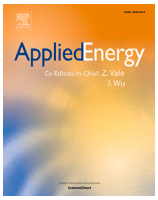
Applied Energy 401 (2025) 126753

Contents lists available at ScienceDirect

Applied Energy

journal homepage: www.elsevier.com/locate/apen



Advancing microgrid cyber resilience: Fundamentals, trends and case study on data-driven practices

Subrata K. Sarker[a,*], Hamidreza Shafei[a], Li Li[a], Ricardo P. Aguilera[a], M.J. Hossain[a], S.M. Muyeen[b]

[a] School of Electrical and Data Engineering, University of Technology Sydney, Sydney, Australia
[b] Electrical Engineering Department, Qatar University, Doha, Qatar

HIGHLIGHTS

- Explore the cyber-resilience scopes of MGs in technical, regulatory, and economic standards, briefly describing their fundamentals and modeling approaches.
- Investigate critical practices for ensuring cyber-resilient MGs and highlight emerging research issues in MG security.
- Discuss the key phases and features of data-driven cyber-resilient MGs to examine how they enhance cybersecurity. Also, summarize the recent progress of data-driven approaches to improve the MG cyber-resilience.
- A case study on a two-area isolated microgrid (IMG) is presented, in which a data-driven framework optimized using Bayesian learning approximation is examined to demonstrate enhanced security performance of the IMGs.
- Examine the integration challenges of data-driven techniques in MG cyber-resilience while highlighting some suggestions to overcome them.

ARTICLE INFO

Keywords:
Cyber-attack
Cyber-security
Data-driven methods
Microgrids
Resilient operation

ABSTRACT

Microgrids (MGs) serve as the core components of the upcoming sustainable power systems, and ensuring their security against cyber threats presents a critical research challenge due to the widespread use of advanced energy technologies. This paper explores various strategies for maintaining the cyber-resilient operation of MGs, focusing on technical, economic, and regulatory frameworks, in addition to their operational essentials for seamless functionality. In this paper, cyber-resilient operation refers to the system's ability to withstand, respond to, and recover from cyber incidents, thereby ensuring the continuous and reliable operation of the MG. An outline of the various security challenges linked to different cyber-attacks and MG frameworks, highlighting the importance of developing effective and adaptable solutions, is also studied in this paper. While model-based approaches offer precise detection accuracy under steady-state conditions, they often struggle in real-time dynamic scenarios due to their complexity and dependence on accurate system modeling. Conversely, data-driven approaches offer enhanced flexibility and adaptability, enabling swift responses to emerging cyber threats. This makes them a compelling alternative to dynamic model-based methods for ensuring cyber-secure operations of MGs. This study focuses on data-driven techniques, acknowledging the comparative strengths and limitations of both paradigms. This paper also outlines crucial steps for crafting scalable and efficient data-driven cyber solutions, highlighting their key characteristics that enhance MG security. It provides a thorough overview of recent data-driven cyber solutions for MGs, offering careful analysis to evaluate the effectiveness of these methods in enhancing security while identifying operational and implementation challenges. A case study on a two-area isolated microgrid is presented, where a data-driven framework optimized by Bayesian learning approximation is examined. This case study demonstrates the capability of the studied data-driven framework in enhancing the resilience of IMGs against cyber threats. Ultimately, the paper concludes with recommendations for the field of data-driven cyber solutions and MGs, aiming to foster further advancements in sustainable and reliable cybersecurity measures for MG frameworks.

* Corresponding author.
Email addresses: SubrataKumar.Sarker@student.uts.edu.au (S.K. Sarker), Hamidreza.Shafei@student.uts.edu.au (H. Shafei), Li.Li@uts.edu.au (L. Li), raguilera@ieee.org (R.P. Aguilera), Jahangir.Hossain@uts.edu.au (M.J. Hossain), sm.muyeen@qu.edu.qa (S.M. Muyeen).

https://doi.org/10.1016/j.apenergy.2025.126753
Received 11 May 2025; Received in revised form 3 August 2025; Accepted 11 September 2025
Available online 27 September 2025

1. Introduction

Microgrids (MGs) have emerged as a practical solution in today's rapidly changing energy market to meet the sustainable energy demand. An MG can be thought of as a specialized energy source that combines different types of distributed energy resources (DERs), such as solar (PV), wind, hydrogen sources, batteries, and generators, to provide electricity to a specific area or community. They can operate independently or in conjunction with the central grid, offering several advantages over traditional centralized grids in terms of energy reliability, efficiency, and environmental sustainability [1]. During independent operation from the grid, MGs utilize renewable energy sources (RESs) like solar, wind, hydro, or biomass, along with energy storage units (ESUs), ensuring a continuous supply of clean power even during outages or natural disasters, thereby reducing the risk of essential services being disrupted. The demand for such kinds of energy resilience is particularly acute in areas susceptible to hurricanes, floods, or where the traditional grid is unreliable or offline for extended periods [2].

Further, the MGs offer opportunities for improving local energy resource optimization and energy efficiency through the use of RESs, reducing transmission losses, and intelligently balancing supply and demand with advanced control and management systems. Additionally, they can store excess energy during periods of low demand and release it when needed, which increases overall system efficiency and reduces dependency on fossil fuels. From the environmental perspective, MGs significantly contribute to expediting the transition to low-carbon electricity as they mitigate the environmental impacts of conventional fossil fuel-based generation and substantially lower greenhouse gas emissions by harnessing RESs. However, the installation of MGs promotes the decentralization of the energy grid and the use of distributed generation, leading to increased local self-reliance and energy independence [3].

1.1. Background study

While MGs are increasingly becoming a growing trend in energy sources, there are still several obstacles to confirming their effective operation, such as regulatory hurdles, budgetary limitations, and technical difficulties [4]. One of the major barriers to the expansion of MG infrastructure is regulations that strongly favor centralized energy systems [5]. This makes it difficult for MGs to navigate the complexity of licensing, permitting, and compliance procedures. In contrast, policymakers need to create flexible and straightforward frameworks or operating standards that accommodate the decentralized nature of MG systems while maintaining security, reliability, and grid interoperability to overcome regulatory roadblocks [6]. Again, financial constraints pose a significant challenge for the cost-effective operation of MGs as they require energy storage and advanced control systems, leading to substantial upfront costs for planning, construction, and commissioning [7]. Moreover, due to the perceived risks and uncertainties associated with emerging technologies and regulatory frameworks, securing financing for MG projects can be difficult [8].

Further, the technical difficulties in various disciplines, such as energy management [9], cyber-security [10], and grid integration, [11] may hinder the widespread use of MGs. Additionally, combining different natures of DERs into a reliable MG network poses challenges related to system stability, control, and interoperability. To address these issues, emerging decentralized regulation technology needs to collaborate with MG networks to develop standardized solutions and enhanced control algorithms. While integrating emerging technology in decentralized MG networks brings significant advancements in operations such as monitoring, controlling, and diagnosis, it also creates potential vulnerabilities for unauthorized users to exploit security protocols and standards, highlighting the need for an additional security layer [12].

A security layer integration for the cyber-safe operation of MG becomes challenging in the modern landscape due to heavy reliance on interconnected technology. The effective operation of all MG elements depends on properly sharing the signals/commands through interconnected technology. While this shared signaling enhances the overall reliability of the MG operation, it also heightens the possibility of attackers gaining access to the system, as shown in Fig. 1. When attackers attempt to inject unwanted signals by inserting false commands or signals into the interconnected technologies, the MG network experiences continuous degradation in its performance, resulting in undesirable responses over time [13]. To restore normal operation in the MG, detecting attackers and precisely mitigating their impact on the system is challenging due to their increased intelligence in creating attacking signals.

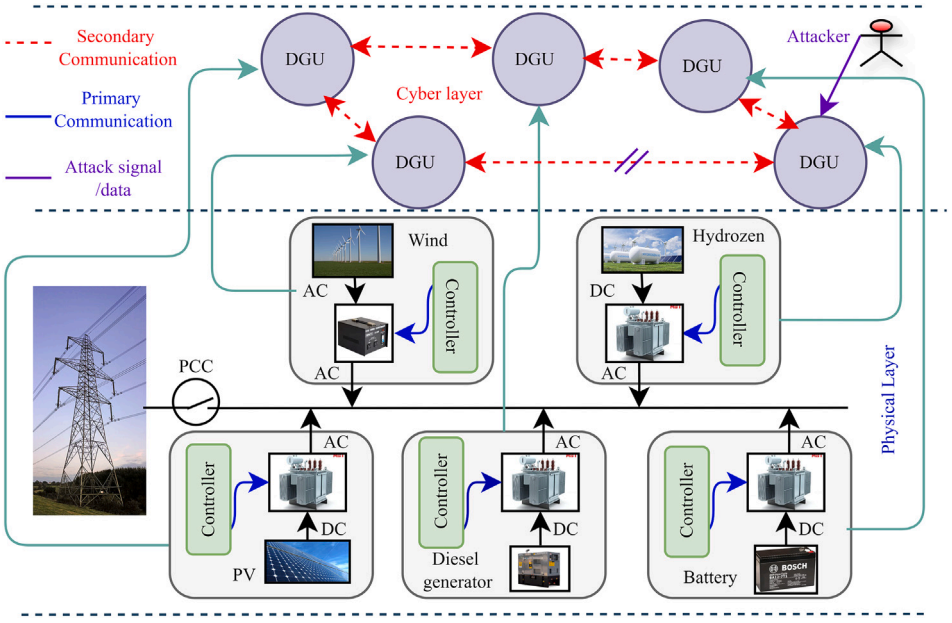


Fig. 1. A layout of cyber-affected microgrid with multiple distributed generation units.

Table 1
A systematic comparison among model-driven, data-driven, and hybrid cybersecurity methods for MGs.

Metric	Model-driven [14]	Data-driven [15]	Hybrid [16]
Accuracy (Steady-State)	High	Moderate	High
Accuracy (Dynamic)	Low to Moderate	High	High
Computational Complexity	Low	High	Moderate to high
Real-time capability	Limited (Nonlinear models)	Good (with optimized models)	Moderate
Data dependency	Low	High	Moderate
Interpretability	High	Moderate	High to moderate
Adaptability	Low	High	High
Robustness to novel attacks	Low	High (if trained well)	High
Implementation complexity	High	Low	High
Scalability (to large MGs)	Low	Moderate (depends on ML model)	High
Sensitivity to model uncertainty	High	Low	Low

1.2. Motivations and contributions

Several early attempts based on state estimation and dynamic models were developed to detect the appearance of attacks and mitigate their effects by subtracting the estimation signal from the corrupted signal [22–25]. However, implementing these models in real-time scenarios could lead to complex issues due to their intricate mathematical structures and non-linear dynamic nature. Additionally, a lack of precise and updated knowledge about the operational nature of MGs, including their topology and dynamic models, may reduce the performance of these models when changes are made to the system. On the other hand, effectively mitigating the impact of cyber threats requires a sophisticated control model with proper parameter tuning to reconfigure the network parameters.

Motivated by the limitations of dynamic model-based approaches, researchers have started exploring data-driven techniques to detect and mitigate cyber threats. These methods are resilient, applicable in real-time, and effective against various cyber threats in the MG infrastructure [26]. While addressing the limitations of model-based approaches, data-driven methods have introduced new challenges, such as data acquisition, the requirement for large and diverse datasets, and increased computational times. A summary of current research problems on the cyber-threat detection and mitigation of MGs is reported as follows:

- Dynamic model-based cybersecurity systems for MG architecture encounter challenges in real-time applications, particularly when quick responses are needed, as is often the case in dynamic MG scenarios.
- Data-driven methods, like machine learning-based cyber-security systems, encounter challenges in gathering sufficient data for training. In addition, challenges in data acquisition, management, and storage include sparse and diverse data sources, data privacy concerns, and budget constraints.
- Implementation of data-driven approaches experiences high computational costs, specifically, extended training times and large memory requirements due to handling substantial amounts of data.
- Modification of MG system parameters affects the efficacy of both model-based and data-driven methods. Further training is necessary for data-driven methods, while proper tuning is required for the model-based approach.

A systematic comparison among model-driven, data-driven, and hybrid approaches is presented in Table 1, covering key dimensions such as computational complexity, real-time feasibility, data dependency, and interpretability. This comparison reveals that model-driven methods excel under steady conditions but struggle to adapt to new threats. Similarly, the hybrid approaches aim to combine both strengths, although their implementation remains challenging and is the subject of ongoing research. In contrast, data-driven techniques offer strong flexibility and can learn from real-time data to detect evolving attack patterns, making them well-suited for dynamic MG environments. Despite the data dependency and computational challenges of data-driven methods, it is essential to acknowledge their ability to significantly enhance the cybersecurity of MGs when compared with model-based approaches. The dynamic and intricate nature of modern MG systems is particularly conducive to data-driven strategies, which provide unmatched adaptability and scalability. Further, data-driven methods can process large amounts of real-time data to identify patterns and anomalies. Additionally, these solutions can continuously improve as more data becomes available, allowing them to evolve with the system. This ability to learn and adapt in real-time makes data-driven approaches effective in identifying new and emerging threats as well as detecting known threats. These techniques are expected to provide scalable, efficient, and robust cybersecurity solutions that can adapt to the changing threat landscape. This review emphasizes the importance of data-driven methods as a critical area of focus for advancing cyber-security in MGs. Apart from these, this work contributes to the below-highlighted points:

- Explore the cyber-resilience scopes of MGs in technical, regulatory, and economic standards, briefly describing their fundamentals and modeling approaches.
- Investigate critical practices for ensuring cyber-resilient MGs and highlight emerging research issues in MG security.
- Discuss the key phases and features of data-driven cyber-resilient MGs to examine how they enhance cybersecurity. Also, summarize the recent progress of data-driven approaches to enhance the MG cyber-resilience.
- Examine the integration challenges of data-driven techniques in MG cyber-resilience while highlighting some suggestions to overcome them.

This work is important for both academic research communities and practical engineering as it provides an in-depth summary of emerging research issues, recent advancements in data-driven techniques while highlighting key features, and implementation steps on the MG frameworks for their cyber-secured operations. This is significant because model-based cyber-security solutions struggle to adapt to the unknown challenges that may arise from emerging state-of-the-art energy technologies. To address these unknown challenges, this work not only presents an essential platform for both researchers and practitioners to comprehend these issues but also offers a structured solution to develop a model-free cyber-security solution for MGs. Finally, the outstanding research issues, challenges associated with the implementation of the data-driven frameworks, and highlighted recommendations in this paper will motivate new researchers to conduct further investigations on the development of new and more effective cyber-security solutions for MG frameworks. A comparative study between the current work and other relevant review papers on microgrid (MG) networks under cyber-attacks is summarized in Table 2. This comparison provides a foundation for future studies to improve the cyber-resilience of MG networks.

1.3. Review methodology

This work aims to emphasize the important aspects of cyber-resilience in MGs along with future research areas and the potential of

Table 2
A comparative study on different review works on microgrid networks under cyber-attacks [17–21].

Features	Current study	Ref. [17]	Ref. [18]	Ref. [19]	Ref. [2]	Ref. [20]	Ref. [21]
Fundamentals of MGs	✓	✓	✓	✓	✓	✓	✓
Cyber-security challenges	✓	✓	✓	✓	✓	✓	✓
Possible scopes of cyber-resilient MGs	✓	×	×	×	✓	×	✓
Emerging research issue on cyber-resilient MGs	✓	×	×	×	×	×	×
Critical need for Cyber-resilient MGs	✓	✓	×	✓	✓	×	✓
Discuss the various types of attack and their impact on MG frameworks.	✓	×	✓	×	×	✓	×
Summarize modelling steps for the data-driven approach in MGs	✓	×	×	✓	×	×	×
Highlight recent trends on data-driven cyber-secured solutions for MGs	✓	×	×	✓	×	×	×
Case study	✓	×	×	×	×	×	×
Future recommendations	✓	✓	✓	✓	✓	✓	✓

data-driven frameworks to address these issues. To provide a comprehensive overview, recent literature on cyber issues of MGs is thoroughly reviewed using the approach shown in Fig. 2 to identify and analyze key findings. The details are given below:

(i) **Scopes and objectives:** The scope of this review starts from the initial use of data-driven techniques and extends to the current state of enhancing the cyber-resiliency of MGs. Moreover, potential future research issues related to the data-driven cyber-resiliency of MGs and their fundamental features fall within the scope of this work. A comprehensive literature review, including high-index journals, conferences, technical reports, and lectures, is undertaken to highlight the objectives. The main objectives of this review are to identify the cyber-resiliency factors of MGs with current practices, explore potential unresolved research issues, and summarize recent progress related to data-driven techniques and their implementation challenges in MGs.

(ii) **Literature searching approach:** The literature search is performed in various esteemed academic databases like IEEE, Elsevier, Google Scholar, and Springer, among others. The search utilizes keywords such as “Data-driven cyber-security,” “Microgrid,” “Cyber-attack,” “Cyber-resilience,” and “Machine and Deep learning,” etc. It is important to note that the search was restricted to the English language only.

(iii) **Selection criteria:** The works were chosen based on exclusion and inclusion criteria. Initially, the evaluation focused on abstracts, titles, and retracted information to assess their alignment with the scope of this work. Additionally, the related articles published in 2020–2024 in reputed peer-reviewed journals and conferences were selected for further analysis.

(iv) **Data analysis:** The selected articles were carefully reviewed to identify data such as publication year, research technique, key findings with limitations, and future scope, highlighting the significant role of data-driven approaches in enhancing the cyber-resiliency of MGs.

2. Fundamentals of microgrids

MGs are independent electricity sources that can operate autonomously or connect directly to the main power grid to ensure a consistent electricity supply, even during unexpected outages. They offer a practical and considerate solution for meeting the increasing demand for reliable, cost-effective, and eco-friendly electricity. Additionally, MGs can efficiently expand power distribution to remote areas without requiring significant investments in power transmission infrastructure. They can also address the need for electricity in areas without access to the main grid by strategically placing small-scale generation capabilities closer to end customers [27]. The fundamentals of an MG comprise several key operating principles, with various modeling approaches described in the subsequent part.

2.1. Microgrid operating standards

The MG operating standards outline the regulatory and organizational principles essential for the successful conception, development, and functioning of MGs. They provide a comprehensive set of protocols addressing the technical, regulatory, and economic aspects of MG deployment. From a technical perspective, standards like IEEE 1547 ensure efficiency and interoperability, while regulatory standards like IEEE 2030.7 establish rules and communication protocols. The economic standards for MGs include mechanisms for revenue generation from the energy market, cost-benefit analyses to evaluate feasibility, and various financing options to facilitate investment. The environmental framework illustrates how integrating RESs reduces emissions and includes assessments to minimize environmental impact, thereby achieving sustainability goals. By adhering to these standards, stakeholders can ensure the development of resilient, eco-friendly, and effective MG systems that have a positive impact on energy sustainability and dependability [11]. A summary of available frameworks used for MG networks is reported in Table 3.

2.2. Microgrid modeling approaches

Accurate modeling is essential for improving the understanding and performance of MG networks. Utilizing advanced modeling methods such as optimization algorithms, simulation tools, and mathematical modeling is necessary for simulating the behavior of MG networks. These techniques enable researchers and practitioners to analyze MGs’ resilience, performance, and dynamic behavior under various operational scenarios. Additionally, modeling enhances MGs’ design, planning, and management by facilitating informed decisions regarding system layout, resource utilization, and operational strategies. A needs-driven modeling approach is an initial step in developing and implementing sustainable, efficient, and resilient MG energy systems.

(i) **Modeling of AC MG [37]:** AC MG modeling is essential for developing and enhancing localized energy networks. By carefully modeling the electrical power flow in MGs, designers can gain valuable insights into system behavior and performance, enabling informed decision-making and efficient design methodologies [38]. A block diagram representation of MG is depicted in Fig. 3, where the left side contains the elements of AC MG. This modeling provides a comprehensive understanding of energy distribution across the network, considering aspects such as voltage regulation, current dynamics, and power distribution. The modeling begins with a detailed

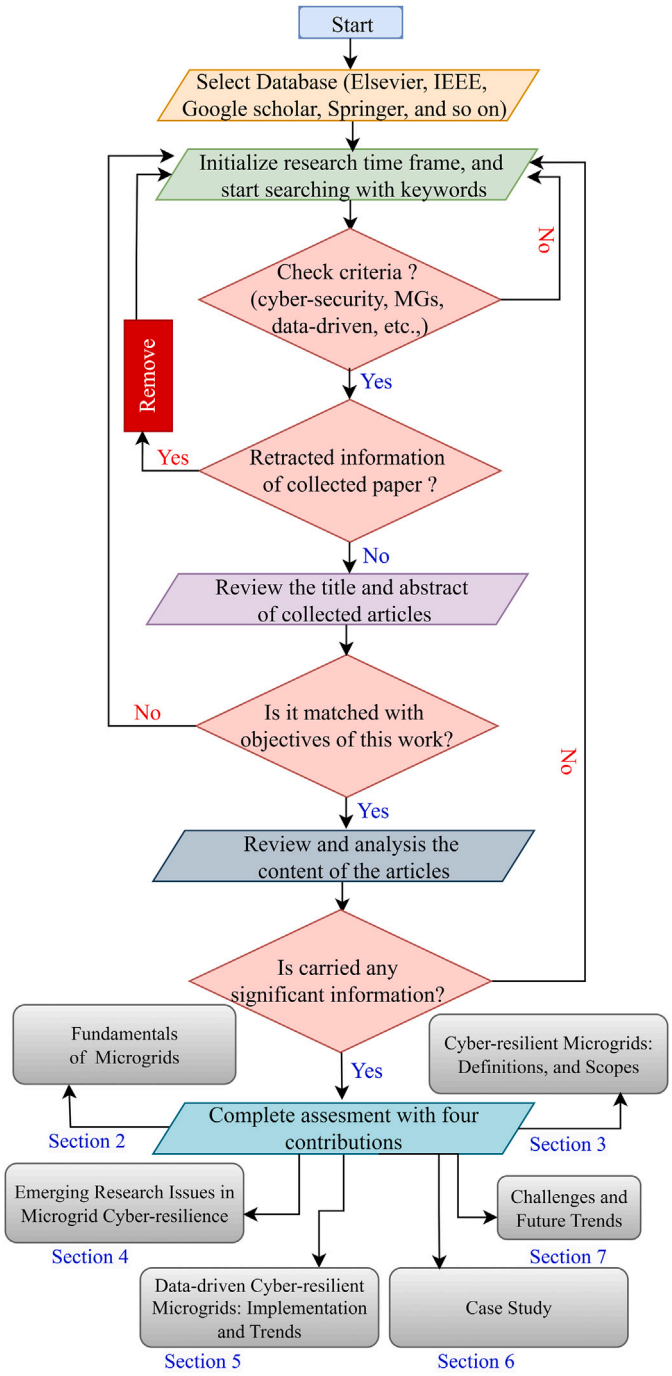


Fig. 2. A block diagram representation of literature analysis used in this work.

description of the MG's physical configuration and components, including network architecture identification, load determination, and recognition of ESSs, generation sources, and control modules.

(ii) **Modeling of DC MG [14]:** DC MGs use direct current instead of AC, providing distinctive features and significant improvement potential. When modeling DC MGs, it is essential to understand the inherent advantages of DC power systems. A block diagram representing the MG is shown in Fig. 3, with the right side containing the elements of DC MG. Using DC transmission reduces energy losses caused by AC conversion, making DC MGs particularly suitable for applications involving RESs or long-distance power transmission. DC systems also offer improved control capabilities, enabling precise voltage regulation and efficient power flow management.

(iii) **Modeling of hybrid AC/DC MG [39]:** MGs comprising both AC and DC components can be analyzed using hybrid modeling, which incorporates both AC and DC forms of MG. This method works well for hybrid MG systems that combine AC and DC energy distribution networks. Fig. 3 shows a visual representation of the hybrid MG.

(iv) **Modeling of load-frequency control MG [40]:** The modeling of Load-Frequency Control (LFC) is the conductor in the complex environment of MG systems, as shown in Fig. 4. A detailed description of all the components used in this modeling can be found in [41,42]. It coordinates the smooth operation of multiple components within the system. At the core of this model are the generators, which are controlled by governor control mechanisms to regulate their output and maintain system frequency stability. The precise design of Energy Storage Systems (ESSs) is extremely important in reducing variations in energy supply and demand to prevent frequency deviations. The control mechanisms, such as Automatic Generation Control (AGC), are carefully calibrated to monitor grid frequency and adjust generator outputs continuously. This modeling approach ensures system stability by strictly adhering to specified frequency targets.

(v) **Modeling of dynamic phasor MG [43]:** Dynamic phasor modeling of MG uses complex numbers to combine phase angle and magnitude information, describing the system's dynamic behavior. It helps analyze dynamic phenomena in MGs, such as fault response, stability analysis, and control system design. This approach balances computational efficiency and accuracy by accurately representing the sinusoidal nature of AC signals and considering transient effects. Specialized simulation tools capable of utilizing dynamic phasor approaches enable designers to study MG behavior under various operating conditions. Furthermore, this modeling approach allows for assessing MG performance, stability, and resilience, potentially leading to the development of reliable and efficient energy solutions.

A comparative summary of various modeling approaches used in MG is reported in Table 4. These different modeling approaches in MG design create a larger attack surface, allowing unauthorized users to inject unwanted data or signals. Thus, it is important to study cyber-secured MGs from different modeling perspectives for their safe operation.

2.3. Innovative technologies for advanced microgrid operation

Integrating innovative technologies across the modeling of physical and cyber layers enhances the operation of modern MGs. The physical layer includes the hardware and electrical systems, while the cyber layer encompasses data analytics, control algorithms, and communication networks. These elements combine to form a cohesive system that improves the MG's intelligence, efficiency, and adaptability in response to ongoing changes.

(i) **Physical layer [44]:** The physical layer of an MG comprises the foundational hardware and electrical infrastructure that enables energy generation, distribution, storage, and consumption. This includes components such as DERs like solar panels, wind turbines, fuel cells, and diesel generators; energy storage systems like batteries and flywheels; power converters; protection devices; and the associated electrical wiring and switchgear. It is responsible for the real-time physical flow of electricity and ensures the reliable operation of the MG under various conditions. The physical layer interacts closely with the cyber-layer, receiving control signals and providing data feedback, thus forming the backbone for secure and resilient energy management within the MG.

(ii) **Cyber layer [45]:** The cyber layer of an MG is the digital framework enabling seamless coordination, control, and optimization of all physical components. It acts as the MG's central nervous system, integrating computational, control, and communication technologies for real-time decision-making and autonomous operation. The core elements include:

Table 3
A summary of available operating standards used for MG networks.

Standard name	Highlighted points
Technical framework	
IEEE 1547 Standard [11]	(i) Set the standard of DERs Interconnection (ii) Cover protection, voltage regulation, and safety requirements of MG
Modular Approach [28]	(i) Employ a modular framework and placement of MG components (ii) Offer fast integration, adaptability, and versatility (iii) Comprise the same structures of load, generation, and storage
IEC 61,850 [29]	(i) Incorporate intelligent electronic devices (IEDs) into MG's management systems (ii) Specify data models and communication protocols to make the integration of DERs and ESSs easier
OpenADR [30]	(i) Provide communication protocols for automated demand response (ADR) between MG controllers and utility grids (ii) Facilitate the optimization of energy use through price signals and system demands
HOMERS [31]	(i) Accessible platform for optimal MG's design and simulation (ii) Provide a wide range of modeling resources and libraries (iii) Promote collaboration and creativity
Regulatory Framework	
IEEE 2030.7 Standard [11]	(i) Promote MG's communication protocols and interoperability (ii) Assure seamless interaction of various MG and grid resources
Net Metering Policies [32]	(i) Allow MG to contribute additional energy to the public grid (ii) Stimulate the investment of RESs
Feed-in Tariffs [33]	(i) Secure payment for grid-fed renewable energy (ii) Deliver fixed-rate long-term contracts (iii) Accelerate MG utilization for the development of nations
Licensing Schemes [34]	(i) Offer frameworks for granting licenses and monitoring MG activities (ii) Specify what needs to be done for MG operation, maintenance, and ownership
Economic Framework	
Cost-benefit Evaluation [31]	(i) Examine the economic rewards and viability of MG initiatives (ii) Adopt prospective sources of revenue, operating expenses, and the initial expenditure (iii) Assist stakeholders in making sensible decisions on MG investments
Energy Market Collaboration [35]	(i) Enable MGs to make revenue by entering energy markets (ii) Facilitate the trading of extra energy, provision of ancillary services, or involvement in ADR initiatives
Environmental Framework	
RESs Utilization [36]	(i) Support the integration of RESs (ii) Minimize dependency on fossil fuels and carbon gas emissions
SDGs [36]	(i) Combine MG activities with global sustainability targets (ii) Promote MG to meet SDGs (iii) Encompass climate action, energy availability, and environmental sustainability

- Collects real-time data such as voltage, current, and frequency from distributed energy resources, loads, and storage systems using sensors and smart meters.
- Utilizes wired and wireless networks like Ethernet, 5 G, and LoRaWAN, along with protocols such as Modbus and IEC 61850, to enable secure and efficient communication between microgrid components.
- Employs hierarchical control strategies—primary, secondary, and tertiary—to regulate voltage, frequency, and optimize power flow based on system dynamics.
- Uses machine learning and advanced analytics for load forecasting, system optimization, fault detection, and adaptive control.
- Implements encryption, authentication, intrusion detection, and secure protocols to protect against cyber threats and maintain data integrity.

When the cyber and physical layers of an MG are strongly coupled, various systemic risks arise due to their interdependencies. Here, the strong coupling implies that any change or failure in one layer can cause significant ripple effects in the other, potentially leading to widespread system disruptions. The primary risks associated with such scenarios include:

- *Cascading failures [46]:* In a highly interconnected cyber-physical MG, a failure in one layer can initiate a cascade of effects impacting other layers. For instance, if a cyberattack hampers the communication network, it will delay or halt the energy management system (EMS) from performing control actions, resulting in an imbalance between energy supply and demand.
- *Compromised decision-making [47]:* As the strongly interconnected MGs heavily depend on information from the physical layer to make control decisions in the cyber layer, any cyber threats, such as malware, data manipulation, or system hacking, can compromise the flow of information, leading to incorrect control decisions based on outdated data.
- *Inadequate fault tolerance [47]:* During a cyber-attack or physical failure, the MGs should be resilient enough to detect, isolate, and recover from faults. However, excessive interdependence between the cyber and physical layers can cause a failure in the cyber layer, preventing effective fault isolation in the physical system, such as malfunctioning generators or storage units.
- *Increased attack surface [48]:* The integration of communication and control systems in the cyber layer with physical systems

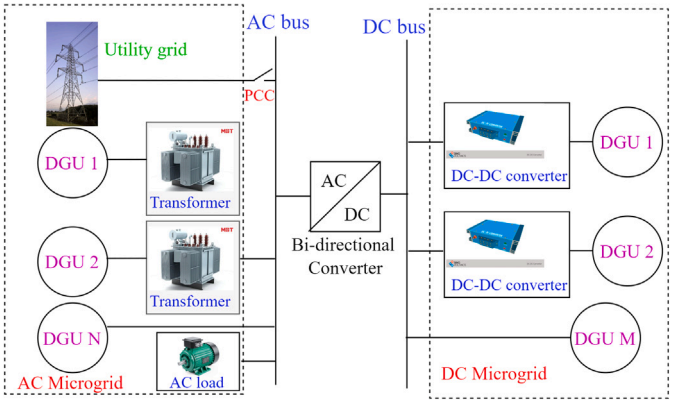


Fig. 3. A basic illustration of a hybrid AC-DC microgrid.

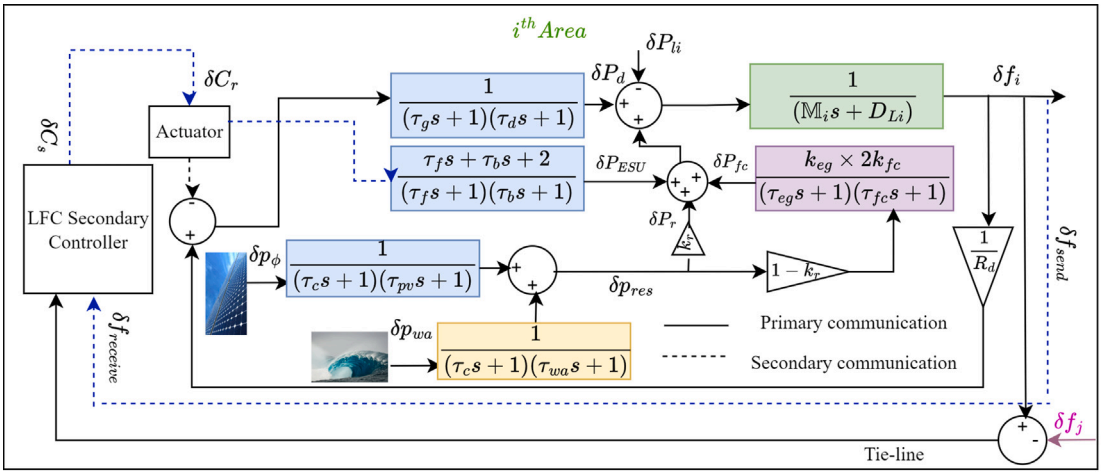


Fig. 4. A basic illustration of load frequency control enabled microgrid.

Table 4
A comparative summary of various modeling approaches used in MGs.

MG modeling approach	Applicability	Advantages	Limitations	Efficiency
AC modeling	(i) Appropriate for grid-tied and isolated AC MGs (ii) Suitable for precise AC power flow evaluation	(i) Preserve system stability and voltage management via a thorough depiction of AC behavior	(i) Nonlinear loads and transient effects add complexity (ii) Simulation requires advanced computing resources	Moderate to High
DC modeling	(i) Suitable for DC MGs powered by RESs	(i) Allow simple analysis (ii) Provides quick simulation (iii) Promote off-grid distribution systems	(i) Require extra conversion techniques (ii) Limit operation for AC loads	Moderate
AC/DC hybrid modeling	(i) Incorporate the applicability aspects of both AC and DC modeling	(i) Provide a detailed hybrid MG behavior (ii) Enhance MG resilience and reliability via a hybrid framework	(i) Increase framework complexity (ii) Require advanced tools for handling MGs	Moderate to High
Load frequency control modeling	(i) Suitable for MGs with variable generation and loads, maintaining grid stability (ii) Facilitate a quick adjustment to frequency irregularities (iii) Offer control strategies adaptability to adjust to changing conditions	(i) Reduce the possibility of shortages or disruptions and increase system reliability (ii) Facilitate seamless transition between off- and on-grid modes	(i) Require sophisticated algorithms for effective management of complex interactions	High
Dynamic-phasor modeling	(i) Suitable for MG temporal and dynamic evaluation (ii) Assist in enabling robust control algorithms for resiliency	(i) Strike a balance between productivity and precision for real-time simulations (ii) Provide design information on rapid responses for resilient control strategies	(i) Demand specialized knowledge and equipment for dynamic-phasor modeling (ii) Require a substantial amount of processing power	Moderate

creates new attack surfaces. Attackers can exploit vulnerabilities in communication protocols, control software, or even physical components (e.g., power meters, controllers) to launch attacks.

- *Compromised security and privacy [49]:* Strong cyber-physical coupling in MGs involves exchanging sensitive data such as energy consumption, generation, and user behavior between the cyber and physical layers. Attacks on these exchanges can jeopardise grid performance, user privacy, and system security.

2.4. Synchrophasor-driven microgrid operation

A synchrophasor is a device that measures electrical quantities, such as voltage, current, and frequency in real-time, typically at 30 to 60 samples per second. Using Phasor Measurement Units (PMUs) and Global Positioning System (GPS) synchronization, it ensures accurate, time-stamped data across multiple locations. This device is essential for the real-time operation of MGs because it delivers synchronized data, enabling the EMS to immediately detect issues such as voltage sags, frequency changes, or faults [50]. The EMS then triggers control actions, such as adjusting generation, managing storage, or isolating faults, to stabilize the MG. Unlike traditional monitoring systems, it enables predictive capabilities by analyzing past and present data to foresee potential disruptions and initiate proactive control actions, improving grid stability, minimizing the risk of cascading failures, and boosting overall system resilience [51,52]. This dynamic and adaptive response mechanism ensures the MG operates efficiently and remains resilient under varying conditions.

3. Cyber-resilient microgrids: definitions, requisites, and scopes

3.1. Definition of cyber-resilient microgrids

While cyber-security primarily focuses on protecting systems from unauthorized access, data breaches, and cyber-attacks through preventive measures, cyber-resilience encompasses a broader scope, extending beyond prevention to include the system's ability to withstand, respond to, and recover from cyber incidents. Specifically, cyber-security aims to block or mitigate threats before they cause harm, and cyber-resilience ensures that critical operations can continue and recover rapidly even in the face of successful attacks. A cyber-resilient MG incorporates advanced cybersecurity techniques to withstand and recover from threats or unauthorized access, ensuring the continuous and secure operation of essential MG components. This involves implementing robust security procedures, surveillance systems, and information security processes to dynamically recognize and eliminate threats [53]. Additionally, cyber-resilient MGs are characterized by their ability to swiftly adapt and recover operations during a cyber attack, minimizing downtime and preserving critical services. By combining adaptive security measures with resilient architecture, these systems enhance grid reliability, mitigate the impact of attacks, and safeguard against interruptions in energy delivery. Various attacks, such as malware infiltration, distributed denial-of-service (DDoS) attacks, data manipulation, and market threats, can occur within different MG frameworks, including technical, regulatory, or economic domains. Each type of cyber-resilient MG framework can be customized to counter specific attack vectors, bolstering overall system resilience and protecting against potential vulnerabilities [54]. A summary outlining the definition and types of attacks likely to occur in MG frameworks, their level of impact, and the corresponding countermeasures to protect MG frameworks is provided in Table 5.

3.2. Critical requisite of cyber-resilient microgrid

It is essential to examine the cyber-security of MGs because of their unique and critical role in modern energy systems. As MGs become more integrated into the overall energy infrastructure, their security becomes increasingly vital for the following reasons [63–66].

3.2.1. Ensuring reliable energy supply

The reliable operation of modern energy systems relies heavily on MGs and their cyber-security. The cyber-security of MGs is crucial for maintaining a consistent and uninterrupted energy supply. It protects the critical infrastructure, ensures the integrity of operational data, and prevents unauthorized access to control systems. Additionally, it enhances the resilience of MGs to intrusions, enabling quick detection and recovery from incidents to minimize disruption. Furthermore, adhering to cyber-security standards guarantees regulatory compliance and cultivates consumer and stakeholder confidence in the dependability and security of distributed energy systems. Thus, it is increasingly crucial to implement comprehensive cyber-security measures to guarantee the consistent and secure delivery of energy and safeguard MG operations as they become more integrated.

3.2.2. Protecting microgrids against evolving threats

As MGs face increasing threats from sophisticated cyber attacks, they are at risk of experiencing physical or operational damage, including equipment failure, power outages, and potentially catastrophic events. The study of cyber-security in MGs is essential for comprehending and safeguarding against these evolving risks.

3.2.3. Supporting grid resilience

The maintenance of cyber-security is crucial to safeguard MG control systems and communication networks from intruders or attackers. It helps prevent disruptions that could impact the broader power grid. In the case of cyber incidents, strong cybersecurity measures enable rapid recovery, allowing MG to continue supporting the grid during critical situations. Furthermore, cybersecurity is important for maintaining grid stability by protecting DERs and ensuring the integrity of data used in grid operations. As the energy landscape becomes increasingly complex and interconnected, the significance of cyber-security in enhancing grid resilience continues to grow.

3.2.4. Ensuring techno-economic microgrids

Cyber-security is essential for maintaining economic stability and cost-effectiveness by protecting MGs against cyber-attacks. These measures help to prevent costly disruptions that could lead to power outages, equipment damage, and operational delays. Additionally, robust cyber-security measures can reduce the risk of data breaches and intellectual property theft, thus safeguarding sensitive information and maintaining the competitive edge for organizations utilizing MGs. Furthermore, this security helps to prevent hidden costs arising from inefficiencies or compromised performance, ensuring the secure and reliable operation of MGs. This leads to more predictable and manageable operational expenses and helps avoid penalties for non-compliance with regulatory standards, as well as loss of revenue and reparation costs due to security incidents. In this way, cyber-security is not just a protective measure but also a strategic asset that contributes to the economic viability and cost savings of MG operations.

3.2.5. Promoting technological innovation and progress

The increasing reliance on advanced digital technologies is improving the integration of MGs with the broader energy framework and fostering technological innovation and progress by developing cyber-security. In this context, MGs need to implement comprehensive cyber-security measures to protect these innovations from cyber threats. These threats can potentially undermine the functionality and reliability of MGs as they integrate new technologies such as automated intelligent control systems, advanced analytics, and smart sensors. However, cyber-security enables the safe implementation and testing of advanced technologies within MGs by providing a secure environment. This promotes innovation without worrying about data breaches or operational disruptions from intruders. This protection supports developing and implementing creative solutions that can improve grid resilience, optimize energy management, and facilitate the shift to more sustainable energy sources.

3.2.6. Global energy revolution and sustainability

As the global energy landscape transitions to greener, decentralized sources, MG has become essential for facilitating the integration of renewable energy, improving grid resilience, and promoting sustainable development. Nevertheless, the heightened connectivity and digitalization necessary for these developments also introduce vulnerabilities to cyber threats. The implementation of cybersecurity measures is imperative to protect MGs from these attacks and guarantee their seamless integration with RESs. By safeguarding the integrity and availability of these systems, cybersecurity facilitates the continuous operation of RESs, thereby reducing carbon emissions and achieving sustainability objectives.

3.3. Scopes of cyber-resiliency in microgrids

In MGs, cyber-resilience refers to the ability to withstand and recover from cyber-attacks and other adverse events without compromising essential functions. This includes the MG's capacity to adapt to changing conditions, keep critical loads powered, and restore operations in the event of equipment malfunctions, natural disasters, cyber-attacks, or grid disruptions. The cyber-resilience is crucial for MG operations as it improves energy security, ensures a stable power supply, and enhances local resilience [67]. Additionally, a cyber-resilient MG supports emergency response, safeguards critical infrastructure, and ensures public safety by providing reliable electricity. Furthermore, it reduces reliance on centralized infrastructure, minimizes the impacts of grid vulnerabilities, and promotes sustainability by integrating green technologies

Table 5
A summary outlining the definition and types of attacks likely to occur in MG frameworks, their level of impact, and the corresponding countermeasures to protect MG frameworks.

Type of attack	Description	Implementation cases	Potential MG framework	Countermeasure	Impact
Data Manipulation [55]	(i) Data tampering in MG control systems to mislead operators (ii) Cover illegal activities (iii) Affect data integrity, and trigger faulty choices	(i) Effect on system operation and process decisions (ii) Difficult to verify altered data	(i) Technical (ii) Regulatory	(i) Set blockchain-powered data tracking and verification tools for imperative operation (ii) Employ cryptography tools to secure and verify data integrity	High
Denial-of-Service (DoS) [56]	(i) Heavy traffic overloads MGs and blocking authorized users from accessing them (ii) Implement via exploiting weaknesses or flooding the system with requests	(i) Effect on energy availability (ii) Interruption of services	(i) Technical	(i) Prioritize critical loads by implementing load transfer methods (ii) Utilize intelligent EMSs to dynamically resource allocation	High
Malware Injection [57]	(i) Infect MG control unit by malicious malware (ii) Hinder operations by manipulating controller (iii) Compromise sensitive data security	(i) Collapse in control over critical structure (ii) Impair integrity of the control mechanism	(i) Technical, (ii) Regulatory	(i) Provide MG controllers with safe startup procedures (ii) Apply software security certification and code signatures	Moderate
Phishing and Social Engineering [58]	(i) Implement via designer to click malicious links or download malware (ii) Increase risk of exposing sensitive operational data to hackers	(i) Allow illegal access and data breaches (ii) Possibly exposure of confidential information	(i) Regulatory	(i) Arrange cybersecurity training for MG operators (ii) Include multi-factor authorization in operation with sensitive data	Low
DDoS [59]	(i) Attempt to deplete MG resources by making huge traffic floods (ii) Focus on resources including memory, computing power, and bandwidth	(i) Rise grid blackouts and downtime (ii) Increase difficulties in sustaining network resilience	(i) Technical	(i) Choose attributes to identify anomalous in the energy supply or demand (ii) Utilize intelligent decentralized control to mitigate localized impacts	Moderate
Man-in-the-Middle (MitM) [60]	(i) Allow for data manipulation, and spoofing by intercepting the communication between MG nodes (ii) Implement via breaching network security	(i) Undermine data security and reliability (ii) Feasible interruption of connections	(i) Technical	(i) Use encrypted techniques between end-to-end communication (ii) Set secured channels of communication	High
Zero-Day Exploits [57]	(i) Find uncovered vulnerability in MG hardware for access without authorization (ii) Can strike before updates or fixes are ready	(i) Apply in both MG software and hardware parts (ii) Hurdle to rapid mitigation and patching	(i) Technical	(i) Frequently check the MG security over vulnerabilities (ii) Implement program-based system resiliency	High
Advanced Persistent Threats (APTs) [61]	(i) Intelligent, protracted attack against the workforce, supply chain, or infrastructure of MG (ii) Adopt modern tools to avoid detection and keep access	(i) Recurrent and invisible dangers on network	(i) Technical (ii) Regulatory	(i) Employ threat hunting of MG methods to identify signs of intrusion (ii) Utilize network division and isolation to contain APTs	Very High
Market Manipulation [62]	(i) Manipulate prices or trading activities in the MG energy markets (ii) Cover spoofing, collusion, or fraudulent data reporting	(i) Threat of nepotism and market fraud	(i) Economic (ii) Regulatory	(i) Set governance and market monitoring mechanisms for energy market activity (ii) Apply blockchain for secure transaction	High
Compliance Violations	(i) Manipulate norms or rules regarding MG operations	(i) Break rules about security, privacy, or the environment	(i) Regulatory	(i) Establish compliance with industry standards via periodic audits (ii) Provide compliance instruction for MG operator	Moderate

and renewable energy sources [68]. Key factors that contribute to MG cyber-resilience include:

3.3.1. Enabling diverse energy resources

Diverse forms of energy are essential for enabling MG cyber-resilience in numerous ways, including redundancy, flexibility, and various other factors. The redundancy within MGs encompasses multiple energy sources, allowing them to continue running even in a cyber-attack event where one source fails or is interfered with. It provides a crucial backup layer, ensuring uninterrupted power supply to critical loads and communities [69]. Additionally, diverse energy sources contribute to the flexibility of MGs, enabling them to dynamically adjust energy generation and consumption based on factors such as availability, cost, and environmental conditions [70].

3.3.2. Optimal sensor placement for cyber-resilient microgrids

The cost of real-time MG monitoring largely depends on the strategic placement of sensors, as improper placement can lead to increased communication costs due to the need to transmit more data over longer distances. This cost can be minimized by strategically placing the sensors to maintain network efficiency. Again, adding more sensors improves the observability of the MG, however, it also raises costs because of additional devices, maintenance, and data processing. The strategic and optimal sensor placement minimizes unnecessary redundancy while

ensuring adequate coverage. Thus, the strategic positioning of sensors enhances observability, allowing for real-time detection of anomalies, faults, or cyber threats. At the same time, it minimizes redundancy and ensures cost-effectiveness by avoiding over-saturation of sensor data. This can be achieved through the application of optimization algorithms that consider factors such as the physical topology of the MG [71], communication latency [72], and the potential impact of cyber-attacks on critical components [73]. Thus, proper sensor placement ensures that critical points of the MG are adequately monitored, thereby enhancing the system's ability to detect anomalies or cyberattacks.

3.3.3. Incorporating smart adaptive control technology

The advanced monitoring, management, and optimization capabilities provided by smart control technology significantly enhance the cyber-resilience of MGs. The intelligent control unit utilizes real-time data and sophisticated algorithms to regulate power production, storage, and distribution within the MG. It can autonomously adjust the operation of various assets, such as ESSs, generators, and RESs, by continuously evaluating energy demand, supply, and grid conditions [74]. This control unit also supports predictive maintenance, ensuring the reliability of critical components and identifying potential cyber-issues before they escalate into failures. Additionally, these technologies facilitate seamless connectivity with external grids, enabling MGs to participate in collaborative energy exchanges, ancillary services marketplaces, and demand response programs [68].

3.3.4. Adding redundant components and backups

The resilience of MG can be significantly improved by adding redundant components and backup systems, guaranteeing uninterrupted operation in the face of cyber-attack events. As essential protections, these components may offer additional support in case the initial component fails, or there are unplanned outages [2]. This might include battery backup devices, inverters, and backup generators that are carefully added to the MG infrastructure to lessen the effects of malfunctions and guarantee a steady supply of electricity. Furthermore, they minimize the risk of downtime and strengthen the reliability of MG operations, particularly in scenarios where a single point of failure could lead to widespread service disruptions [68].

3.3.5. Enabling adaptive demand-side management

The cyber-resilience of MG can be increased significantly by enabling adaptive demand-side management (DSM), which improves the MG's capacity to adjust to changes in the supply and demand of electricity. Using DSM techniques, MGs can dynamically modify their energy consumption behaviours according to customer needs, grid limits, and real-time situations. Also, MGs can minimize grid pressure when there is elevated demand or supply unpredictability due to cyber-attacks, reducing peak loads and utilizing cutting-edge technologies like smart meters, sensors, and automated control systems. This adaptive strategy reduces the chance of cyber-stresses or disruptions, increasing energy utilization and improving the MG's cyber-resilience [75]. In addition, adaptive DSM gives customers the power to take an active role in energy management by providing them with the information they need to decide how and when to utilize electricity. In general, the implementation of adaptive demand-side management improves the cyber-resilience of MGs through the optimization of energy consumption, less dependence on external resources, and the facilitation of consumer participation in the creation of a more stable and sustainable energy system [76].

3.3.6. Incorporating scalable and adaptive cyber-security solutions

Implementing a scalable and adaptable cybersecurity solution is crucial for managing the systemic risks arising from the strong interdependencies between the cyber and physical layers in MGs. As these MG systems become more complex and interconnected, traditional cybersecurity measures become inadequate in addressing evolving threats. A scalable solution enables the cybersecurity framework to manage MG growth in terms of size and complexity, including increased data, devices, and networks [77], while an adaptable solution allows the system to learn from new data, evolving threats, and changing conditions [41]. Data-driven methods offer significant advantages in this regard. These methods can scale seamlessly as MGs grow, accommodating increasing complexity and allowing for real-time analysis of vast amounts of operational data from both layers. Moreover, they are adaptable, continuously learning from data to evolve and improve in response to new threats or changes in operating conditions [26]. This adaptability ensures that the system remains resilient to emerging cyberattacks and unforeseen physical failures.

3.3.7. Implementing secure communication technology

Secure communication technology significantly improves the cyber-resilience of MGs by protecting essential networks and data transfers from cyber-attacks. The sensitive data transmitted within the MG network remains private and unaltered due to reliable communication methods, including authentication, encryption, and other techniques. This technology prevents unauthorized access and alteration of critical operational information by encrypting information transfers between smart meters, controllers, sensors, and energy management technologies [78]. These measures prevent hackers' attempts to compromise vital data, disrupt MG operations, or undermine MG's stability. Furthermore, securing communication technologies also enables more reliable remote monitoring and control systems, empowering operators to manage MG assets confidently from remote locations [2]. By establishing secure data transfer and communication channels, MG operators can further reduce the risk of service interruptions and ensure uninterrupted energy delivery to critical infrastructure and end-users. This allows them to effectively detect and respond to cyber-security threats [79,80].

3.3.8. Policy and regulatory support

The policy and regulatory support creates a favourable environment for MG regulation and reduces the chances of cyber-attacks in the MG regulatory framework. This type of support can incentivize investments in MG technology, innovation, and infrastructure, making them more accessible to various communities and industries [68]. Regulations that provide financial incentives, streamline the permitting process, and establish performance benchmarks can reduce entry barriers and encourage widespread adoption of MGs. Furthermore, policies that facilitate the integration of RESs and technologies support grid modernization and the deployment of ESSs. Additionally, they enhance grid stability and cyber-resilience by enabling MGs to enter the larger energy network. This is achieved by promoting interconnection standards, grid interactivity, and market participation [81]. Moreover, policies prioritizing resilience planning, risk reduction, and disaster recovery for MG networks are essential.

3.3.9. Developing DLR-enabled MGs and resilience modeling

The integration of Dynamic Line Rating (DLR) technology into MGs offers a transformative approach to enhancing the resilience and reliability of modern energy systems. It optimizes the operation of power transmission lines by adjusting their capacity in real-time based on environmental conditions. In MGs, the operational challenges due to the intermittent and variable nature of RESs can lead to system instability. DLR plays a crucial role in mitigating these challenges by enabling real-time adjustments to power flow. For instance, during periods of high wind or solar activity, DLR increases transmission capacity to transfer excess power to storage or the grid and decreases capacity to prevent overloads when generation is low, thereby ensuring reliability. The resilience modeling in DLR-enabled MGs focuses on forecasting and mitigating potential disruptions to power supply caused by cybersecurity threats, environmental factors, or system failures. Traditional cybersecurity models rely on static data and predefined assumptions, often failing to account for the dynamic behavior of RESs

Table 6
A summary of DLR frameworks and their potential impacts on MG resilience operation.

Framework	Key insights	Potential effects on MGs	Applications	Resiliency enhancement
Cyber-Physical Reliability Framework [82]	(i) Models DLR reliability in cyber-physical systems	(i) Improves MG reliability via real-time data	(i) Assesses line reliability with real-time data	(i) Addresses data vulnerabilities
Grid Flexibility Integration Framework [83]	(i) Merges DLR and grid flexibility for enhanced adaptability	(i) Enhances microgrid flexibility through dynamic transmission line adjustments	(i) Analyzes line behavior and adaptability	(i) Improves coordination in MGs and grid
Dynamic Thermal Rating(DTR) Framework [84]	(i) Describes real-time line capacity under operating conditions	(i) Optimizes MG power distribution by adjusting line ratings	(i) Assesses line behavior in real conditions	(i) Preserves stability via real-time adjustments
DLR Forecasting and Security Framework [85]	(i) Develops models to optimize DLR and boost security	(i) Improves MG resilience using load and line forecasts	(i) Predicts line behavior and load fluctuations	(i) Assists MGs avoid disruptions
Real-World DLR assessment Framework [86]	(i) Evaluates DLR performance in real-world settings	(i) Provides real-world insights for MG reliability and stability	(i) Analyzes line performance in real conditions	(i) Mitigates equipment wear and flow variations
Multi-Agent DLR Coordination Framework [87]	(i) Introduces multi-agent systems for coordinating DLR and MGs	(i) Optimizes decentralized control in MGs using DLR	(i) Decentralized control of lines and DERs	(i) Enables autonomous coordination in MGs
Data-Driven DLR Optimization Framework [88]	(i) Uses data-driven methods to optimize DLR in smart grids	(i) Improves MG efficiency through real-time data for optimal dispatch	(i) Uses data to adjust transmission line behavior	(i) Enhances decision-making in MGs

and the adaptive operations enabled by DLR. By incorporating real-time data from DLR systems, cyber-resilience models can dynamically adjust to environmental changes and cyber threats, simulating load balancing, energy storage management, and failure recovery scenarios in response to actual system conditions. A summary of existing DLR frameworks and their potential impacts on MG resilience operation is illustrated in Table 6. This ensures that DLR-enabled MGs can effectively maintain resilient operation in the face of unforeseen events.

3.3.10. Enabling risk assessment technology

Enabling risk assessment technology is essential for strengthening MG resilience since it may reveal possible threats and vulnerabilities and facilitate proactive mitigation techniques. This system reveals hazards like harsh weather, cyber-attacks, equipment failures, or supply chain disruptions by utilizing sophisticated analytics, machine learning algorithms, and real-time data monitoring [89]. With this all-encompassing comprehension, MG operators can create robust backup plans, distribute resources sensibly, and execute resilience-enhancing strategies to mitigate recognized threats effectively. Moreover, risk assessment technology simplifies scenario planning and modeling, enabling operators to examine the effectiveness of alternative response methods and determine the impact of different threats on MG operations [90]. Furthermore, this technology encourages stakeholders to collaborate and share information, strengthening a group approach to risk management and cyber-resilience planning. Ultimately, MG operators enhance their capacity to predict, adapt, and recover from cyber-attacks by incorporating risk assessment technologies into their operations [91].

4. Emerging research issues in microgrid cyber-resilience

The field of cyber-resilient MG research is rapidly growing as it addresses various complex issues essential for improving the security and reliability of DERs. Among the different ways DERs interact, the key challenge is establishing a robust and flexible framework to swiftly identify and mitigate cyberattacks. It also presents a significant challenge to ensure the security and integrity of data transferred in MG networks, requiring innovative cryptographic solutions tailored to the specific limitations of decentralized energy infrastructures [92]. Additionally, developing new methods to prevent cyber-physical attacks is crucial as MGs become more integrated with smart grid technology and the Internet of Things. To fortify the resilience of MGs against the expanding array of cyber threats in an interconnected energy landscape, it is imperative to focus on the following research domains.

4.1. Developing autonomous and adaptive response techniques

The focus of current research is to develop autonomous and adaptive response techniques (AARTs) for MG cyber-resiliency, aimed at enhancing MG's real-time cyber threat detection and response capabilities without the need for human interaction. This entails creating sophisticated frameworks and algorithms that recognize unusual activity on networks, prevent possible cyberattacks, and quickly return to regular operations [63]. The following are crucial phases in creating such mechanisms [63,93–96]:

- *Attack detection*: Design and implement advanced anomaly detection algorithms to constantly monitor MG networks for any unusual activity or deviations from standard operating procedures.
- *Risk evaluation*: Evaluate the degree of severity and effect of identified risks on MG operations while considering safety concerns, possible outages, and equipment urgency.
- *Decision-making*: Integrate decision-making processes to assess available resources, possible outcomes, and the attack's severity when determining the best action plan. This involves determining the most effective mitigation techniques and evaluating the most suitable action strategy.
- *Enabling autonomous response*: Enable automatic response mechanisms ready to carry out planned measures to eliminate threats and restore the system's normal operations. Avoiding further exploitation could involve rearranging network settings, isolating impacted components, or implementing countermeasures.
- *Adaptation*: Utilize machine learning approaches to ensure adaptability over time in reaction to new attackers, system upgrades, and response data from the past. Changing cyber-threat environments guarantees ongoing enhancement and optimization of response techniques.

4.2. Enabling edge computing security

Edge computing security is crucial for protecting the confidentiality and integrity of data in MG energy systems. Enhancing security protocols for decentralized data processing and storage ensures the reliable operation of MG. Several critical measures are required to incorporate edge computing security into the MG network. Firstly, conducting a comprehensive risk assessment is essential to identify potential edge computing-related attacks on MG infrastructure. This assessment will serve as the basis for developing targeted security strategies [97]. Additionally, it is important to implement secure communication protocols and encryption technologies to ensure secure data transmission

between centralized control systems, MG components, and edge devices, thus safeguarding sensitive information from unauthorized access and interception. Furthermore, integrating attack detection techniques is vital in preventing unauthorized users from accessing edge computing resources and detecting anomalies [98,99]. Lastly, securing update mechanisms and managing patches are crucial steps to keep edge devices and software components up-to-date with the latest security fixes, thereby minimizing the risk of known vulnerabilities being exploited by malicious actors.

4.3. Preserving data mining privacy

The main focus of MG data mining privacy is to find a balance between the need to protect sensitive data and the use of data mining techniques to strengthen MG systems. This balance is challenging due to the growing reliance on data-driven methods, which require large amounts of data from different sources. One way to address this challenge is to develop privacy-preserving data mining tools for MG cyber-resiliency [100]. This involves several key processes. First, secure data anonymization and encryption techniques are essential to protect critical operational data and personally identifiable information during data mining. Second, it's important to preserve the privacy of each contributor while enabling meaningful evaluation of aggregated data through unique privacy methods. To prevent unauthorized sharing and manipulation of sensitive data, it's crucial to implement secure data exchange protocols and access control systems. Additionally, exploring new techniques such as federated learning [101] and homomorphic encryption [102], which allow for collaborative data analysis without compromising data privacy, can enhance overall security.

4.4. Developing intelligent adaptive access control techniques

The increasing need for flexible and responsive security measures to safeguard essential data and facilities within MG can be addressed by developing intelligent adaptive access control approaches. Model-based static access control methods may not be adequate against the rising intelligent cyber threats. Instead, we require adaptive intelligent solutions that can dynamically adjust access rights in response to changing threat landscapes and system conditions. Here are some important steps to consider when creating such techniques: first, identifying vulnerabilities or threats through comprehensive risk assessments and developing access control rules using machine learning that can dynamically adjust permissions in response to threats, user behavior, and real-time system monitoring. The next step involves implementing advanced authorization and authentication methods, such as attribute-based access control and multi-factor authentication, to enhance security flexibility and granularity. Furthermore, the use of artificial intelligence and machine learning algorithms to analyze access patterns enables proactive detection of unusual activity in MG for timely intervention. In summary, intelligent adaptive access control-based MG cyber-resiliency enables systems to adapt to evolving security threats, ensuring continued safe operation and reliable energy distribution while safeguarding sensitive data and reassuring communities [103].

4.5. Implementing regenerative cyber-resilience

Implementing regenerative cyber-resiliency in MGs enables proactive security measures to enhance the system's capacity for recovery and adaptation in the face of cyber threats. This approach focuses on recovering from setbacks and emphasizes growth and learning to develop barriers against future occurrences. Unlike traditional resilience approaches focused solely on recovery, regenerative cyber-resiliency promotes continual learning and improvement, drawing on past experiences to enhance future defences. This resilience approach may attract more attention from designers as it promotes comprehensive security measures by fostering a resilient and adaptable culture, encouraging cooperation, creativity, and continuous improvement of cybersecurity procedures.

Several critical processes are involved in accomplishing regenerative cyber-resilience within the MG framework [104]. This process begins with thorough risk assessments to identify weak points and dangers. The second step is to create robust and adaptive incident response plans and procedures, which are essential for quick recovery and restoration of operations. Thirdly, real-time cyber threat identification and elimination through the integration of automated threat detection and mitigation capabilities are essential. The utilization of data-driven algorithms is necessary to evaluate security events and modify protections as needed. Moreover, the maintenance of regenerative cyber-resilience initiatives depends on establishing an organization-wide culture of resilience and continual development. These procedures outline how MG frameworks can successfully integrate regenerative cyber-resilience, encouraging a proactive cybersecurity strategy and ensuring the safe and reliable operation of distributed energy systems.

4.6. Resiliency toward multi-vector attacks

In MG, resiliency toward multi-vector attacks refers to the system's ability to withstand and recover from complex cyber-attacks that utilize multiple attack vectors simultaneously. These coordinated attacks, often orchestrated by advanced persistent threats (APTs), pose a significant threat to MG operations by employing various tactics and entry points to compromise or disrupt the system [105]. Resiliency against multi-vector attacks is crucial, as it can mitigate the impact of sophisticated cyber threats and ensure MG systems' consistent and reliable operation. Achieving resilience against these attacks requires a multifaceted, intelligent approach, including proactive defense, rapid incident response, and robust threat detection. Multiple steps are necessary to establish resilience against multi-vector attacks within an MG framework. Like other forms of attack resilience, the initial step in building resilience against multi-vector attacks is identifying potential attack vectors and vulnerabilities through thorough risk assessments. A layered security approach, encompassing network segmentation, access controls, and encryption, can help reduce the attack surface and mitigate the impact of attacks. Moreover, the implementation of adaptive and advanced attack detection and mitigation techniques based on learning algorithms is crucial for promptly identifying and countering multi-vector attacks. To maintain resilience against evolving attack surfaces, automated incident response plans and regular security audits and drills must be integrated as the next step. Ultimately, a proactive and comprehensive cybersecurity strategy involving the integration of technological solutions, organizational procedures, and stakeholder participation is needed to make MG resilient to multi-vector attacks.

4.7. Ensuring cyber-safe operation of synchrophasor-driven MGs

While the integration of synchrophasor devices in the MGs domain initiates real-time monitoring and dynamic operation, it can introduce additional cyber vulnerabilities due to increased interconnectivity, real-time data exchange, and reliance on synchronized control mechanisms [106]. The use of PMUs and GPS synchronization necessitates communication networks that link various devices and locations, which raises the potential for cyberattacks. Malicious actors can exploit weaknesses in the communication infrastructure or devices to launch data manipulation attacks, leading to unstable performance [107]. Furthermore, as PMUs rely on GPS synchronization for precise data time-stamping, GPS signals can be susceptible to spoofing or jamming, resulting in inaccuracies in time synchronization [108]. This may result in the processing of erroneous data, leading to improper system responses such as incorrect control actions, potentially jeopardising the stability of the MG.

Again, the real-time data supplied by synchrophasors is essential for the EMS to execute prompt control decisions. Any compromise or corruption of this data will result in erroneous judgments, thereby causing

operational disturbances such as power outages or equipment damage. Here, the attackers can target the communication networks responsible for transmitting data from PMUs to the EMS, potentially leading to a denial-of-service (DoS) attack [109]. Such an attack could flood the system with false data or cause delays, hindering control actions and making the MG vulnerable. Furthermore, attackers can also inject malware into EMS or PMUs to compromise system integrity, enabling them to monitor, modify, or redirect data, and potentially take control of the grid. The required equipment and software, often supplied by third-party vendors, can introduce vulnerabilities through insecure coding or weak security practices, giving attackers opportunities to exploit these flaws for unauthorized access. Moreover, many modern MG systems support remote monitoring and control, which also pose risks of unauthorized remote access, allowing attackers to seize control of MG's systems and potentially threaten grid stability [110,111]. Considering these challenges, the development of an advanced cyber-safe methodology is necessary to integrate robust security measures that safeguard communication networks, prevent GPS spoofing or jamming, protect the integrity of real-time data, and defend against both internal and external cyber threats.

4.8. Integrating optimized blockchain technology

The integration of blockchain technology in MG cyber-resiliency offers a promising solution to enhance the security and reliability of distributed energy systems. MGs can provide a transparent and impermeable track of energy transactions by utilizing the decentralized feature of blockchain technology [112]. In addition to lowering the possibility of cyberattacks, this guarantees data integrity and increases the MG network's overall resilience. Smart contracts powered by blockchain technology can also automate grid management and energy transaction procedures, reducing the need for centralized agents and promoting secure, efficient peer-to-peer energy transactions. This technology also improves MG systems' access control and authentication procedures by enabling safe and decentralized identity management. However, the blockchain-enabled MG network frequently experiences difficulties with excessive energy consumption, high latency, and restricted scalability, making it unsuitable for effective MG operations. These flaws can compromise the resiliency and sustainability of MG networks by causing delays in transaction processing, scalability issues, and higher resource consumption. In contrast, optimized blockchain solutions tailored for MG cyber-resiliency prioritize low-latency transaction processing, scalability to accommodate growing energy transactions, and energy efficiency to minimize resource usage. In general, optimized blockchain technology overcomes the drawbacks of non-optimized systems to provide a stable and robust foundation for MG cyber-resiliency.

4.9. Compatible and interoperable security standard

In MG cyber-resiliency, adopting compatible and interoperable security standards is paramount to ensure the robust protection of distributed energy systems against cyber threats. These standards establish a common framework for implementing security measures across different components and devices within the MG network, enabling seamless communication and collaboration between diverse systems and stakeholders [113]. By adhering to compatible security standards, the MG operators can ensure that security protocols and mechanisms are interoperable, allowing for effective coordination and response to cyber incidents. Moreover, compatible security standards facilitate the integration of new technologies and solutions into the MG system, promoting innovation while maintaining system resilience. Overall, implementing compatible and interoperable security standards in MG cyber-resiliency is essential for fostering a cohesive and comprehensive approach to cybersecurity, safeguarding critical infrastructure and ensuring the reliable delivery of energy services to communities.

5. Data-driven cyber-resilient microgrids: implementation and trends

5.1. Essential phases for implementing data-driven approaches

Data-driven methods are utilized to enhance MGs' ability to identify and address cyber-attacks. This involves using both historical and real-time data to develop predictive models that bolster cyber-resilience. The process encompasses several elements, including real-time monitoring systems, machine learning algorithms, and advanced data analytics to examine historical and current data related to energy generation, consumption, resiliency, and grid dynamics. The implementation of data-driven cyber-secured MGs involves various stages: data collection, preprocessing, feature engineering, model selection, training, validation, deployment, and continuous monitoring, as shown in Fig. 5. A summary of the steps involved and the impact, challenges, and solutions for data-driven MG is reported in Table 7.

Unlike static or rule-based models, data-driven MGs can dynamically modify operations in response to changing circumstances, such as variations in the energy demand, fluctuations in the weather, or faults and attacks during operation. A significant issue arises from the volume and complexity of the data, necessitating advanced data processing techniques and a substantial amount of computing power for analysis. Additionally, ensuring the accuracy and reliability of predictive models can be challenging, as data quality issues and uncertainties in the MG environment may affect model performance [26]. Furthermore, there are logistical and technological difficulties in incorporating data-driven models into existing MG frameworks while maintaining compatibility and interoperability with legacy systems. A multidisciplinary strategy integrating knowledge of data science, energy management, and grid resilience operations is needed to address these issues and develop efficient data-driven solutions for MG cyber-resilience and optimization.

5.2. Core attributes of data-driven techniques

When considering model- or rule-based MGs, it is important to recognize the inherent difficulties. Firstly, model-based MGs often rely on simplified assumptions about the dynamics and behavior of the system, which may not fully capture the complexity of the real world. This can lead to poor operational decisions and incorrect predictions. Moreover, the practical application of model-based MGs may be limited in dynamic circumstances where flexibility is essential for cyber-resiliency, as they struggle to adapt to changing operational conditions or unforeseen occurrences. Additionally, scalability can be problematic because model-based techniques can be difficult to implement in large-scale MG systems or when combining various data sources and variables [114].

On the other hand, data-driven solutions can provide more precise and comprehensive views of system behavior by utilizing vast amounts of historical and current data, helping operators make well-informed decisions and maximize performance. Furthermore, data-driven techniques are inherently scalable and flexible, allowing for integration of diverse data sources and adaptation to varying system sizes and complexities [115]. This section will explore how data-driven cyber-solutions in MG overcome model-based limitations, offering case studies and practical insights into enhancing cyber-resilience. We will discuss these features of data-driven MGs in detail, explaining how they overcome model-based limitations and offering practical insights into enhancing cyber-resilience.

5.2.1. Rapid incident response

One essential feature of data-driven cyber-resilience in MGs is rapid incident response capabilities, which are often lacking in model-based MGs. The model-based MGs are useful for comprehending system behavior in typical scenarios; however, they are not flexible enough to respond quickly to cyberattacks in real time as they rely on predefined models and assumptions. These models may not account for the dynamic nature

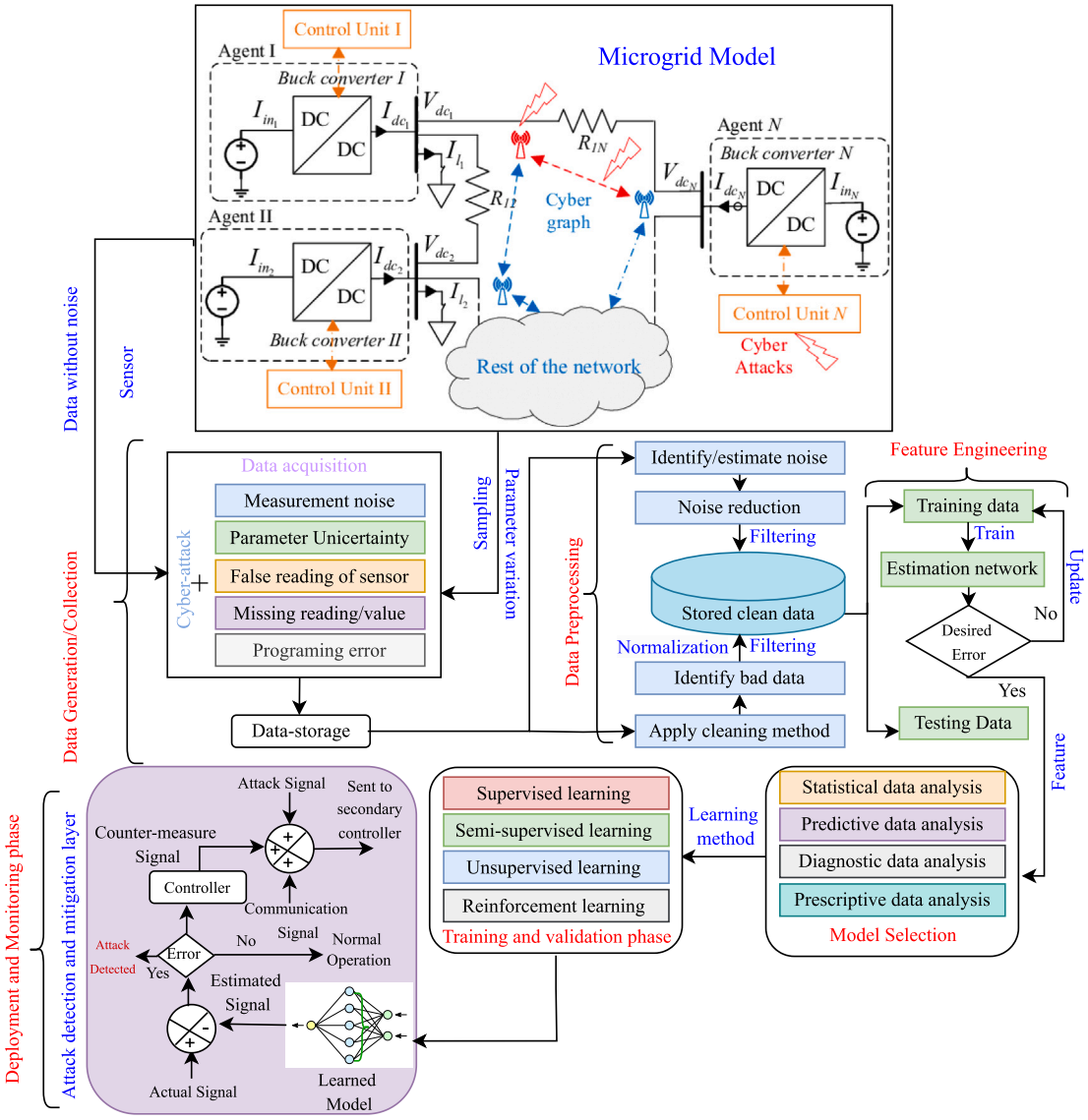


Fig. 5. Critical steps for applying data-driven methods in microgrid cyber-security.

of cyber-attacks and evolving threat landscapes. As a result, they struggle to identify and address emerging cyber issues, which could cause responses to be sluggish or incomplete. On the other hand, data-driven cyber-solutions use machine learning algorithms and real-time data analytics to continuously monitor and evaluate system behavior. This allows for the quick identification of anomalies and the timely reaction to cyber threats. This inherent capability of data-driven MGs provides operators with the agility to swiftly mitigate the impact of cyber incidents, ensuring system integrity and reliability [116].

5.2.2. Real-time adaptation

The ability to adapt in real-time is an essential part of data-driven cyber-resilience in MGs, allowing MG systems to instantly adjust to changing environments and new threats [117]. Through the constant analysis of enormous volumes of both historical and current data, data-driven systems are able to identify inconsistencies and deviations from typical operating patterns, which enable quick reactions and parameter adjustments. This ability to adjust in real-time is especially essential in minimizing the effects of cyber disasters, while a prompt response is necessary to preserve the dependability and integrity of the system. As model-based MGs rely on static conditions that may not capture dynamic system behavior or emerging threats, achieving real-time adaptability requires additional re-calibration, which can increase computational complexity. This difficulty makes it challenging to achieve the agility and fast responsiveness needed for rapid adaptation to respond effectively against cyber incidents, highlighting the advantages of data-driven approaches in enhancing cyber resilience.

5.2.3. Early identification of threats

Data-driven cyber-resiliency in MGs utilizes machine learning techniques, complex data analytics, and monitoring from various data sources to identify threats early [118]. An MG operator can minimize the risk of damage and disruption to the system by employing a proactive approach to promptly respond to developing cyber problems before they spread. Although data-driven MG cyber-resiliency is effective for identifying attacks early on, it demands training using historical and current data over time. However, this training process is essential for improving accuracy and adaptability, ensuring the system can effectively identify and respond to emerging cyber threats. In contrast, model-based MGs may not require extensive training but may lack the ability to adapt and learn from new data, limiting their effectiveness in early threat detection. Thus, even if training is required for data-driven MGs, this

Table 7
A summary of modeling steps, impact, challenges, and solutions for data-driven MGs.

Step	Description	Impact	Challenges	Solutions
Data Collection	(i) Collect prior data on energy production, utilization, and security threats (ii) Data collection should be relevant for specific analysis	(i) Collect essential data for evaluation	(i) Lack of data quality (ii) Inconsistency	(i) Apply data normalization and cleaning techniques into practice
Data Preprocessing	(i) Prepare the data for analysis (ii) Restore data quality and uniformity	(i) Facilitate precise analysis and modeling	(i) Difficult to manage missing values	(i) Employ methods of identifying aberrant data and replacement
Feature Engineering	(i) Find relevant features to increase the interpretability and accuracy of the model	(i) Reduce computational cost of the model	(i) Find redundant or unnecessary features can be challenging	(i) Utilize domain expertise and feature mapping techniques
Model Selection	(i) Select suitable method to predict cyber-resilience (ii) Choose models based on performance indicators	(i) Verify the model's efficacy	(i) Difficult to find the most effective algorithms	(i) Conduct thorough evaluation and make comparison
Training Phase	(i) Utilize the prepared data to train the chosen model (ii) Conduct optimization based on parameter	(i) Develop a trained predictive model for resilience	(i) Model's Overfitting or underfitting	(i) Adopt cross-validation and regularization techniques
Validation Phase	(i) Validate the model's efficiency with cross-validation tools or datasets (ii) Assess the model's generalization ability	(i) Guarantee the model's robustness and dependability	(i) Model's Overfitting on the training data	(i) Use k-fold cross-validation and distinct validation datasets
Deployment Phase	(i) Incorporate the trained model into the MG to enable fast decision-making	(i) Enable real-time assessment of cyber-resilience	(i) Lack of interoperability	(i) Create interfacing and APIs to enable simple integration
Monitoring and Updating	(i) Track the model's performance and add additional data to keep it updated (ii) Monitor risks and variations in system behavior	(i) Guarantee long-term efficacy of the model	(i) Drift detection and (ii) Model degradation	(i) Set automated monitoring and retraining processes

investment is essential for improving cyber-resiliency and guaranteeing the dependability of MG systems.

5.2.4. Integration with emerging technologies

Integrating emerging technologies is relatively simpler in data-driven MG systems as they inherently embrace flexibility and adaptability, making them well-suited for this integration. Emerging technologies like blockchain, Internet of Things (IoT) devices, and digital twins [119] can be easily integrated into data-driven MG systems through advanced data analytics. These technologies support the data-driven approach by improving system monitoring, optimization, and cybersecurity capabilities. Additionally, since data-driven approaches are iterative, MG systems can enhance cyber-resiliency accompanying new technologies through ongoing learning and development. Conversely, integrating new technologies into model-based MG systems poses challenges due to their reliance on predefined static models and assumptions. These models may not accurately capture the complexities introduced by emerging technologies, leading to inaccuracies and limitations in system performance. Integrating new technologies into model-based MG systems can be difficult and time-consuming, necessitating a large investment of time and knowledge.

5.2.5. Enhanced critical decision-making capability

Data-driven MGs have the potential to provide "granular insight", defined as precise and in-depth knowledge gathered from data analysis. This could entail a thorough awareness of several MG operational aspects, such as system performance indicators, energy usage trends, and potential vulnerabilities. These insights are frequently gained by finely analyzing enormous volumes of data, enabling operators to identify minor patterns, anomalies, and trends that might not be visible at a higher level of abstraction. Furthermore, data-driven methodologies enable predictive modeling and scenario analysis, allowing operators to predict possible outcomes and assess the efficacy of various mitigation techniques. By addressing vulnerabilities and threats, these insights assist MG operators in making better decisions quickly, maximizing system performance, and improving cyber-resilience [80].

5.2.6. Allowing collaboration enhancement

Since data-driven approaches are inherently flexible and interoperable, collaboration is essential for data-driven MG systems, facilitating improved collaboration between cybersecurity specialists, energy providers, and system operators. Utilizing machine learning algorithms and advanced data analytics enables data-driven MG to integrate data from multiple sources and stakeholders seamlessly. This collaboration enhances cyber-resiliency by fostering information sharing, rapid response coordination, and collective threat mitigation efforts. For example, real-time data sharing allows for the early detection of cyber threats and enables swift response actions to minimize their impact. Furthermore, cooperative data analysis and scenario planning support proactive risk management for data-driven MG, creating robust cyber-resilience plans [130]. In contrast, collaboration is limited in model-based MG systems due to their rigid structure, which may not easily accommodate collaborative data sharing or adapt to diverse stakeholder needs and perspectives.

5.3. Recent trends

In MG cyber-resilience, various data-driven techniques are employed to fortify defences against cyber threats. Using labeled data, supervised learning techniques recognize patterns indicative of cyber attacks, enabling accurate detection and response mechanisms. Conversely, utilizing known risks and new trends, semi-supervised data-driven techniques integrate labeled and unlabeled data to improve attack forecasting and mitigation. However, unsupervised data-driven methods use MG data analysis without labeled examples to find abnormalities and deviations that can indicate possible security vulnerabilities. Through trial and error in dynamic contexts, reinforcement learning techniques allow agents

to learn and constantly adapt to emerging threats, optimizing cyber defense strategies over time and improving response capabilities. By developing these diverse data-driven approaches, MG operations can effectively safeguard critical infrastructure, ensuring the reliability and resilience of energy distribution systems against cyber threats.

A summary of the recent developments in data-driven techniques for the cyber-resiliency enhancement of MG is reported in Table 8, which demonstrates significant advancements in data-driven techniques, particularly in terms of performance and feature capabilities. A notable improvement is the high detection accuracy achieved by many models, with some reaching up to 99.4 % accuracy, as seen in frameworks using Bayesian Change Point Detection. This high level of accuracy is crucial for detecting complex cyber-attacks such as FDI, which manipulate critical grid parameters like voltage and frequency. Additionally, several models emphasize rapid detection times, with some systems capable of identifying threats within 5 to 10 ms, making them highly responsive to potential breaches.

The ability of data-driven frameworks to remain operationally resilient in the face of attacks is a crucial attribute. An event-driven resilient control technique helps MGs quickly recover from cyber attacks, maintaining system consensus and minimizing operational disturbances. This is particularly crucial in situations involving stealth attacks, where recovery should occur instantly. Additionally, machine learning methods like reinforcement learning (RL) and long short-term memory (LSTM) continuously learn from new data, improving protection mechanisms over time and enhancing MG flexibility. Furthermore, many of these frameworks are still limited by high computational demands and scalability concerns, which make it challenging to implement them on a large scale, limiting their real-time viability. However, the effectiveness of these models depends on the availability of precise and trustworthy data, and many solutions continue to face challenges with data quality. Nevertheless, ongoing development of these data-driven techniques can address these constraints and improve the security and resilience of MG systems.

6. Case study

In today's advanced power systems, MGs are recognized as essential infrastructure, capable of autonomous operation and integrating RESs. However, their growing dependence on digital control and communication technology exposes them to complex cyber threats. This case study introduces a data-driven framework designed to enhance the cyber resilience of MGs. By utilizing a recurrent neural network (RNN) model trained on operational data, this approach enables the detection of cyber anomalies, a precise assessment of system deviations, and the swift implementation of countermeasures. The efficacy of the developed framework is measured using a two-area connected isolated microgrid (IMG) simulated in MATLAB. The results illustrate how a data-driven methodology not only enhances threat detection accuracy but also improves control performance during cyberattacks, representing a crucial advancement toward secure and intelligent microgrid operations. A detailed analysis is presented in the following parts, demonstrating the RNN model's ability to adapt to changing operating conditions and maintain system stability through learning and control adaptation under cyber-attack scenarios.

6.1. System setup

6.1.1. Modeling of two-area connected IMG

Fig. 4 illustrates the generalized block diagram of a load frequency control (LFC)-guided two-area interconnected IMG. This reduced-order dynamic representation captures the core relationship between active power and system frequency, while also accounting for the system's susceptibility to potential cyber threats. The modeling framework has been validated in recent studies [169,170] as an effective and reliable tool for analyzing cyber-resilient frequency control strategies in IMG environments. The system architecture includes multiple distributed energy resources (DERs), such as batteries, fuel cells, and RESs like solar, wave energy, and flywheel systems, all coordinated through a communication network. A conventional diesel generator is also integrated to support the stable operation under diverse loading conditions. To regulate frequency deviations and maintain system stability, a distributed secondary control mechanism is employed. This mechanism utilizes a conventional PID controller tailored for each area and leverages communication links to receive measurements, such as frequency deviations and tie-line power flow. It is important to note that, for the frequency response model illustrated in Fig. 4, the other components do not need to interact with the control center. Consequently, these components present a significantly lower risk of cyber compromise. Based on the received inputs, the secondary controller generates control signals for each local area IMG and transmits them to the energy storage systems (ESSs) and diesel generators. These signals adjust the charging/discharging behavior of the ESSs and the governor speed settings of the diesel generators, thereby supporting frequency regulation within the IMG. The adjustment in the speed governor's control signal δW_g can be expressed as follows:

$$\delta W_g = \left(\frac{1}{\tau_g s + 1}\right)\left(\frac{1}{R_d}\delta f - \delta C_r\right), \tag{1}$$

where $\mathcal{R}_d$, τ_g, and δf_i indicate the droop coefficient for the primary control layer, the governor's time constant, and frequency deviation, respectively, while δC_r indicates the control signal generated from the secondary controller based on input signals, such as frequency and tie-line power signal ($\delta\tau$). Then, for i^{th} area of IMG, we can write as:

$$\delta C_r^* = \mathcal{G}_{sc,i}\left(\delta f_i(t) + \sum_{j=1, j\neq i}^{K} \delta\tau_{\text{tie},ij}(t)\right)$$

Here, $\mathcal{G}_{sc}$ and K denote the gain of the secondary controller and the total number of tie-lines. Now, the turbine system is activated by the adjusted speed governor signal from (1), initiating power generation. Thus, the power δP_d produced by the i^{th} IMG synchronous generator fluctuates as follows:

$$\delta P_d = \left(\frac{1}{\tau_g s + 1}\right)\left(\frac{1}{\tau_d s + 1}\right)\left(\frac{1}{R_d}\delta f - \delta C_r\right),$$

where τ_d is the turbine time-constant of a diesel generator. This reinstates the IMG frequency, allowing the system to keep the frequency deviation δf zero over the disturbances, which can be measured for i^{th} IMG as:

$$\delta f_i = \frac{1}{\mathbb{M}_{si} + D_{Li}}[\delta P_{ri} + \delta P_{bi} + \delta P_{fi} + \delta P_{fci} + \delta P_{di} - \delta P_{li}] \tag{2}$$

In (2), the terms $\delta P_{ri}, \delta P_{bi}, \delta P_{fi}, \delta P_{fci}, \delta P_{di}$ and δP_{li} denote the per unit power change for RESs, battery, flywheel, fuel cell, diesel generator and load, respectively. The system's inertia and damping coefficient of the load are denoted by $\mathbb{M}_s$ and D_L, respectively. The parameters of each component in the studied IMG follow the model detailed in [42]. Accordingly, the frequency deviation in the i^{th} area, denoted by δf_i, can be expressed as:

If the operation of the system remains free from attacks targeting global and local communication channels, it adheres to the following communication principle:

$$\delta\tau_{tie,ij} = \delta\tau^S_{tie,ij} = \delta\tau^R_{tie,ij}. \tag{3}$$

$$\delta f_i = \delta f_i^S = \delta f_i^R. \tag{4}$$

Here, δf_i^S and $\delta\tau^S_{tie,ij}$ represent the sending end signal from the system to the secondary controller, while δf_i^R and $\delta\tau^R_{tie,ij}$ indicate the receiving end signal at the controller. However, when FDI attacks manipulate

Table 8
Recent research trends on data-driven techniques for cyber-resilient MGs (2020-2025).

Ref.	Year	Algorithm	Algorithm type	Types of attack	Framework	Features	Limitations	Attack implementation
[55]	2022	LSTM-SAE with SGD	Unsupervised	Stealth-attacks, FDI	Technical	i. Can detect zero-day attacks ii. Outperform the ML detectors by 3.5–18.3 %, 2.6–12.7 %,and 6.1–31 % in DR, FA, and HD	i. Scalability and real-time feasibility are not discussed ii. Dependent on assumed data accuracy and sole use of reconstruction error	Voltage and Current Manipulation
[120]	2021	Third-order Lagrange extrapolation	Supervised	Cyber-attacks, FDI	Technical	i. Deviation is found to be within 3 % of the limits ii. Detect and recover in 20 ms for voltage sensor missing, 16 ms for current sensor intrusion, and 9 ms for voltage sensor intrusion	i. Historical data dependency ii. Vulnerability to advanced attacks iii. Limit testing coverage	Voltage and Current Manipulation
[121]	2021	Hilbert-Huang Transform (HHT)	Unsupervised	Cyber-attacks, FDI	Technical	i. 95 % accuracy, DNN training time is 2713.2 s ii. Average detection time 5 ms	i. Signal processing dependence ii. Blockchain complexity iii. Limit real-world evaluation	Frequency alteration
[122]	2020	Event-driven resilient control strategy	Supervised	Stealth-attacks, FDI	Technical	i. Quick recovery from ±8 V stealth voltage attacks ii. Consensus maintained during 4 A and 24 A stealth current attacks	i. Trust node dependency ii. Limited detection scope iii. Communication overhead	Voltage and Current Manipulation
[123]	2021	MPC with artificial neural network (ANN)	Supervised	Cyber-attacks, FDI	Technical	i. Validation performances: Two converters: 2.9542×10^{-10}. Six converters: 2.3324×10^{-10}	i. High computational demand ii. Communication delays ii. Complex integration	Frequency alteration
[124]	2022	Bayesian Change Point Detection (BCPD)	Unsupervised	Cyber-attacks, FDI	Technical	i. 99.40 % accuracy of estimated output ii. Performance validated across various attack scenarios	i. Data reliance ii. Sensitivity to changes iii. Computational load	Abrupt Load Change
[125]	2024	Nonlinear controller	Data-driven	DDoS and FDI	Technical	i. 2 % improvement with nonlinear controller ii. Voltage index improvement	i. Specific system arrangement ii. Simulation-based evaluation	Voltage and power parameters
[126]	2021	Levenberg-Marquardt with ANN	Supervised	Cyber-attacks, FDI	Technical	i. Error less than 0.02 % in steady state ii. DE value around 4 during the transient state	i. Dependency on training data quality ii. Susceptibility to adversarial attacks iii. Limited generalization	Voltage and current manipulation
[127]	2022	Robust Parity-based Attack Detection	Supervised	Cyber-attacks, FDI	Technical	i. Accuracy: 95 % ii. False positive rate: 2 %	i. Limit data availability ii. Simplify the network model iii. Scope is restricted to specific scenarios	Voltage and current manipulation
[128]	2021	Autoencoders	Supervised	Cyber-attacks, FDI	Technical	i. Detection precision: 95.36 % ii. Detection time: 10 ms	i. Vulnerable to cyber-attacks due to interconnectedness ii. Limited reliability in detecting anomalies iii. Potential production disruption	Voltage and Current Manipulation
[129]	2023	Multi-level detection and mitigation paradigm	Hybrid	MitM, FDI	Technical	i. Achieve 95 % accuracy in malware detection ii. Reduce false positives by 80 % compared to previous methods	i. Limited scalability ii. Reliance on existing network for detection iii. Challenge in real-time response to cyber threats	Voltage and Current Manipulation

(*continued on next page*)

Table 8 *(continued)*

Ref.	Year	Algorithm	Algorithm type	Types of attack	Framework	Features	Limitations	Attack implementation
[131]	2020	Data-driven controller	Supervised	MITM	Technical	i. Sensitivity analysis ii. Experimental validation of resilient controller	i. Scalability constraints ii. Topology dependency iii. Resource overhead	Voltage manipulation
[132]	2020	Relative Entropy-based algorithm	Semi-supervised	FDI	Technical	i. Restore critical bus voltage to 1500 V after the attack ii. DER shutdown triggered by overcurrent protection at 1.2 pu	i. Communication reliance ii. Narrow attack scope iii. Increase computation	Voltage and Current Manipulation
[133]	2022	Describing function (DF)	Semi-supervised	Stealth-attacks	Technical	i. Improve stability margin ii. Maintain stability under varying τ	i. Limited resources can compromise security ii. Instability diverges from traditional definitions	Voltage and Current Manipulation
[134]	2021	ANN-MPC	Supervised	Cyber attack	Technical	i. Improve stability with ANN-based MPC ii. Reduce voltage stress on the DC bus	i. MPC computational overhead ii. Dependency on training data quality	DC bus voltage
[135]	2021	Cooperative Control algorithm	Supervised	DDoS	Technical	i. Accuracy: 95 % ii. False Positive Rate: 3 %	i. Scalability concerns ii. Dependency on network infrastructure	Frequency alteration
[136]	2023	Distributed Data-Driven Secondary Control (DDSC)	Supervised	FDI	Technical	i. DDSC voltage and current responses ii. Controller performance with time delay	i. Parameter tuning dependency ii. Lack analysis over time delay	Control command
[137]	2023	Data-driven DSC	Supervised	FDI, DoS	Technical	i. Consider hybrid attack ii. Experimentally validated	i. Ignore meshed-configuration DC microgrids ii. Implementation challenges due to hardware constraints	Voltage and current manipulation
[138]	2023	DF Stability Method	Data-driven	FDIA	Technical	1. Voltage regulation error: ≤ 0.05 V. 2. Current sharing error: ≤ 0.01 A	i. Complexity of stability region mapping ii. Sensitivity to parameter variations iii. Lack of scalability	Voltage sensors
[139]	2022	DBSCAN-ANFIS	Semi-supervised	FDI	Technical	i. Successful detection and mitigation ii. Real-time simulation validation	i. Limited to specific attack types ii. Uncertain scalability iii. Offline training dependency	DC sources, battery SoC
[140]	2021	Deep Adversarial Learning	Supervised	Adversarial-attacks, FDI	Technical	i. RL vs PID: ITAE 4766.5 vs 10848 ii. Max frequency deviation: RL 0.0132, PID 0.442	i. Tuning difficulty ii. Q-value overestimation iii. Variable effectiveness	Frequency alteration
[141]	2024	SVM, TD3	Reinforcement learning	FDI	Technical	i. Frequency: Stable ii. Reactive Power: Controlled	i. Unspecific Algorithm ii. Data Dependency iii. Scalability Challenges	Voltage and current
[142]	2022	Adversarial Deep Learning	Supervised	Adversarial attacks	Technical	i. Achieve 95 % accuracy on test dataset ii. Reduce false positive rate by 20 %	i. Vulnerable to adversarial examples ii. Limited robustness against sophisticated attacks	Frequency

[143]	2021	DDPG, DQN	Reinforcement learning	Stealthy, FDI	Technical	i. Successful stealthy FDI generation ii. Detection within 2–3 s	i. Miss coordinated attacks ii. Susceptible to link disconnections	Current signals
[144]	2020	DeepFool	Supervised	Adversarial attack	Technical	i. Accuracy reduction ii. Perturbation magnitude	i. Computational complexity ii. Vulnerability to defense mechanisms	Voltage and current
[145]	2021	Nonlinear observer	Supervised	FDI	Technical	i. Mitigate simultaneous attacks and maintain stability ii. Effective mitigation	i. Open-loop integration ii. Sensitivity to noise and uncertainty iii. Bias in load estimation	Voltage and current
[146]	2024	Deep Belief Network (DBN)	Unsupervised learning	DoSA, FDI	Technical	i. Accuracy: 98.72 % ii. False alarm rate: <1 %	i. Dependency on rules ii. Potential overfitting	Energy domain
[147]	2021	Data-driven MPC	Supervised	FDI	Technical	i. Stable DC bus voltage ii. Reduce battery charge/discharge cycles	i. Communication requirement ii. Computational burden iii. Dependency on external factors	Not specified
[148]	2022	Data-driven Control	Supervised	FDI	Technical	i. Mitigate attacks ii. Real-time implementation	ii. Limited real-world validation iii. Scalability concerns	SoC and voltage
[149]	2021	DPI-NIDS	Supervised	Network intrusion	Technical	i. Detection accuracy: 98.5 % ii. False positive rate: 0.1 %	i. Limited to unknown attacks ii. Vulnerable to adversarial attacks	Frequency domain
[150]	2022	BPDPS	Supervised	Latency attack	Technical	i. Output currents: 2.2 A, 4.4 A, 4.4 A, 2.2 A ii. Distribution factor: [1 2 2]	i. Communication network dependency ii. Ideal conditions assumption	Communication network
[151]	2020	DSMO	Supervised	FDI	Technical	i. Voltage restoration ii. Current regulation	i. Implementation complexity ii. Scalability constraints	Voltage and current
[152]	2023	DeepATTACK	Semi-supervised	Cyber attack	Technical	i. 95 % attack success rate ii. Reduce detection accuracy by 30 %	i. Limited robustness ii. High computational cost	Frequency domain
[25]	2023	Dynamic Signature Function	Data-driven	FDI	Technical	i. Validate on a four-node MG ii. Maintain stability with up to 50 % compromised agents	i. Detect and mitigate FDIA ii. Need accurate tuning iii. Introduce latency attack	Voltage and current
[153]	2023	ANFIS	Data-driven	FDI	Technical	i. Achieve 99.40 % accuracy ii. Outperform FFNN and DT estimators in precision, recall, accuracy, and F1-score	i. Performance depends on training ii. Steady-state errors persist iii. Limited applicability	Voltage and current
[154]	2023	GRU	Data-driven	Cyber attack, FDI	Technical	i. Loss: 1.4×10^{-5} ii. RMSE: 0.0049	i. Highly dependent on the precision ii. Lack of robustness	DC bus voltage
[155]	2022	Median-based Consensus	Unsupervised learning	Cyber-physical attack, FDI	Technical	i. Achieve 92 % accuracy in anomaly detection ii. Reduce false positive rate by 30 %	i. Dependent on accurate system modeling ii. Vulnerability to sophisticated cyber attacks iii. Lack of scalability	Frequency alteration
[156]	2024	XGBoost	Supervised	DoS, MITM, FDI	Technical	i. AUC values ranged from 0.916 to 0.998 ii. Prediction time: 0.1 ms	i. No consideration for diverse DERs and loads ii. Dependency on periodic model updates	Voltage and Current

(*continued on next page*)

Table 8 *(continued)*

Ref.	Year	Algorithm	Algorithm type	Types of attack	Framework	Features	Limitations	Attack implementation
[157]	2024	Autoencoder Neural Network	Deep Learning	Cyber-physical anomalies, FDI, cyber attack	Technical	i. Unsupervised learning capability ii. Effective at detecting unknown anomalies iii. Can model complex nonlinear behavior	i. Requires substantial training data ii. Sensitive to hyperparameter tuning iii. Difficult to interpret results	Voltage, and current
[158]	2024	Reinforcement Learning (RL)	Model-free Learning	Information vulnerabilities, Market manipulation	Technical and Regulatory	i. Adaptable to dynamic market conditions ii. Enhances decision-making in real-time trading iii. Can handle uncertainties in renewable energy output	i. Requires large amounts of historical data ii. High computational cost iii. May not perform well in highly volatile environments	RESs generation data, Market trading data
[159]	2024	LSTM	Deep Learning	Data integrity issues	Technical	i. Effective in time-series anomaly detection ii. Capable of real-time monitoring iii. Robust to noisy sensor data	i. Requires a large amount of labeled time-series data ii. Computationally expensive iii. May overfit in small datasets	Voltage, current, and control data
[160]	2024	Nonlinear Autoregressive Exogenous Input	Time-Series Modeling	FDI Attack	Technical	i. Effective for small anomalies in data ii. Works well in nonlinear systems iii. Provides real-time mitigation strategies	i. Sensitive to noise in measurements ii. High computational complexity iii. Requires accurate model parameters	Voltage, current, control signals from controllers
[161]	2025	Predictive Droop Control	Data-driven Control	FDI	Technical	i. Improves transient dynamics stabilization ii. Adaptive to varying grid conditions iii. Provides predictive control to enhance system stability	i. Requires accurate system state prediction ii. May require high computational resources for real-time predictions	Voltage, current, system load, droop parameters
[162]	2025	ANN	Supervised Learning	Data integrity issues	Technical	i. High accuracy in identifying cyber threats ii. Real-time detection of anomalies iii. Adaptive to various types of cyber threats	i. Requires large labeled datasets for training ii. May face challenges with new, unknown attack patterns iii. High computational cost for real-time monitoring	Voltage communication signals, control data
[163]	2025	1D Convolution Neural Network (CNN)	Deep Learning	FDI and DoS	Technical	i. Combines deep learning with signal processing for robust detection ii. Adaptable to varying operational conditions iii. Efficient at mitigating different attack scenarios	i. Requires substantial computational resources ii. Needs accurate sensor data iii. May struggle in high-noise environments	Voltage and Current
[164]	2025	Improved MFAC	Event-triggered Control	Time Delays, Load Disturbances	Technical	i. No dependency on model information ii. Utilizes event-triggered mechanism for reducing communication overhead iii. Employs Lyapunov stability theory for system stability	i. High dependence on data quality ii. Susceptible to feedback signal deviations and noise iii. Limited by computational resources for real-time applications	Frequency

[165]	2025	k-Nearest Neighbors (k-NN)	Supervised Learning	FDI	Technical	i. Simple and interpretable model ii. Robust to noise in data iii. Efficient for real-time monitoring and anomaly detection	i. Computationally expensive ii. Performance sensitive to the choice of 'k' iii. Not suitable for high-dimensional data without preprocessing	Voltage, current, and power
[166]	2025	Data-Driven Unknown Input Observer (UIO)	Data-driven	FDI	Technical	i. Detects and localizes FDI attack effectively in communication links ii. Uses fewer data samples compared to ML methods	i. Relies on the quality of data ii. Computationally intensive for large systems iii. Sensitive to noise and disturbances in system data	Voltage, and current
[167]	2025	Data-driven I/O Model	Supervised learning	FDI	Technical	i. Detects and localizes FDI attacks based on I/O model ii. Adaptive detection threshold improves performance iii. Uses process data for attack detection without system model	i. Sensitive to model error and disturbances ii. Computationally intensive iii. Requires high-quality and synchronized data	Voltage, and current
[168]	2025	Actor-Critic Proximal Policy Optimization (PPO)	Reinforcement Learning	Load-Altering Attacks	Technical	i. Model-free and multi-agent framework ii. Mitigates frequency deviation caused by EV load-switching attacks iii. Handles external disturbances and parametric uncertainties effectively	i. Requires adequate data for training ii. High computational cost iii. Complexity in coordinating multiple DERs	Frequency
Koduru et al.	2025	Hybrid Physics-Informed Neural Network (HPINN)	Data-driven and Model-based	FDI	Technical	i. Combines Kalman filter-based state estimation with NN ii. Mitigates cyber-attacks effectively while maintaining system stability	i. Requires careful tuning of hybrid parameters ii. Computationally demanding	Voltage, and current

transmitted data inputs within the control layer, they potentially result in inaccurate frequency control decisions. This attack generally involves injecting falsified variables by gaining unauthorized access to communication pathways, measurement devices, or sensory networks. These disruptions target frequency deviation and tie-line power signals, which reduce data integrity and compromise control loop efficiency. For example, manipulating frequency deviation signals for i^{th} area of the IMG can be defined as:

$$\delta C_r^* = \mathcal{G}_{sc,i}\left((\delta f_i(t)+\Psi_i(t)) + \sum_{j=1,j\neq i}^{K} \delta\tau_{\text{tie},ij}(t)\right)$$

Here, the terms Ψ_i and δC_r^* represent the malicious signal injected into the communication pathway to disrupt the system performance and corrupt the control signal, respectively.

6.1.2. Data-driven cyber-attack detection and mitigation framework

This case study introduces a data-driven framework to identify and mitigate cyberattacks in the secondary control layer (SCL) of a two-area interconnected IMG. This framework incorporates the Laplace approximation method to integrate Bayesian inference, allowing for nonlinear modeling and exogenous input integration. This paper primarily aims to create a model-free framework that addresses the challenges of model-based methods while also overcoming the high computational demands of current data-driven techniques by facilitating faster convergence during training. This allows for quicker updates and re-calibrations of the model parameters when new data arrive, making the proposed framework a powerful tool for real-time threat detection. The mathematical framework of the studied model is elaborated on in the following section.

Consider a mathematical mapping showing the connection between the network's input-output dynamics and predicted outputs in the time-varying domain as:

$$\delta\hat{C}_{r,i}(t) = f(\mathcal{N}_i(t-1),\ldots,\mathcal{N}_i(t-d_{\mathcal{N}}),\delta C_{r,i}(t-1),\ldots,\delta C_{r,i}(t-d_{\delta C_r}),\vartheta), \tag{5}$$

In (5), $\mathcal{N}_i(t) = [\delta f_i \ \sum_{j=1,i\neq j}^{K}\delta\tau_{tie,ij}]$ and $\delta\hat{C}_{r,i}$ represent the input to the network and the predicted output of the i^{th} area of IMG, respectively, concerning the parameter ϑ. The output estimation relies on prior time-series inputs $\mathcal{N}_i$ and outputs $\delta C_{r,i}$. Here, $d_{\mathcal{N}}$ and $d_{\delta C_r}$ are positive integers indicating the memory order of the network's inputs and outputs. The work in [171] develops a cyber-resilient framework based on the recurrent neural network without integrating Bayesian learning. While this method effectively addresses cyber issues on DC microgrids, it demands substantial computational resources, which can hinder its real-time application. The fundamental modeling of the proposed framework is described in [171] without Bayesian learning. The use of Laplace approximation within the Bayesian framework in the proposed framework enhances its computational efficiency by maximizing the posterior distribution. This allows for faster updates and recalibrations of the model parameters when new data arrive, making the proposed framework a powerful tool for real-time threat detection.

Now, as per the Bayesian rule, we can define the notion of posterior distribution for the given parameters ϑ and data $\mathbb{D}$ as follows:

$$\mathbb{P}(\vartheta|\mathbb{D}) = \frac{\mathbb{P}(\mathbb{D}|\vartheta)\cdot\mathbb{P}(\vartheta)}{\mathbb{P}(\mathbb{D})}, \tag{6}$$

where $\mathbb{P}(\vartheta|\mathbb{D})$ indicates the posterior distribution of parameters, $\mathbb{P}(\mathbb{D}|\vartheta)$ defines likelihood, representing how probable the observed data is under the parameters, $\mathbb{P}(\vartheta)$ is prior belief, and $\mathbb{P}(\mathbb{D})$ is the marginal likelihood of the given parameters. Now, it is assumed that the observations of the data are corrupted by noise with standard deviation α, the likelihood of the dataset $\mathbb{D} = \{(Y(t),\mathcal{N}(t))\}_{t=1}^{\mathbb{T}}$ is given by:

$$\mathbb{P}(\mathbb{D}|\vartheta) = \prod_{t=1}^{\mathbb{T}} \frac{1}{\sqrt{2\pi\alpha^2}} \exp\left(-\frac{(Y(t)-f(\delta\hat{C}_r,\mathcal{N};\vartheta))^2}{2\alpha^2}\right).$$

Here, $Y(t)$ is the actual output at time t, and $f(\delta\hat{C}_r,\mathcal{N};\vartheta)$ is the model's prediction based on prior outputs and exogenous inputs. Now, taking the logarithm of the likelihood, which simplifies the product into a sum:

$$\log\mathbb{P}(\mathbb{D}|\vartheta) = -\sum_{t=1}^{\mathbb{T}}\left[\frac{(Y(t)-f(\delta\hat{C}_r,\mathcal{N};\vartheta))^2}{2\alpha^2} + \frac{1}{2}\log(2\pi\alpha^2)\right]$$

This leads to the negative log-posterior, often known as a regularized loss function:

$$\mathcal{L}(\vartheta) = \sum_{t=1}^{\mathbb{T}}\frac{(Y(t)-f(t;\vartheta))^2}{2\alpha^2} - \log\mathbb{P}(\vartheta), \tag{7}$$

which is minimized to obtain the Maximum a Posteriori (MAP) estimate:

$$\vartheta_{\text{MAP}} = \arg\min_{\vartheta}\mathcal{L}(\vartheta). \tag{8}$$

This estimation simplifies Bayesian inference by enabling the Laplace approximation, which approximates the posterior distribution as a Gaussian centered at ϑ_{MAP}. This is done using a second-order Taylor expansion of the log-posterior around the MAP estimate, thereby reducing the computational burden of exact Bayesian inference.

$$\log\mathbb{P}(\vartheta|\mathbb{D}) \approx \log\mathbb{P}(\vartheta_{\text{MAP}}|\mathbb{D}) - \frac{1}{2}(\vartheta-\vartheta_{\text{MAP}})^T H(\vartheta-\vartheta_{\text{MAP}}),$$

where H is the Hessian matrix of the negative log-posterior evaluated at ϑ_{MAP} that can be defined as:

$$H = \nabla^2\mathcal{L}(\vartheta)\Big|_{\vartheta=\vartheta_{\text{MAP}}}. \tag{9}$$

Thus, the posterior is approximated by:

$$\mathbb{P}(\vartheta|\mathbb{D}) \approx \mathcal{N}(\vartheta_{\text{MAP}}, H^{-1}). \tag{10}$$

The approximation of the posterior distribution enables the framework to estimate the local IMG measurements in the presence of attacks that pass through the error block to generate the subsequent error as:

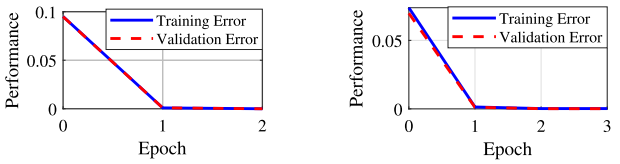
$$E_i = \delta\hat{C}_{r,i}(t) - \delta C_{r,i}^*(t) \tag{11}$$

In (11), the term $\delta\hat{C}_{r,i}(t)$ indicates the estimated control error for i^{th} IMGs. If the system operates under normal conditions and the studied framework functions properly, the estimation error value will converge to 0 for all IMGs. Thus, the operation of the system under normal conditions behaves as follows:

$$\lim_{t\to\infty} E_i = 0 \tag{12}$$

The PI controller in the mitigation layer utilizes the estimated error signal to generate an attack-compensating signal $\mathcal{M}_{c,i}(t)$, which is then combined with the corrupted communication signals before being sent to the SCL. This enables a coordinated response to mitigate the effects of the attacks. The entire detection and mitigation process for the studied data-driven approach is illustrated in Fig. 5.

Remark 1. When the two-area connected MGs experience an attack on the local communication of the secondary control layer, the estimator for the affected IMG will exhibit a prominent estimation error characterized by a sharp spike during the initial sampling phase, followed by either a stabilization of the error or an inability to converge to zero. In contrast, spikes induced by load changes will eventually diminish and converge to zero over time.



(a) Training error for area 1 (b) Training error for area 2

Fig. 6. Training performance of the studied framework.

6.2. Performance evaluation

6.2.1. Training data generation for studied framework

The studied data-driven framework for detecting injected attacks and compromised channels critically relies on system data acquisition. The detailed process of collecting the training data is given as follows:

(i) *Data sources:* The dataset used in this work is entirely generated through simulation. The system depicted in Fig. 4 was simulated in MATLAB using the parameters listed in [171]. The simulation was performed under normal operating conditions of the MG system, reflecting typical behavior without any explicit attack scenarios. It was designed to replicate the real-world operation of the MG, incorporating typical load variations and other system dynamics that occur during normal operation.

(ii) *Sample Size:* The dataset consists of 1,000,000 data samples generated from a 50-s simulation, which includes periods of normal operation as well as a load variation between 20–25 s. These 1,000,000 samples cover the entire simulation period, with inputs such as frequency measurements, tie-line power signals, and the target variable, such as the local ACE signal.

(iii) *Quality Control:* Since the dataset was generated under controlled conditions to mimic real-world operations, no synthetic measurement noise was introduced, eliminating the need for any filtering. It was also ensured that the data was transmitted without any loss of information under normal conditions. However, we use dropout during training to mimic missing values, randomly ignoring a subset of data points to improve model generalization.

This extensive dataset is then utilized to train the proposed DNN framework, enabling it to accurately detect attack signals in the communication channels of the INMG. Since the dataset consists entirely of normal operation data with load changes, there is no inherent class imbalance between normal and attack scenarios. The load change was part of the simulation, and the model is trained to learn the temporal dependencies within the data, capturing how the ACE signal evolves under normal and load variation conditions. After training, when new data is presented, the model uses the learned patterns to estimate the ACE signal based on the observed input data. It is important to note that an attack is detected based on the estimation error, which is the difference between the measured and estimated outputs.

6.2.2. Faster convergence of the studied framework

Fig. 6 shows the training efficacy of the studied method for both areas of IMGs, as indicated by the training and validation errors, while Table 9 lists their quantitative error measurements. These responses exhibit the high computational efficiency of the studied framework, especially in terms of training time and accuracy. The model reaches minimal training error in only two epochs for both areas of IMGs, taking about 4 s, which underscores the quick convergence of the studied framework. Moreover, the reduced mean absolute error (MAE) and root mean square error (RMSE) further confirm the framework's efficacy in estimating the target variables.

Table 9
Training results with estimated error of the studied framework.

Scenarios	Training time (s)	Epoch to reach a minimum	MAE	MSE	RMSE
1	4.0906	2	3.40×10^{-05}	3.439×10^{-05}	0.00584
2	4.6089	2	3.24×10^{-05}	3.34×10^{-05}	0.00584

6.2.3. Performance of studied framework under constant FDI attack on frequency signal

To evaluate the effectiveness of the studied framework, a scenario involving load fluctuations and persistent FDI attacks is considered. In this setup, adversaries exploit local communication links to manipulate frequency deviations by injecting false data. The assessment process spans detection, estimation, and mitigation phases, as depicted in Fig. 7. Specifically, Fig. 7(a) illustrates the frequency deviation responses of two areas of IMGs affected by load variations occurring between t = 20–25 s. Subsequently, a constant FDI attack with a magnitude $\Psi = 0.3$ is launched at t = 30 s, interfering with the normal frequency behavior. This scenario highlights the critical need for advanced techniques capable of effective attack detection and mitigation. The attack detection process starts by measuring the estimation error between the predicted and actual control signal for both areas of the IMG. The estimation error for both areas is illustrated in Fig. 7(b), revealing that only the area 1 estimator exhibits a significant spike at $t = 30$ s, followed by a stable error. This pattern indicates the presence of the attack signal in the local communication channel of area 1, as mentioned in Remark 1. Notably, during the load changes from t = 20–25 s, the estimation error stays minimal and ultimately approaches 0. This analysis demonstrates how the studied method successfully distinguishes natural system dynamics from cyberattack incidents, allowing for accurate attack detection without generating false positives and facilitating an effective mitigation process. The mitigation process feeds the estimated error into a PI controller, generating a countermeasure signal that neutralizes the attack within the corrupted communication path before reaching the secondary controller. The attack mitigation response, driven by the estimated error, is shown in Fig. 7(c). This result validates the framework's ability to ensure the cyber-safe operation of the IMG.

6.2.4. Performance of studied framework under hybrid attack on frequency signal

In practical operations, communication within the IMG system is susceptible to delays and data inaccuracies, often caused by factors such as network congestion, data packet transmission rates, or inadequate encryption mechanisms. An attacker can exploit these vulnerabilities to execute latency attacks, wherein intentional delays are introduced to disrupt timely data transmission. Such disruptions can impair decision-making processes and destabilize the system. Therefore, evaluating the effectiveness of cyber-security measures against such attacks is crucial for the secure operation of IMGs. Thus, the efficacy of the studied framework is assessed through an attack scenario involving FDI and latency attacks. Here, a latency attack causes delays of 0.7 s in the communication network. Similar to the previous experimental setup, the combined attack is injected into the local communication channel of area 1 at t = 30 s. In Fig. 8(a), the measurement of frequency deviation response under this scenario is shown. Based on Remarks 1 and 2, and the estimated error for both areas shown in Fig. 8(b), it is evident that the attack occurs in the frequency communication channel of area 1. In response, the mitigation layer employs the computed estimation error to construct a compensatory signal, which is then superimposed onto the original signal before transmission through the compromised channel. The attacked frequency deviation response after mitigation for both areas of the IMG is illustrated in Fig. 8(c). Initially, some oscillatory behavior is observed due to the injection of the hybrid attack, but these oscillations diminish over time, eventually converging to zero. The results affirm that the

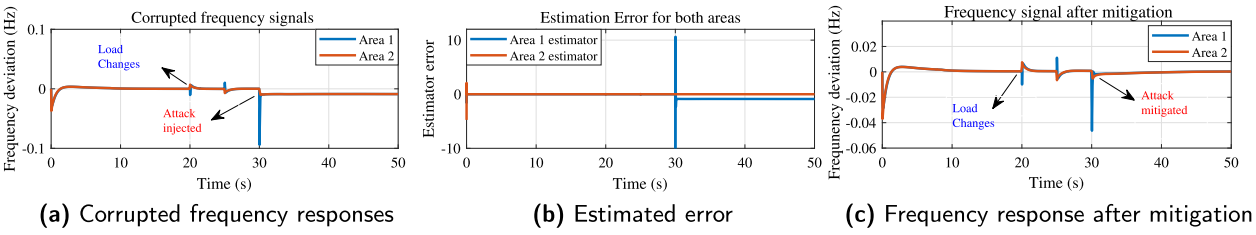


Fig. 7. Performance evaluation of the studied framework under constant FDI attack.

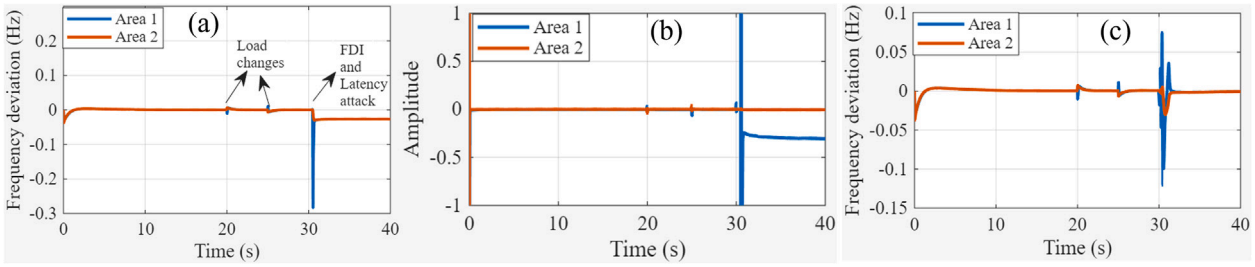


Fig. 8. Performance evaluation of the studied framework under the study of simultaneously applying FDI and latency attack on frequency signal (a) Frequency response, (b) Estimated error for both areas, and (c) Attacked frequency responses after mitigation.

studied framework not only detects such cyber threats with precision but also demonstrates effective mitigation capabilities under complex attack conditions.

6.2.5. Scalability assessment of the studied framework

The studied framework employs decentralized inputs for estimating the target outputs of local IMGs. In contrast, a centralized detection mechanism, based on the dynamic behavior of the estimated signals, is utilized to identify potential attack signals affecting those IMGs. Owing to the decentralized nature of its input structure, the framework exhibits high scalability, making it suitable for the deployment in large-scale interconnected IMG systems. To measure its scalability, an experiment involving six IMGs as shown in Fig. 9(a) is simulated, where an FDI attack is triggered at t = 20 s in the local channel of area 1 IMG, and the frequency response is illustrated in Fig. 9(b). The error estimation from the local estimators, shown in Fig. 9(c), demonstrates that the attack injected into area 1 IMG is easily detectable, as the local estimator for IMG 1 displays a notable error, as explained in Remark 1. Finally, the mitigated performance is illustrated in Fig. 9(d), demonstrating that the studied framework can effectively mitigate the impact of attacks across multiple IMGs. This assessment confirms that the framework successfully detects and mitigates attacks in a scalable way across a larger network.

6.2.6. Comparative analysis and discussion

Table 10 presents a comprehensive comparison of the proposed method with several recent state-of-the-art approaches designed to enhance cybersecurity for MGs. The selected methods include both model-based and data-driven frameworks as reported in [42,94,170,172], and [173]. While it is true that several studies have already applied machine learning or data-driven models for detecting cyber threats, the studied method described in the case study distinguishes itself in the following key aspects:

(i) **Concurrent detection and mitigation of attacks:** The studied method in the case study employs concurrent detection and mitigation of attacks, which are essential for maintaining the security and resilience of MGs. While several methods rely on fixed threshold values for attack detection, the studied approach stands out by using dynamic patterns of estimated responses, as noted in Remark 1. This enables more accurate identification of attacks and enhances the system's adaptability to evolving attack patterns. By seamlessly integrating attack detection with estimation and control modules, the studied method enables easy real-time adjustments to mitigation strategies, ensuring an adaptive response without performance degradation. The dynamic response pattern enhances system resilience by easily distinguishing performance deviations due to load changes and attacks, thereby continuously providing adaptive security against threats and maintaining stable operation during attacks.

Remark 2. In normal operation of the interconnected IMG, two communication channels—local and global—are used to enable fast data transmission without any loss of information. The identification of the compromised channel depends on the characteristics of the observed spikes. If a spike occurs only in the initial sampling of the local area estimator's response, it indicates an attack on the local communication channel. However, if both areas' estimators exhibit sharp spikes, this suggests a breach in the global communication channel, with one of the estimators possibly converging to zero.

(ii) **Compromised channel detection:** The significant improvement of the studied method is its ability to detect the compromised channels of multi-area connected MG, as detailed in Remark 2. Unlike traditional methods, which generally focus on system-wide detection, the proposed framework incorporates a mechanism that pinpoints the exact communication channel affected by the attacks. This detection enables more precise and targeted mitigation strategies, ensuring that only the compromised channel is addressed, thus minimizing the impact on unaffected channels. The ability to swiftly adapt to compromised communication channels, even in unforeseen situations, minimizes unnecessary strain on the system. Overall, the ability to detect compromised communication channels makes the studied approach more adaptive, efficient, and effective in securing microgrid operations compared to existing techniques.

(iii) **Rapid convergence:** The convergence rate of the learning framework is crucial for the applications that require real-time detection and control, such as in MG security. The studied approach excels in achieving rapid convergence, which is essential for

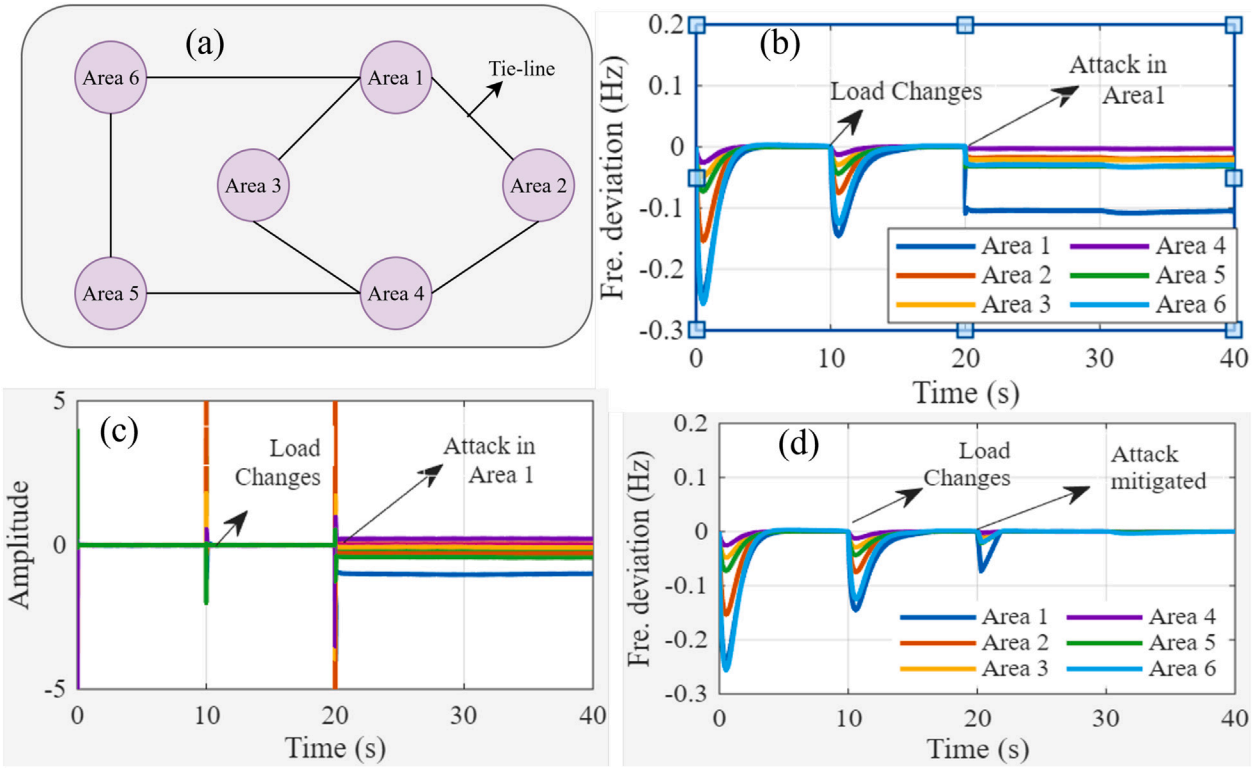


Fig. 9. Scalability assessment of the proposed framework under constant FDI attack: (a) Configuration of INMG, (b) Frequency response, (c) Estimation error, (d) Frequency post-mitigation.

Table 10
Comparison of the studied method with others.

Method features	[172]	[170]	[94]	[42]	[173]	Studied approach
Learning-based scalability	N/A	✓	N/A	✓	N/A	✓
Attack mitigation	✓	✓	✓	✓	✓	✓
FDI attack detection	✓	✓	✓	✓	✓	✓
Compromised area detection	×	×	×	×	×	✓
Compromised channel detection	×	×	×	×	×	✓
Rapid convergence	N/A	×	N/A	×	N/A	✓
FDI + Latency attack	×	×	×	×	×	✓

quickly identifying and mitigating threats in dynamic environments. Unlike most existing methods, which either do not prioritize or exhibit slower convergence rates, the studied method is designed to achieve high convergence, which is significant as it enables the framework to learn from incoming data and apply the learned knowledge immediately to real-time decision-making processes. Most traditional methods fail to incorporate rapid convergence, resulting in slower responses to threats and making them less suitable for real-time operations. In contrast, the studied approach's ability to converge rapidly enables it to effectively address threats without compromising system performance, ensuring a more reliable and responsive MG operation.

(iv) **Learning-based scalability:** The studied method introduces enhanced scalability for MG systems by utilizing learning-based principles and decentralized inputs, enabling efficient deployment across various configurations. Several existing methods, as shown in Table 10, attempt to address scalability but rely on comprehensive data from every DGU, which can overwhelm the system with large volumes of information. This approach slows down performance and makes it less suitable for large-scale systems. In contrast, the studied approach focuses solely on inputs from neighboring areas or DGUs. This targeted input reduces the data processing load, making the framework more efficient and scalable for larger-scale MGs.

Overall, the studied method described in the case study demonstrates a more holistic cybersecurity framework, combining detection, estimation, and mitigation with enhanced observability of both physical and cyber layers in an MG. These features make it well-suited for deployment in dynamic and complex energy systems where adaptability and cyber-resilience are crucial.

7. Challenges and future trends

7.1. Implementation challenges

7.1.1. Data integration and fusion

MG cyber-resilience requires integrating and fusing data from disparate sources, including sensors, control systems, and external threat intelligence feeds. However, integrating heterogeneous data sources with varying formats and frequencies poses data fusion and synchronization challenges. Developing robust data integration pipelines, standardizing data formats, and implementing data fusion techniques are crucial for deriving actionable insights from diverse data sources.

7.1.2. Real-time processing

Timely detection and response to cyber threats are critical to ensuring the resilience of MG infrastructure. However, processing and analyzing large volumes of data in real time to detect anomalies and trigger appropriate responses presents significant challenges. Implementing efficient real-time data processing frameworks, stream processing technologies, and automated response mechanisms is essential for minimizing response times and mitigating the impact of cyber attacks on MG operations.

7.1.3. Implementing edge computing in MGs [174]

The major challenge for implementing edge computing is to manage real-time data processing demands, as MGs operate in highly dynamic environments where rapid decision-making is crucial, especially during events like cyber-attacks. It also aims to overcome the latency of centralized systems by processing data locally, but integrating and optimizing this capability across distributed MG components can be complex. Another key challenge is ensuring data privacy and security. While edge computing minimizes data transmission to centralized servers, securing local nodes with strong encryption and anomaly detection is still crucial. As MGs expand and incorporate more DERs, scalability becomes a pressing concern. Managing large volumes of data across various edge nodes without overloading central infrastructure requires careful planning and architectural design. Additionally, interoperability with existing legacy systems in MGs poses a challenge, as older infrastructure cannot natively support edge technologies. While edge computing greatly enhances the resilience, security, and scalability of MGs, overcoming these challenges is essential for its effective implementation.

7.1.4. Implementing federated learning [175]

Federated learning in MGs faces key challenges in data privacy, security, and model accuracy. While it enables model training without transferring sensitive data, securing communication between devices and the central server is essential. Another challenge for the implementation of federated learning in MGs is to ensure the model accuracy and consistency across decentralized nodes. Since models are trained on diverse devices, potentially incomplete data from various MG components, differences in devices, and data distributions can lead to inconsistencies or biases, affecting the model's generalizability. Additionally, the computational burden and limited resources make it challenging to train machine learning models efficiently, especially in remote areas. Furthermore, frequent communication for model updates requires high bandwidth, which can lead to latency issues, particularly in large, distributed microgrids. While federated learning has the potential to significantly enhance the performance and security of microgrids by enabling decentralized, privacy-preserving machine learning, overcoming challenges related to data privacy, model accuracy, computational constraints, communication overhead, and training time is essential for its successful implementation in MG environments.

7.1.5. Quality and availability of data

The success of data-driven techniques heavily relies on the quality and availability of data. In many cases, MG data may be incomplete, inconsistent, or noisy, which can hinder the performance of algorithms and lead to inaccurate results. Ensuring data integrity and implementing robust data collection mechanisms are essential challenges to overcome.

7.1.6. Lack of scalability

MG environments generate vast amounts of data from diverse sources, including sensors, smart meters, and control systems. Scaling data-driven techniques to handle large volumes of data efficiently while maintaining real-time performance is a significant challenge. Thus, implementing scalable algorithms, distributed computing frameworks, and efficient data processing pipelines is fundamental for addressing scalability and performance challenges.

7.1.7. Interoperability

An MG system comprises diverse parts from multiple vendors, each with unique interfaces, protocols, and data formats. Because of incompatibilities, data silos, and proprietary standards, integrating and coordinating data-driven procedures across various disparate systems can be difficult. Creating standardized data models, protocols, and interfaces can aid in overcoming interoperability and complexity issues.

7.1.8. Interpretability and subject awareness

Cybersecurity and power systems subject expertise are prerequisites for successfully applying data-driven approaches. It is imperative to comprehend the distinct attributes of MG infrastructure, operational limitations, and cyber threats to develop and implement appropriate algorithms. Additionally, algorithmic outputs must be interpretable for human operators to comprehend, trust, and act upon cybersecurity insights produced by data-driven methodologies.

7.1.9. Lack of real-time communication network performance

Effective communication networks are crucial for the real-time deployment of data-driven methods in MGs' cyber-resilience, as these approaches depend on the uninterrupted and prompt flow of data to operate effectively. Data-driven cyber defense systems rely on real-time data streams from diverse MG sensors and devices to identify anomalies, forecast failures, and counter cyber threats. Nevertheless, these approaches face challenges related to the performance of the communication network, including its reliability, speed, and resilience. High latency, data packet loss, and network congestion can delay critical data transmission, leading to slower threat detection and response times [176]. This delay can prevent the cyber defense system from reacting swiftly to emerging threats, thereby compromising the MG's security and operational stability. Additionally, MGs often operate in decentralized, heterogeneous environments with diverse communication technologies, making it even more challenging to maintain consistent network performance. To effectively deploy data-driven methods in real-time, it is essential to ensure a resilient, delay-tolerant communication infrastructure capable of handling large data volumes and minimizing disruptions to support timely and effective defense mechanisms.

7.2. Future research trends

7.2.1. Securing quantum-safe communication

As quantum computing capabilities advance, traditional cryptographic algorithms used to secure communication channels in MGs are increasingly vulnerable to quantum-based attacks. In the context of MGs, secure communication is crucial to maintaining grid stability, as it ensures the safe and reliable transmission of data across DERs, control systems, and EMS. The quantum-safe communication techniques, such as quantum-resistant encryption algorithms and quantum key distribution protocols, provide robust security by safeguarding sensitive data against the potential threats posed by quantum computers. Moreover, the quantum-safe measures ensure that the integrity and confidentiality of data transmitted within the MG network remain intact, even in the face of quantum-enabled cyber-attacks [177]. This is especially important as MGs become more interconnected and depend on real-time data for efficient operation and decision-making. By proactively adopting quantum-safe communication technologies, MG operators can safeguard critical infrastructure, prevent unauthorized access, and mitigate emerging cyber threats, thereby enhancing the overall resilience and reliability of the MG system. Furthermore, as the threat landscape evolves, MGs need to stay ahead by supporting research and development efforts to tailor quantum-safe communication solutions to the unique requirements of decentralized, multi-layered MG environments. This will ensure long-term security and the protection of MGs as they integrate new technologies, including RESs, storage systems, and advanced control algorithms.

7.2.2. Implementing advanced data integration models

MGs require advanced data integration strategies to address the issues of collecting and pre-processing data. The integration of various MG components and external data sources requires the implementation of middleware solutions capable of handling different data formats and protocols [178]. A middleware platform can facilitate seamless communication throughout the MG system by standardizing and translating data from diverse devices. Additionally, the use of unified data standards, such as the Common Information Model (CIM) [179], can enable uniform data representation across different systems, streamlining the integration and fusion process. The development of a robust data preprocessing pipeline is essential for cleaning, normalizing, and synchronizing data from disparate sources. These integrations can effectively address data-handling challenges and empower the data-driven approaches for enhancing cyber-security in MGs.

7.2.3. Enabling distributed ledger technology

Enabling Distributed Ledger Technology (DLT) can be crucial in enhancing MGs' cyber security. It offers a decentralized and immutable framework for recording transactions and data exchanges within the MG, ensuring transparency, integrity, and security [180]. By leveraging this technology, MG systems can secure communication between DERs, grid operators, and consumers, preventing unauthorized access and tampering. Each transaction or data entry is cryptographically signed and linked to previous entries, making it virtually impossible for malicious actors to alter records without detection. Additionally, smart contracts—self-executing contracts with the terms directly written into code—can automate and secure MG operations, such as energy trading and demand response, reducing the risk of human error and cyber-attacks. Implementing DLT in MG infrastructures fortifies against cyber threats and enhances operational efficiency, trust, and resilience, ensuring a robust and secure energy distribution system.

7.2.4. Enhancing communication network resilience for real-time cyber defense

The limited performance of communication networks hampers the real-time deployment of data-driven cybersecurity approaches in MGs. One solution is to adopt edge computing, which processes data near its source [181]. This reduces latency and lessens the dependence on long-distance data transmission, thereby enhancing real-time responsiveness. Another solution is to utilize redundant communication paths, which ensure continuous data transmission and thereby improve network resilience [182]. Additionally, network slicing and prioritization [183] enable critical cyber defense data to be transmitted with higher precedence, while low-latency network protocols [184], such as Time-Sensitive Networking (TSN) and 5G, ensure rapid data delivery, facilitating swift threat detection and response. Moreover, decentralized [185] and fault-tolerant communication protocols [186] help the network recover swiftly from disruptions. These strategies enable data-driven methods to address communication challenges, maintaining a continuous data flow that is crucial for real-time cyber defense of MGs. Furthermore, optimizing network performance under changing conditions with machine learning algorithms and incorporating emerging technologies like blockchain can further boost MG cyber-resilience by reinforcing data-driven approaches.

7.2.5. Facilitating cross-domain security

Cross-domain security intelligence can be utilized to enhance the cyber-security of MG by integrating and analyzing data from various domains such as information technology (IT), operational technology (OT), and physical security systems [187]. This comprehensive approach provides a more holistic understanding of potential threats and vulnerabilities. By sharing security intelligence across these domains, MG operators can detect and respond to sophisticated cyber threats that might go unnoticed when monitoring each domain in isolation. Cross-domain intelligence facilitates the correlation of disparate data points, uncovering patterns and compromise indicators crucial for early threat detection. Furthermore, this integrated security strategy supports real-time situational awareness and coordinated incident response, enhancing the overall resilience of the MG. The collaboration and data sharing between IT, OT, and physical security teams enable a unified defense strategy, reducing the risk of cyber-attacks and ensuring energy distribution systems' reliable and secure operation.

7.2.6. Enabling interpretable data-driven techniques

The use of data-driven cybersecurity techniques in MGs relies on the interpretability of the model. To ensure that complex data-driven models' outputs are understandable for human operators, it's important to incorporate explainable AI techniques. For instance, in an MG system, an explainable AI model could identify specific data patterns or anomalies that lead to a particular security alert, enabling operators to grasp the reasoning behind the AI's decision. Again, human judgment and machine efficiency can be combined through human-in-the-loop systems, allowing operators to monitor and confirm the outputs. This integration with explainable AI could be an effective solution to enhance the effectiveness and reliability of data-driven cyber-security measures in MGs.

8. Conclusion

This research provides a thorough analysis of how MGs can operate resiliently in the face of cyber threats, highlighting the importance of using data-driven techniques to secure MG networks. The energy sector has evolved with the increased use of DERs and digital technology, making it crucial to protect these networks from cyber-attacks. While model-based approaches have been effective in some cases, they have limitations in dynamic, real-time situations, making it important to explore alternative options. Data-driven approaches offer a practical way to provide more flexible and adaptable responses to evolving threats. This study focused on the progress, challenges, and potential applications of data-driven approaches to ensure the cyber-resilient operation of MGs. It emphasized key components and implementation strategies for enhancing cyber-security while addressing limitations related to data collection, computing costs, and system adaptability. This was achieved by focusing on technical, financial, and regulatory frameworks. Furthermore, this research explored a case study on the application of Bayesian learning-based data-driven techniques for enhancing the cyber-resilience of the load frequency control model in interconnected IMGs. The findings provide valuable insights for the industry on how these data-driven techniques can strengthen the overall resilience of MGs, offering improved safe operation against cyber threats and enabling more scalable, adaptable solutions for future challenges. Based on this assessment, it became clear that data-driven solutions have significant potential for improving MG cybersecurity. However, additional research and development are needed to properly integrate these methodologies and eliminate existing barriers. The proposals aim to encourage further research and innovation in this vital field, paving the way for more resilient, scalable, and adaptable cybersecurity solutions for MG infrastructures.

CRediT authorship contribution statement

Subrata K. Sarker: Writing – original draft, Investigation, Formal analysis, Data curation, Conceptualization. **Hamidreza Shafei:** Writing – original draft, Visualization, Formal analysis, Data curation. **Li Li:** Writing – review & editing, Visualization, Validation, Supervision. **Ricardo P. Aguilera:** Writing – review & editing, Visualization, Validation, Supervision. **M.J. Hossain:** Writing – review & editing, Visualization, Validation, Supervision. **S.M. Muyeen:** Writing – review & editing, Validation, Supervision, Methodology, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available upon request.

References

[1] Uddin M, Mo H, Dong D, Elsawah S, Zhu J, Guerrero JM. Microgrids: a review, outstanding issues and future trends. Energy Strateg Rev 2023;49:101127.
[2] Mishra S, Anderson K, Miller B, Boyer K, Warren A. Microgrid resilience: a holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. Appl Energy 2020;264:114726.
[3] Yousef MY, Mosa MA, Masry SME, Ghany AA, Ali A. Decentralized utilization of distributed energy storage resources for simultaneous frequency regulation in a microgrid. J Energy Storage 2024;86:111357.
[4] Saeed MH, Fangzong W, Kalwar BA, Iqbal S. A review on microgrids' challenges & perspectives. IEEE Access 2021;9:166502–17.
[5] Gholami M, Muyeen S, Mousavi SA. Optimal sizing of battery energy storage systems and reliability analysis under diverse regulatory frameworks in microgrids. Energy Strateg Rev 2024;51:101255.
[6] Mariam L, Basu M, Conlon MF. Microgrid: architecture, policy and future trends. Renew Sustain Energy Rev 2016;64:477–89.
[7] Ishraque MF, Shezan SA, Rashid M, Bhadra AB, Hossain MA, Chakrabortty RK, et al. Techno-economic and power system optimization of a renewable rich islanded microgrid considering different dispatch strategies. IEEE Access 2021;9:77325–40.
[8] Colucci R, Mahgoub I, Yousefizadeh H, Al-Najada H. Survey of strategies to optimize battery operation to minimize the electricity cost in a microgrid with renewable energy sources and electric vehicles. IEEE Access 2024.
[9] Nivolianiti E, Karnavas YL, Charpentier J-F. Energy management of shipboard microgrids integrating energy storage systems: a review. Renew Sustain Energy Rev 2024;189:114012.
[10] Shafei H, Li L, Aguilera RP. A comprehensive review on cyber-attack detection and control of microgrid systems. Power Syst Cybersecurity Methods Concepts Best Pract 2023:1–45.
[11] Shi J, Ma L, Li C, Liu N, Zhang J. A comprehensive review of standards for distributed energy resource grid-integration and microgrid. Renew Sustain Energy Rev 2022;170:112957.
[12] Rani P, Parkash V, Sharma NK. Technological aspects, utilization and impact on power system for distributed generation: a comprehensive survey. Renew Sustain Energy Rev 2024;192:114257.
[13] Tang Z, Zhang P, Krawec WO. A quantum leap in microgrids security: the prospects of quantum-secure microgrids. IEEE Electrification Mag 2021;9:66–73.
[14] Shafei H, Farhangi M, Aguilera RP, Alhelou HH, et al. A novel cyber-attack detection and mitigation for coupled power and information networks in microgrids using distributed sliding mode unknown input observer. IEEE Trans Smart Grid 2024.
[15] De Caro F, Collin AJ, Giannuzzi GM, Pisani C, Vaccaro A. Review of data-driven techniques for on-line static and dynamic security assessment of modern power systems. IEEE Access 2023;11:130644–73.
[16] Koduru SS, Machina VSP, Madichetty S, Mishra S. Securing DC microgrids against cyber-attacks: hybrid physics-informed neural network control strategy with real-time implementation. IEEE J Emerg Sel Top Power Electron 2025.
[17] Solat A, Gharehpetian GB, Naderi MS, Anvari-Moghaddam A. On the control of microgrids against cyber-attacks: a review of methods and applications. Appl Energy 2024;353:122037.
[18] Rouhani SH, Su C-L, Mobayen S, Razmjooy N, Elsisi M. Cyber resilience in renewable microgrids: a review of standards, challenges, and solutions. Energy 2024:133081.
[19] Beg OA, Khan AA, Rehman WU, Hassan A. A review of AI-based cyber-attack detection and mitigation in microgrids. Energies 2023;16:7644.
[20] Shrivastava S, Subudhi B. Comprehensive review on hierarchical control of cyber-physical microgrid system. IET Gener Transm Distrib 2020;14:6397–416.
[21] Liu M, Teng F, Zhang Z, Ge P, Sun M, Deng R, et al. Enhancing cyber-resiliency of DER-based smart grid: a survey. IEEE Trans Smart Grid 2024;15(5):4998–5030.
[22] Callenes J, Poshtan M. Dynamic reconfiguration for resilient state estimation against cyber attacks. IEEE Trans Emerg Top Comput 2023;12(2):559–71.
[23] El-Ebiary AH, Attia MA, Awad FH, Marei MI, Mokhtar M. Kalman filters based distributed cyber-attack mitigation layers for DC microgrids. IEEE Trans Circuits Syst I Regul Pap 2024.
[24] Vafamand N, Razavi-Far R, Arefi MM, Saif M. Fuzzy EKF-based intrusion detection and accurate state estimation of interconnected DC MGs with CPLs. IEEE Trans Power Syst 2023;38(6):5245–56.
[25] Kachhwaha M, Modi H, Nehra MK, Fulwani D. Resilient control of DC microgrids against cyber attacks: a functional observer based approach. IEEE Trans Power Electron 2023;39(1):459–68.
[26] Ahsan F, Dana NH, Sarker SK, Li L, Muyeen S, Ali MF, et al. Data-driven next-generation smart grid towards sustainable energy evolution: techniques and technology review. Prot Control Mod Power Syst 2023;8:1–42.
[27] Badal FR, Das P, Sarker SK, Das SK. A survey on control issues in renewable energy integration and microgrid. Prot Control Mod Power Syst 2019;4:1–27.
[28] Michaelson D, Jiang J. Review of integration of small modular reactors in renewable energy microgrids. Renew Sustain Energy Rev 2021;152:111638.
[29] Aboelezz AM, El-Saadawi MM, Eladl AA, Sedhom BE. IEC 61850 communication-based pilot distance protective IED for fault detection and location in DC zonal shipboard microgrid. IEEE Trans Ind Appl 2023;59:5559–69.
[30] Zhou Y, Liu X, Zhao Q. A stochastic vehicle schedule model for demand response and grid flexibility in a renewable-building-e-transportation-microgrid. Renew Energy 2024;221:119738.
[31] Islam MA, Ali MN, Mollick T, Islam A, Benitez IB, Habib SS, et al. Assessing the feasibility and quality performance of a renewable energy-based hybrid microgrid for electrification of remote communities. Energy Convers Manag X 2024;23:100674.
[32] Marcelino C, Leite G, Wanner E, Jiménez-Fernández S, Salcedo-Sanz S. Evaluating the use of a net-metering mechanism in microgrids to reduce power generation costs with a swarm-intelligent algorithm. Energy 2023;266:126317.
[33] Oviedo-Cepeda JC, Serna-Suárez I, Osma-Pinto G, Duarte C, Solano J, Gabbar HA. Design of tariff schemes as demand response mechanisms for stand-alone microgrids planning. Energy 2020;211:119028.
[34] Wouters C. Towards a regulatory framework for microgrids—the Singapore experience. Sustain Cities Soc 2015;15:22–32.
[35] Wu Y, Wu Y, Cimen H, Vasquez JC, Guerrero JM. Towards collective energy community: potential roles of microgrid and blockchain to go beyond P2P energy trading. Appl Energy 2022;314:119003.
[36] Chandak S, Rout PK. The implementation framework of a microgrid: a review. Int J Energy Res 2021;45:3523–47.
[37] Planas E, Andreu J, Gárate JI, De Alegría IM, Ibarra E. AC and DC technology in microgrids: a review. Renew Sustain Energy Rev 2015;43:726–49.
[38] Shafei H, Sarker SK, Li L, Aguilera RP, Alhelou HH. Innovative observer-based framework for attack reconstruction and mitigation in AC microgrids. In: 2024 IEEE 34th Australasian Universities Power Engineering Conference (AUPEC); IEEE; 2024. p. 1–6.
[39] Lotfi H, Khodaei A. Hybrid AC/DC microgrid planning. Energy 2017;118:37–46.
[40] Siti M, Mbungu N, Tungadio D, Banza B, Ngoma L. Application of load frequency control method to a multi-microgrid with energy storage system. J Energy Storage 2022;52:104629.
[41] Sarker SK, Shafei H, Shi T, Li L, Hossain M, Aguilera RP. A data-driven multivariable adaptive cybersecurity framework for isolated microgrids. In: 2024 IEEE 34th Australasian Universities Power Engineering Conference (AUPEC); IEEE; 2024. p. 1–6.
[42] Heidary J, Oshnoei S, Gheisarnejad M, Khalghani MR, Khooban MH. Shipboard microgrid frequency control based on machine learning under hybrid cyberattacks. IEEE Trans Ind Electron 2023;71(7):7136–46.
[43] Guo X, Lu Z, Wang B, Sun X, Wang L, Guerrero JM. Dynamic phasors-based modeling and stability analysis of droop-controlled inverters for microgrid applications. IEEE Trans Smart Grid 2014;5:2980–7.
[44] Jin H, Zhang Z, Yang G-H, Zuo Z, Gao Z, Wang Y. An event-triggered interval observer scheme for fault diagnosis of cyber-physical DC microgrids. IEEE Trans Ind Informatics 2025.
[45] Jadidi S, Badihi H, Zhang Y. Design of an intelligent hybrid diagnosis scheme for cyber-physical PV systems at the microgrid level. Int J Electr Power Energy Syst 2023;150:109062.
[46] Islam MZ, Lin Y, Vokkarane VM, Venkataramanan V. Cyber-physical cascading failure and resilience of power grid: a comprehensive review. Front Energy Res 2023;11:1095303.
[47] Jadidi S, Badihi H, Zhang Y. Active fault-tolerant and attack-resilient control for a renewable microgrid against power-loss faults and data integrity attacks. IEEE Trans Cybern 2023;54:2113–28.
[48] Alshammari A. Securing smart microgrids with a novel multi-layer cybersecurity framework for industry 4.0 renewable energy systems. Discov Comput 2025;28:80.
[49] Ahmed I, El-Rifaie AM, Akhtar F, Ahmad H, Alaas Z, Ahmed M. Cybersecurity in microgrids: a review on advanced techniques and practical implementation of resilient energy systems. Energy Strateg Rev 2025;58:101654.
[50] Choi S, Meliopoulos AS. Effective real-time operation and protection scheme of microgrids using distributed dynamic state estimation. IEEE Trans Power Deliv 2016;32:504–14.
[51] Rodrigues YR, Abdelaziz M, Wang L, Kamwa I. PMU-based frequency regulation paradigm for multi-area power systems reliability improvement. IEEE Trans Power Syst 2021;36:4387–99.
[52] Rodrigues YR, Abdelaziz MMA, Wang L. D-PMU based distributed voltage and frequency control for DERs in islanded microgrids. IEEE Trans Sustain Energy 2020;12:451–68.
[53] Venkataramanan V, Srivastava AK, Hahn A, Zonouz S. Measuring and enhancing microgrid resiliency against cyber threats. IEEE Trans Ind Appl 2019;55:6303–12.
[54] Rahmani-Sane G, Azad S, Jalilpoor K, Ameli MT. Introduction and literature review of resilience concept in power systems. Future Modern Distribution Networks Resilience 2024:1–21.
[55] Takiddin A, Rath S, Ismail M, Sahoo S. Data-driven detection of stealth cyber-attacks in DC microgrids. IEEE Syst J 2022;16:6097–106.
[56] Chen X, Zhou J, Shi M, Chen Y, Wen J. Distributed resilient control against denial of service attacks in DC microgrids with constant power load. Renew Sustain Energy Rev 2022;153:111792.
[57] Kuruvila AP, Zografopoulos I, Basu K, Konstantinou C. Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids. Int J Electr Power Energy Syst 2021;132:107150.
[58] Sudha A, Sudha CN, Shajina A. Detecting and mitigating cyber-physical attacks in microgrids to ensure resilient and sustainable communities. In: Next-generation cyber-physical microgrid systems. Elsevier; 2024. pp. 215–31.

[59] Said D. Quantum computing and machine learning for cybersecurity: distributed denial of service (DDoS) attack detection on smart micro-grid. Energies 2023;16:3572.
[60] Elrawy MF, Hadjidemetriou L, Laoudias C, Michael MK. Detecting and classifying man-in-the-middle attacks in the private area network of smart grids. Sustain Energy Grids Netw 2023;36:101167.
[61] Tian W, Ji X, Liu W, Liu G, Zhai J, Dai Y, et al. Prospect theoretic study of honeypot defense against advanced persistent threats in power grid. IEEE Access 2020;8:64075–85.
[62] Veerasamy V, Hu Z, Qiu H, Murshid S, Gooi HB, Nguyen HD. Blockchain-enabled peer-to-peer energy trading and resilient control of microgrids. Appl Energy 2024;353:122107.
[63] Vosughi A, Tamimi A, King AB, Majumder S, Srivastava AK. Cyber–physical vulnerability and resiliency analysis for DER integration: a review, challenges and research needs. Renew Sustain Energy Rev 2022;168:112794.
[64] Rath S, Das T, Sengupta S. Improvise, adapt, overcome: dynamic resiliency against unknown attack vectors in microgrid cybersecurity games. IEEE Trans Smart Grid 2024.
[65] Chu Z, Lakshminarayana S, Chaudhuri B, Teng F. Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch. IEEE Trans Smart Grid 2022;14:3164–75.
[66] Khan MMS, Giraldo J, Parvania M. Real-time cyber attack localization in distribution systems using digital twin reference model. IEEE Trans Power Deliv 2023.
[67] Bie Z, Bian Y. Microgrids resilience: definition, measures, and algorithms. Microgrids Theory Pract 2024:197–218.
[68] Hamidieh M, Ghassemi M. Microgrids and resilience: a review. IEEE Access 2022;10:106059–80.
[69] Spiegel MH, Veith EM, Strasser TI. The spectrum of proactive, resilient multi-microgrid scheduling: a systematic literature review. Energies 2020;13:4543.
[70] Shayeghi H, Shahryari E, Moradzadeh M, Siano P. A survey on microgrid energy management considering flexible energy sources. Energies 2019;12:2156.
[71] Babakmehr M, Simões MG, Wakin MB, Harirchi F. Compressive sensing-based topology identification for smart grids. IEEE Trans Ind Informatics 2016;12:532–43.
[72] Rameshrao AG, Koley E, Ghosh S. An optimal sensor location based protection scheme for DER-integrated hybrid AC/DC microgrid with reduced communication delay. Sustain Energy Grids Netw 2022;30:100680.
[73] Vaidya U, Fardad M. On optimal sensor placement for mitigation of vulnerabilities to cyber attacks in large-scale networks. In: 2013 European Control Conference (ECC); IEEE; 2013. p. 3548–53.
[74] Muhtadi A, Pandit D, Nguyen N, Mitra J. Distributed energy resources based microgrid: review of architecture, control, and reliability. IEEE Trans Ind Appl 2021;57:2223–35.
[75] Kanakadhurga D, Prabaharan N. Demand side management in microgrid: a critical review of key issues and recent trends. Renew Sustain Energy Rev 2022;156:111915.
[76] Kou W, Park S-Y. Distributed demand-side management for microgrids in modern power system. In: Uncertainties in modern power systems. Elsevier; 2021. pp. 163–94.
[77] Wan Y, Dragičević T. Data-driven cyber-attack detection of intelligent attacks in islanded DC microgrids. IEEE Trans Ind Electron 2022;70:4293–9.
[78] Yadav M, Pal N, Saini DK. Microgrid control, storage, and communication strategies to enhance resiliency for survival of critical load. IEEE Access 2020;8:169047–69.
[79] Kumar A, Singh AR, Raghav LP, Deng Y, He X, Bansal R, et al. State-of-the-art review on energy sharing and trading of resilient multi microgrids. Iscience 2024.
[80] Mohammadi M, Kavousi-Fard A, Dabbaghjamanesh M, Farughian A, Khosravi A. Effective management of energy internet in renewable hybrid microgrids: a secured data driven resilient architecture. IEEE Trans Ind Informatics 2021;18:1896–904.
[81] Shahzad S, Abbasi MA, Ali H, Iqbal M, Munir R, Kilic H. Possibilities, challenges, and future opportunities of microgrids: a review. Sustainability 2023;15:6366.
[82] Lawal OA, Teh J. A framework for modelling the reliability of dynamic line rating operations in a cyber–physical power system network. Sustain Energy Grids Netw 2023;35:101140.
[83] Keyvani B, Flynn D. Coordinated investment in wind-rich regions using dynamic line rating, energy storage and distributed static series compensation to facilitate congestion management. IET Renew Power Gener 2022;16:1882–96.
[84] Kosec G, Maksić M, Djurica V. Dynamic thermal rating of power lines–model and measurements in rainy conditions. Int J Electr Power Energy Syst 2017;91:222–9.
[85] Lawal OA, Teh J. Dynamic line rating forecasting algorithm for a secure power system network. Expert Syst Appl 2023;219:119635.
[86] Rácz L, Németh B, Göcsei G, Zarchev D, Mladenov V. Performance analysis of a dynamic line rating system based on project experiences. Energies 2022;15:1003.
[87] Zhang B, Hu W, Ghias AM, Xu X, Chen Z. Multi-agent deep reinforcement learning-based coordination control for grid-aware multi-buildings. Appl Energy 2022;328:120215.
[88] Danish MSS. A framework for modeling and optimization of data-driven energy systems using machine learning. IEEE Trans Artif Intell 2023;5:2434–43.
[89] Mishra S, Kwasnik T, Anderson K. Microgrid resilience: a holistic and context-aware resilience metric. Energy Syst 2023;14:1081–105.
[90] Diahovchenko IM, Kandaperumal G, Srivastava AK. Enabling resiliency using microgrids with dynamic boundaries. Electr Power Syst Res 2023;221:109460.
[91] Mishra DK, Wang J, Li L, Zhang J, Hossain M. Resilience-driven scheme in multiple microgrids with secure transactive energy system framework. IEEE Trans Ind Appl 2023.
[92] Canaan B, Colicchio B, Abdeslam DO. Microgrid cyber-security: review and challenges toward resilience. Appl Sci 2020;10:5649.
[93] Mishra DK, Eskandari M, Abbasi MH, Sanjeevkumar P, Zhang J, Li L. A detailed review of power system resilience enhancement pillars. Electr Power Syst Res 2024;230:110223.
[94] Kerdphol T, Ngamroo I, Surinkaew T. Enhanced robust frequency stabilization of a microgrid against simultaneous cyber-attacks. Electr Power Syst Res 2024;228:110006.
[95] Gkoktsis G, Lauer H, Jäger L. Towards mission aware cyber-resiliency with autonomous agents. In: Proceedings of the 2023 Australasian Computer Science Week; 2023. p. 36–9.
[96] Marnay C, Xu T, Hatziargyriou ND, Hirase Y, Mendoza-Araya P. Microgrids 2023 editorial. 2023.
[97] Sarker PS, Venkataramanan V, Cardenas DS, Srivastava A, Hahn A, Miller B. Cyber-physical security and resiliency analysis testbed for critical microgrids with IEEE 2030.5. In: 2020 8th workshop on modeling and simulation of cyber-physical energy systems; IEEE; 2020. p. 1–6.
[98] Xia Q, Wang Y, Zou Y, Yan Z, Zhou N, Chi Y, et al. Regional-privacy-preserving operation of networked microgrids: edge-cloud cooperative learning with differentiated policies. Appl Energy 2024;370:123611.
[99] Venkataramanan V, Hahn A, Srivastava A. CP-SAM: cyber-physical security assessment metric for monitoring microgrid resiliency. IEEE Trans Smart Grid 2019;11:1055–65.
[100] Yan L, Chen X, Chen Y. A consensus-based privacy-preserving energy management strategy for microgrids with event-triggered scheme. Int J Electr Power Energy Syst 2022;141:108198.
[101] Pu X, Xiao H, Pei W, Yang Y, Ma L, Ma T, et al. Optimal energy management of networked multi-energy microgrids based on improved multi-agent federated reinforcement learning. CSEE J Power Energy Syst 2024.
[102] Rieyan SA, News MRK, Rahman AM, Khan SA, Zaarif STJ, Alam MGR, et al. An advanced data fabric architecture leveraging homomorphic encryption and federated learning. Inf Fusion 2024;102:102004.
[103] Mahmood K, Tariq T, Sangaiah AK, Ghaffar Z, Saleem MA, Shamshad S. A neural computing-based access control protocol for AI-driven intelligent flying vehicles in industry 5.0-assisted consumer electronics. IEEE Trans Consumer Electron 2023;70:3573–81.
[104] Kott A, Paziuk A, Galaitsi SE, Trump BD, Linkov I, et al. Russian cyber onslaught was blunted by Ukrainian cyber resilience, not merely security, arXiv preprint arXiv:2408.14667 2024.
[105] Aguru AD, Erukala SB. A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning. Inf Sci 2024;662:120209.
[106] Tu C, He X, Liu X, Li P. Cyber-attacks in PMU-based power network and countermeasures. IEEE Access 2018;6:65594–603.
[107] Elimam M, Isbeih YJ, Azman SK, Moursi MSE, Al Hosani K. Deep learning-based PMU cyber security scheme against data manipulation attacks with WADC application. IEEE Trans Power Syst 2022;38:2148–61.
[108] Risbud P, Gatsis N, Taha A. Vulnerability analysis of smart grids to GPS spoofing. IEEE Trans Smart Grid 2018;10:3535–48.
[109] Taherian-Fard E, Niknam T, Sahebi R, Javidsharifi M, Kavousi-Fard A, Aghaei J. A software defined networking architecture for DDoS-attack in the storage of multimicrogrids. IEEE Access 2022;10:83802–12.
[110] Jena PK, Koley E, Ghosh S. An optimal scheme for installation of PMUs and IEDs to reinforce electricity market immunity against data attacks in smart grid. IEEE J Emerg Sel Top Ind Electron 2022;4:603–13.
[111] Khalafi ZS, Dehghani M, Khalili A, Sami A, Vafamand N, Dragičević T. Intrusion detection, measurement correction, and attack localization of PMU networks. IEEE Trans Ind Electron 2021;69:4697–706.
[112] Irudayaraj AXR, Qiu H, Veerasamy V, Tan W-S, Gooi HB. Blockchain-based distributed frequency control of sustainable networked microgrid system with P2P trading. Appl Energy 2024;373:123849.
[113] Alonso R, Haber RE, Castaño F, Recupero DR. Interoperable software platforms for introducing artificial intelligence components in manufacturing: a meta-framework for security and privacy. Heliyon 2024;10.
[114] Mbungu NT, Ismail AA, AlShabi M, Bansal RC, Elnady A, Hamid AK. Control and estimation techniques applied to smart microgrids: a review. Renew Sustain Energy Rev 2023;179:113251.
[115] Ruan G, Qiu D, Sivaranjani S, Awad AS, Strbac G. Data-driven energy management of virtual power plants: a review. Adv Appl Energy 2024:100170.
[116] Naseer A, Naseer H, Ahmad A, Maynard SB, Siddiqui AM. Moving towards agile cybersecurity incident response: a case study exploring the enabling role of big data analytics-embedded dynamic capabilities. Comput Secur 2023;135:103525.
[117] Sawas A, Farag HE. Real-time detection of stealthy IoT-based cyber-attacks on power distribution systems: a novel anomaly prediction approach. Electr Power Syst Res 2023;223:109496.
[118] Wang X, Pan Y, Li M, Chen J. A novel data-driven optimization framework for unsupervised and multivariate early-warning threshold modification in risk assessment of deep excavations. Expert Syst Appl 2024;238:121872.
[119] Hellenborn B, Eliasson O, Yitmen I, Sadri H. Asset information requirements for blockchain-based digital twins: a data-driven predictive analytics perspective. Smart Sustain Built Environ 2024;13:22–41.
[120] Madichetty S, Mishra S. Cyber attack detection and correction mechanisms in a distributed DC microgrid. IEEE Trans Power Electron 2021;37:1476–85.
[121] Ghiasi M, Dehghani M, Niknam T, Kavousi-Fard A, Siano P, Alhelou HH. Cyber-attack detection and cyber-security enhancement in smart DC-microgrid

based on blockchain technology and hilbert huang transform. IEEE Access 2021;9:29429–40.
[122] Sahoo S, Dragičević T, Blaabjerg F. An event-driven resilient control strategy for DC microgrids. IEEE Trans Power Electron 2020;35:13714–24.
[123] Habibi MR, Baghaee HR, Blaabjerg F, Dragičević T. Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids. IEEE Syst J 2021;16:1487–98.
[124] Basati A, Guerrero JM, Vasquez JC, Bazmohammadi N, Golestan S. A data-driven framework for FDI attack detection and mitigation in DC microgrids. Energies 2022;15:8539.
[125] Ali MH, Akhter SR. Nonlinear controller-based mitigation of adverse effects of cyber-attacks on the DC microgrid system. Electronics 2024;13:1057.
[126] Habibi MR, Baghaee HR, Blaabjerg F, Dragičević T. Secure control of DC microgrids for instant detection and mitigation of cyber-attacks based on artificial intelligence. IEEE Syst J 2021;16:2580–91.
[127] Tan S, Xie P, Guerrero JM, Vasquez JC. False data injection cyber-attacks detection for multiple DC microgrid clusters. Appl Energy 2022;310:118425.
[128] Dehghani M, Niknam T, Ghiasi M, Bayati N, Savaghebi M. Cyber-attack detection in DC microgrids based on deep machine learning and wavelet singular values approach. Electronics 2021;10:1914.
[129] Jena S, Padhy NP. Cyber-secure global energy equalisation in DC microgrid clusters under data manipulation attacks. IEEE Trans Ind Appl 2023.
[130] Ji G, Yu M, Tan KH, Kumar A, Gupta S. Decision optimization in cooperation innovation: the impact of big data analytics capability and cooperative modes. Ann Oper Res 2024;333:871–94.
[131] Sahoo S, Dragičević T, Blaabjerg F. Multilayer resilience paradigm against cyber attacks in DC microgrids. IEEE Trans Power Electron 2020;36:2522–32.
[132] Poudel BP, Mustafa A, Bidram A, Modares H. Detection and mitigation of cyber-threats in the DC microgrid distributed control system. Int J Electr Power Energy Syst 2020;120:105968.
[133] Leng M, Sahoo S, Blaabjerg F, Molinas M. Projections of cyberattacks on stability of DC microgrids—modeling principles and solution. IEEE Trans Power Electron 2022;37:11774–86.
[134] Akpolat AN, Habibi MR, Baghaee HR, Dursun E, Kuzucuoğlu AE, Yang Y, et al. Dynamic stabilization of DC microgrids using ANN-based model predictive control. IEEE Trans Energy Convers 2021;37:999–1010.
[135] Jena S, Padhy NP, Guerrero JM. Cyber-resilient cooperative control of DC microgrid clusters. IEEE Syst J 2021;16:1996–2007.
[136] Yu Y, Liu G-P, Huang Y, Guerrero JM. Distributed data-driven secondary regulation for the conflict between voltage recovery and accurate current sharing in DC microgrids. IEEE Trans Power Electron 2023.
[137] Liu X-K, Wang S-Q, Chi M, Liu Z-W, Wang Y-W. Resilient secondary control and stability analysis for DC microgrids under mixed cyber attacks. IEEE Trans Ind Electron 2023.
[138] Leng M, Sahoo S, Blaabjerg F. Stabilization of DC microgrids under cyber attacks–optimal design and sensitivity analysis. IEEE Trans Smart Grid 2023.
[139] Abazari A, Zadsar M, Ghafouri M, Atallah R, Assi C. A data mining/anfis and adaptive control for detection and mitigation of attacks on DC MGS. IEEE Trans Smart Grid 2022;14:2406–22.
[140] Shi D, Lin P, Wang Y, Chu C-C, Xu Y, Wang P. Deception attack detection of isolated DC microgrids under consensus-based distributed voltage control architecture. IEEE J Emerg Sel Top Circuits Syst 2021;11:155–67.
[141] Tabassum T, Lim S, Khalghani MR. Artificial intelligence-based detection and mitigation of cyber disruptions in microgrid control. Electr Power Syst Res 2024;226:109925.
[142] Liu M, Zhao C, Deng R, Cheng P, Chen J. False data injection attacks and the distributed countermeasure in DC microgrids. IEEE Trans Control Netw Syst 2022;9:1962–74.
[143] Abianeh AJ, Wan Y, Ferdowsi F, Mijatovic N, Dragičević T. Vulnerability identification and remediation of FDI attacks in islanded DC microgrids using multiagent reinforcement learning. IEEE Trans Power Electron 2021;37:6359–70.
[144] Cheng Z, Chow M-Y. Resilient collaborative distributed energy management system framework for cyber-physical DC microgrids. IEEE Trans Smart Grid 2020;11:4637–49.
[145] Cecilia A, Sahoo S, Dragičević T, Costa-Castelló R, Blaabjerg F. Detection and mitigation of false data in cooperative DC microgrids with unknown constant power loads. IEEE Trans Power Electron 2021;36:9565–77.
[146] Durairaj D, Venkatasamy TK, Mehbodniya A, Umar S, Alam T. Intrusion detection and mitigation of attacks in microgrid using enhanced deep belief network. Energy Sources Part A Recovery Utilization Environ Eff 2024;46:1519–41.
[147] Ni F, Zheng Z, Xie Q, Xiao X, Zong Y, Huang C. Enhancing resilience of DC microgrids with model predictive control based hybrid energy storage system. Int J Electr Power Energy Syst 2021;128:106738.
[148] Jena S, Padhy NP. Resilient operation of BESS in a cooperative DC microgrid under data manipulation attacks. In: 2022 IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT); IEEE; 2022. p. 1–7.
[149] Liu X-K, Wen C, Xu Q, Wang Y-W. Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks. IEEE Trans Smart Grid 2021;12:3742–54.
[150] Yu Y, Liu G-P, Hu W. Blockchain protocol-based secondary predictive secure control for voltage restoration and current sharing of DC microgrids. IEEE Trans Smart Grid 2022;14:1763–76.
[151] Jiang Y, Yang Y, Tan S-C, Hui SY. Distributed sliding mode observer-based secondary control for DC microgrids under cyber-attacks. IEEE J Emerg Sel Top Circuits Syst 2020;11:144–54.
[152] Sadabadi MS. A resilient-by-design distributed control framework for cyber-physical DC microgrids. IEEE Trans Control Syst Technol 2023;32(2):625–36.
[153] Basati A, Bazmohammadi N, Guerrero JM, Vasquez JC. Real-time estimation in cyber attack detection and mitigation framework for DC microgrids. In: 2023 23rd International Scientific Conference on Electric Power Engineering (EPE); IEEE; 2023. p. 1–6.
[154] He Q, Shah P, Zhao X. Resilient operation of DC microgrid against FDI attack: a GRU based framework. Int J Electr Power Energy Syst 2023;145:108586.
[155] Sheng L, Gu W, Cao G. Distributed detection mechanism and resilient consensus strategy for secure voltage control of AC microgrids. CSEE J Power Energy Syst 2022;9:1066–77.
[156] Gupta K, Chaudhary I, Chukkapalli SSL, Joshi A, Panigrahi BK. A privacy-preserving anomaly diagnosis scheme for AC microgrids. Sustain Energy Grids Netw 2024;38:101346.
[157] Tabassum T, Toker O, Khalghani MR. Cyber–physical anomaly detection for inverter-based microgrid using autoencoder neural network. Appl Energy 2024;355:122283.
[158] Sabzevari K, Habib S, Tabar VS, Shaillan HM, Hassan Q, Muyeen S. Energy market trading in green microgrids under information vulnerability of renewable energies: a data-driven approach. Energy Rep 2024;11:4467–84.
[159] Gokulraj K, Venkatramanan C. Advanced machine learning-driven security and anomaly identification in inverter-based cyber-physical microgrids. Electr Power Compon Syst 2024:1–18.
[160] Taher MA, Behnamfar M, Sarwat AI, Tariq M. False data injection attack detection and mitigation using nonlinear autoregressive exogenous input-based observers in distributed control for DC microgrid. IEEE Open J Ind Electron Soc 2024;5:441–57.
[161] Nandakumar A, Li Y, Xu Z, Huang D. Enhancing transient dynamics stabilization in islanded microgrids through adaptive and hierarchical data-driven predictive droop control. IEEE Trans Smart Grid 2025;16(1):396–410. https://doi.org/10.1109/TSG.2024.3448460.
[162] Taher MA, Tariq M, Sarwat AI. Enhancing security in islanded AC microgrid: detecting and mitigating cyber attacks in secondary control through ai-based method. IEEE Trans Ind Appl 2025;61(2):2124–34. https://doi.org/10.1109/TIA.2024.3523882.
[163] Ali Z, Hussain T, Su C-L, Sadiq M, Jurcut AD, Tsao S-H, et al. A new paradigm for adaptive cyber-resilience of DC shipboard microgrids using hybrid signal processing with deep learning method. IEEE Trans Transp Electr 2025;11(1):4280–95. https://doi.org/10.1109/TTE.2024.3459856.
[164] Bu X, Zhang Y, Ren X, Hou Z. Event-triggered data-driven LFC of multi-microgrid interconnected systems with time delays. IEEE Trans Control Netw Syst 2025;12(3):2266–77. https://doi.org/10.1109/TCNS.2025.3559198.
[165] Zhang X, Gao Q, Qu Y. A K-nearest neighbors approach for mitigating false data injection attacks in industrial microgrids. Smart Grids Sustain Energy 2025;10:40.
[166] Yang G, Herrera L, Yao X. False data injection attack detection in DC microgrids based on data-driven unknown input observers. IEEE J Emerg Sel Top Power Electron 2025;13(3):3803–16. https://doi.org/10.1109/JESTPE.2025.3539958.
[167] Wang X, Zhu H, Luo X, Guan X. Data-driven-based detection and localization framework against false data injection attacks in DC microgrids. IEEE Internet Things J 2025;12(17):36079–93. https://doi.org/10.1109/JIOT.2025.3579915.
[168] Abazari A, Ghafouri M, Jafarigiv D, Atallah R, Assi C. Data-driven framework for mitigating EV-based load-altering attacks on LFC model of microgrid. IEEE Trans Consumer Electron 2025;71(2):6093–108. https://doi.org/10.1109/TCE.2025.3563392.
[169] Wang X, Ding D, Dong H, Yi X. PI-based security control against joint sensor and controller attacks and applications in load frequency control. IEEE Trans Syst Man Cybern Syst 2022;53:970–80.
[170] Saxena A, Shankar R, Kumar C, Parida SK. A resilient frequency regulation for enhancing power system security against hybrid cyber-attacks. IEEE Trans Ind Appl 2024;60(3):4583–97. https://doi.org/10.1109/TIA.2024.3354228.
[171] Habibi MR, Baghaee HR, Dragičević T, Blaabjerg F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. IEEE J Emerg Sel Top Power Electron 2020;9:5294–310.
[172] Javanmardi H, Dehghani M, Mohammadi M, Siamak S, Hesamzadeh MR. BMI-based load frequency control in microgrids under false data injection attacks. IEEE Syst J 2021;16:1021–31.
[173] Hu S, Ge X, Chen X, Yue D. Resilient load frequency control of islanded AC microgrids under concurrent false data injection and denial-of-service attacks. IEEE Trans Smart Grid 2022;14:690–700.
[174] Munir MS, Abedin SF, Tran NH, Hong CS. When edge computing meets microgrid: a deep reinforcement learning approach. IEEE Internet Things J 2019;6:7360–74.
[175] Veerasamy V, Sampath LPMI, Singh S, Nguyen HD, Gooi HB. Blockchain-based decentralized frequency control of microgrids using federated learning fractional-order recurrent neural network. IEEE Trans Smart Grid 2023;15:1089–102.
[176] Tan S, Wu Y, Xie P, Guerrero JM, Vasquez JC, Abusorrah A. New challenges in the design of microgrid systems: communication networks, cyberattacks, and resilience. IEEE Electrification Mag 2020;8:98–106.
[177] Nosouhi MR, Sood K, Chamola V, Jeong JJ, Gaddam A. Towards quantum-secure software defined networks. IET Quantum Commun 2024;5:66–71.
[178] De Diego R, Martínez J-F, Rodríguez-Molina J, Cuerva A. A semantic middleware architecture focused on data and heterogeneity management within the smart grid. Energies 2014;7:5953–94.
[179] Shahid K, Nainar K, Olsen RL, Iov F, Lyhne M, Morgante G. On the use of common information model for smart grid applications—a conceptual approach. IEEE Trans Smart Grid 2021;12:5060–72.

[180] Ghaffari F, Bertin E, Crespi N, Hatin J. Distributed ledger technologies for authentication and access control in networking applications: a comprehensive survey. Comput Sci Rev 2023;50:100590.
[181] Algarni A, Ahmad Z, Ala'anzy MA. An edge computing-based and threat behavior-aware smart prioritization framework for cybersecurity intrusion detection and prevention of IEDs in smart grids with integration of modified LGBM and One class-SVM models. IEEE Access 2024;12:104948–63. https://doi.org/10.1109/ACCESS.2024.3435564.
[182] Vu TL, Mukherjee S, Adetola V. Resilient communication scheme for distributed decision of interconnecting networks of microgrids. In: 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT); IEEE; 2023. p. 1–5.
[183] Carrillo D, Kalalas C, Raussi P, Michalopoulos DS, Rodríguez DZ, Kokkoniemi-Tarkkanen H, et al. Boosting 5G on smart grid communication: a smart RAN slicing approach. IEEE Wirel Commun 2022;30:170–8.
[184] Elsayed M, Erol-Kantarci M, Kantarci B, Wu L, Li J. Low-latency communications for community resilience microgrids: a reinforcement learning approach. IEEE Trans Smart Grid 2019;11:1091–9.
[185] Wang Y, Yemula P, Bose A. Decentralized communication and control systems for power system operation. IEEE Trans Smart Grid 2014;6:885–93.
[186] Pradhan, Pradhan. A fault-tolerant communication architecture for distributed systems. IEEE Trans Comput 1982;100:863–70.
[187] Zahra S, Gong W, Khattak HA, Shah MA, Song H. Cross-domain security and interoperability in internet of things. IEEE Internet Things J 2021;9:11993–2000.