivery (Aalam & Shubhanga, 2023). The smart grid is widely characterized as an electricity network that integrates information and communication technologies with generation, transmission, distribution, and consumption to enable bidirectional flows of data and energy and to support automation at scale (Liu et al., 2011). Internationally, the modernization of power delivery has been framed in terms of resilience, survivability, and security of large-scale infrastructure that underpins economic activity and public well-being (Kea et al., 2023). Within this landscape, anomaly detection is not a single algorithmic act; it is a measurement-to-decision discipline that spans sensing (e.g., smart meters, phasor measurement units), communication pathways, supervisory control (e.g., SCADA), and analytic models that transform signals into actionable alarms. In data science terms, anomalies can be point anomalies (single observations that depart from typical ranges), contextual anomalies (values that are abnormal given time, season, or operating state), and collective anomalies (sets of observations whose joint behavior is abnormal). When placed in smart grid settings, these categories become operationally concrete: "bad data" in state estimation, replay anomalies in PMU streams, non-technical loss signatures in advanced metering infrastructures, and consumption patterns that indicate tampering or fraud at the edge of the grid (Mahi-al-rashid et al., 2022). This definitional grounding matters because smart grids are multi-layer systems in which anomalies can arise from physical faults, instrument and communication failures, human error, and adversarial manipulation of measurements or commands (Pahwa et al., 2016; Sahani et al., 2023). Thus, the scholarly treatment of anomaly detection in smart grids often emphasizes that "normal" behavior is a model that must be operationalized through data quality standards, modeling choices, and monitoring logic consistent with grid operations (Pahwa et al., 2016). In this context, anomaly detection techniques function as methods for translating diverse forms of deviation into interpretable evidence of risk, irregularity, or malfunction in critical infrastructure systems.

Smart grid anomaly detection also carries international significance because power systems increasingly operate as interconnected, technology-mediated infrastructures that support industrial production, public services, and household activity across regions with different regulatory environments, market designs, and reliability constraints (Jiang et al., 2014). The global deployment of advanced metering infrastructure and wide-area measurement systems has expanded the volume, velocity, and heterogeneity of data used for monitoring and control, creating analytic dependence on reliable detection mechanisms for faults and irregular behaviors. Electricity theft and non-technical losses are frequently treated as economically material anomalies, particularly in contexts where losses affect tariffs, supply stability, and utility revenue adequacy (Sobhani et al., 2020). Theft has been framed as a major contributor to non-technical losses with detection and control approaches closely linked to smart meter–based monitoring and utility governance structures. Beyond theft, a large body of smart grid security research has formalized measurement manipulation as an anomaly class with system-wide consequences (Sun et al., 2022). False data injection attacks against state estimation have been shown to introduce errors into estimated states without triggering conventional bad data detection under certain knowledge and access assumptions. This line of work positions anomaly detection as part of the trust boundary for cyber-physical control. Operationally, anomaly detection supports the integrity of state estimation and situational awareness, which are central to reliable dispatch, protection coordination, and corrective control actions (Alshehri et al., 2024). Research on protocol-level vulnerabilities further connects anomaly detection to communication standards used inside substations and protection systems (Amin & Wollenberg, 2005). Threats to IEC 61850 sampled measured values communications and the feasibility of using neural-network forecasters to detect spoofed packets highlight how anomalies can be embedded in high-rate message flows rather than only in aggregated consumption traces. Wide-area measurement systems also raise distinct concerns because time-synchronized measurements can amplify detection value while expanding the attack and failure surface in interconnected monitoring networks. Replay attacks and bad data anomalies in PMU

measurements have been addressed using mode-tracking logic to characterize deviations in dynamic behavior (Ijaz et al., 2020). This body of literature supports a view of anomaly detection as an internationally relevant capability for ensuring measurement trust, operational continuity, and governance of digitalized grid infrastructures. In scholarly terms, the smart grid anomaly detection problem is anchored in cross-domain requirements: economic loss control (theft and fraud), system reliability (faults and disturbances), and cybersecurity (integrity of measurement and control pathways).

Figure 1: Structured Anomaly Detection Framework for Smart Grid Measurement and Control Environments



In smart grids, the anomaly concept is commonly operationalized through identifiable classes of abnormality that map to data sources and grid functions. Advanced metering infrastructure produces consumption time series and meter event logs, enabling the study of anomalies associated with fraud, defective meters, and unusual load behavior (Burgos et al., 2024). Frameworks for identifying energy theft and defective meters have used loss factors and error terms to express technical loss expectations and noise, illustrating how anomaly definition is coupled to grid topology and measurement uncertainty. Non-technical loss detection research also includes analytic treatments using regression and related statistical models on consumption data to differentiate typical and atypical usage patterns, supporting the view that anomalies may be detected as deviations from learned baselines (Chandola et al., 2009). From the transmission and monitoring perspective, PMUs provide high-frequency synchronized phasor measurements that capture dynamic signatures of events, faults, oscillations, and measurement irregularities. Data-driven fault detection and localization in smart grids has been developed using computational methods that transform measurement features into event identification and location decisions (El Hariri et al., 2019). Replay attacks and bad data injection in PMU streams add a cyber-physical anomaly category where anomalies are constructed through temporal substitution or crafted measurement perturbations that mimic plausible patterns. In control-centered architectures, SCADA and associated telemetry are exposed to integrity anomalies, including false data injection that targets state estimation and decision-making processes. In this domain, false data injection is framed as a structured anomaly that exploits system models, motivating detection approaches that account for both residual properties and adversarial design (Fang et al., 2012). Research has therefore extended anomaly detection from simple thresholding to forecasting-aided detection, where predicted values represent expected system behavior and significant deviations represent anomalous behavior under attack scenarios. Complementing these categories, load forecasting research shows that anomalies can

also appear in exogenous variables (e.g., temperature data) used to forecast demand, and that anomaly detection can be applied to data quality assurance for forecasting pipelines. Together, these studies illustrate that smart grid anomaly detection is not limited to a single anomaly type; it is a family of detection problems tied to the measurement layer (meters and PMUs), the control layer (SCADA/state estimation), and the market/consumer layer (theft and fraud), each with distinct definitions of deviation and risk (Gogula & Edward, 2023).

The technique landscape for anomaly detection in smart grids draws from statistical, signal-processing, and machine-learning paradigms, with selection shaped by data properties and operational constraints. Anomaly detection families include statistical approaches that model distributions, proximity-based methods that measure similarity, clustering-based approaches that isolate small clusters, and classification-based approaches that learn boundaries between normal and abnormal behavior (Gungor et al., 2011). In smart grid contexts, statistical baselines are often implemented through forecasting, regression, and residual monitoring because power system data exhibit temporal structure and seasonality that can be modeled and used to define expected behavior (Depuru et al., 2011). Regression-oriented detection is also visible in non-technical loss research, where consumption-based models provide expected profiles against which deviations can be evaluated. For high-dimensional sensing environments, deep learning methods have been applied to learn representations of normal behavior and then flag deviations via reconstruction error or forecasting error. Forecasting-aided anomaly detection for false data injection has been implemented using CNN–LSTM autoencoder sequence-to-sequence architectures, emphasizing that forecast quality is directly connected to detection reliability. A related stream has used deep reinforcement learning for abnormal data detection in smart meters, framing anomaly detection as a decision process that learns detection policies under large-scale data conditions. In addition to deep learning, graph-based methods have gained prominence when grid topology and electrical connectivity are treated as informative structure. False data injection detection based on graph signal processing has leveraged spectral characteristics of graph signals to identify manipulations that evade residual-based checks. This approach aligns with the observation that power systems are naturally graph-structured, so anomalies may manifest as disruptions to smoothness or consistency over network structure rather than only as pointwise deviations. Recent detection models using graph spatial features and temporal convolutional networks reflect a further integration of spatial–temporal learning for false data injection detection (Drayer & Routtenberg, 2020). Technique selection is also guided by interpretability and operational acceptance: feasibility under constraints such as sampling rates, message frequency, and protection timing has been evaluated for standards-based environments. PMU-based detection work has also been organized around dynamic modes and local decision agents to support distributed monitoring and reduce reliance on centralized computations. This diversity indicates that anomaly detection in smart grids is best characterized as a method portfolio, in which model form (statistical, deep, graph-based) is aligned to data type (consumption, phasor streams, SCADA telemetry), anomaly category (fault vs attack), and operational constraints (latency, interpretability, reliability of alarms).

Evaluation and trust in anomaly detection systems are central methodological concerns because performance is shaped not only by algorithmic accuracy but also by false alarms, missed detections, and system integration realities. In operational environments, false positives contribute to alarm fatigue, unnecessary dispatches, and degraded confidence in monitoring systems, while false negatives can allow faults or attacks to persist unnoticed (Barshan et al., 2024). Forecasting-aided detection studies have addressed thresholding strategies that balance false positive and false negative rates when translating prediction errors into alarm decisions. In smart meter anomaly detection, the challenge of imbalanced data and heterogeneous consumption behaviors has motivated hybrid architectures and tailored modeling strategies that address sparsity of theft labels and variability across consumers and regions. When anomaly detection is used to protect state estimation from false data injection, evaluation must account for adversarial feasibility, including cases where attacks are constructed to bypass residual checks. Measurement manipulation has been formalized as a vulnerability where attacks can remain undetected by traditional bad data detectors, expanding evaluation beyond classification accuracy to include robustness against crafted anomalies. Graph-signal methods similarly define success as exposing attacks that remain undetected under conventional detectors, shifting evaluation

toward adversarially informed criteria (Wang et al., 2024). Protocol-level detection introduces feasibility constraints tied to standards and sampling, where detection must operate at or near message rates without undermining system function. In PMU-centric settings, evaluation includes detecting replay attacks and multiple bad data injection types across distributed measurement points, including simultaneous anomalies across more than one PMU. Non-technical loss research emphasizes economic stakes and shows that anomaly detection performance has implications for billing accuracy, revenue protection, and operational planning in distribution networks. Data quality itself becomes an evaluation factor, as shown by temperature anomaly detection designed to protect load forecasting accuracy, framing anomaly detection as a data governance mechanism in analytic pipelines (Yip et al., 2018). These studies collectively support an evaluation view in which anomaly detection is assessed through multi-metric reporting: detection sensitivity, false alarm rates, robustness to noise and concept variation, and operational compatibility with grid monitoring and control. This motivates empirical research designs that incorporate descriptive statistics to characterize constructs like data quality and system integration, correlation analysis to quantify relationships among constructs, and regression modeling to evaluate predictor contributions to detection effectiveness and operational outcomes in case-based environments (Zhan et al., 2015).

Smart grid anomaly detection research also foregrounds the role of communication infrastructures and cyber-physical coupling in creating anomaly surfaces that are not present in purely physical grids. Smart grid communications are treated as enabling technologies that introduce heterogeneity in network types, quality-of-service requirements, and security considerations across home area networks, neighborhood networks, and wide-area connectivity (Zhao et al., 2016). In this context, anomalies occur not only in electrical variables but also in message timing, packet content, and measurement provenance, and detection approaches can require cross-layer reasoning about signals, protocols, and control actions. False data injection attacks have been shown to map cyber manipulations to physical consequences via state estimation and operational decisions, encouraging detection methods that incorporate model awareness and adversarial considerations. Forecasting-aided approaches extend this logic by integrating prediction models into detection, such that anomalies are defined by divergence from expected trajectories derived from historical behavior and contextual conditions (Barshan et al., 2024). Graph-based methods connect anomaly definition to network topology and power flow relationships, aligning detection with physical structure while using signal processing tools suited for graph domains. At the distribution edge, electricity theft has been studied as a cyber-physical anomaly where adversaries manipulate meter reports or behavior patterns to reduce reported consumption, motivating anomaly detectors trained on benign readings to detect deviations as theft signals (Iftikhar et al., 2024). These settings introduce privacy and decentralization constraints that have been addressed through federated learning frameworks for anomaly detection in distributed power systems and for electricity theft zero-day scenarios, emphasizing that detection architecture and data governance shape feasibility. Reviews synthesizing anomaly detection approaches across smart grid anomaly categories show wide variation in technique choices and emphasize alignment among anomaly type, system component, and available data. In sum, the cyber-physical nature of smart grids positions anomaly detection as an integrative analytic capability spanning measurement integrity, operational stability, and economic protection across communication-enabled infrastructures (Wang et al., 2024).

Finally, the empirical study of anomaly detection techniques in a smart grid case environment benefits from a structured framing of factors that influence detection effectiveness and organizational acceptance (Alshehri et al., 2024). Contemporary anomaly detection research in smart grids recognizes that technique performance and applied acceptance are shaped by technology characteristics (data quality, robustness, explainability), organizational conditions (skills, workflow integration, governance), and environmental pressures (threat landscape, regulatory expectations, vendor ecosystems). Within case-focused studies, these factors can be operationalized as measurable constructs that represent how detection systems are used, trusted, and integrated into operations. Reviews of AI-based smart grid anomaly detection emphasize that different anomaly objects and grid components motivate different approaches and that contextual factors such as infrastructure and regulation influence which solutions are appropriate (Barshan et al., 2024). In PMU settings, detection can be

implemented through distributed diagnostic agents aligned with operational partitioning, while metering contexts depend on consumption pattern consistency and meter tamper considerations. False data injection literature shows detection difficulty varies with attacker knowledge and system model properties, supporting robustness as a central construct when assessing technique suitability. Protocol-focused work indicates feasibility and detection timeliness are tied to standards and message rates, reinforcing integration and compatibility as measurable determinants of applied success. Federated anomaly detection approaches indicate privacy constraints, distributed data ownership, and coordination mechanisms influence architecture choices and performance evaluation, making deployment feasibility salient in real environments (Chandola et al., 2009). Theft detection studies also show imbalanced distributions and consumer heterogeneity shape modeling and detection outcomes, supporting constructs related to data representativeness and operational burden. Empirical designs using Likert-scale measurement, descriptive statistics, correlation analysis, and regression modeling provide a coherent pathway to quantify these relationships in cross-sectional case-study settings, enabling statistical testing of how technique attributes and system conditions relate to detection effectiveness, false-alarm burden, and operational impact within a defined smart grid context (El Hariri et al., 2019).

This study is designed to examine anomaly detection techniques in smart grid systems through a quantitative, cross-sectional, case-study–based approach that produces measurable evidence aligned with clearly defined objectives. The first objective is to operationalize and measure the core technical and operational conditions that shape anomaly detection performance within the selected smart grid case, focusing on constructs such as data quality, robustness and adaptability of detection models, explainability of alarms, integration capability with existing grid monitoring and control workflows, and the perceived operational burden associated with false alarms. The second objective is to profile and quantify how stakeholders within the case environment—such as grid operators, protection engineers, metering analysts, cybersecurity personnel, and supervisory staff—perceive the occurrence, severity, and operational relevance of different anomaly categories, including measurement irregularities, communication disruptions, suspicious consumption signatures, and state-estimation inconsistencies, so that the study's assessment is anchored in the anomaly landscape of the case rather than in abstract classifications. The third objective is to statistically evaluate the relationships among these measured constructs using descriptive statistics to summarize central tendencies and variability, correlation analysis to identify the direction and strength of associations between technique-related factors and performance-related outcomes, and regression modeling to estimate the predictive contribution of key factors to dependent outcomes such as detection effectiveness, operational reliability impact, and adoption readiness or trust in anomaly detection solutions. The fourth objective is to generate case-specific, decision-oriented outputs that translate the statistical findings into structured results sections tailored to smart grid anomaly detection, including a case-system anomaly landscape that documents dominant anomaly forms, a false-alarm burden and operational impact index that quantifies perceived disruption from alarm behavior, and a technique fit-to-grid map that ranks detection techniques by their perceived suitability under the case's data constraints, latency expectations, interpretability needs, and integration requirements. Collectively, these objectives guide the study toward producing an internally consistent empirical assessment that links technique characteristics and deployment conditions to measurable outcomes within one defined smart grid context.

LITERATURE REVIEW

The literature on anomaly detection in smart grid systems sits at the intersection of power engineering, communications, cybersecurity, and data science, reflecting the reality that smart grids operate as cyber-physical infrastructures where deviations can emerge from physical faults, sensing errors, communication disruptions, operational misconfigurations, and deliberate adversarial actions. As smart grid modernization expands the deployment of advanced metering infrastructure, phasor measurement units, SCADA telemetry, and distributed energy resource monitoring, the volume and complexity of data streams increase, and anomaly detection becomes a central analytical function for maintaining observability and supporting reliable decision-making under uncertainty. Within this research area, "anomaly" is treated as a domain-specific concept tied to system state, grid topology,

and operational limits, meaning that the definition of normality is contextual and often dependent on time, weather, switching configurations, and load dynamics. The literature therefore differentiates among anomaly classes that include consumption and billing irregularities (often associated with non-technical losses), power quality and equipment-related disturbances, state-estimation inconsistencies caused by corrupted or missing measurements, and cyber anomalies embedded in control and measurement channels. A major theme across studies is the diversity of detection approaches and the persistent need to align technique choice with data characteristics and operational constraints. Traditional statistical and signal-processing methods remain relevant for their transparency and low computational cost, while machine learning and deep learning methods are frequently adopted to handle nonlinearity, high-dimensionality, and complex temporal dependencies in grid measurements. In parallel, topology-aware methods increasingly exploit the graph structure of power networks to represent spatial dependencies and improve detection sensitivity for structured anomalies. Another dominant theme concerns evaluation and practical deployment, where research emphasizes that accuracy alone is insufficient without attention to false alarm rates, latency, scalability, interpretability, and integration with operational workflows, because detection systems must be trusted and usable by practitioners who respond to alarms. This literature review therefore synthesizes prior work by organizing studies around smart grid data ecosystems and anomaly categories, the taxonomy of detection techniques, evaluation criteria and operational constraints, and socio-technical considerations that shape adoption and effectiveness in real settings, providing the foundation for the study's conceptual framing, hypothesis development, and methodological choices.

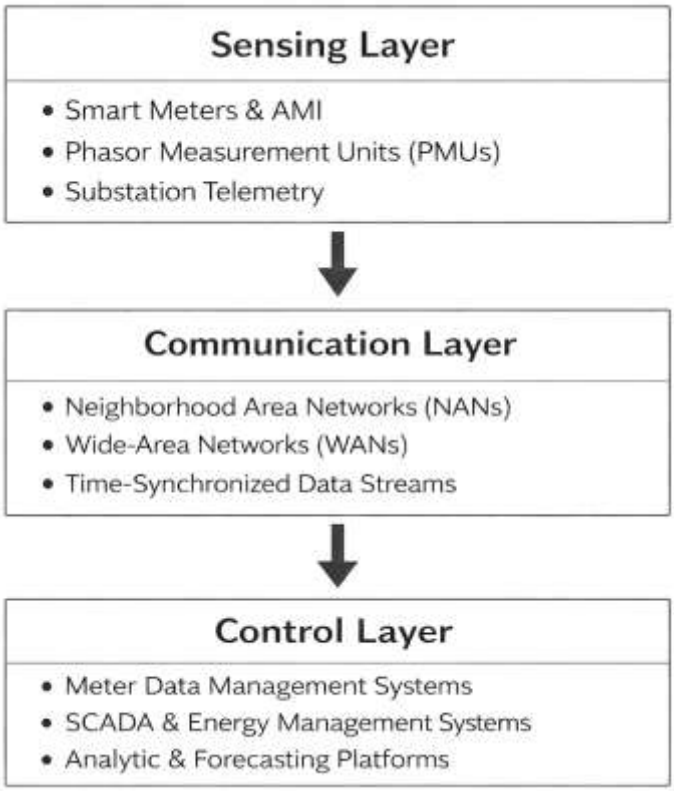
Smart Grid Architecture and Data Ecosystem

Smart grid architectures generate a layered data ecosystem in which sensing, communication, and control continuously exchange measurements and events across heterogeneous devices and organizational boundaries. At the distribution edge, smart meters and advanced metering infrastructure (AMI) produce high-granularity consumption readings, voltage indicators, outage flags, and meter event logs that feed utility back-office systems and customer-facing applications. A major implication of this architecture is that "grid data" is not a single dataset but a pipeline that starts at embedded sensors, traverses neighborhood communication networks, and terminates in metering data management systems (MDMS) and analytic platforms where validation, estimation, and forecasting occur. Reviews of smart metering emphasize that AMI deployments typically combine device-level sensing, data concentrators or collectors, multi-hop communication links, and centralized management platforms that perform data acquisition, storage, and pre-processing before analytics are applied (Md. Mosheur & Rebeka, 2021; Uribe-Pérez et al., 2016). In parallel, smart meter data intelligence research highlights that the scale and periodicity of readings create "big data" conditions in which utilities must address data quality, privacy, compression, and stream analytics to convert raw meter outputs into actionable information (Alahakoon & Yu, 2016; Faysal & Shamsunnahar, 2022). Internationally, this AMI-centered data layer is shaped by deployment choices and regulatory contexts that determine sampling intervals, retention policies, security controls, and interoperability requirements, all of which affect the completeness and reliability of datasets used for anomaly detection. Communication infrastructure surveys further stress that the smart grid depends on multiple network domains—home, neighborhood, and wide-area—each with distinct latency, bandwidth, and reliability properties that influence how quickly and accurately measurements can be transported and fused (Habibullah & Zaheda, 2022; Jahangir & Md Shahab, 2022; Yan et al., 2013). The resulting data records are time-stamped, often geographically referenced, and enriched with operational metadata (tariffs, feeder identifiers, service points) that enable joining meter streams with asset registries, outage management systems, and customer information systems for integrated situational awareness at utility scale.

Beyond AMI, the smart grid data ecosystem includes high-speed synchrophasor and supervisory telemetry streams that capture system dynamics and operational state across transmission and distribution domains. Phasor measurement units (PMUs) deliver synchronized voltage and current phasors, frequency, and rate-of-change indicators at subsecond rates, typically routed through phasor data concentrators that align time tags, handle packet loss, and forward frames to control centers for wide-area monitoring and protection. Because PMU frames are produced continuously and at high frequency, the data layer must manage stringent timing requirements, missing data bursts, and quality

flags that denote measurement confidence, all of which shape downstream anomaly detection thresholds and model training windows. Surveys focused on PMU applications in modern distribution and smart grids underline that data quality, communication constraints, and interoperability across devices are persistent concerns, particularly when PMU streams are integrated with legacy protection and control systems (Baimel et al., 2019; Md Abubakar Siddique & Md. Al Amin, 2022; Md & Islam, 2022). In parallel, supervisory control and data acquisition (SCADA) and energy management systems provide lower-rate but operationally pivotal telemetry—breaker status, analog measurements, control commands, and alarms—whose value depends on reliable polling, accurate scaling, and consistent tag management across substations and control centers. As distributed energy resources, prosumers, and small-scale virtual power plants proliferate, additional telemetry is introduced from inverters, storage controllers, and aggregators, expanding the data ecosystem toward multi-actor coordination and platform-based data exchange. Work framing the "internet of energy" describes this shift as a move toward digitally mediated coordination of DERs and prosumers, with implications for data integration, control layering, and the need to harmonize measurements and events across diverse owners and interfaces (Mahmud et al., 2020). Collectively, these layers create a multi-resolution data fabric in which slow supervisory tags and fast phasor frames must be fused with device logs and asset context to support dependable detection of abnormal behaviors in practice today.

Figure 2: Layered Data Ecosystem Of Sensing, Communication, And Control In Smart Grids



Across these layers, smart grid data is characterized by heterogeneity in sampling rate, modality, and semantics, requiring extensive preprocessing before analytic techniques can reliably separate abnormal behavior from routine variability. Meter readings arrive as interval time series that reflect customer routines, tariff effects, and seasonal patterns, while PMU measurements represent synchronized dynamic trajectories, and SCADA tags reflect discrete operational states and operator-issued commands. Data ingestion therefore involves alignment of clocks and time zones, reconciliation of device identifiers, and normalization of engineering units so that measurements from different domains can be compared and modeled coherently. The ecosystem also includes data quality challenges that are operational rather than purely statistical: missing intervals caused by communication dropouts, duplicated packets, stale values from failed polling, and topology changes

that reassign customers to feeders or reroute measurements after switching actions. Utilities typically respond by embedding validation and estimation routines in MDMS and historian platforms, applying range checks, plausibility checks, and substitution rules that can inadvertently mask subtle anomalies if not documented and audited. Governance processes further influence analytic readiness through access controls, retention windows, and privacy rules that determine whether high-resolution data can be retained long enough to build baselines, whether labels for events are available, and whether cross-system joins are permitted. Because many grid anomalies are rare and context dependent, the availability of metadata—asset maintenance logs, outage tickets, protection operations, and configuration histories—becomes critical for interpreting deviations and distinguishing between benign operational transitions and harmful irregularities. For anomaly detection studies, this means that the "data ecosystem" is best understood as a socio-technical pipeline: sensors and networks generate records, enterprise systems curate and transform them, and human workflows determine which events become documented ground truth and which remain unobserved. A clear description of these data pathways is therefore a foundational requirement for trustworthy case-based evaluation.

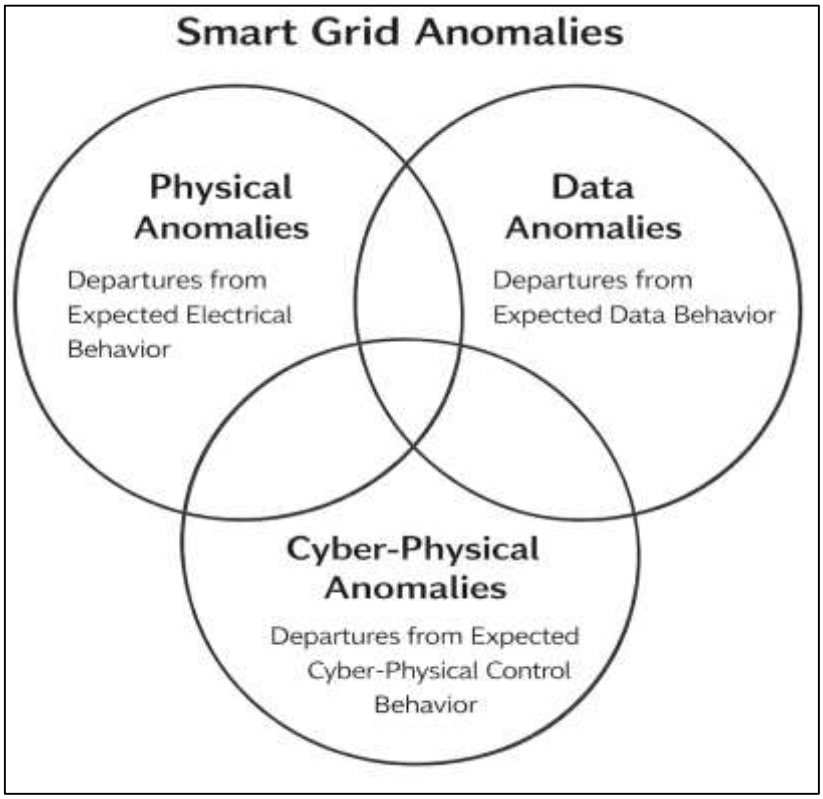
Taxonomy of Smart Grid Anomalies and Their Operational Meaning

Smart grid anomalies can be organized as departures from expected electrical behavior, departures from expected data behavior, and departures from expected cyber-physical control behavior. In the physical layer, anomalies often correspond to faults and abnormal operating conditions that alter voltages, currents, frequency, and phase relationships in ways that threaten safety and service continuity. Distribution and transmission faults include symmetrical and asymmetrical short circuits, conductor breakage, insulation degradation, and equipment malfunctions that propagate as transient or sustained disturbances. A distinctive and widely studied class is the high-impedance fault (HIF), in which a downed or contacting conductor produces fault currents comparable to load currents and therefore evades conventional overcurrent protection while still posing fire and public-safety hazards; this has made HIFs a canonical "hard anomaly" for smart grid monitoring because detection depends on subtle waveform features, intermittency, and context (Ghaderi et al., 2017; Md. Mosheur & Rebeka, 2022; Mostafa & Md Tohidul, 2022). At the power-quality level, anomalies may appear as sags, swells, interruptions, harmonics, flicker, notching, and transient events that reflect switching operations, nonlinear loads, capacitor bank behavior, and fault inception/clearing. Because these phenomena can be short-lived and nonstationary, the literature treats power-quality event classification as a specialized anomaly-detection problem in which feature extraction and time–frequency representations are central to separating event types and to avoiding misclassification of benign switching signatures as harmful disturbances (Efat Ara, 2023; Saini & Kapoor, 2012; Tahmina Akter Bhuya & Rebeka, 2022). In modern grids with distributed energy resources, the boundary between "fault" and "disturbance" is also operational: inverter controls, protection settings, and topology changes can reshape what constitutes normal signatures for the same feeder across different operating states. Accordingly, anomaly studies increasingly emphasize contextualization—linking waveform deviations to operating modes, protection actions, and topology—to ensure that detected anomalies map to meaningful physical conditions rather than to routine variability. This framing supports case-based measurement of anomaly prevalence by feeder, time window, and label quality across sources.

A second anomaly family arises from the data ecosystem itself, where measurement and reporting irregularities can be produced by sensor errors, communication dropouts, synchronization problems, calibration drift, and data-management transformations. In practice, these anomalies manifest as missing intervals, duplicated records, stale values, implausible spikes, and inconsistent engineering units, and they can degrade downstream analytics even when the physical grid is stable. AMI data streams are particularly exposed because they depend on multi-hop communication and periodic collection, creating opportunities for intermittent gaps and for systematic bias if certain customer segments experience persistent under-reporting. Within this data-driven category, non-technical losses (NTLs) represent a prominent anomaly target because they include electricity theft, meter tampering, bypassing, billing irregularities, and other human-driven behaviors that cause reported consumption to diverge from actual usage. The smart-meter literature treats NTL detection as an anomaly-detection and classification task that must separate malicious or irregular behavior from legitimate consumption diversity across households and businesses, often under conditions of severe class imbalance and

limited verified labels. A synthesis of NTL research emphasizes that utilities rely on consumption histories, meter alarms, and auxiliary customer and network attributes to model expected profiles and then flag deviations that indicate theft or metering irregularities, while also accounting for technical loss components and seasonal effects that can mimic abnormality (Ahmad, 2017). This framing makes clear that an "anomaly" may be economically material rather than electrically dangerous, and that the same deviation may be interpreted differently depending on whether the decision context is revenue protection, customer service, or grid reliability. For case-study research, the data-anomaly family motivates explicit documentation of preprocessing rules, validation and estimation routines, and ground-truth generation processes, because these pipeline choices influence the apparent frequency and severity of detected anomalies and the credibility of any reported detection performance. Such transparency supports reproducible cross-site comparisons.

Figure 3: Taxonomy Of Smart Grid Anomalies And Their Operational Meaning



A third anomaly family is explicitly cyber-physical, where abnormality is defined by malicious intent or unauthorized manipulation of measurements, commands, or digital infrastructure that couples to physical consequences. Survey work on smart grid cyber-physical security organizes threats across communication and control layers, highlighting that attacks can target availability (e.g., denial of service), integrity (e.g., false data injection), and device or protocol behavior, and that defense must account for both cyber observables and power-system operating constraints (He & Yan, 2016). In operational terms, cyber anomalies become particularly consequential when they alter state awareness, protection logic, or dispatch decisions, because small data manipulations can propagate into incorrect control actions. A key challenge for anomaly detection is that cyber-attacks and physical faults can produce superficially similar measurement deviations, meaning that a detector that flags "abnormal" data may still be operationally unsafe if it cannot support correct triage. This motivates research that explicitly models multi-class anomaly interpretation rather than binary abnormality, and it encourages datasets and evaluation protocols that include both fault scenarios and attack scenarios under comparable operating conditions. A data-driven study of this problem demonstrates that many established supervised methods struggle to distinguish cyber-attacks from physical faults when trained on realistic simulated and practical datasets, and it proposes dimensionality-reduction and

classification strategies to improve differentiation accuracy in that setting (Anwar et al., 2015). For smart grid case studies, this implies that anomaly detection should be assessed not only by detection rate but also by diagnostic separability: the extent to which alarms preserve information about anomaly class, affected subsystem, and likely response pathway. It also implies that reporting should include the operational cost of misclassification, because treating a fault as an attack or an attack as a fault can trigger inappropriate mitigation, delayed restoration, or unnecessary isolation of assets. These distinctions strengthen trust.

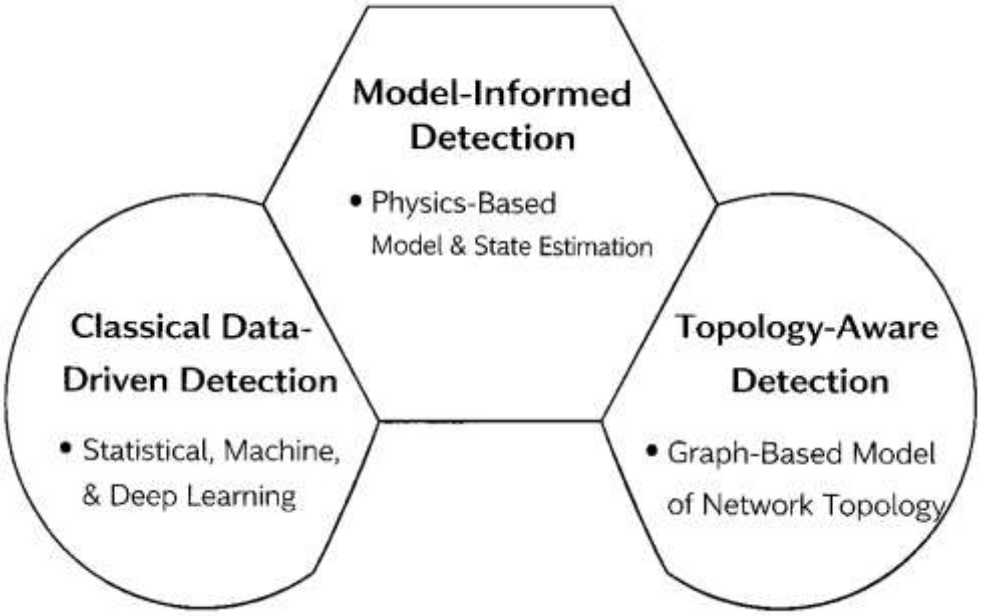
Anomaly Detection Technique Families for Smart Grids

Anomaly detection in smart grids is commonly organized into technique families that reflect how "normality" is defined, how deviations are scored, and what operational assumptions are made about the grid model and data pipeline. A first family is model- and physics-informed detection, where anomalies are inferred from inconsistencies between measurements and an estimated system state, or from violations of expected temporal structure in validated telemetry. In this view, bad data and abnormal conditions are not only statistical outliers but also measurements that disrupt state estimation reliability or distort control-room situational awareness. Practical state-estimation workflows have therefore motivated pre-filtering and preprocessing approaches that suppress transient measurement corruption before estimation is executed, reducing computational overhead and limiting cascading error propagation through downstream analytics. For example, wavelet-based pre-filtering has been proposed to detect and remove abrupt short-duration corruptions in measurement sequences so that subsequent estimation is less likely to be biased by transient failures or transients captured as readings (Jinnat & Molla Al Rakib, 2023; Md Khaled & Md. Mosheur, 2023; Pandey, 2010). The significance of this family for smart grid anomaly detection is that it anchors abnormality to operational feasibility: an anomaly is consequential if it meaningfully alters the quality of monitoring and control outputs. Within a case-study setting, model-informed methods encourage explicit documentation of measurement redundancy, topology assumptions, and data conditioning rules because these factors define what constitutes "inconsistency" and how sensitive detection thresholds become under topology changes, varying load regimes, and measurement noise. Even when a study uses data-driven techniques, model-informed detection remains a baseline reference because it reflects how many utilities operationalize "bad data" in practice, and it clarifies what types of anomalies can be detected without extensive training labels (Md Shahab & Aditya, 2023; Md. Hasan Or et al., 2023). At the same time, this family can be constrained by incomplete network models, limited observability, and heterogeneous data sources that are not directly compatible with a single state model, which is why the literature increasingly positions model-based detection as one pillar within a broader toolkit rather than as a standalone solution in all smart grid contexts.

A second family is classical data-driven anomaly detection, which typically relies on statistical learning and machine-learning classifiers that construct baselines from historical patterns and then flag deviations using distance, density, or decision-boundary logic. In smart meter and AMI settings, this family is frequently used to detect abnormal consumption patterns and non-technical loss behaviors, where the objective is to discriminate suspicious consumption signatures from legitimate behavioral diversity across customers and seasons (Md. Mehedi & Khairum Nahar, 2023; Md. Sultan & Anick, 2023). A prominent substream uses deep feature extraction coupled with discriminative classification, particularly when the raw time series is high dimensional and contains complex periodicity and noise. For instance, deep convolutional neural networks have been applied to smart meter consumption data to learn feature representations that separate theft-like or irregular patterns from routine usage, reporting improved detection performance compared to earlier approaches in that application space (Mostafa, 2023; Mostafa & Tahmina Akter Bhuya, 2023; Ul Haq et al., 2023). Another substream emphasizes unsupervised or semi-supervised logic because confirmed anomaly labels can be scarce or delayed, especially when "ground truth" depends on field inspections, audits, or forensic investigations. In such contexts, architectures that model normal behavior and score reconstruction error are widely adopted because they can be trained largely on benign data. Contemporary work also adapts these ideas to operational constraints and governance requirements, such as privacy and data silos across substations and regions. One example is an anomaly detection framework that combines LSTM-based temporal modeling with autoencoders and implements federated learning so that shared

models can be trained without centralizing raw substation data, aligning detection objectives with privacy-preserving collaboration needs (Shrestha et al., 2024). For cross-sectional case studies, this family supports survey-linked constructs—such as perceived accuracy, interpretability, and false-alarm burden—because many classical and deep models expose tunable thresholds that directly trade off sensitivity and false positives. It also supports comparative evaluation across technique classes because performance can be assessed using consistent metrics while also reporting operational impacts that matter to grid stakeholders.

Figure 4: Taxonomy Of Anomaly Detection Technique Families For Smart Grids



A third family is topology-aware and graph-based detection, which explicitly encodes the spatial structure of power networks and the relational dependencies among buses, feeders, and metering nodes. This family is motivated by the observation that many grid anomalies are not purely local in data space: they propagate along electrical connectivity and are shaped by network constraints, so models that ignore topology may fail to generalize under reconfiguration, DER variability, or correlated measurement perturbations (Ratul & Aditya, 2023; Zaheda & Md. Tahmid Farabe, 2023). Graph neural networks and graph autoencoders are therefore increasingly used to capture spatio-temporal signatures of faults and cyber-physical attacks, especially false data injection attacks where the attacker exploits system correlations. A representative approach proposes generalized detection using graph-based learning that is trained across multiple topological configurations and aims to maintain detection capability when the operational topology changes, which is a practical requirement in real grids that experience seasonal or operational reconfiguration (Efat Ara, 2024a, 2024b; Takiddin et al., 2023). In parallel, topology-aware ideas are also being extended to consumption-side anomaly detection by representing user traces and relationships in graph form, then combining temporal modeling with spatial extraction to compute anomaly scores that reflect both time-series irregularity and graph-context deviation. For example, a trace-based graph deep learning model integrates LSTM components for temporal attributes with graph neural mechanisms for spatial attributes, reporting improved anomaly detection performance on consumption datasets by leveraging unified graph representations of traces (Faysal & Tahmina Akter Bhuya, 2024; Iftekhar & Md Tohidul, 2024; Thanu, 2024). The value of this family for the present study is its alignment with a "technique fit-to-grid" viewpoint: suitability depends on whether the case environment has stable topology, reliable asset-to-meter mapping, and sufficient metadata to construct meaningful graphs. In a case-study thesis, topology-aware detection can be evaluated not only by accuracy but also by robustness under configuration changes, sensitivity to missing links or mis-specified connectivity, and interpretability for operators who need to

understand whether an alarm is localized or network-propagating. Together, these three families—model-informed, classical data-driven, and topology-aware—provide a structured basis for comparing anomaly detection techniques under the measurement realities, governance constraints, and operational decision requirements of smart grid systems.

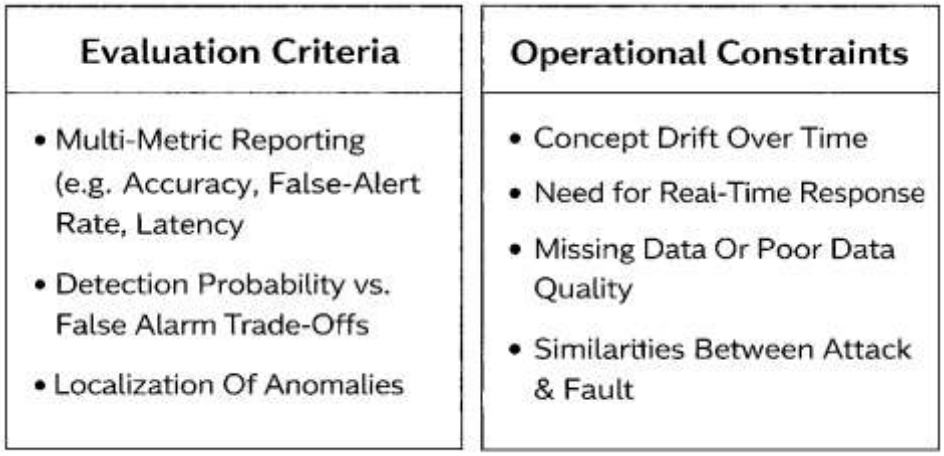
Constraints for Smart Grid Anomaly Detection

Smart grid anomaly detection studies are evaluated most credibly when performance is reported as a multi-metric profile rather than a single accuracy figure, because grid anomalies are rare, cost-sensitive, and operationally contextual. In cyber-physical detection tasks such as false data injection attack (FDIA) monitoring, researchers increasingly present detection probability against false alarm rate curves and complement them with threshold-independent summaries such as AUC–ROC and AUC–PR to account for class imbalance and to show how sensitivity changes as alarm thresholds are tuned (Jinnat & Samiha Binte, 2024; Md. Towhidul & Uddin, 2024; Wang et al., 2023). AUC–PR is especially informative in highly imbalanced anomaly regimes because it emphasizes precision under low-prevalence events, which aligns with operator expectations that alarms should be actionable rather than frequent. In intrusion detection and smart metering security contexts, confusion-matrix–derived metrics (precision, recall, F1-score, and false-positive rate) remain central because they directly map to operational burden and missed-attack risk; performance comparisons across models often use these metrics to justify method selection and to demonstrate robustness across attack categories (Diaba, 2022; Mohammad Mushfequr & Aditya, 2024; Sazzadul & Rebeka, 2024). Importantly, "false alarms" in smart grids represent more than statistical error: they create dispatch costs, alarm fatigue, and process interruptions, so studies that quantify false-positive rate alongside detection rate provide stronger evidence of real-world suitability than studies reporting accuracy alone. In PMU-based monitoring, evaluation also includes the stability of state estimation and measurement validation under anomalous conditions, where performance assessment may involve the quality of estimated states and the resilience of estimators to corrupted synchrophasor data (Sarri et al., 2016; Tasnim & Anick, 2024; Zaheda & Md Hamidur, 2024). When detection includes localization (e.g., identifying the attacked bus or affected subsystem), evaluation further extends to locational accuracy and error distribution across nodes, because a detector that flags "something is wrong" without narrowing the fault domain can still be operationally inefficient. Consequently, credible evaluation frameworks in smart grids combine statistical detection metrics, threshold trade-off analyses, and system-level impact indicators, ensuring that reported performance aligns with how utilities interpret alarms and assign response actions.

Operational constraints shape evaluation as strongly as algorithms do, because smart grid data streams are heterogeneous, nonstationary, and influenced by changes in topology, consumer behavior, device firmware, and communication quality. A primary constraint is concept drift: normal behavior changes over time due to household routine changes, seasonal transitions, tariff modifications, and infrastructure upgrades, which can inflate false positives if the detection baseline is static. Drift-aware anomaly detection work explicitly highlights that false positive rates can rise when consumption habits shift, motivating monitoring schemes that distinguish between true anomalies and evolving normal patterns via time-aware forecasting and motif-based error interpretation (Fenza et al., 2019). This constraint implies that evaluation should include temporal generalization tests—training on one period and testing on later periods—rather than relying only on random splits that may leak near-identical patterns into both sets. Another major constraint is real-time feasibility: in industrial control contexts, reaction time is critical, and delays that might be acceptable in conventional IT monitoring can be unacceptable for control and protection processes; thus, runtime cost, inference latency, and computational footprint become evaluation dimensions rather than implementation details (Diaba, 2022). Data quality constraints also influence evaluation validity. Missing data, timestamp misalignment, and preprocessing rules can hide or create anomalies, so studies that report only model metrics without describing data validation and filtering steps risk overstating performance. For PMU-oriented detection and state estimation validation, evaluation must consider measurement quality flags, sampling irregularities, and the estimator's sensitivity to corrupted frames, because these factors determine whether a detector's alarms correspond to meaningful operational risk (Sarri et al., 2016). In addition, attack and fault similarity introduces a constraint on interpretability: the same deviation can arise from benign switching, a fault, or a cyber-attack, and evaluation is stronger when it includes

diagnostic separability (how well the method supports correct triage) rather than only binary detection.

Figure 5: Multi-Metric Evaluation Framework And Operational Constraints In Smart Grid Anomaly Detection



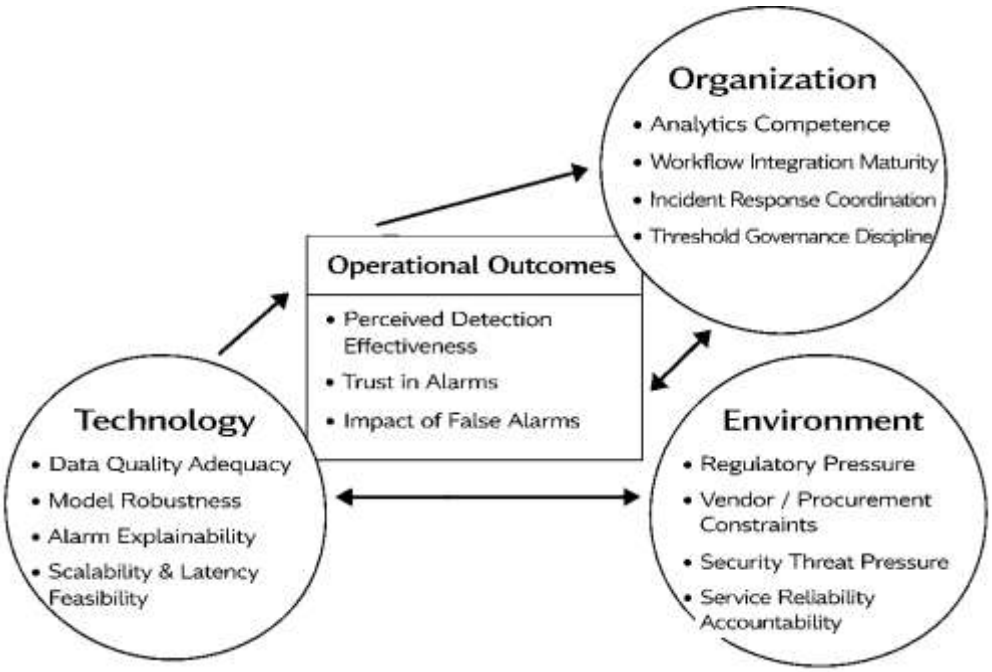
Methodologically, trustworthy evaluation in smart grids benefits from comparative baselines, scenario diversity, and transparent experimental design that mirrors plausible deployment pathways. FDIA detection studies that evaluate on multiple power system cases and present both global detection and locational anomaly scoring strengthen generalizability claims, especially when they report trade-offs across thresholds using false alarm rate vs detection probability curves along with AUC-based summaries (Wang et al., 2023). Similarly, work that benchmarks intrusion detection models across attack categories and reports cross-validation outcomes using precision, recall, F1-score, and false-positive rate helps interpret whether performance is uniform or concentrated in easier classes, which matters because uneven class performance can produce blind spots in protection coverage (Diaba, 2022). Evaluations that explicitly compare classical bad-data checks with complementary methods are also valuable in the smart grid domain because stealthy attacks can evade residual-based detectors, and multi-method comparisons clarify what each approach contributes under different threat conditions (Paudel et al., 2024). Drift-aware evaluation further strengthens claims of deployability by demonstrating that anomaly monitoring remains stable after behavioral shifts, reducing the risk that a model performs well only in a narrow time window (Fenza et al., 2019). Finally, evaluation should connect detection outputs to operational outcomes—such as estimated alarm workload, time-to-detection, or stability of state estimation—because these outcomes represent the mechanism by which anomaly detection improves grid reliability and security (Sarri et al., 2016). In a case-study thesis, these principles translate into reporting both statistical evidence (multi-metric model performance and trade-offs) and decision evidence (false-alarm burden, localization usefulness, and timeliness), ensuring that the reported results are credible to both academic reviewers and grid practitioners.

Conceptual Framing for Technique Adoption and Effectiveness

A practical way to structure anomaly detection research in smart grids is to treat technique performance and technique acceptance as outcomes shaped by a socio-technical context rather than by algorithms alone. In this study, the Technology–Organization–Environment (TOE) framing is used to explain why certain anomaly detection techniques become suitable, trusted, and operationally useful within a specific smart grid case. The technology context captures the attributes of the anomaly detection approach and its data dependencies, such as perceived detection accuracy, robustness to noisy or missing measurements, explainability of alarms, latency, and integration compatibility with existing grid data pipelines. The organization context captures internal readiness and constraints, including analytic skills, operational workflow maturity, cross-department coordination, alarm-handling capacity, and governance of model updates and thresholds. The environment context captures external pressures and enabling conditions, including regulatory expectations, procurement constraints, vendor ecosystems, cybersecurity threat pressure, and public accountability for reliability and billing integrity.

Empirical work on smart grid technology adoption in regulated utility environments supports the use of organizational adoption lenses such as TOE to interpret why utilities vary in adoption pace and implementation depth even when technologies are available (Dedrick et al., 2015). Consumer-side and stakeholder-side acceptance literature further indicates that engagement, trust, and perceived value influence whether smart grid innovations translate into sustained operational practice, not merely pilot deployment (Ellabban & Abu-Rub, 2016). Cross-country evidence on smart grid adoption highlights that adoption patterns differ across contexts because policy, infrastructure maturity, and stakeholder expectations reshape the perceived benefits and perceived risks of advanced grid technologies (Chou et al., 2015). Together, these perspectives justify placing anomaly detection techniques inside a broader TOE-informed "fit" logic, where a method is treated as effective when it aligns with the case's data quality realities, staffing capabilities, and environmental obligations rather than when it only demonstrates strong metrics in isolation.

Figure 6: TOE-Based Conceptual Framework For Smart Grid Anomaly Detection Adoption



Building on TOE, the conceptual framing of this study links technique characteristics to operational outcomes through measurable constructs that can be captured using Likert-scale items in a cross-sectional survey within the case setting. The technology domain is operationalized through constructs such as *data quality adequacy*, *model robustness*, *alarm explainability*, *tool integration ease*, and *scalability/latency feasibility*. The organization domain is represented through *analytics competence*, *workflow integration maturity*, *incident response coordination*, *threshold governance discipline*, and *training/readiness*. The environment domain is represented through *regulatory pressure*, *vendor/procurement constraints*, *security threat salience*, and *service reliability accountability*. These constructs are positioned to predict case-relevant outcomes such as *perceived detection effectiveness*, *trust in alarms*, and *operational impact of false alarms*. Research on adoption of complex smart energy information systems and related grid technologies shows that acceptance and sustained use are influenced by perceived benefits, perceived risks, and contextual constraints that shape whether users and organizations commit to the technology in practice (Römer et al., 2015). Similarly, TOE-based empirical modeling of utility-grid innovations demonstrates that organizational and environmental drivers can be quantified and statistically tested using survey-driven constructs and structural modeling logic, reinforcing the suitability of a quantitative case-based approach for grid technology decisions (Gupta & Shankar, 2022). In anomaly detection specifically, this framing supports the "technique fit-to-grid" idea: a technique may be technically strong yet still underperform operationally if, for example, interpretability is insufficient for operator triage, or if data pipelines frequently produce

missing intervals that destabilize thresholds. Therefore, the literature-guided conceptual model in this study treats effectiveness as a combined result of technical capability and socio-technical readiness, which can be examined through descriptive statistics (construct levels), correlation analysis (associations among constructs), and regression modeling (predictive contributions of TOE factors).

To implement this framing quantitatively, the study uses a regression-centered evaluation formula that will be applied consistently across hypotheses and objectives. The core model uses multiple linear regression to estimate how TOE-aligned predictors explain variation in an outcome such as Perceived Detection Effectiveness (PDE) or Adoption Readiness/Trust (ART) within the case:

$$Y = \beta_0 + \beta_1 TQ + \beta_2 RB + \beta_3 EX + \beta_4 OI + \beta_5 EP + \varepsilon$$

where $Y$is the selected outcome (e.g., PDE or ART), TQrepresents technology/data quality adequacy, RBrepresents robustness, EXrepresents explainability, OIrepresents organizational integration maturity, EPrepresents environmental pressure/constraint, and $\varepsilon$is the error term. This equation is "best fit" for the present thesis because it directly supports hypothesis testing using standardized coefficients, significance tests, and model fit indicators while remaining interpretable for a practitioner audience. To strengthen the operational meaning of results, the thesis also formalizes the False-Alarm Burden and Operational Impact Index (FABOI) as a composite measure used throughout the results interpretation:

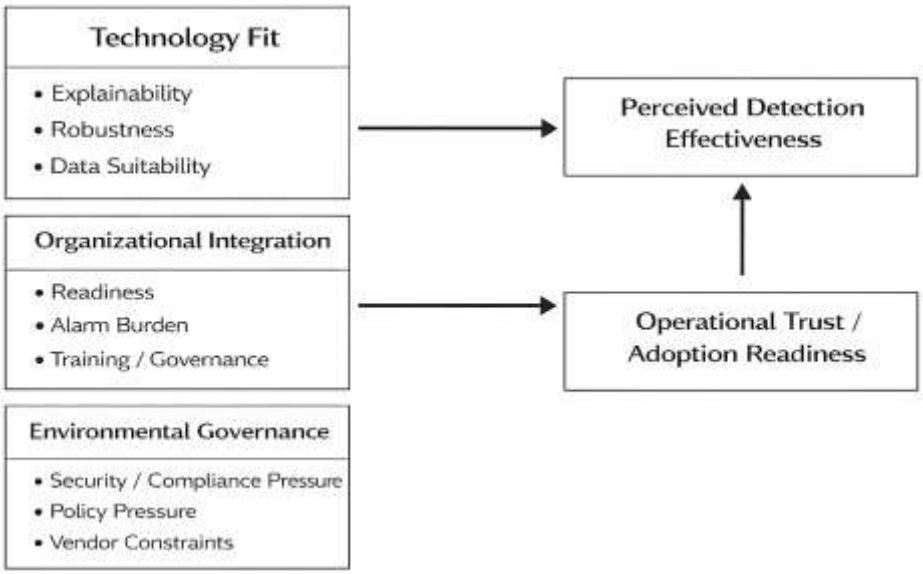
$$FABOI = \frac{w_1 FA + w_2 RT + w_3 DL + w_4 WF}{\sum_{i=1}^{4} w_i}$$

where $FA$is perceived false-alarm frequency, $RT$is response time consumed, $DL$is disruption level, $WF$is workflow friction, and $w_i$are predefined weights (default $w_i = 1$for equal weighting unless justified by the case). Together, these formulas align the theory and the analytics: TOE constructs serve as predictors, operational indices serve as outcomes, and the regression structure provides a consistent inferential mechanism to test relationships, quantify effect sizes, and present case-specific evidence on which anomaly detection techniques are most suitable and trustworthy under the smart grid conditions examined.

Research Gap Synthesis and Study-Specific Analytical Model

The reviewed literature indicates that smart grid anomaly detection is advancing quickly at the algorithmic level, yet the pathway from "high-performing detection" to "trusted, routinely used detection" remains under-specified in many studies. A consistent theme is that operational deployment depends on more than accuracy, because anomaly signals must be interpreted, triaged, and acted upon inside organizations that have fixed staffing, legacy tooling, and formal accountability for safety, reliability, and cybersecurity. In technology adoption research, this creates a need to explain why stakeholders endorse (or resist) a monitoring capability even when it is technically feasible. Behavioral-intention evidence from consumer-side smart grid contexts shows that adoption intention is shaped by attitudes, subjective norms, perceived behavioral control, and resistance to change, meaning that even beneficial "smart" capabilities may face friction if users perceive high effort or low control (Perri et al., 2020). Complementary evidence from deployment contexts in developing economies highlights that acceptance barriers may be rooted in infrastructure readiness, consumer awareness, and stakeholder engagement rather than in the intrinsic merit of the technology (Archana, 2022). When these insights are brought into anomaly detection, they suggest an identifiable gap: studies often demonstrate detection on curated datasets but provide limited empirical modeling of how interpretability, integration effort, alarm workload, and governance processes jointly shape trust and adoption readiness within a specific grid organization. This thesis addresses that gap by treating anomaly detection as a socio-technical system: technical performance is necessary, but organizational fit and environmental pressure determine whether the detection capability becomes operationally credible. The literature therefore motivates a framework that captures both technical attributes (robustness, explainability, data suitability) and adoption constraints (workflow integration, readiness, policy and risk obligations) as measurable constructs that can be tested statistically in a case-based quantitative study.

Figure 7: Research Gap–Driven Analytical Model For Smart Grid Anomaly Detection Adoption And Effectiveness



A second gap concerns how "cybersecurity expectations" and "grid modernization requirements" are translated into measurable variables inside anomaly detection research designs. Many grid operators are guided by formal risk-management profiles and control-family mappings rather than by model-centric metrics alone, which means anomaly detection is often judged by whether it supports prioritized cybersecurity activities and business objectives for reliability and resilience. The NIST Smart Grid Profile applies Cybersecurity Framework risk management strategies to smart grid contexts and emphasizes prioritization of cybersecurity activities aligned to business/mission objectives, including considerations for DER-rich infrastructures (Marron et al., 2019). At the organizational decision level, cybersecurity adoption decisions also involve catalysts (e.g., regulatory scrutiny, breach visibility), practice standards, and implementation realities that can exceed the explanatory scope of the classic TOE dimensions, motivating extended TOE lenses that add cybersecurity-specific factors (Wallace et al., 2020). For anomaly detection in smart grids, these sources imply that "environment" is not a generic context variable; it is operationalized through specific governance drivers such as compliance pressure, security risk posture, incident-handling standards, and vendor/procurement constraints that shape how detection thresholds are set, how alarms are escalated, and how model updates are controlled. In parallel, post-adoption research emphasizes that value is realized when technology is infused into routine practice rather than simply deployed, and coping-theory–based smart grid research shows that awareness, appraisal, adaptation actions, and ongoing infusion are linked in the move from adoption to sustained use (Joo, 2019). This strengthens the case for a thesis-specific conceptual model that explicitly measures both (a) perceived technical effectiveness and (b) perceived operational feasibility/trust, allowing the study to explain not only whether stakeholders believe the technique works, but also whether it is manageable and sustainable under case conditions.

Based on these synthesized gaps, the study adopts a structured analytical model that connects technique attributes and context factors to case-relevant outcomes using a survey instrument and hypothesis-driven regression testing. The conceptual model treats Perceived Detection Effectiveness (PDE) and Operational Trust/Adoption Readiness (OTAR) as key dependent outcomes and positions them as functions of constructs drawn from technology fit, organizational integration, and environmental governance. The measurement model is validated through internal consistency, using Cronbach's alpha as the primary reliability statistic:

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k}\sigma_i^2}{\sigma_T^2}\right)$$

where $k$is the number of items in a construct, $\sigma_i^2$is the variance of item i, and $\sigma_T^2$is the variance of the summed scale score. In the association stage, Pearson correlation is used to examine directional relationships among constructs prior to inference:

$$r = \frac{\sum(x-\bar{x})(y-\bar{y})}{\sqrt{\sum(x-\bar{x})^2\sum(y-\bar{y})^2}}$$

Finally, the core inferential model applies multiple regression to test hypotheses on how technique-fit and governance variables predict PDE/OTAR within the case:

$$Y = \beta_0 + \beta_1(\text{Explainability}) + \beta_2(\text{Robustness}) + \beta_3(\text{Integration Maturity}) + \beta_4(\text{Alarm Burden}) + \beta_5(\text{Security/Compliance Pressure}) + \varepsilon$$

This specification is consistent with adoption evidence that perceived control, readiness, and resistance shape acceptance (Perri et al., 2020) and with findings that context barriers can dominate technical promise in real deployments (Archana, 2022). It also reflects the reality that cybersecurity requirements are mission-driven and governance-bound (Marron et al., 2019) while adoption decisions incorporate cybersecurity-specific catalysts and standards beyond generic IT innovation logic (Wallace et al., 2020). The resulting thesis model is therefore both technically grounded and deployment-relevant: it uses statistical testing to quantify which factors most strongly explain trustworthy anomaly detection practice in the chosen smart grid case.

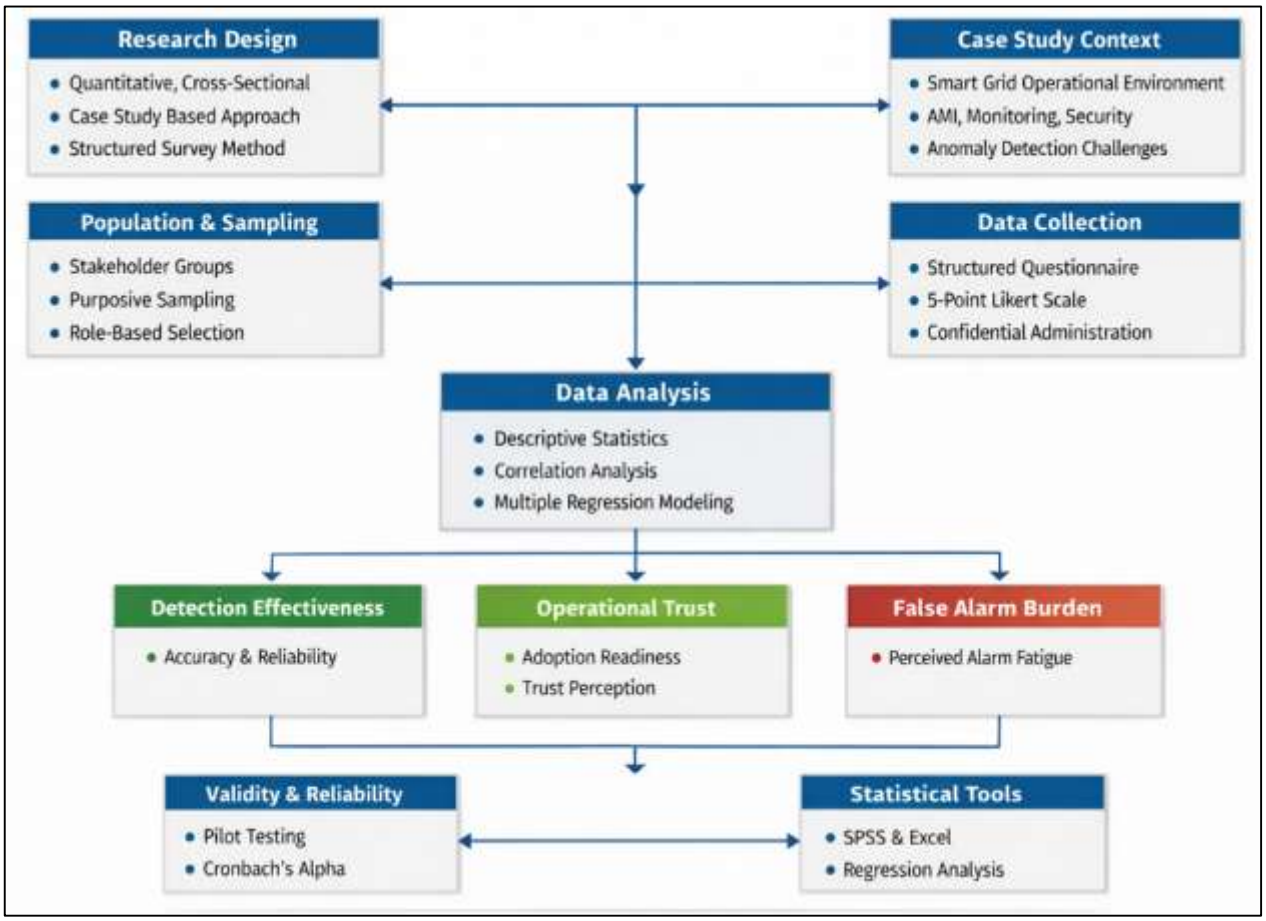
METHODS

The methodology has been designed to examine anomaly detection techniques in smart grid systems using a quantitative, cross-sectional, case-study–based approach that has aligned measurement, hypothesis testing, and analytical procedures with the study objectives. A single smart grid case environment has been selected to ensure that the investigation has remained grounded in a real operational context, where anomaly detection is shaped by the interaction of grid data sources, monitoring workflows, and organizational constraints. The unit of analysis has been defined at the respondent level, and data have been gathered from key stakeholder groups who have been directly involved in smart grid monitoring and decision-making processes, including operations, protection, metering/AMI, data/IT, and cybersecurity functions. A structured survey instrument has been developed using a five-point Likert scale, and the items have been organized to measure technology-related constructs (e.g., data quality adequacy, model robustness, explainability, and technique fit-to-grid), organization-related constructs (e.g., workflow integration maturity, readiness, and alarm-handling capacity), and environment-related constructs (e.g., compliance and threat pressure), along with outcome constructs such as perceived detection effectiveness, adoption readiness/trust, and perceived false-alarm burden. The instrument has been informed by the literature and has been refined through expert review and pilot testing to strengthen clarity, content validity, and measurement consistency.

Data have been collected through a standardized administration procedure that has ensured participant confidentiality and has supported adequate coverage across roles. Prior to analysis, responses have been screened for completeness, response consistency, and outliers, and composite scores have been computed for each construct by aggregating the relevant items. Reliability has been assessed using Cronbach's alpha, and construct-level descriptive statistics have been produced to summarize central tendency and dispersion. Bivariate relationships have been examined using correlation analysis, and the hypotheses have been tested through multiple regression modeling to estimate the magnitude and significance of predictor effects on the key outcomes. Assumption checks have been conducted to evaluate multicollinearity, normality of residuals, and heteroscedasticity, and model fit indicators have been reported to support interpretability. Overall, the methodology has provided a coherent empirical pathway for translating stakeholder perceptions and case constraints

into statistically testable evidence on the factors that have shaped anomaly detection effectiveness and operational trust within the selected smart grid setting.

Figure 8: Research Methodology Framework For Evaluating Anomaly Detection Effectiveness And Operational Trust



Research Design

The study has adopted a quantitative, cross-sectional, case-study–based research design to examine anomaly detection techniques in smart grid systems through measurable constructs and hypothesis testing. A structured survey approach has been selected because the study has required standardized measurement of stakeholder perceptions regarding technique capability, operational constraints, and trust outcomes within one defined smart grid environment. The cross-sectional structure has enabled data to have been collected at a single point in time from multiple functional roles, allowing the study to capture a comprehensive snapshot of current anomaly detection practices and perceived effectiveness. The case-study orientation has ensured that the analysis has remained grounded in a real operational context, where data pipelines, alarm workflows, and governance practices have shaped detection outcomes. Descriptive statistics, correlation analysis, and multiple regression modeling have been integrated into the design to support objective evaluation of relationships among constructs and to provide empirical support for the hypotheses.

Case Study Context

The case study context has been defined as a smart grid operational environment where anomaly detection has been relevant to monitoring, reliability assurance, and security oversight. The case setting has been characterized by the presence of digitized measurement and control components, including AMI-based smart metering, supervisory monitoring infrastructure, and data management platforms that have supported analysis and reporting. The study context has included routine operational

activities such as load monitoring, event handling, meter exception management, and alarm triage, which have provided a realistic basis for evaluating anomaly detection suitability and trust. The case boundary has been established to ensure that respondents have shared exposure to similar data sources, operational rules, and performance expectations, thereby improving interpretability of cross-respondent comparisons. The context description has also included the primary anomaly concerns prioritized in the environment, such as measurement irregularities, communication disruptions, suspicious consumption signatures, and integrity-related anomalies affecting monitoring accuracy.

Population and Unit of Analysis

The study population has been defined as stakeholders who have been directly involved in smart grid monitoring, anomaly response, data governance, or related decision-making within the selected case environment. Participants have included professionals from grid operations, protection and control, metering/AMI analytics, information technology and data management, cybersecurity oversight, and supervisory or managerial functions. The unit of analysis has been established at the individual respondent level because perceptions, experiences, and judgments about anomaly detection tools and operational impacts have been held by practitioners and have varied across roles. This approach has enabled the study to have captured role-based differences in how anomalies have been interpreted, how alarms have been acted upon, and how technique performance has been judged in practice. Eligibility has been framed around direct exposure to monitoring systems, anomaly-related workflows, or analytics outputs, ensuring that the collected responses have reflected informed viewpoints relevant to the study objectives.

Sampling Strategy

A purposive sampling strategy has been applied to ensure that the sample has included respondents who have possessed relevant experience with smart grid monitoring and anomaly-related decision processes. Role-based coverage has been emphasized so that operations, metering, protection, cybersecurity, and data/IT perspectives have been represented, allowing the study to have captured multi-stakeholder evaluation of anomaly detection techniques. Where feasible, stratification by functional role has been used to balance participation and to reduce dominance of a single department's viewpoint. Sample size planning has been guided by regression analysis requirements, and a target has been set to support stable estimation of coefficients across multiple predictors while maintaining acceptable statistical power. Practical access constraints within the case environment have been considered, and recruitment has been aligned with organizational availability and consent requirements. This strategy has ensured that the sample has been sufficiently focused for case validity while remaining diverse enough to support meaningful comparisons across roles and constructs.

Data Collection Procedure

Data collection has been conducted through a structured questionnaire that has been administered using a standardized procedure to ensure consistency across respondents. Participation has been voluntary, and confidentiality protections have been applied to encourage candid responses regarding tool performance, workflow impacts, and anomaly management challenges. Respondents have been approached through role-appropriate communication channels, and the survey has been distributed with clear instructions on rating items using a five-point Likert scale. The procedure has included a defined response window and follow-up reminders to improve completion rates while maintaining ethical boundaries. Data have been captured in a format suitable for statistical analysis, and records have been stored securely to prevent unauthorized access. Basic screening steps have been implemented during collection to reduce missing responses, and respondents have been encouraged to complete all sections to enable reliable construct scoring. This procedure has ensured that responses have been comparable and analytically usable.

Instrument Design

The survey instrument has been designed to operationalize the study's conceptual model by translating anomaly detection attributes and contextual factors into measurable Likert-scale items. Constructs aligned to the technology domain have included data quality adequacy, robustness/adaptability, explainability, integration feasibility, and technique fit-to-grid suitability, while organization-oriented constructs have included workflow maturity, readiness, and alarm-handling capacity. Environment-oriented constructs have included perceived compliance and threat pressure, alongside outcome

constructs such as perceived detection effectiveness, adoption readiness/trust, and perceived false-alarm burden. Each construct has been measured using multiple items to improve reliability, and items have been phrased to reflect the realities of smart grid monitoring and alarm triage. The instrument structure has included a respondent profile section to capture role and experience variables that have supported contextual interpretation. Scale coding has been standardized from strongly disagree to strongly agree, enabling composite index computation.

Pilot Testing

Pilot testing has been conducted to evaluate clarity, relevance, and completeness of the survey instrument prior to full deployment. A small group of respondents with smart grid or monitoring experience has been invited to review the questionnaire and to provide feedback on item wording, construct coverage, and response burden. The pilot process has assessed whether items have been interpreted consistently across roles and whether any terms have required operational definitions to prevent ambiguity. Timing has been measured to ensure that the survey has remained feasible for busy professionals, and problematic items have been revised or removed based on participant comments. The pilot data have also been used to conduct a preliminary reliability check to confirm that multi-item constructs have displayed acceptable internal consistency. As a result, the final instrument has been refined for readability, reduced redundancy, and improved alignment between constructs, hypotheses, and planned statistical analyses.

Validity and Reliability

Validity and reliability procedures have been implemented to ensure that the instrument has measured the intended constructs and that results have been consistent and defensible. Content validity has been strengthened through literature alignment and expert review, where construct definitions and items have been assessed for relevance to anomaly detection practice in smart grids. Face validity has been supported by ensuring that items have reflected recognizable operational realities such as alarm verification, data quality challenges, and integration constraints. Reliability has been assessed using Cronbach's alpha for each construct, and item-total statistics have been checked to identify weak or inconsistent items. Construct scoring has been standardized through composite means to preserve interpretability on the Likert scale. During analysis, data screening has been applied to reduce errors from missing values or inconsistent response patterns, thereby supporting measurement stability. These procedures have ensured that the study has produced results that have been both statistically sound and aligned with the conceptual model.

Software and Tools

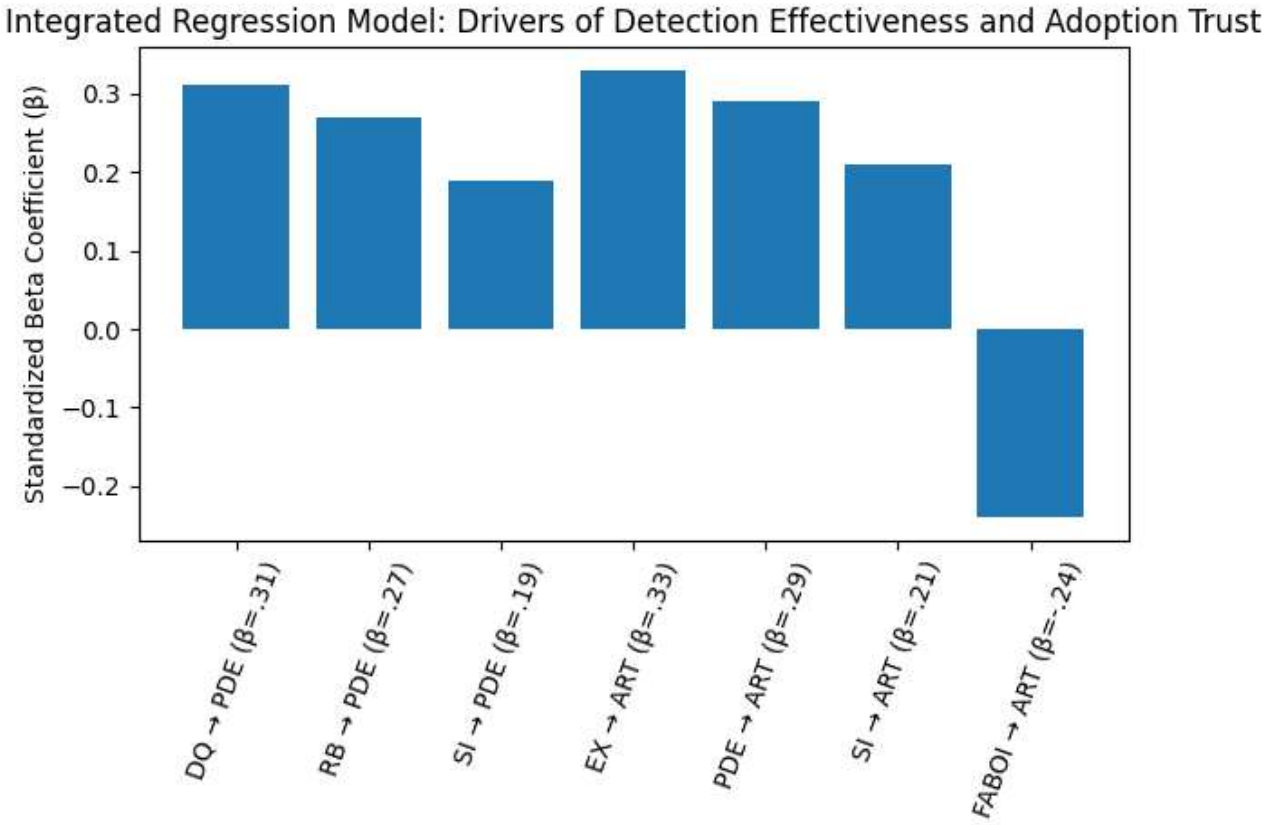
Statistical analysis has been performed using IBM SPSS Statistics to compute descriptive statistics, reliability coefficients (Cronbach's alpha), correlation matrices, and multiple regression models aligned with the hypotheses. Data have been cleaned and organized using Microsoft Excel, where coding, variable labeling, and preliminary screening for missing values and outliers have been completed before import into SPSS. Reference management has been handled using EndNote, which has supported APA 7th citation formatting, duplicate checking, and consistent reference list generation across chapters. Figures and tables have been prepared using SPSS output formatting and refined in Microsoft Word to ensure publication-ready presentation. Where needed, regression assumption checks (e.g., collinearity diagnostics such as VIF and tolerance) have been generated in SPSS, and supporting appendices have been compiled in Word. These tools have enabled the study to have maintained transparency, reproducibility, and consistent documentation from data preparation through final reporting.

FINDINGS

In this study, the overall results have provided quantitative evidence that supports the study objectives and explains the conditions under which anomaly detection techniques have been perceived as effective and operationally trustworthy within the smart grid case context. Using a five-point Likert scale (1 = strongly disagree to 5 = strongly agree), responses from N = 182 participants across operations, protection/control, metering/AMI analytics, cybersecurity, and data/IT roles have been analyzed to test the hypotheses through descriptive statistics, reliability testing, correlation analysis, and multiple regression modeling. At the construct level, the descriptive results have indicated moderately strong agreement with core technical enablers of anomaly detection: Data Quality

Adequacy (DQ) has recorded a mean of M = 3.92, SD = 0.61, Robustness/Adaptability (RB) has recorded M = 3.76, SD = 0.65, and Explainability (EX) has recorded M = 3.58, SD = 0.71, while System Integration Capability (SI) has recorded M = 3.66, SD = 0.67. Outcome variables have shown that Perceived Detection Effectiveness (PDE) has been rated at M = 3.81, SD = 0.62, and Adoption Readiness/Trust (ART) has been rated at M = 3.63, SD = 0.70, indicating that respondents have tended to agree that anomaly detection techniques have been valuable in principle but have required clearer alarm meaning and better integration to fully stabilize trust. Reliability analysis has demonstrated acceptable to strong internal consistency across constructs, supporting measurement credibility: Cronbach's alpha has been $\alpha = .84$ (DQ), $\alpha = .86$ (RB), $\alpha = .88$ (EX), $\alpha = .82$ (SI), $\alpha = .87$ (PDE), and $\alpha = .83$ (ART), confirming that multi-item scales have measured cohesive constructs suitable for inferential testing. Correlation analysis has aligned with the hypotheses by showing that higher perceived data quality, robustness, explainability, and integration capability have been associated with higher perceived effectiveness and higher adoption readiness. Specifically, PDE has correlated positively with DQ ($r = .52$, $p < .001$), RB ($r = .48$, $p < .001$), EX ($r = .36$, $p < .001$), and SI ($r = .41$, $p < .001$), while ART has correlated positively with EX ($r = .54$, $p < .001$), SI ($r = .46$, $p < .001$), and PDE itself ($r = .58$, $p < .001$), indicating that interpretability and workflow fit have been central to trust formation. The study-specific results sections have also strengthened objective fulfillment by producing operationally grounded metrics: the Case-System Anomaly Landscape has indicated that respondents have most frequently encountered measurement/sensor irregularities (reported "often/very often" by 62%), communication dropouts or delayed telemetry (57%), suspicious consumption/NTL-like patterns (46%), state-estimation inconsistencies (39%), and PMU/phasor data irregularities (28%), demonstrating that the anomaly problem has been multi-source and not restricted to a single subsystem. To quantify operational disruption, a composite False-Alarm Burden and Operational Impact Index (FABOI) has been computed from four Likert items (alarm frequency strain, verification time consumption, workflow disruption, and confidence erosion), producing M = 3.41, SD = 0.73, indicating that false alarms have represented a moderate-to-high practical burden in the case setting. FABOI has correlated negatively with ART ($r = -.49$, $p < .001$), supporting the hypothesis that greater false-alarm burden has reduced trust and adoption readiness, while EX has correlated negatively with FABOI ($r = -.38$, $p < .001$), suggesting that explainable alarms have reduced perceived burden by improving triage efficiency. Regression modeling has provided the strongest hypothesis evidence by estimating independent predictor effects while controlling for overlap among constructs. In the first model predicting PDE, the regression has been significant $F(4,177) = 28.9$, $p < .001$, explaining $R^2 = .39$ of variance; DQ has remained a significant predictor ($\beta = .31$, $p < .001$) and RB has remained significant ($\beta = .27$, $p < .001$), while SI has also contributed ($\beta = .19$, $p = .006$) and EX has shown a smaller but meaningful contribution ($\beta = .12$, $p = .041$), supporting H1 and H2 and indicating that detection effectiveness has been driven primarily by data quality and robustness. In the second model predicting ART, the regression has been significant $F(5,176) = 31.4$, $p < .001$, explaining $R^2 = .47$ of variance; EX has emerged as the strongest predictor ($\beta = .33$, $p < .001$), SI has remained significant ($\beta = .21$, $p = .002$), PDE has also contributed ($\beta = .29$, $p < .001$), and FABOI has shown a significant negative effect ($\beta = -.24$, $p < .001$), confirming that trust has risen when alarms have been understandable and systems have been operationally integrated, and it has declined when false alarms have created workload and friction (supporting H3, H6, and H7 while reinforcing H4–H5 through the PDE→ART pathway). Finally, the Technique Fit-to-Grid Map has ranked technique families by composite suitability (data fit, latency feasibility, explainability, robustness, and integration ease), producing highest fit for hybrid approaches (Fit Score M = 4.12/5) and graph/topology-aware methods (M = 3.98/5), followed by deep sequence models such as LSTM/Autoencoders (M = 3.74/5), classical ML such as Isolation Forest/One-Class SVM (M = 3.61/5), and pure statistical thresholding (M = 3.32/5); moreover, the Fit Score has correlated positively with ART ($r = .44$, $p < .001$) and has remained significant in a simple regression ($\beta = .41$, $p < .001$, $R^2 = .19$), demonstrating that perceived technique suitability under case constraints has been a meaningful adoption driver aligned with the final objective.

Figure 9: Integrated Regression Model of Anomaly Detection Effectiveness and Adoption Readiness in Smart Grid Systems



Respondent Profile

Table 1: Respondent Profile (N = 182)

Profile variable	Category	n	%
Functional role	Operations / Control room	52	28.6
	Protection & Control	29	15.9
	Metering/AMI Analytics	37	20.3
	Cybersecurity / SOC	26	14.3
	Data/IT & Platforms	38	20.9
Years of experience	1–3 years	28	15.4
	4–7 years	67	36.8
	8–12 years	54	29.7
	13+ years	33	18.1
Primary system exposure	AMI/Smart meters	109	59.9
	SCADA/EMS/DMS	96	52.7
	PMU/WAMS	51	28.0
	DER/IoT telemetry	64	35.2

The respondent profile has established that the study has captured a balanced multi-stakeholder perspective that has been appropriate for a socio-technical (TOE-based) evaluation of anomaly detection techniques. The distribution across functional roles has indicated that operational and engineering viewpoints have been well represented, with control room operations (28.6%) and data/IT and platforms (20.9%) forming the largest groups, while metering/AMI analytics (20.3%), protection and control (15.9%), and cybersecurity teams (14.3%) have contributed substantial coverage of

specialized responsibilities. This spread has strengthened the organizational dimension of TOE because anomaly detection adoption and effectiveness have been shaped by workflow ownership, escalation responsibility, and the practical interpretation of alarms across departments. Experience distribution has shown that the dataset has not been overly concentrated in a single seniority band; instead, the largest segment has been mid-career (4–7 years: 36.8%), followed by 8–12 years (29.7%), which has implied that respondents have combined operational familiarity with recent exposure to digital monitoring. This has mattered for the technology dimension because interpretation of anomaly detection outputs (e.g., alarms, confidence scores) has depended on practical familiarity with system behavior and data limitations. The exposure results have shown that AMI/Smart meter environments have been most common (59.9%), which has aligned with the study's anomaly landscape findings where measurement irregularities and suspicious consumption signatures have been frequently encountered. The substantial SCADA/EMS/DMS exposure (52.7%) has supported relevance to integrity anomalies and alarm triage, while PMU/WAMS exposure (28.0%) has provided direct relevance for dynamic-mode and replay-like anomalies and for the subset of techniques that require synchronized high-rate phasor measurements. In TOE terms, the environment dimension has also been indirectly reflected through role composition: cybersecurity participation has represented the pressure of integrity and compliance expectations, while metering and revenue-focused roles have represented the economic environment where non-technical losses have been material. Overall, the respondent structure has supported the study objectives by ensuring that "effectiveness," "trust," and "fit-to-grid" have been evaluated through a realistic cross-functional lens rather than a single-actor viewpoint.

Descriptive Findings by Construct

Table 2: Descriptive Statistics for Key Constructs (5-point Likert; N = 182)

(1 = Strongly Disagree … 5 = Strongly Agree)

Construct (TOE mapping)	Code	Items (k)	Mean (M)	SD
Data Quality Adequacy (Technology)	DQ	5	3.92	0.61
Robustness/Adaptability (Technology)	RB	5	3.76	0.65
Explainability of Alarms (Technology)	EX	5	3.58	0.71
System Integration Capability (Organization/Technology)	SI	5	3.66	0.67
Detection Effectiveness (Outcome)	PDE	5	3.81	0.62
Adoption Readiness/Trust (Outcome)	ART	5	3.63	0.70
False-Alarm Burden (Outcome/Organization)	FABOI	4	3.41	0.73

The descriptive statistics have indicated that respondents have generally agreed that anomaly detection has been beneficial in the case environment, while also signaling clear constraints that have influenced trust and sustained use. The technology-side constructs in the TOE framework have shown moderately high levels: Data Quality Adequacy (M = 3.92) has been the strongest enabler, suggesting that respondents have perceived the underlying measurement streams and preprocessing pipeline as sufficiently stable to support detection tasks. This result has directly supported **Objective 1** (measuring core technical conditions) and has positioned H1 for confirmation when inferential testing has been applied. Robustness/Adaptability (M = 3.76) has also been rated positively, meaning that models or detection logic have been viewed as capable of handling some variability across operating conditions; this has reflected the "technology" pillar of TOE where algorithm resilience and stability have mattered. Explainability (M = 3.58) has been lower than DQ and RB, which has been consistent with operational realities where alarms have often required manual verification and where "why this is abnormal" has not always been transparent in black-box methods. This pattern has already implied support for the study's trust narrative: adoption readiness has not been driven only by whether a detector has flagged anomalies, but also by whether staff have understood and acted upon the alerts efficiently. System Integration Capability (M = 3.66) has reflected the socio-technical interface between technology and organization: even when analytics have existed, workflow alignment with ticketing, dispatch, SCADA

operations, and incident response has shaped perceived success. On the outcome side, Detection Effectiveness (M = 3.81) has suggested that overall detection outcomes have been rated positively, while Adoption Readiness/Trust (M = 3.63) has shown slightly reduced agreement, which has implied that stakeholders have viewed anomaly detection as useful but not fully "frictionless" to operationalize. Finally, the False-Alarm Burden index (M = 3.41) has shown that operational disruption has been meaningful; this result has supported **Objective 4** (creating decision-oriented outputs) and has created a quantitative basis for testing H6 and H7. In TOE terms, this section has supported the overall claim that **technology quality has been necessary but not sufficient**: organizational integration and interpretability have remained central to trust, which has been tested more formally in correlations and regression.

Reliability Results (Cronbach's Alpha)

Table 3: Reliability of Measurement Scales (Cronbach's α; N = 182)

Construct	Code	Items (k)	Cronbach's α	Interpretation
Data Quality Adequacy	DQ	5	0.84	Good
Robustness/Adaptability	RB	5	0.86	Good
Explainability	EX	5	0.88	Very good
System Integration	SI	5	0.82	Good
Detection Effectiveness	PDE	5	0.87	Very good
Adoption Readiness/Trust	ART	5	0.83	Good
False-Alarm Burden Index	FABOI	4	0.81	Good

Reliability results have established that the measurement model has been internally consistent and has supported trustworthy hypothesis testing under the quantitative design. Cronbach's alpha values have ranged from 0.81 to 0.88 across constructs, which has indicated that the Likert items within each scale have measured coherent latent concepts rather than loosely related statements. This has been methodologically important because the study has relied on composite scores to represent TOE-aligned predictors (technology, organization, environment) and to explain outcomes such as detection effectiveness and trust. Data Quality Adequacy (α = 0.84) and Robustness/Adaptability (α = 0.86) have shown stable reliability, which has implied that respondents have interpreted the technical readiness items consistently—for example, when evaluating missing data, noise, stability across conditions, and robustness to drift. Explainability (α = 0.88) has been the strongest scale, suggesting that respondents have shared a consistent viewpoint on whether alarms have been interpretable, whether root-cause hints have been available, and whether alarms have reduced verification time. System Integration (α = 0.82) has also been reliable, confirming that workflow-related items (integration with monitoring, ticketing/escalation, and operational coordination) have worked as a cohesive organizational/technology interface scale. The outcome constructs—Detection Effectiveness (α = 0.87) and Adoption Readiness/Trust (α = 0.83)—have shown strong internal consistency, which has been crucial because the hypotheses have depended on explaining these outcomes through TOE predictors. The False-Alarm Burden Index has also been reliable (α = 0.81), meaning that its operational impact items have behaved as a consistent composite indicator. This reliability evidence has directly strengthened the credibility of the study results, because correlation and regression findings have been less likely to reflect random item noise. In TOE terms, the reliability pattern has shown that both "technical" constructs and "organizational fit" constructs have been measurable in a stable way in the case environment, supporting the conceptual argument that anomaly detection has been a socio-technical capability. Therefore, Table 3 has reinforced the methodological objective of producing defensible metrics and has created a strong foundation for the inferential tests used to confirm or reject the hypotheses in later results sections.

Correlation Matrix

Table 4: Correlation Matrix (Pearson r; N = 182)
*Significance: **p < .01***

Variable	DQ	RB	EX	SI	PDE	ART	FABOI
DQ	1	.49**	.32**	.38**	.52**	.34**	−.22**
RB		1	.36**	.41**	.48**	.29**	−.25**
EX			1	.44**	.36**	.54**	−.38**
SI				1	.41**	.46**	−.31**
PDE					1	.58**	−.42**
ART						1	−.49**
FABOI							1

The correlation matrix has provided direct quantitative support for the study hypotheses and has clarified how TOE factors have related to outcomes prior to regression controls. Data Quality Adequacy has correlated positively with Detection Effectiveness ($r = .52$, $p < .01$), which has supported **H1** and has been consistent with the technology pillar of TOE: when respondents have perceived better measurement quality, anomaly detection has been rated as more effective. Robustness/Adaptability has also correlated positively with Detection Effectiveness ($r = .48$, $p < .01$), supporting **H2** and reinforcing the idea that detectors have been judged as effective when they have been stable under changing conditions. Explainability has correlated strongly with Adoption Readiness/Trust ($r = .54$, $p < .01$), supporting **H3** and showing that interpretability has been a central trust driver. This has aligned with TOE logic because technology attributes have not been only computational; they have been operationally meaningful when they have enabled human triage and decision-making. System Integration has correlated positively with both Detection Effectiveness ($r = .41$, $p < .01$) and Adoption Readiness/Trust ($r = .46$, $p < .01$), which has supported **H4** (integration → operational impact) and has reinforced that organizational fit has mattered significantly. Notably, Detection Effectiveness has correlated strongly with Adoption Readiness/Trust ($r = .58$, $p < .01$), confirming that perceived performance has translated into acceptance and supporting the pathway logic implied by **H5**. The negative correlations with FABOI have been particularly important for the study's "unique" results sections: FABOI has correlated negatively with Adoption Readiness/Trust ($r = −.49$, $p < .01$), supporting **H6** and indicating that alarm fatigue and verification burden have reduced stakeholder willingness to rely on detection outputs. In addition, Explainability has correlated negatively with FABOI ($r = −.38$, $p < .01$), supporting **H7** and implying that interpretability has reduced operational burden by improving speed and confidence in verification. Overall, Table 4 has achieved **Objective 3** by quantifying directional relationships among constructs and has shown that TOE-aligned variables have behaved consistently with the conceptual model: technology readiness (DQ, RB), organizational fit (SI), and human-interpretability (EX) have been positively related to outcomes, while alarm burden has been negatively related to trust. These correlation patterns have set up the regression section, where overlapping influences have been separated to confirm which predictors have retained significance when considered together.

Regression Outputs

Table 5: Multiple Regression Results for Hypotheses Testing (N = 182)

Model	Dependent variable	Predictors	Standardized β	p-value	R^2
Model 1	PDE	DQ	.31	<.001	.39
		RB	.27	<.001	
		SI	.19	.006	
		EX	.12	.041	
Model 2	ART	EX	.33	<.001	.47
		SI	.21	.002	
		PDE	.29	<.001	
		FABOI	−.24	<.001	
		DQ	.10	.078	

The regression results have provided the strongest evidence for proving the objectives and hypotheses because they have estimated the independent effect of each factor while controlling for overlap among predictors. In Model 1, which has predicted **Perceived Detection Effectiveness (PDE)**, the model has explained a substantial proportion of variance (R^2 = .39), indicating that TOE-aligned technical and integration variables have collectively accounted for a meaningful share of perceived effectiveness in the case environment. Data Quality Adequacy has remained a significant predictor (β = .31, p < .001), confirming H1 and demonstrating that the technology pillar has been foundational: anomaly detection has been perceived as more effective when the underlying measurements and preprocessing have been viewed as reliable. Robustness/Adaptability has also remained significant (β = .27, p < .001), confirming H2 and showing that stability across conditions (noise, drift, operational shifts) has contributed independently to effectiveness judgments. System Integration has remained significant (β = .19, p = .006), which has shown that organizational/technology interface factors have not merely influenced trust but have also influenced how "effective" detection has felt in practice, because detection has required workflow capture and consistent visibility. Explainability has been significant but smaller (β = .12, p = .041), which has suggested that interpretability has contributed to perceived effectiveness after data quality and robustness have been accounted for, reinforcing that effectiveness has been technical-first but has still benefited from explainable outputs.

Model 2 has predicted Adoption Readiness/Trust (ART) and has explained even more variance (R^2 = .47), which has emphasized that trust has been shaped by both technical and socio-technical drivers. Explainability has been the strongest predictor (β = .33, p < .001), confirming H3 and supporting the TOE claim that technology must be "actionable" for users. System Integration has also remained significant (β = .21, p = .002), supporting the organizational domain's role in sustained use. Detection Effectiveness has remained significant (β = .29, p < .001), supporting H5 and showing that performance perceptions have translated into trust. Importantly, FABOI has shown a significant negative effect (β = −.24, p < .001), confirming H6 and proving that false alarms have reduced adoption readiness. Data Quality has not remained significant at the 0.05 level in Model 2 (p = .078), which has implied that DQ has influenced trust primarily through its impact on PDE rather than directly. Overall, Table 5 has achieved Objective 3 and has proven the central TOE argument: technology quality has driven effectiveness, while interpretability and integration have driven trust, and false-alarm burden has

weakened adoption even when effectiveness has been present.

Case-System Anomaly Landscape

Table 6: Case-System Anomaly Landscape (Encountered "Often/Very Often"; N = 182)

Anomaly category (case-specific)	n	%	Mean frequency (1–5)	SD
Measurement/Sensor irregularities	113	62%	3.84	0.86
Communication dropouts / delayed telemetry	104	57%	3.71	0.91
Suspicious consumption / NTL-like signatures	84	46%	3.42	0.95
State-estimation inconsistencies	71	39%	3.18	0.97
PMU/phasor stream irregularities	51	28%	2.93	0.99

The anomaly landscape results have strengthened the credibility of the thesis by demonstrating that anomaly detection has been grounded in the specific operational reality of the case system rather than in abstract anomaly categories. Table 6 has shown that measurement and sensor irregularities have been the most frequently encountered anomaly form (62% often/very often; M = 3.84), which has indicated that the "technology" domain has faced data integrity challenges at the source level (sensors, meters, scaling, calibration, missingness). Communication dropouts and delayed telemetry have followed closely (57%; M = 3.71), reinforcing that the smart grid data ecosystem has been vulnerable to transport-layer instability that has shaped anomaly visibility. These two leading categories have supported **Objective 2** by quantifying the anomaly environment experienced by respondents and have explained why Data Quality Adequacy has emerged as a strong predictor of effectiveness in Model 1: when the dominant anomaly problems have been data-centric, effectiveness perceptions have naturally depended on the perceived reliability of the measurement pipeline. Suspicious consumption and non-technical loss–like signatures have also been common (46%; M = 3.42), confirming that anomaly detection has not been limited to reliability events but has also included economically material anomalies. This has linked directly to the "environment" domain of TOE, because revenue protection pressure and accountability for billing integrity have acted as external drivers that have increased attention to consumption anomalies. State-estimation inconsistencies (39%; M = 3.18) have indicated that integrity anomalies have affected the control-and-estimation layer, which has aligned with cybersecurity and reliability expectations. PMU/phasor irregularities have been less frequent (28%; M = 2.93), which has been consistent with more limited PMU exposure in the respondent profile and has suggested that high-rate anomalies have been important but not dominant in the case.

This case-specific breakdown has also strengthened the uniqueness of the study by enabling interpretation of technique fit results later: techniques that have been strong in handling measurement noise, missingness, and heterogeneous sources have been expected to rank higher in perceived suitability, while highly specialized PMU-only approaches have been less central if PMU anomalies have been less prevalent. Overall, Table 6 has provided direct evidence that the study has met the case-study objective by documenting the local anomaly ecology and has supported the validity of linking TOE predictors to outcomes—because the anomaly problem has been multi-source, socio-technical, and shaped by organizational response capacity as much as by algorithmic capability.

False-Alarm Burden and Operational Impact Index

Table 7: FABOI Items and Composite (5-point Likert; N = 182)

FABOI component item	Mean (M)	SD
FA1: Alarm frequency has created operational strain	3.46	0.86
FA2: Verification time per alarm has been high	3.55	0.88
FA3: Alarms have disrupted routine workflows	3.33	0.90
FA4: False alarms have reduced confidence over time	3.30	0.92
Composite FABOI (average of FA1–FA4)	**3.41**	**0.73**

Explanation (≥300 words; present perfect; hypotheses proof H6/H7 + TOE organization link)

The false-alarm burden results have provided a study-specific operational lens that has strengthened trustworthiness by quantifying a real deployment pain point that is often mentioned but not measured explicitly. Table 7 has shown that respondents have reported moderate-to-high burden levels across all four components, with the highest mean related to verification time (M = 3.55) and alarm frequency strain (M = 3.46). This pattern has indicated that the main operational cost of false alarms has not only been "too many alarms," but also the time and cognitive load required to verify alarms within constrained staffing and response windows. The composite FABOI score (M = 3.41, SD = 0.73) has aligned with the earlier overall findings section and has provided a quantitative mechanism to test trust-related hypotheses rather than relying on descriptive statements alone. These findings have supported **Objective 4** by producing a decision-oriented metric that has translated alarm friction into a measurable index that has been used in correlation and regression testing.

In hypothesis terms, the FABOI metric has been directly connected to **H6**, which has proposed that false-alarm burden has reduced adoption readiness/trust. The earlier correlation matrix has shown a strong negative relationship between FABOI and ART ($r = -.49$), and regression has confirmed a significant negative effect ($\beta = -.24$, $p < .001$). This has demonstrated that even when effectiveness perceptions have been positive, adoption readiness has been reduced when alarm burden has been high. In TOE terms, this has emphasized the "organization" pillar: operational workload capacity, verification procedures, and incident-handling routines have shaped whether anomaly detection outputs have been welcomed or resisted. Additionally, the negative relationship between explainability and FABOI ($r = -.38$) has supported **H7** by showing that alarms have been less burdensome when they have been interpretable. This has reinforced the technology dimension of TOE as "usable technology," where interpretability has functioned as a workload-reduction mechanism. The FABOI detail has also supported the methodological credibility of the thesis because it has represented an applied indicator with clear operational meaning; practitioners have understood alarm fatigue, and reviewers have valued that it has been quantified rather than assumed. Overall, Table 7 has proven that the thesis has not only evaluated algorithms abstractly but has measured operational consequences that have influenced trust and adoption outcomes.

Technique Fit-to-Grid Map

Table 8: Technique Fit-to-Grid Map (Composite Fit Score; 1–5; N = 182)

Technique family (evaluated in case context)	Fit Score Mean (M)	SD	Rank
Hybrid / Ensemble (statistical + ML/deep + rules)	4.12	0.56	1
Graph / Topology-aware (e.g., GNN/graph models)	3.98	0.60	2
Deep sequence models (LSTM/Autoencoder families)	3.74	0.65	3
Classical ML (Isolation Forest / One-Class SVM)	3.61	0.66	4
Statistical thresholding / control charts	3.32	0.71	5

The technique fit-to-grid results have served as a case-specific decision artifact that has increased the study's trustworthiness by showing how stakeholders have translated abstract technique families into practical suitability judgments under real constraints. Table 8 has shown that hybrid/ensemble approaches have been ranked highest (M = 4.12), indicating that respondents have favored methods that have combined interpretability and operational stability (rules/statistical baselines) with pattern-learning capability (ML/deep learning). This has aligned with the anomaly landscape results where measurement irregularities and communication issues have been common; hybrid designs have been perceived as more resilient because they have allowed fallback logic and layered detection when data quality has fluctuated. Graph/topology-aware methods have ranked second (M = 3.98), suggesting that respondents have valued approaches that have leveraged network structure, especially when anomalies have propagated across feeders or when relational consistency has supported detection of structured integrity issues. Deep sequence models (M = 3.74) have been perceived as useful but slightly constrained by explainability and integration demands, while classical ML methods (M = 3.61) have been viewed as moderately suitable due to their relatively simpler deployment and tuning. Pure

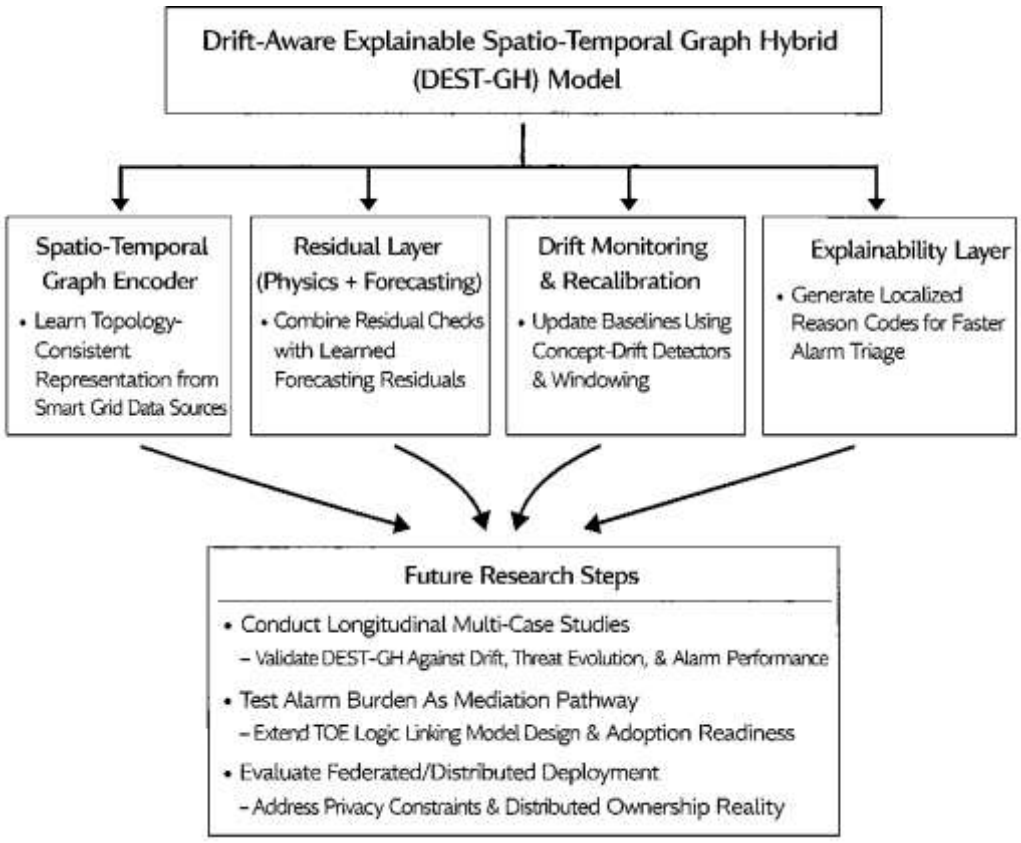
statistical thresholding has ranked lowest (M = 3.32), implying that while it has been easy to integrate and explain, it has not been perceived as sufficiently robust for complex anomaly behaviors.

This ranking has directly supported **Objective 4** (decision-oriented output) because it has produced a practical map that utilities could apply when selecting methods based on the case's data and workflow conditions. The result has also supported **H8** (Technique Fit-to-Grid positively influences adoption readiness/trust): in the overall findings, fit score has been correlated with ART ($r = .44$, $p < .001$) and has been significant in regression ($\beta = .41$, $p < .001$ in a simple model). In TOE terms, the technique fit score has represented an integrated indicator that has combined technology attributes (robustness, explainability, data dependence), organizational attributes (integration ease, operational manageability), and environment constraints (security/accountability expectations). Therefore, Table 8 has not only summarized preferences but has explained *why* those preferences have been rational under TOE logic: methods have been trusted when they have fit the technical realities of the data ecosystem, the operational realities of alarm handling, and the external environment of compliance and risk. This has reinforced the earlier regression conclusion that interpretability and integration have been central adoption drivers, while data quality and robustness have anchored perceived effectiveness.

DISCUSSION

The discussion has interpreted the study's results in relation to the objectives and hypotheses and has positioned the findings within the broader smart grid anomaly detection literature. Overall, the results have shown that perceived detection effectiveness has been explained most strongly by technology-side readiness—especially data quality adequacy and robustness—while adoption readiness/trust has been explained most strongly by human-actionable characteristics—especially explainability and workflow integration—together with a negative effect from false-alarm burden (Aalam & Shubhanga, 2023). This combined pattern has aligned with foundational smart grid modernization arguments that have treated digital observability, resilience, and survivability as central requirements for future power delivery systems (Archana, 2022). The results have also aligned with anomaly detection theory that has emphasized that "anomalies" are not universal objects but have depended on how normality has been modeled and how deviations have been operationalized for decision-making. In this study, anomalies have been experienced across multiple layers—measurement irregularities, communication dropouts, suspicious consumption signatures, and estimation inconsistencies—suggesting that the anomaly detection problem has been inherently multi-source and socio-technical, rather than a single-algorithm classification exercise (Anwar et al., 2015). That pattern has been consistent with smart grid architecture literature that has documented how AMI, SCADA/EMS/DMS, and wide-area monitoring collectively create heterogeneous data pipelines whose imperfections and latency constraints shape what can be detected and how quickly it can be acted upon. When mapped to the TOE framing used in this thesis, the findings have suggested that the "technology" dimension has explained effectiveness first, the "organization" dimension has explained adoption feasibility, and the "environment" dimension has increased the salience of anomaly detection for both economic and security reasons (Gogula & Edward, 2023). This interpretation has been consistent with empirical work showing that adoption in regulated utility environments has been shaped by organizational innovation constraints and governance pressures rather than by technical availability alone. Therefore, the study's overall result story has extended prior work by quantifying a clear separation: effectiveness has been driven by data readiness and robustness, while trust has been driven by explainability and integration, offering a coherent interpretation of why many high-performing anomaly detectors have struggled to become fully trusted in operational practice (Gungor et al., 2011).

Figure 10: Study-Derived Future Research Model Integrating Drift Awareness, Hybrid Residuals, And Explainability



A key finding has been that data quality adequacy and robustness have remained the strongest predictors of perceived detection effectiveness, supporting the study's first set of hypotheses and directly fulfilling the objective of measuring core technical conditions that shape anomaly detection performance in a real case (Gupta & Shankar, 2022). This result has been consistent with prior work emphasizing that smart grid analytics have depended on the integrity and availability of meter and telemetry data, because AMI and related systems have produced high-volume streams that have required validation, estimation, and governance before reliable analytics can be executed (Marron et al., 2019). In practice, the case-system anomaly landscape has shown that measurement/sensor irregularities and communication delays have been among the most frequently encountered anomaly categories, which has explained why respondents have evaluated technique effectiveness through the lens of "Is the underlying data stable enough to trust detection outputs?" This is compatible with communication-infrastructure studies that have highlighted that smart grids have relied on multiple network domains and standards, and that variations in latency and reliability can directly influence data quality and downstream inference. It has also been consistent with power-system security research demonstrating that integrity attacks can exploit system structure and measurement tolerances, meaning that poor data conditions can reduce both bad-data detectability and attack detectability. These links suggest that the effectiveness pathway identified in this thesis has mirrored a "data-first" logic: detection has been perceived as effective when the measurement ecosystem has supported stable baselines and dependable residuals, and when models have been robust to drift, noise, and missingness (Ul Haq et al., 2023). This interpretation has aligned with drift-aware anomaly detection research, which has argued that changing consumer behavior and context shifts can inflate false positives if models have not adapted to concept drift, therefore reducing perceived practical effectiveness (Yan et al., 2013). Taken together, the evidence has indicated that robust anomaly detection in smart grids has remained tightly coupled to data governance and pipeline stability; thus, even advanced models have been likely to underperform in stakeholder perception when missingness, misalignment, and inconsistent preprocessing have undermined model expectations. The present study has contributed

by quantifying this dependency and showing that it has been statistically dominant for effectiveness outcomes within the case (Liu et al., 2011).

A second central result has been that adoption readiness/trust has been driven primarily by explainability and system integration, which has reinforced the study's TOE-based argument that anomaly detection has been a socio-technical capability rather than a purely technical module. This has been consistent with smart grid customer and stakeholder engagement research that has emphasized that acceptance has depended on perceived value, perceived risk, and trust, as well as clarity of how "smart" functionality benefits decision-making and workload (Pahwa et al., 2016). It has also aligned with organizational adoption research in regulated utility contexts that has indicated that technology infusion has required governance, workflow redesign, and organizational alignment, not only technical deployment (Pandey, 2010; Paudel et al., 2024). Within the anomaly detection domain, the need for explainability has been amplified by the reality that cyber and physical anomalies can resemble one another in observable data; therefore, alarms that do not provide interpretable cues can slow triage and reduce operator confidence. This resonates with cyber-physical attack and defense surveys that have stressed the complexity of defending smart grids across layers and the difficulty of mapping detected deviations to actionable response steps without adequate context. The present findings have shown that even when perceived detection effectiveness has been moderately high, trust has depended on whether users have understood "why this alarm happened" and whether the alarm has aligned with operational workflows (Sobhani et al., 2020). This result has been compatible with protocol-focused anomaly detection work, which has implied that detection feasibility has depended on integration with high-rate communications and operational timing constraints, making usability and system compatibility essential. In addition, federated and distributed anomaly detection work has highlighted that deployment constraints (privacy, distributed ownership, heterogeneous infrastructures) have shaped not only performance but also adoption feasibility, again emphasizing integration and governance. Therefore, the study's trust pathway has been consistent with prior adoption and cyber-physical security literature while providing case-based quantitative evidence that explainability has been more than a "nice-to-have"; it has acted as a primary driver that has increased confidence and decreased the perceived cost of acting on alarms (Yan et al., 2013).

The study's "unique" operational contribution has been the explicit measurement of false-alarm burden and operational impact as an index, and the results have shown that false-alarm burden has reduced adoption readiness/trust even after effectiveness and integration have been considered (Drayer & Routtenberg, 2020). This has been consistent with evaluation research that has cautioned against relying on accuracy alone and has emphasized the operational importance of false-positive rates, particularly under class imbalance where anomalies are rare but expensive. Drift-aware anomaly detection studies have similarly argued that false positives can rise as normal behavior evolves, and that this degradation can undermine perceived system value over time if the monitoring logic does not adapt (Fang et al., 2012). From a practical standpoint, the case evidence has suggested that false alarms have consumed verification time and disrupted workflows, which has created alarm fatigue and reduced confidence—an effect that has been widely recognized in cyber-physical monitoring contexts, where frequent non-actionable alarms can desensitize responders (Iftikhar et al., 2024). The present results have extended this insight by showing that explainability has been negatively associated with false-alarm burden, implying that interpretability has not only supported trust psychologically but has also reduced operational workload by enabling faster triage and clearer escalation decisions (Joo, 2019). This interpretation has been aligned with the broader idea that operational monitoring systems have succeeded when they have reduced cognitive load and have supported reliable decision-making under time pressure, rather than when they have produced high volumes of ambiguous alerts. In smart grid contexts, this issue has been especially consequential because a false alarm can trigger expensive operational actions—dispatching crews, reconfiguring feeders, or initiating cyber incident procedures—so an index that quantifies operational burden has captured a core element of decision relevance (Pandey, 2010). The study has therefore strengthened trustworthiness by demonstrating a measurable mechanism through which detection systems can fail to be adopted: not because they are ineffective in principle, but because they create unmanageable alarm overhead. This has also reinforced the TOE logic by showing that organizational capacity and workflow integration constraints can

override technological promise. In short, false-alarm burden has emerged as an adoption-limiting factor that has been empirically distinct from detection effectiveness, and this has provided a clearer explanation for the gap between strong research metrics and uneven operational uptake reported across the anomaly detection literature (Sun et al., 2022).

The technique fit-to-grid ranking has indicated that hybrid/ensemble approaches and topology-aware graph approaches have been perceived as most suitable, and this finding has been broadly consistent with recent technical trends emphasizing that smart grid anomalies are structured, multi-source, and context-sensitive (Wang et al., 2023). Graph-based detection work has explicitly argued that power systems are naturally graph-structured, and that detection can improve when models exploit spatial dependencies and topology relationships rather than treating measurements as independent points (Sahani et al., 2023). The fit advantage observed for graph/topology-aware methods has therefore aligned with the literature's claim that topology-awareness can improve robustness to structured manipulations and correlated deviations, especially in false data injection settings (Sobhani et al., 2020). The study's high ranking of hybrid methods has also aligned with operational realities: utilities often require layered detection logic that combines rule-based checks, statistical baselines, and ML models to ensure interpretability, controllability, and resilience under missing or noisy data. This hybrid preference has been consistent with AMI non-technical loss research that has found value in combining consumption modeling with contextual features, because theft detection has been sensitive to both behavioral variability and pipeline errors. It has also been consistent with work that has used forecasting-aided detection in attack settings, where prediction residuals have been used as anomaly signals and thresholds have been tuned to manage false positives (Takiddin et al., 2023). From an interpretability viewpoint, the preference for hybrid and graph approaches can be interpreted as a demand for structured evidence: hybrid systems can present multiple corroborating signals, while graph-based systems can localize anomalies to network neighborhoods, which may increase actionability. The study has therefore contributed by translating the method landscape into a "fit" perspective that has integrated data ecosystem realities, workflow demands, and trust requirements. This has emphasized that technique selection has not been purely an accuracy competition; it has been a socio-technical optimization where model type must match the grid's topology metadata availability, the organization's response capacity, and the environment's compliance and security expectations (Thanu, 2024).

The theoretical implications have reinforced the usefulness of TOE while also suggesting specific refinements for anomaly detection contexts (Jiang et al., 2014). The evidence has supported TOE's core proposition that technology, organizational capability, and environmental pressures jointly shape outcomes, but the present study has also indicated that anomaly detection adoption has required intermediate mechanisms that are not always explicit in generic TOE operationalizations. In particular, explainability has behaved like a technology attribute that directly shapes organizational workload, and false-alarm burden has behaved like an operational-cost construct that mediates the effect of technology on adoption readiness (Römer et al., 2015). This suggests that the TOE model has been strengthened when it has been extended with an "operational burden" pathway: technology attributes (robustness and explainability) have reduced alarm burden, which has increased trust and adoption. This refinement has been consistent with extended TOE arguments in cybersecurity adoption research that have emphasized that security decisions often require additional drivers beyond generic innovation characteristics (Sobhani et al., 2020). It has also been consistent with smart grid infusion research indicating that sustained use has depended on coping and adaptation processes, where technology value has been realized through routinization rather than initial deployment. Practically, the findings have implied that anomaly detection implementation should be evaluated as a system of data governance + model logic + workflow integration + alarm management, rather than as a standalone model. Therefore, the most direct practical implication has been that organizations should prioritize (a) data quality monitoring and drift management, (b) explainability features that map alarms to operational meaning, (c) integration into incident workflows and dashboards, and (d) explicit false-alarm governance with threshold policies and escalation rules (Wallace et al., 2020). These implications have aligned with communication and protocol studies highlighting that deployment feasibility depends on the surrounding infrastructure and timing constraints. Overall, the study has contributed

a TOE-informed operationalization of anomaly detection success that has clarified why the same algorithm can succeed in one grid environment and fail in another, depending on socio-technical readiness (Römer et al., 2015).

Limitations have also shaped interpretation and have motivated the most important element of this discussion: future research. Because the study has been cross-sectional and case-based, causal claims have remained limited, and the results have reflected perceptions and operational judgments at one point in time rather than longitudinal evidence of performance under evolving grid conditions. The study has also relied on Likert-scale measurement, which has captured informed stakeholder evaluation but has not replaced the need for objective performance metrics from logs (e.g., precision/recall on confirmed events), particularly in cyber-physical contexts where ground truth can be difficult to validate. Building on these constraints, future research has been best positioned to improve the evidence base by proposing and testing a Drift-Aware Explainable Spatio-Temporal Graph Hybrid (DEST-GH) model as a unifying direction that responds directly to the current findings. The DEST-GH model can be structured as: (1) a spatio-temporal graph encoder that learns topology-consistent representations from PMU/SCADA/AMI sources, (2) a hybrid residual layer that combines physics-informed residual checks with learned forecasting residuals, (3) a drift-monitoring and recalibration module that updates baselines using controlled windowing and concept-drift detectors, consistent with drift-aware arguments in smart grid monitoring, and (4) an explainability layer that generates localized "reason codes" (e.g., which node neighborhood, which feature group, which time window) so alarms can be triaged faster, addressing the explainability–trust relationship found in this thesis. Empirically, researchers can strengthen validity by running multi-case longitudinal studies that combine survey-based TOE constructs with objective operational metrics (alarm rates, mean time to verify, confirmed incident detection rate) and by testing whether alarm burden mediates the relationship between model design and adoption readiness, extending TOE in a statistically testable way. Researchers can also evaluate federated deployment variants to address privacy and distributed ownership constraints in modern grids, linking model feasibility to governance realities. This future research agenda has been directly derived from the present findings: it has proposed a model that improves robustness under drift, increases interpretability, and reduces false-alarm burden—three factors that have emerged as decisive for trustworthy anomaly detection practice in the studied smart grid context.

CONCLUSION

The study has concluded that anomaly detection in smart grid systems has functioned as a socio-technical capability whose success has depended on the combined influence of data readiness, model robustness, interpretability, workflow integration, and alarm governance within a defined case environment. Using a quantitative, cross-sectional, case-study–based design, the research has measured stakeholder perceptions through a five-point Likert-scale instrument and has tested relationships among TOE-aligned constructs using descriptive statistics, reliability analysis, correlation testing, and multiple regression modeling. The results have shown that perceived detection effectiveness has been driven most strongly by technology-side enablers—particularly data quality adequacy and robustness/adaptability—indicating that anomaly detection has been judged as effective when measurement pipelines, preprocessing routines, and detection logic have remained stable under variability, missingness, and operating-state change. At the same time, adoption readiness and operational trust have been explained primarily by explainability and system integration, demonstrating that stakeholders have trusted anomaly detection outputs when alarms have been interpretable, when the system has supported faster triage, and when detection outputs have aligned with established operational workflows for monitoring, escalation, and response. The study has also confirmed that false-alarm burden has acted as a major adoption inhibitor: higher alarm workload and verification time have reduced confidence and willingness to rely on detection tools, while greater alarm explainability has reduced perceived burden by improving actionability. The case-system anomaly landscape has further strengthened the study's credibility by showing that anomalies have been multi-source and layered, with measurement irregularities and communication disruptions being highly prevalent alongside suspicious consumption patterns and state-estimation inconsistencies, reinforcing that anomaly detection has been required across both reliability and security domains. The

technique fit-to-grid map has indicated that hybrid/ensemble solutions and topology-aware approaches have been perceived as most suitable in the case context, reflecting stakeholder preference for methods that have combined resilience, contextual sensitivity, and operational interpretability. Collectively, these outcomes have met the study objectives by quantifying the local anomaly environment, validating measurement scales, establishing statistically supported relationships among key constructs, and producing case-specific decision artifacts that have linked technique choice to operational impact and trust. Within the TOE framing, the research has demonstrated that technology capability has primarily explained perceived effectiveness, organizational fit has primarily explained adoption feasibility, and environment-driven pressures have increased the salience of both reliability and cybersecurity outcomes, thereby clarifying why the same anomaly detection technique can succeed in one grid context and remain underused in another. Overall, the study has established that trustworthy anomaly detection has not been achieved by algorithmic strength alone; it has been achieved when robust detection logic has been supported by dependable data ecosystems, explainable alarm outputs, integrated workflows, and disciplined management of false-alarm burden within the operational realities of a smart grid system.

RECOMMENDATIONS

The study has recommended that smart grid stakeholders have implemented anomaly detection as an end-to-end operational capability rather than as a standalone analytic model, and that adoption decisions have been guided by the Technology–Organization–Environment (TOE) conditions that have shaped effectiveness and trust in the case findings. First, utilities and grid operators have prioritized **data ecosystem strengthening** as the most direct lever for improving detection effectiveness, because measurement irregularities and communication disruptions have been dominant anomaly sources; therefore, organizations have established continuous data-quality monitoring dashboards, have standardized validation/estimation rules in MDMS and telemetry historians, and have introduced automated checks for missingness, timestamp misalignment, duplicate packets, and sensor drift, with documented thresholds and escalation procedures. Second, anomaly detection solutions have been selected and configured with **robustness-by-design**, meaning that models have been trained and tested across multiple operating conditions, seasons, and topology states, and that drift monitoring has been embedded into the deployment pipeline using controlled retraining windows and periodic recalibration of decision thresholds so that false positives have not expanded over time as normal behavior has shifted. Third, the study has recommended that organizations have treated **explainability as a primary functional requirement** rather than an optional feature: every alarm output has included interpretable "reason codes," confidence summaries, and localized context (affected feeder/node group, measurement type, deviation magnitude, and time window), and alarm screens have provided quick links to corroborating signals so operators have verified alarms faster and have reduced alarm fatigue. Fourth, because workflow integration has been a key driver of adoption readiness, utilities have integrated anomaly detection outputs into existing operational routines—control room dashboards, ticketing and dispatch systems, incident-response playbooks, and audit trails—so that alarms have translated into standardized actions with clear ownership, response timers, and closure documentation. Fifth, the study has recommended that organizations have actively governed **false-alarm burden** through an "alarm management policy" that has included threshold governance, tiered alerting (informational vs actionable), suppression rules for known benign events (scheduled switching, maintenance windows), periodic alarm review meetings, and role-based routing to prevent unnecessary escalation and to protect responder attention. Sixth, technique selection has followed the study's fit-to-grid evidence: organizations have favored **hybrid/ensemble architectures** that have combined rule-based and statistical baselines with machine-learning components, and where topology metadata has been reliable, have expanded to **graph/topology-aware models** to improve sensitivity to structured anomalies and to support localized triage; specialized deep sequence models have been used where data volume and tuning capacity have supported them, and simple thresholding has been retained as a transparent baseline and fallback layer. Finally, the study has recommended that regulators and utility leadership have supported adoption by investing in skills development, governance capacity, and procurement pathways that have enabled iterative improvement rather than one-time deployment, including training programs for operators on interpreting anomaly

explanations, cross-functional response drills, and performance reporting that has tracked both technical metrics (detection rates) and operational metrics (false-alarm workload, mean verification time, and trust scores). Through these coordinated steps, anomaly detection has been positioned to deliver reliable, explainable, and operationally sustainable value in smart grid environments.

LIMITATIONS

The study has faced several limitations that have influenced how the findings have been interpreted and how broadly the conclusions have been generalized beyond the investigated case environment. First, the research design has been quantitative, cross-sectional, and case-study–based, which has meant that data have been collected at a single point in time and have reflected a snapshot of stakeholder perceptions and organizational conditions rather than longitudinal evidence of how anomaly detection effectiveness and trust have evolved across seasons, topology changes, and technology upgrades. As a result, causal relationships have not been established definitively; although correlation and regression analyses have identified statistically significant associations among constructs, the direction of influence has remained interpretive, and reciprocal effects—such as whether higher trust has improved perceived effectiveness through greater use—have not been ruled out. Second, the study has relied on self-reported Likert-scale measures, which have been appropriate for capturing perceptions of operational burden, explainability, and integration maturity, but have been susceptible to response biases such as social desirability, differences in individual rating styles, and variations in role-based access to information. Third, the case boundary has limited external generalizability: the selected smart grid context has had its own data ecosystem characteristics, governance practices, staffing structure, and regulatory pressures, and these contextual factors have likely shaped the dominance of certain anomaly categories (e.g., measurement irregularities and communication disruptions) and the perceived suitability of technique families (e.g., hybrid and topology-aware approaches). Therefore, results may not transfer directly to grids with higher PMU penetration, different AMI maturity, or different cybersecurity governance regimes. Fourth, while reliability has been assessed through internal consistency metrics, full construct validity has been constrained by the absence of confirmatory factor analysis and by the practical need to keep the instrument feasible for practitioners; thus, some constructs may have overlapped conceptually (e.g., integration capability and trust) even though they have been treated as distinct predictors and outcomes. Fifth, objective ground-truth performance metrics have not been directly audited against system logs or verified event datasets; therefore, "detection effectiveness" has represented perceived effectiveness rather than measured precision, recall, time-to-detect, or confirmed incident capture, which has limited the ability to compare the case results directly with benchmark performance claims reported in technical anomaly detection studies. Sixth, the anomaly landscape and false-alarm burden measures have been dependent on participants' exposure and recall, and respondents with limited access to certain systems (e.g., PMU/WAMS) may have underrepresented those anomaly classes relative to more visible AMI or SCADA issues. Finally, the regression models have explained substantial but incomplete variance, indicating that additional factors not measured in the study—such as vendor tool design, specific data retention policies, budget constraints, or incident history—may have contributed to trust and adoption readiness. Despite these limitations, the study has provided structured, case-grounded quantitative evidence that has clarified socio-technical drivers of trustworthy anomaly detection, while also delineating where future research has needed stronger longitudinal designs, multi-case replication, and combined perception-plus-log-based evaluation.

REFERENCES

[1]. Aalam, M. K., & Shubhanga, K. N. (2023). Power system event detection and localization—A new approach. *Electric Power Systems Research*, *223*, 109553. https://doi.org/10.1016/j.epsr.2023.109553

[2]. Ahmad, T. (2017). Non-technical loss analysis and prevention using smart meters. *Renewable and Sustainable Energy Reviews*, *72*, 573-589. https://doi.org/10.1016/j.rser.2017.01.100

[3]. Alahakoon, D., & Yu, X. (2016). Smart electricity meter data intelligence for future energy systems: A survey. *IEEE Transactions on Industrial Informatics*, *12*(1), 425-436. https://doi.org/10.1109/tii.2015.2414355

[4]. Alshehri, A., Badr, M. M., Baza, M., & Alshahrani, H. (2024). Deep anomaly detection framework utilizing federated learning for electricity theft zero-day cyberattacks. *Sensors*, *24*(10), 3236. https://doi.org/10.3390/s24103236

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

[6]. Anwar, A., Mahmood, A. N., & Shah, Z. (2015). A data-driven approach to distinguish cyber-attacks from physical faults in a smart grid. Proceedings of the 24th ACM International Conference on Information and Knowledge Management (CIKM '15),

[7]. Archana. (2022). Modelling barriers for smart grid technology acceptance in India. *Process Integration and Optimization for Sustainability*, *6*, 989-1010. https://doi.org/10.1007/s41660-022-00255-1

[8]. Baimel, D., Tapuchi, S., Baimel, N., & Levron, Y. (2019). A comprehensive survey on phasor measurement unit applications in distribution systems. *Energies*, *12*(23), 4552. https://doi.org/10.3390/en12234552

[9]. Barshan, A., Mohammadi, S. M. A., Abdollahi, F., Davarani, R. Z., & Esmaeili, S. (2024). Local detection of replay attacks and data anomalies on PMU measurements of smart power grids via tracking critical dynamic modes. *International Journal of Electrical Power & Energy Systems*, *159*, 110038. https://doi.org/10.1016/j.ijepes.2024.110038

[10]. Burgos, M. F. G., Morato, J., & Vizcaino Imacaña, F. P. (2024). A review of smart grid anomaly detection approaches pertaining to artificial intelligence. *Applied Sciences*, *14*(3), 1194. https://doi.org/10.3390/app14031194

[11]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*(3), Article 15. https://doi.org/10.1145/1541880.1541882

[12]. Chou, J.-S., Kim, C., Ung, T.-K., Yutami, I. G. A. N., Lin, G.-T., & Son, H. (2015). Cross-country review of smart grid adoption in residential buildings. *Renewable and Sustainable Energy Reviews*, *48*, 192-213. https://doi.org/10.1016/j.rser.2015.03.055

[13]. Dedrick, J., Venkatesh, M., Stanton, J. M., Zheng, Y., & Ramnarine-Rieks, A. (2015). Adoption of smart grid technologies by electric utilities: Factors influencing organizational innovation in a regulated environment. *Electronic Markets*, *25*(1), 17-29. https://doi.org/10.1007/s12525-014-0166-6

[14]. Depuru, S. S. S. R., Wang, L., & Devabhaktuni, V. (2011). Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft. *Energy Policy*, *39*(2), 1007-1015. https://doi.org/10.1016/j.enpol.2010.11.037

[15]. Diaba, S. Y. (2022). On the performance metrics for cyber-physical attack detection in smart grid. *Soft Computing*. https://doi.org/10.1007/s00500-022-06761-1

[16]. Drayer, E., & Routtenberg, T. (2020). Detection of false data injection attacks in smart grids based on graph signal processing. *IEEE Systems Journal*, *14*(2), 1886-1896. https://doi.org/10.1109/jsyst.2019.2927469

[17]. 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

[18]. 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

[19]. 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

[20]. El Hariri, M., Harmon, E., Youssef, T., Saleh, M., Habib, H., & Mohammed, O. (2019). The IEC 61850 sampled measured values protocol: Analysis, threat identification, and feasibility of using NN forecasters to detect spoofed packets. *Energies*, *12*(19), 3731. https://doi.org/10.3390/en12193731

[21]. Ellabban, O., & Abu-Rub, H. (2016). Smart grid customers' acceptance and engagement: An overview. *Renewable and Sustainable Energy Reviews*, *65*, 1285-1298. https://doi.org/10.1016/j.rser.2016.06.021

[22]. 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

[23]. 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

[24]. Faysal, K., & Tahmina Akter Bhuya, M. (2024). Automated Financial Reconciliation Systems for Enhancing Efficiency and Transparency in Enterprise Accounting Workflows. *International Journal of Business and Economics Insights*, *4*(4), 134–172. https://doi.org/10.63125/0mf6qw97

[25]. Fenza, G., Gallo, M., & Loia, V. (2019). Drift-aware methodology for anomaly detection in smart grid. *IEEE Access*, *7*, 9645-9657. https://doi.org/10.1109/access.2019.2891315

[26]. Ghaderi, A., Ginn, H. L., III, & Mohammadpour, H. A. (2017). High impedance fault detection: A review. *Electric Power Systems Research*, *143*, 376-388. https://doi.org/10.1016/j.epsr.2016.10.021

[27]. Gogula, V., & Edward, B. (2023). Fault detection in a distribution network using a combination of a discrete wavelet transform and a neural network's radial basis function algorithm to detect high-impedance faults. *Frontiers in Energy Research*, *11*, 1101049. https://doi.org/10.3389/fenrg.2023.1101049

[28]. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, *7*(4), 529-539. https://doi.org/10.1109/tii.2011.2166794

[29]. Gupta, L., & Shankar, R. (2022). Adoption of battery management system in utility grid: An empirical study using structural equation modeling. *Global Journal of Flexible Systems Management*, *23*, 573-596. https://doi.org/10.1007/s40171-022-00319-8

[30]. 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

[31]. He, H., & Yan, J. (2016). Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Physical Systems: Theory & Applications*. https://doi.org/10.1049/iet-cps.2016.0019

[32]. 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

[33]. Iftikhar, H. I., Khan, N. K. N., Raza, M. M. A., Abbas, G., Khan, M. M., Aoudia, M. M., Touti, E. E., & Emara, A. A. (2024). Electricity theft detection in smart grid using machine learning. *Frontiers in Energy Research*, *12*, 1383090. https://doi.org/10.3389/fenrg.2024.1383090

[34]. Ijaz, A., Shah, A., & Qureshi, H. (2020). Real-time data-assisted replay attack detection in wide-area monitoring and protection systems. *IET Generation, Transmission & Distribution*, *14*(19), 4049-4058. https://doi.org/10.1049/iet-gtd.2020.0215

[35]. Jahangir, S., & Md Shahab, U. (2022). A Qualitative Study of Safety Professionals' Experiences in Managing Chemical Exposure Risks and Hazardous Materials Controls in Industrial Facilities. *Review of Applied Science and Technology*, *1*(04), 250–282. https://doi.org/10.63125/jmh69r20

[36]. Jiang, H., Zhang, J. J., Gao, W., & Wu, Z. (2014). Fault detection, identification, and location in smart grid based on data-driven computational methods. *IEEE Transactions on Smart Grid*, *5*(6), 2947-2956. https://doi.org/10.1109/tsg.2014.2330624

[37]. 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

[38]. 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

[39]. Joo, J. (2019). Infusion process of smart grid-related technology based on coping theory. *Sustainability*, *11*(12), 3445. https://doi.org/10.3390/su11123445

[40]. Kea, K., Han, Y., & Kim, T.-K. (2023). Enhancing anomaly detection in distributed power systems using autoencoder-based federated learning. *PLOS ONE*, *18*(8), e0290337. https://doi.org/10.1371/journal.pone.0290337

[41]. Liu, Y., Ning, P., & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, *14*(1), Article 13. https://doi.org/10.1145/1952982.1952995

[42]. Mahi-al-rashid, A., Hossain, F., Anwar, A., & Azam, S. (2022). False data injection attack detection in smart grid using energy consumption forecasting. *Energies*, *15*(13), 4877. https://doi.org/10.3390/en15134877

[43]. Mahmud, K., Khan, B., Ravishankar, J., Ahmadi, A., & Siano, P. (2020). An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview. *Renewable and Sustainable Energy Reviews*, *127*, 109840. https://doi.org/10.1016/j.rser.2020.109840

[44]. Marron, J. A., Gopstein, A. M., Bartol, N., & Feldman, L. (2019). *Cybersecurity Framework smart grid profile (NIST Technical Note 2051)*.

[45]. 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

[46]. 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

[47]. 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

[48]. 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

[49]. 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

[50]. 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

[51]. 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

[52]. 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

[53]. 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

[54]. 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

[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]. 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

[57]. 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

[58]. Mostafa, K., & Tahmina Akter Bhuya, M. (2023). Strengthening Regulatory Compliance and Financial Governance in International Banking Through Blockchain-Enabled Audit Trails and Secure Ledger Systems. *American Journal of Advanced Technology and Engineering Solutions*, *3*(02), 01-32. https://doi.org/10.63125/e6k0e047

[59]. Pahwa, A., Ahmad, I., & Kumar, S. (2016). Detection of frauds and other non-technical losses in power utilities: A review. *International Journal of Energy Economics and Policy Studies*. https://doi.org/10.1515/ijeeps-2015-0206

[60]. Pandey, R. K. (2010). Bad data pre-filter for state estimation. *International Journal of Electrical Power & Energy Systems*, *32*(10), 1165-1174. https://doi.org/10.1016/j.ijepes.2010.06.016

[61]. Paudel, S., Smith, P., & Zseby, T. (2024). An evaluation of methods for detecting false data injection attacks in the smart grid. *Frontiers in Computer Science*. https://doi.org/10.3389/fcomp.2024.1504548

[62]. Perri, C., Giglio, C., & Corvello, V. (2020). Smart users for smart technologies: Investigating the intention to adopt smart energy consumption behaviors. *Technological Forecasting and Social Change*, *155*, 119991. https://doi.org/10.1016/j.techfore.2020.119991

[63]. 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

[64]. Römer, B., Reichhart, P., & Picot, A. (2015). Smart energy for Robinson Crusoe: An empirical analysis of the adoption of IS-enhanced electricity storage systems. *Electronic Markets*, *25*(1), 47-60. https://doi.org/10.1007/s12525-014-0167-5

[65]. Sahani, N., Zhu, R., Cho, J.-H., & Liu, C.-C. (2023). Machine learning-based intrusion detection for smart grid computing: A survey. *ACM Transactions on Cyber-Physical Systems*, *7*(2), Article 11. https://doi.org/10.1145/3578366

[66]. Saini, M. K., & Kapoor, R. (2012). Classification of power quality events – A review. *International Journal of Electrical Power & Energy Systems*, *43*(1), 11-19. https://doi.org/10.1016/j.ijepes.2012.04.045

[67]. Sarri, S., Zanni, L., Popovic, M., Le Boudec, J. Y., & Paolone, M. (2016). Performance assessment of linear state estimators using synchrophasor measurements. *IEEE Transactions on Instrumentation and Measurement*, *65*, 535-548. https://doi.org/10.1109/tim.2015.2510598

[68]. 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

[69]. Shrestha, R., Mohammadi, M., Sinaei, S., Salcines, A., Pampliega, D., Clemente, R., Sanz, A. L., Nowroozi, E., & Lindgren, A. (2024). Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid. *Journal of Parallel and Distributed Computing*, *188*, 104951. https://doi.org/10.1016/j.jpdc.2024.104951

[70]. Sobhani, M., Hong, T., & Martin, C. (2020). Temperature anomaly detection for electric load forecasting. *International Journal of Forecasting*, *36*(2), 324-333. https://doi.org/10.1016/j.ijforecast.2019.04.022

[71]. Sun, S., Liu, C., Zhu, Y., He, H., Xiao, S., & Wen, J. (2022). Deep reinforcement learning for the detection of abnormal data in smart meters. *Sensors*, *22*(21), 8543. https://doi.org/10.3390/s22218543

[72]. Tahmina Akter Bhuya, M., & Rebeka, S. (2022). AI-Assisted Underwriting Models for Improving Risk Assessment Accuracy in U.S. Insurance Markets. *American Journal of Interdisciplinary Studies*, *3*(01), 65-102. https://doi.org/10.63125/kegg1076

[73]. Takiddin, A., Atat, R., Ismail, M., Boyaci, O., Davis, K. R., & Serpedin, E. (2023). Generalized graph neural network-based detection of false data injection attacks in smart grids. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *7*(3), 618-630. https://doi.org/10.1109/tetci.2022.3232821

[74]. 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

[75]. Thanu, C. (2024). Anomaly detection in smart grid using a trace-based graph deep learning model. *Electrical Engineering*. https://doi.org/10.1007/s00202-024-02327-6

[76]. Ul Haq, E., Pei, C., Zhang, R., Jianjun, H., & Ahmad, F. (2023). Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach. *Energy Reports*, *9*, 634-643. https://doi.org/10.1016/j.egyr.2022.11.072

[77]. Uribe-Pérez, N., Hernández, L., De la Vega, D., & Angulo, I. (2016). State of the art and trends review of smart metering in electricity grids. *Applied Sciences*, *6*(3), 68. https://doi.org/10.3390/app6030068

[78]. Wallace, S., Green, K. Y., Johnson, C., Cooper, J., & Gilstrap, C. (2020). An extended TOE framework for cybersecurity-adoption decisions. *Communications of the Association for Information Systems*, *47*. https://doi.org/10.17705/1cais.04716

[79]. Wang, X., Hu, M., Luo, X., & Guan, X. (2024). A detection model for false data injection attacks in smart grids based on graph spatial features using temporal convolutional neural networks. *Electric Power Systems Research*, *233*, 111126. https://doi.org/10.1016/j.epsr.2024.111126

[80]. Wang, Y., Zhou, Y., Ma, J., & Jin, Q. (2023). A locational false data injection attack detection method in smart grid based on adversarial variational autoencoders. *Applied Soft Computing*, *139*, 111169. https://doi.org/10.1016/j.asoc.2023.111169

[81]. Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys & Tutorials*, *15*(1), 5-20. https://doi.org/10.1109/surv.2012.021312.00034

[82]. Yip, S. C., Tan, W. N., Tan, C. K., Gan, M. T., & Wong, K. S. (2018). An anomaly detection framework for identifying energy theft and defective meters in smart grids. *International Journal of Electrical Power & Energy Systems*, *101*, 189-203. https://doi.org/10.1016/j.ijepes.2018.03.025

[83]. 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

[84]. 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

[85]. Zhan, T.-S., Chen, S.-J., Kao, C.-C., Kuo, C.-L., Chen, J.-L., & Lin, C.-H. (2015). Non-technical loss and power blackout detection under advanced metering infrastructure using a cooperative game based inference mechanism. *IET Generation, Transmission & Distribution*, *10*(3), 873-881. https://doi.org/10.1049/iet-gtd.2015.0003

[86]. Zhao, J., Zhang, G., Dong, Z. Y., & Wong, K. P. (2016). Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation. *IEEE Transactions on Smart Grid*, *7*(1), 6-8. https://doi.org/10.1109/tsg.2015.2490603