Advancing Energy Infrastructure Modeling And Cyber Security: An Ai Perspective

SAKSHI SHARMA

CENTER FOR AUTOMOTIVE RESEARCH AND TRIBOLOGY

INDIAN INSTITUTE OF TECHNOLOGY DELHI

MAY 2025

Advancing Energy Infrastructure Modeling And Cyber Security: An Ai Perspective

by

SAKSHI SHARMA

CENTER FOR AUTOMOTIVE RESEARCH AND TRIBOLOGY

Submitted

In fulfillment of the requirement of the Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

MAY 2025

CERTIFICATE

This is to certify that the thesis titled **"Advancing Energy Infrastructure Modeling and Cyber Security: An AI Perspective"**, submitted by **Ms. Sakshi Sharma** in partial fulfillment of the requirements for the award of the degree of **Doctor of Philosophy**, represents original and independent research conducted by her at the Centre for Automotive Research and Tribology, Indian Institute of Technology Delhi.

Ms. Sakshi Sharma carried out the research under my guidance and supervision. To the best of my knowledge, the thesis meets the necessary academic standards and has not been submitted to any other university or institution for the award of a degree.

Date: 1-5-2025

Place: New Delhi

Prof. Bijiya Ketan Panigrahi
Department of Electrical Engineering
Indian Institute of Technology Delhi
Hauz Khas, New Delhi-110016, India

ACKNOWLEDGEMENTS

As I approach the end of this transformative PhD journey, I am filled with immense gratitude and a deep sense of reflection. This milestone is not solely mine but belongs to the many individuals whose unwavering support and belief have carried me through the highs and lows of this endeavor.

First and foremost, my deepest appreciation goes to my supervisor, **Prof. Bijaya Ketan Panigrahi**. Your faith in my abilities gave me the confidence to persist during the most challenging moments. Your mentorship has been far more than academic; it has been a source of inspiration, shaping not just my research but my outlook as a human. I am deeply thankful for the facilities, funding, and unwavering support extended to me. Your generosity and assistance have been invaluable, and for this, I will always remain profoundly grateful.

I also sincerely thank the members of research review committee at IIT Delhi, **Prof. Shahab Fatima**, **Prof. Deepak Umakant Patil**, and **Prof. Krishna Ramachandran**, for their thoughtful guidance and critical feedback. Their expertise and rigor challenged me to refine my work and elevate its quality. A special acknowledgment goes to the **Indian Institute of Technology, Delhi**, for creating an environment that fosters innovation and learning, and to the **Ministry of Education, India**, for the financial support throughout this journey. Without these foundational pillars, this work would not have been possible.

To my parents, **Ms. Vandana Sharma** and **Mr. Aalok Sharma**, and sibling **Ms. Rashi Sharma** your constant encouragement and sacrifices have been my bedrock. Balancing the demands of being a researcher and a mother was no small feat, but your unwavering support made it possible. And to my five-year-old son, **Viraaj Sharma**, you are my brightest light. Your smile, your laughter, and your boundless energy have been my greatest motivation to keep striving. I extend my heartfelt gratitude to my beloved *Nana Ji* **Mr. Madhuresh**, and all my extended family members, for their constant support and encouragement in every possible way. To my mentor at Bluestar Ltd., **Mr. Prashant Jadav**, your constant support and belief in me have been a source of strength throughout this journey. You've been the guiding light I could always turn to, from sharing morning affirmations to practice, to gifting me meditation and self-help books. I am truly grateful for everything you've done.

I wish to express my profound gratitude to **Prof. Ravishankar Dudhe**, under whose mentorship I had the privilege to work during my tenure as an adjunct faculty at Manipal Academy of

Higher Education, Dubai. He was the first to recognize and vocalize a potential in me that I had not yet seen in myself. His thoughtful encouragement to return to India and pursue a PhD at an IIT planted the seed of a journey I had never imagined embarking upon. His faith in my abilities became the spark that ignited my aspirations, and for that, I will always be deeply grateful.

I am equally grateful to my seniors and peers who have stood by me, offering their wisdom, camaraderie, and encouragement. **Prof. Akhil Garg**, **Prof. Deepak Kumar**, **Dr. Pankaj Dilip Achlerkar**, **Dr. Furkan Ahmad**, **Dr. Khalid Siddiqui**, **Dr. Upendra**, and **Dr. Jaya**, your guidance during crucial phases of this journey was invaluable. To my colleagues and friends, including **Ms. Nitika Ghosh**, **Ms. Vandana**, **Mr. Bibaswan Bose**, **Mr. Rismaya Kumar Mishra**, **Dr. Anurag Chawdhary**, **Dr. Bhavya Vats**, **Ms. Sunali**, **Mr. Jonty Mago**, **Mr. Afroz Ahmad** and **Mr. Mohit Murarka**, thank you for sharing both the challenges and the triumphs. To my juniors, **Mr. Kavi Bhatia**, **Mr. Pranav Mathur**, and **Mr. Chandan**, and industrial and academic collaborators, including **Dr. Prashant Srivastava**, **Dr. Arnab Bhattarjee**, **Ms. Arjita Pal**, **Mr. Divy Ranjan** and **Dr. Prabhat Ranjan Tripathi** your insights and shared discussions have been integral to shaping this work.

Lastly, to everyone who has played a part in this journey, be it through words of encouragement, thoughtful critique, or silent support, I extend my heartfelt gratitude. The countless memories and lessons I learnt from my teachers, mentors, gurus, friends, family and loved ones. Each of you has left an indelible mark on this thesis, and by extension, on me.

As I stand at this threshold, I look to the future with both humility and hope. This journey has been a testament to the power of collaboration, perseverance, and shared purpose. With the lessons learned and the relationships cultivated, I am eager to contribute to meaningful change and innovation in the years ahead. As Paulo Coelho so beautifully writes in **The Alchemist**, *"When you are loved, you can do anything in creation. When you are loved, there's no limit to what you can achieve!"*. This truth has guided me at every step of my journey, and with the love and support I've received, I look forward to the endless possibilities ahead.

with profound gratitude,

Sakshi Sharma

Date: 1-5-2025

ABSTRACT

The energy sector is undergoing a profound transformation driven by the unprecedented integration of renewable energy resources, the electrification of transportation, and the rise of advanced grid technologies. This shift is reshaping the conventional paradigms of power systems, which were historically dominated by synchronous machines and unidirectional power flows. As renewable energy generation is inherently influenced by variable ambient conditions, it introduces significant uncertainties, posing challenges to accurately predicting and integrating generation into modern power systems. Simultaneously, the proliferation of inverter-based resources, intelligent loads, and energy storage systems is introducing significant complexities on the demand side, including bidirectional energy flows, evolving network dynamics, and heightened system uncertainties. Furthermore, the increasing reliance on digital technologies for grid management, coupled with the interconnected nature of modern infrastructure, has expanded the attack surface for potential cyber threats. Amidst this evolution, two critical challenges emerge (a) the growing analytical intractability in accurately modeling advanced energy systems and their components, and (b) the escalating susceptibility of modern grids to sophisticated cyberattacks. These challenges demand innovative solutions that transcend the limitations of traditional techniques and establish secure, adaptive, and reliable frameworks for energy systems of the future.

Despite the increasing interest in AI/ML approaches for power system applications, several significant challenges persist, including the need for extensive and diverse training datasets, limited generalizability to unknown operating conditions, lack of interpretability in model behavior, scalability issues, and challenges in validating models under real-world conditions. Also, the transactional data from the power system network often cannot be shared publicly due to regulatory, security, and privacy concerns. These challenges collectively raise valid concerns about the feasibility, reliability, and effectiveness of deploying AI/ML models in complex, real-world energy system environments. This thesis addresses these gaps by introducing a conceptual framework for AI, identifying key attributes necessary for effective integration within such systems. It explores targeted strategies to embed these attributes through innovative model architectures, advanced training techniques, and Power hardware-in-the-loop (PHIL) prototyping.

This thesis addresses the limitations of traditional power system methods in handling the increasing complexities of energy systems modeling and cybersecurity. It introduces Artificial Intelligence (AI) frameworks as alternative approaches to overcome these challenges. Organized around the aforementioned broad themes, the chapters focus on specific energy system applications while sharing a common goal: identifying the shortcomings of conventional strategies and demonstrating the effectiveness of AI-driven solutions. Each chapter contributes to its respective area, forming a cohesive approach to modern power system challenges.

(1) As part of the first objective, this thesis is focused on generating in-house data for different energy systems i.e. cells, packs, , to ensure greater control over the experimental conditions and to reflect real-world variability across different battery chemistries, form factors, and operational scenarios. The data includes variations in C-rates, temperature conditions, and drive cycles, along with accelerated aging tests to simulate long-term degradation. This tailored dataset enables more accurate model development and validation. Additionally, a real-time simulation environment is essential to test these strategies under dynamic, real-world conditions facilitating the seamless transition from theoretical models to practical applications for comprehensive validation.

(2) In the second objective of this thesis, the focus is directed towards addressing the complexities in accurately estimating the state of charge (SoC) of lithium-ion battery (LiB) based energy systems, a critical parameter in e-transport applications. State estimation methodologies face inherent challenges due to the nonlinear characteristics of batteries, dynamic operational conditions, and temperature dependencies. To overcome these limitations, this work proposes an advanced ensemble modeling framework. The methodology is specifically designed to iteratively refine model accuracy by minimizing loss functions through regularization and error tolerance mechanisms. Comprehensive evaluations have been conducted across diverse datasets representing distinct battery chemistries, capacities, temperatures, and driving profiles.

(3) The third objective aims to enhance the analytical framework by quantifying the total en-

ergy storage capacity of the energy system through the concurrent estimation of the State of Energy (SoE) along with SoC. The proposed integrated estimation algorithm is rigorously validated in real-time on a scaled-up battery pack system, ensuring its robustness, scalability, and applicability.

(4) Another dimension of this research, outlined as the fourth objective, is the advancement of reliable battery lifecycle management strategies for modern energy systems. By leveraging the synergy of AI-driven methodologies and physics-based principles, this work formulates a comprehensive long-term degradation model. It is tailored to capture the complex dynamics of battery aging, enabling enhanced predictive accuracy and facilitating proactive decision-making in energy storage applications.

(5) As part of the fifth objective, this thesis evaluates AI-based predictive strategies for energy systems by generating in-house data, to ensure greater control over the experimental conditions and to reflect real-world variability across different battery chemistries, form factors, and operational scenarios. The data includes variations in C-rates, temperature conditions, and drive cycles, along with accelerated aging tests to simulate long-term degradation. This tailored dataset enables more accurate model development and validation. Additionally, a real-time simulation environment is essential to test these strategies under dynamic, real-world conditions facilitating the seamless transition from theoretical models to practical applications for comprehensive validation.

(6) Acknowledging the vital importance of cybersecurity in modern energy systems, the fifth objective focuses on fortifying Microgrids through the development of AI-driven anomaly detection frameworks. These frameworks are designed to detect and mitigate cyber threats in real-time, ensuring the operational resilience and security of energy systems. Furthermore, Objective 5 aims to integrate cyber-resilient frameworks that emphasize the principles of interpretability, robustness, and adaptability within AI systems. This integration enhances the deployment of these systems in complex cyber-physical environments, safeguarding the integrity and reliability of critical infrastructure against evolving cyber threats.

सारांश

ऊर्जा क्षेत्र वर्तमान में एक गहन परिवर्तन के दौर से गुजर रहा है, जिसे अक्षय ऊर्जा संसाधनों के अभूतपूर्व एकीकरण, परिवहन के विद्युतीकरण और उन्नत ग्रिड तकनीकों के उदय से प्रेरित किया गया है। यह बदलाव पारंपरिक विद्युत प्रणालियों के उन मानकों को पुनः परिभाषित कर रहा है, जो ऐतिहासिक रूप से समकालिक मशीनों और एकतरफा ऊर्जा प्रवाह पर आधारित थे। अक्षय ऊर्जा उत्पादन स्वाभाविक रूप से परिवर्तनीय पर्यावरणीय परिस्थितियों से प्रभावित होता है, जिससे यह आधुनिक विद्युत प्रणालियों में उत्पादन की सटीक भविष्यवाणी और एकीकरण के लिए महत्वपूर्ण चुनौतियां प्रस्तुत करता है।

इसके अतिरिक्त, ग्रिड प्रबंधन के लिए डिजिटल तकनीकों पर बढ़ती निर्भरता और आधुनिक बुनियादी ढांचे की परस्पर-संबद्ध प्रकृति ने संभावित साइबर खतरों के लिए हमले की सतह को विस्तारित कर दिया है। इस विकास के बीच, दो प्रमुख चुनौतियां उभर कर आती हैं:

१. उन्नत ऊर्जा प्रणालियों और उनके घटकों के सटीक मॉडलिंग में बढ़ती विश्लेषणात्मक जटिलता

२. आधुनिक ग्रिड की परिष्कृत साइबर हमलों के प्रति बढ़ती संवेदनशीलता।

यह शोध प्रबंध ऊर्जा प्रणालियों के मॉडलिंग और साइबर सुरक्षा में बढ़ती जटिलताओं को संभालने में पारंपरिक विद्युत प्रणाली विधियों की सीमाओं को संबोधित करता है।

(क.) पहले उद्देश्य के तहत, यह शोध प्रबंध विभिन्न ऊर्जा प्रणालियों, जैसे कि सेल्स, पैक्स, आदि के लिए इन-हाउस डेटा उत्पन्न करने पर केंद्रित है, ताकि प्रायोगिक परिस्थितियों पर अधिक नियंत्रण सुनिश्चित किया जा सके और विभिन्न बैटरी रसायनों, रूप कारकों, और परिचालन परिदृश्यों में वास्तविक-विश्व परिवर्तनशीलता को दर्शाया जा सके।

(ख.) दूसरे उद्देश्य में, शोध प्रबंध का ध्यान लिथियम-आयन बैटरी (LiB) आधारित ऊर्जा प्रणालियों के चार्ज की स्थिति (SoC) का सटीक अनुमान लगाने की जटिलताओं को संबोधित करने पर है, जो ई-परिवहन अनुप्रयोगों में एक महत्वपूर्ण पैरामीटर है।

(ग.) तीसरे उद्देश्य का लक्ष्य ऊर्जा प्रणाली की कुल ऊर्जा भंडारण क्षमता का मात्रात्मक आकलन करके विश्लेषणात्मक ढांचे को बढ़ाना है।

(घ.) चौथे उद्देश्य में आधुनिक ऊर्जा प्रणालियों के लिए विश्वसनीय बैटरी जीवनचक्र प्रबंधन रणनीतियों की उन्नति शामिल है।

(ङ.) पाँचवाँ उद्देश्य ऊर्जा प्रणालियों के लिए AI-आधारित भविष्यवाणी रणनीतियों का मूल्यांकन करता है। इसे वास्तविक समय वातावरण में परीक्षण किया गया, जो सैद्धांतिक मॉडलों से व्यावहारिक अनुप्रयोगों के संक्रमण को सक्षम करता है।

(च.) आधुनिक ऊर्जा प्रणालियों में साइबर सुरक्षा के महत्व को स्वीकार करते हुए, अंतिम उद्देश्य माइक्रोग्रिड्स को AI-चालित विसंगति पहचान ढांचे विकसित करके मजबूत करने पर केंद्रित है।

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
ANN	Artificial Neural Network
AUC	Area Under Curve
BMS	Battery Management System
CALCE	Center for Advanced Life Cycle Engineering
CC	Constant Current
CT	Computational Time
DERs	Distributed Energy Resources
DFN	Doyle-Fuller-Newman
DNN	Deep Neural Network
DR	Detection Rate
DST	Dynamic Stress Test
ECMs	Equivalent Circuit Models
EKF	Extended Kalman Filter
EVs	Electric Vehicles
FA	False Alarm
FDI	False Data Injection
FL	Federated Learning
FNN	Feed-Forward Neural Network
FOBT	Filter and Observer-Based Techniques
FUDS	Federal Urban Driving Schedule
GBDT	Gradient Boosted Decision Trees
GB-SVR	Gradient Boosted SVR
GP	Gaussian Process
GPU	Graphical Processing Units
HIL	Hardware-in-the-Loop
HWFET	Highway Fuel Economy Test
KF	Kalman Filter
LIBs	Lithium-Ion Batteries
LightGBM	Light Gradient-Boosting Machine
LFP	Lithium Iron Phosphate
LSTM	Long Short-Term Memory
LTO	Lithium Titanate
MAE	Mean Absolute Error

MAPE	Mean Absolute Percentage Error
ME	Maximum Error
ML	Machine Learning
NASA	National Aeronautics and Space Administration
NCA	Nickel Cobalt Aluminum
NMC	Nickel Manganese Cobalt
NN	Neural Network
OCV	Open Circuit Voltage
P2D	Pseudo-Two-Dimensional
PHIL	Power Hardware-in-the-Loop
PI	Proportional Integral
RF	Random Forest
RUL	Remaining Useful Life
SoC	State-of-Charge
SoE	State-of-Energy
SoH	State-of-Health
SoP	State-of-Power
SP	Specificity
SVM/SVR	Support Vector Machine or Regression
UDDS	Urban Dynamometer Driving Schedule
UKF	Unscented Kalman Filter
US06	Urban Supplemental Federal Test Procedure 06
V2G	Vehicle-to-Grid
WLTP	Worldwide Harmonized Light Vehicles Test Procedure
XGBoost	Extreme Gradient Boosting

LIST OF SYMBOLS

$\mathbb{E}_{\mathbf{x},y}\{\boldsymbol{\Psi}\}$	Expectation of loss function $\boldsymbol{\Psi}$ over input-output space i.e. **x** and **y**
$\boldsymbol{\lambda}_0(x)$	Constant function in GBDT
$(\mathbf{x}_i^S, \mathbf{y}_i^S)$	Input and output variables of source domain
K, $\{\boldsymbol{\xi}\}$, $\{\boldsymbol{\alpha}\}$	Kernel, slack variables and Lagrange multipliers
R^2	Goodness of fit
V, I, T	Voltage, current, Temperature (in $^{\circ}C$) across battery
β_k	Weight or the step-size of k^{th} learner in GBDT
κ_i	Error coefficient of i^{th} iteration
$\boldsymbol{\Psi}_{agg}$	Aggregated loss over dataset
$\boldsymbol{\Psi}(\mathbf{y}, \boldsymbol{\lambda}(\mathbf{x}))$	Loss-function corresponding to $\mathbf{y}$ and $\boldsymbol{\lambda}(x)$
$\mathbf{w}$, b, $\phi(x)$	Weight, intercept and feature space in SVR
$\widehat{\lambda}(x)$	Predicted value of function
$\boldsymbol{\nabla}_{k-1}$	Gradient of loss function
h_t	Hidden state at t^{th} instant
f_t	Forget gate
o_t	Output gate
$\|\omega\|_1$	L^1 Norm
$\|\omega\|_2^2$	L^2 Norm
Q_d	Discharge capacity
η_c	Coulombic efficiency
η_e	Energy efficiency
Q_0	Initial capacity (in ampere-hours or Ah)
$\widehat{Q_d}$	Predicted capacity (in ampere-hours or Ah)
CF	Cumulative feature
γ_i	Overall attention output of the attention layer
γ^{h_i}	Attention-score for the i^{th} attention head
d_k	Dimension of the key-vectors
w_i^q	Query weight matrices for the i^{th} attention head
w_i^k	Key weight matrices for the i^{th} attention head
w_i^v	Value weight matrices for the i^{th} attention head
V_{bus}	Bus Voltage
R_d^i	Droop resistance for i^{th} DER
H_1, G_1, G_2	Secondary and Primary Controller Gains
$V_{\text{out}}, I_{\text{out}}$	Measured output voltage and current

y_{anomaly}	Predicted scenario
$\omega_{\text{local},i}$	Local model weights
$\nabla_{\omega_{\text{local},i}} \mathcal{L}(x_i, y_i)$	Gradient of the loss function
ω_{global}	Global model update
V_{recon}	Reconstructed voltage
$\mathcal{L}_{\text{re}}$	Deviation between the reconstructed voltage and the true voltage