PeerJ Computer Science

A comprehensive review of blockchain and machine learning integration for cybersecurity in microgrids

Chou-Mo Yang, Chun-Lien Su and Mahmoud Elsisi

Department of Electrical Engineering, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan

ABSTRACT

The combination of blockchain technology with machine learning (ML) has emerged as a transformative approach to addressing cybersecurity challenges in microgrids (MG). As these systems become increasingly interconnected and dependent on real-time data transmission, they face growing risks from cyber threats such as false data injection attacks (FDIA), data tampering, denial of service (DoS), and adversarial attacks. This study provides a comprehensive analysis of how blockchain and ML can be integrated to mitigate these vulnerabilities. While ML offers advanced capabilities for anomaly detection, threat prediction, and adaptive response, blockchain's decentralized, transparent, and secure architecture provides a reliable foundation for data and transaction processing. By combining these technologies, MGs can enhance operational efficiency, safeguard data integrity, and strengthen system resilience. This article reviews recent developments in blockchain and ML applications for MG cybersecurity and highlights key enabling technologies and implementation challenges. Future research directions include the design of hybrid models and improvements in scalability. The findings highlight the potential of blockchain and ML to transform cybersecurity in MGs and support the development of safer, more reliable, and sustainable energy systems.

Subjects Algorithms and Analysis of Algorithms, Artificial Intelligence, Cryptography, Cryptocurrency, Blockchain

Keywords Blockchain, Machine learning, Cybersecurity, Microgrids

Submitted 1 April 2025
Accepted 2 September 2025
Published 30 September 2025

Corresponding author
Mahmoud Elsisi,
mahmoudelsisi@nkust.edu.tw

Academic editor
Bilal Alatas

Additional Information and Declarations can be found on page 36

DOI **10.7717/peerj-cs.3237**

INTRODUCTION

Global use of microgrids (MGs) has accelerated with the integration of distributed energy resources (DERs), such as energy storage systems and renewable energy sources (RESs) like solar and wind. To meet global energy efficiency and decarbonization goals, these MGs are essential for improving energy reliability, flexibility, sustainability and resilience to disruptions. Despite these advantages, the widespread adoption of MGs has led to a greater reliance on cutting-edge digital technologies, raising cybersecurity concerns (*Dutta & Prasad, 2020*). Due to their widespread use, information and communication technologies (ICT) are particularly vulnerable to operational failures, privacy violations and cyberattacks (*Irmak, Kabalci & Kabalci, 2023*; *Muhammad, Alshra'a & German, 2024*). Smart inverters are critical components of MGs as they connect distributed resources to the grid and provide essential grid support functions, including frequency and voltage control. These devices pose significant cybersecurity risks due to their integration with

various ICT systems and their remote communication capabilities. Their increasing use underscores the urgency of addressing vulnerabilities to mitigate potential cyber threats such as manipulation and unauthorized access (*Li & Yan, 2023*; *Jamil et al., 2021*). These cybersecurity challenges are further complicated by the complexity and diversity of communication protocols and ICT components within MGs, necessitating sophisticated and robust security solutions (*Chen et al., 2025*; *Paul et al., 2024*).

Promising solutions to these cybersecurity problems are provided by emerging technologies such as blockchain and machine learning (ML). The reliable integration and functioning of DERs depends on the secure, transparent and impenetrable transaction management of the blockchain. Due to its decentralized structure, which protects against unwanted changes and guarantees data integrity and secure communication between MG stakeholders, cybersecurity resilience is enhanced (*Dutta & Prasad, 2020*; *Soumya et al., 2024*). ML approaches, on the other hand, significantly improve the proactive protection capabilities of MGs by enabling real-time detection, predictive analytics and automated responses to potential cyberthreats. By improving anomaly detection, threat classification, and response automation, ML is being integrated into MG operations to develop strong defensive tactics against cyber incidents (*Paul et al., 2024*; *Soumya et al., 2024*). This review makes a contribution by:

- providing a thorough overview of the current cybersecurity issues of MGs.
- A thorough analysis of blockchain applications specifically designed for MG cybersecurity.
- Exploring the use of ML algorithms for threat prediction, automated defense plans, and real-time anomaly detection to significantly improve the cybersecurity of MGs.
- Highlighting the joint application of blockchain and ML to strengthen cybersecurity frameworks.

The roadmap of the article structure is shown in Fig. 1. The 'Survey methodology' section describes the formulation of this review. The 'Related work' section covers our literature search and its results. The 'Microgrids overview' section briefly introduces the concept and structure of MG. The 'Foundations of Blockchain' section explains the basics of blockchain. The 'Machine learning techniques' section provides a brief overview of the algorithms and philosophy of machine learning. The section 'Cyberattack types in Microgrids' describes the types of cyberattacks specific to MGs. The section 'Cybersecurity applications in Microgrids' introduces cybersecurity applications that utilize blockchain and machine learning for MGs. The section 'Combine blockchain with machine learning' discusses how blockchain can be combined with machine learning to improve cybersecurity in MGs and makes suggestions. Finally, the 'Conclusions' section concludes this review.

SURVEY METHODOLOGY

The method systematically collects, examines, interprets and integrates information to promote a comprehensive understanding of the topic. We conducted a search strategy that

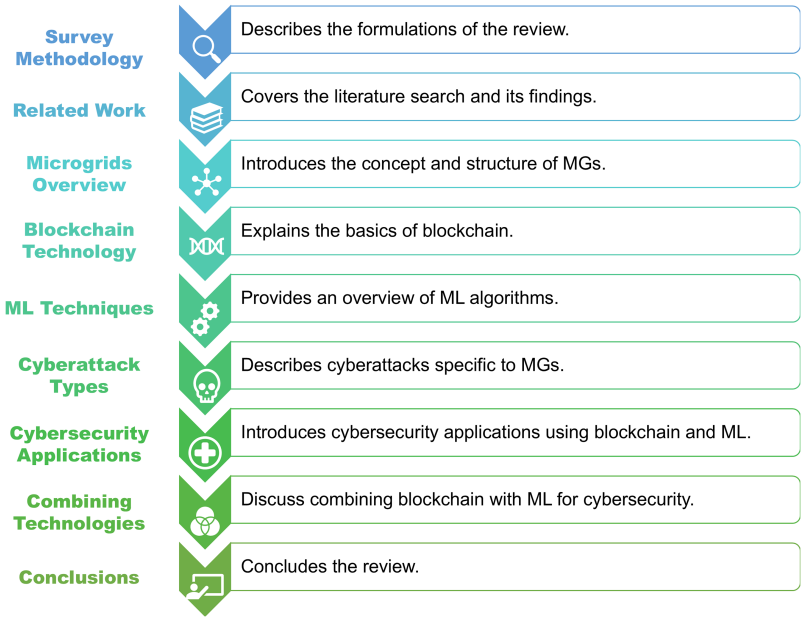

Figure 1 **The roadmap of the article structure.** Full-size DOI: 10.7717/peerj-cs.3237/fig-1

focused on specific keywords, concentrating on articles that included blockchain, machine learning, cybersecurity or microgrids in their titles or abstracts to confirm relevance. We prioritized and focused on searching for recent articles by year within 3 years, from 2022 to 2024; if not, then 5 years, from 2020 to 2024, no more than 10 years, focusing on recent advances, excluding important articles or theoretical background information.

RELATED WORK

To address the growing vulnerabilities created by the widespread digitization and decentralization of energy systems, a potential field of research has emerged: the integration of blockchain and ML technology into cybersecurity applications for MGs. MGs are vulnerable to a range of cyberthreats due to their tightly interconnected cyber-physical nature, especially false data injection attacks (FDIA) (*Soumya et al., 2024*). The stability and resilience of MGs are greatly impacted by these attacks. They pose a serious hazards to protection systems, voltage and frequency regulation and state estimation (SE). The reliance on cutting-edge ICT has brought new, greater cyber-physical risks. To reduce these new cyberattacks, resilient cybersecurity solutions and the integration of secure, resilient and adaptive tactics are of great importance (*Nejabatkhah et al., 2021*).

Decentralized energy management, peer-to-peer transactions, electric vehicles (EV), Internet of Things (IoT) integration, financial transactions and environmental sustainability are all enabled by blockchain technology (*Canaan, Colicchio & Abdeslam, 2020*). This broad classification provides a comprehensive understanding of the adaptability of blockchain in solving various security and operational issues in MG systems. *Mololoth, Saguna & Åhlund (2023)* have investigated how blockchain technology

and machine learning methods can be used together to enable intelligent, decentralized operations in future smart grids. Their analysis highlights how machine learning provides predictive analytics, demand forecasting and effective energy management, while blockchain enables secure transactions.

The digital transformation of MGs is explored by *Irmak, Kabalci & Kabalci (2023)*, who highlight technologies such as cloud computing, augmented reality, big data analytics, digital twin technology and the IoT. They highlight the possible advantages and difficulties of digitalization and emphasize the need for strong cybersecurity safeguards to maintain system stability and operational integrity. A thorough examination of cybersecurity implementation in smart grids is provided by *Swathika et al. (2024)*, who classify cyberattacks by advanced metering infrastructure (AMI), information technology (IT) and operational technology (OT) components. To successfully detect, categorize and combat cyber threats in smart grids, they propose strong mitigation solutions that mainly rely on machine learning, deep learning (DL) and signal processing approaches.

Hasankhani et al. (2021) explore the integration of blockchain and machine learning, especially for smart grids, how these two technologies can work together to improve operational dependability, secure energy trading, and optimize distributed energy management. The analysis points to important areas for future research as well as technical difficulties in successfully combining these two technologies. The analysis highlights important areas for future research as well as technical difficulties in successfully combining these two technologies. *Rajeyyagari et al. (2024)* present a new cybersecurity framework based on convolutional neural networks (CNN) augmented by the African Vulture Optimization Algorithm (AVOA), with excellent accuracy and detection rates in recognizing typical and anomalous network activity. This method dramatically improves cybersecurity performance in blockchain-based smart grids. Utilizing Long Short-Term Memory (LSTM) controllers in conjunction with blockchain technology to integrate digital twin systems. With enhanced real-time monitoring and secure data management capabilities, this cutting-edge framework significantly increases operational stability and resilience, especially in networked MGs during fault circumstances (*Hong et al., 2024*).

To successfully counter the increasingly complex cyber threats and safeguard renewable MGs, *Rouhani et al. (2024)* emphasize the critical need for established cybersecurity standards, especially IEC 61850 and IEC 62351. Their analysis identifies vulnerabilities and suggests thorough preventive and flexible cybersecurity measures. Table 1 summarizes the methods, MG applications, security approaches and contributions of the related work mentioned above.

In addition, seven existing survey articles are also studied. Their contributions and limitations are then organized in Table 2 as follows.

MICROGRIDS OVERVIEW

MG is a small-scale power generation and distribution system consisting of decentralized power sources, energy storage devices, energy conversion devices, loads, monitoring and protection devices, among others (*Ahmethodzic & Music, 2021*; *Mariam, Basu & Conlon, 2016*; *Zhou, Guo & Ma, 2015*). An MG is a localized electrical system that combines small

Table 1 Summary of related work.

Methods	Microgrid applications	Security approaches	Contributions
Markov/Bayesian models, Blockchain (*Soumya et al., 2024*)	Renewable MGs	Threat modeling, risk assessment	Systematic framework addressing cybersecurity gaps
Cyber-physical system review, FDIA analysis (*Nejabatkhah et al., 2021*)	Smart MGs (AC/DC)	Detection and mitigation of FDIAs	Detailed impact analysis of cyber threats on stability
Review of cybersecurity methods (*Canaan, Colicchio & Abdeslam, 2020*)	General MG management	Cyber-physical resilience	Overview of cyber threats and resilience strategies
Blockchain, ML (*Mololoth, Saguna & Åhlund, 2023*)	Energy trading, Demand response, EVs	Distributed ledger, ML-based detection	Integration of blockchain and ML for enhanced security
ML, DL, Signal processing (*Swathika et al., 2024*)	Smart Grid (IT, OT, AMI components)	Taxonomy of cyber threats, Intrusion Detection	Framework for securing smart grids using AI and ML
Blockchain (*Hasankhani et al., 2021*)	P2P trading, EV, Demand response	Smart contracts, decentralized management	Categorizes blockchain uses for secure energy trading
CNN, African vulture optimization (*Rajeyyagari et al., 2024*)	Blockchain-based smart grids	DL, anomaly detection	High accuracy and efficiency in cyber-attack detection
Digital Twin, Blockchain, LSTM controllers (*Hong et al., 2024*)	Networked MGs	Blockchain (PoS), Digital twin validation	Real-time fault detection, system stability improvement
Cyber resilience frameworks (*Rouhani et al., 2024*)	Renewable smart MGs	Defense-in-depth, ML-driven detection	Comprehensive review of standards, attack scenarios, solutions
Dynamic reconfiguration of multi-microgrids (*Yaghoubi et al., 2024*)	Smart power microgrids, specifically multi-microgrids	Protect against cyber-attacks, particularly FDIAs and cyber-physical attacks	A real-time hierarchical framework using LSTM neural networks and multi-objective optimization to dynamically reconfigure multi-microgrids

Table 2 The comparisons to the existing survey articles.

Summary	Limitations	Our contributions
Examines how blockchain and ML enhance peer-to-peer (P2P) energy trading in smart grids (*Fatima & Arshad, 2025*)	Focuses only on P2P energy trading, in which it lacks adversarial attack coverage.	Expands to full-spectrum cyber threats (FDIA, DoS, *etc.*) and integrates real-time ML anomaly detection.
Reviews distributed control (DCT) techniques for microgrids (MGs) (*Ahmad et al., 2025*)	Reviews distributed control but omits blockchain-ML synergy.	Discusses blockchain-enhanced DCT for secure, decentralized MG operations.
Analyzes cybersecurity risks in MGs, emphasizing data protection (*Islam et al., 2025*)	Limited to cybersecurity challenges without ML/blockchain solutions.	Provides ML-driven intrusion detection + blockchain immutability for data integrity.
Explores IoE's role in modernizing energy systems (*Meslouhi et al., 2025*)	Covers IoE but lacks depth in adversarial ML defenses.	Introduces adversarial training for ML models and blockchain-based audit trails.
Surveys DL applications to secure renewable energy supply chains (*Halgamuge, 2024*)	Surveys DL for supply chains, not MG-specific cybersecurity.	Tailors DL + blockchain to MG resilience, with case studies on inverter security.
Reviews architectures and controls for networked MGs (NMGs) (*Mutluri & Saxena, 2024*)	Broad on networked MGs but superficial in attack mitigation.	Details hybrid consensus algorithms (PoS/PBFT) for attack-resistant MGs.
DL-based proactive defense mechanisms for smart grids (*Abdi, Albaseer & Abdallah, 2024*)	Focuses on proactive DL for smart grids, ignoring blockchain.	Combines DL with blockchain for tamper-proof threat detection logs.

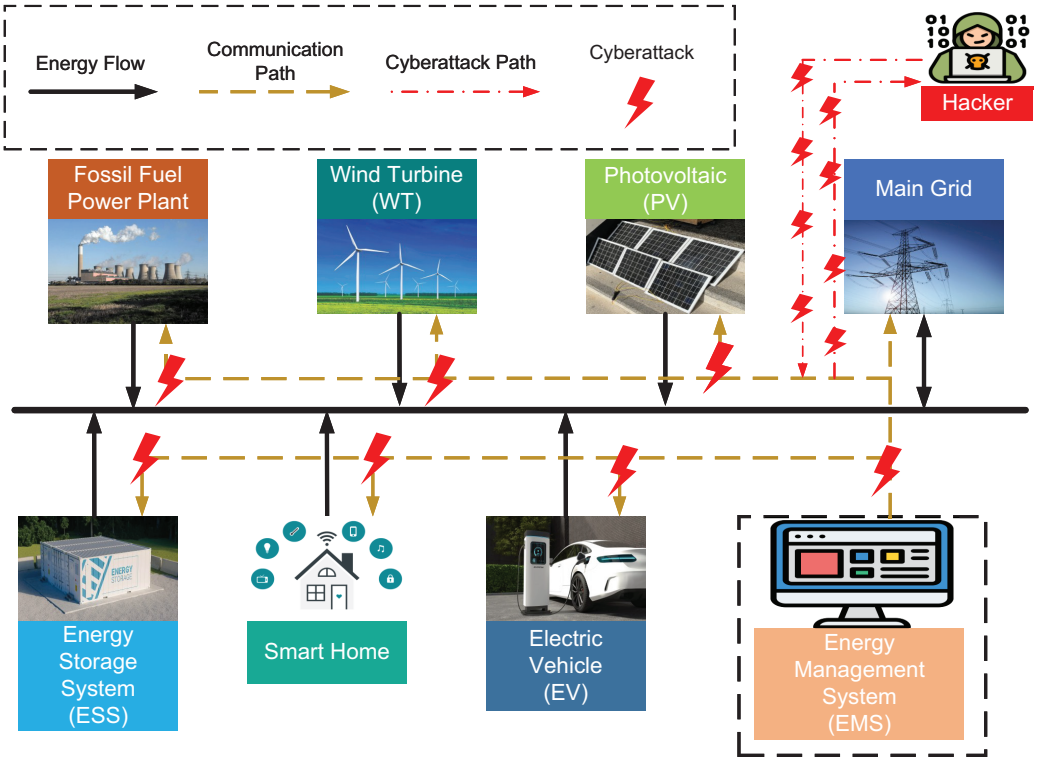

Figure 2 An illustration of MG with cyberattack path. Full-size DOI: 10.7717/peerj-cs.3237/fig-2

power generation sources (such as solar panels, fuel cells, microturbines or small wind turbines), energy storage systems and controllable loads in a coordinated network (*Xiao, Wu & Jenkins, 2010*). From the perspective of the utility, a microgrid functions as a single controllable power source that can automatically disconnect and maintain independent operation in the event of disruptions to the main grid (*Cagnano, Tuglie & Mancarella, 2020*). Unlike the traditional concept of large-scale power grids, MGs refer to a network of distributed power sources and associated loads connected to the regular power grid according to a certain collection and distribution structure. Among the current power grids, decentralized power generation has the advantages of high energy efficiency, low pollution, high reliability and flexible installation locations. However, decentralized renewable energy generation (REG) is intermittent and unstable, and if the proportion of regional renewable energy (RE) gradually increases, it will inevitably affect the stability of regional power system operation. The use of MG is an important means for efficient and stable power supply and the best way to increase the share of RE. Figure 2 illustrates a MG that integrates fossil fuel power plants, wind turbines, photovoltaic (PV) systems, energy storage systems (ESS), EVs, smart homes, and the main grid. The Energy Management System (EMS) actively coordinates energy and communication flows, represented by solid black and dashed yellow arrows, respectively. Red dashed-dotted lines and lightning symbols indicate cyberattack paths and impact points. The figure highlights the potential for hackers to exploit communication channels, underscoring the critical need for robust cybersecurity measures within smart microgrid infrastructures.

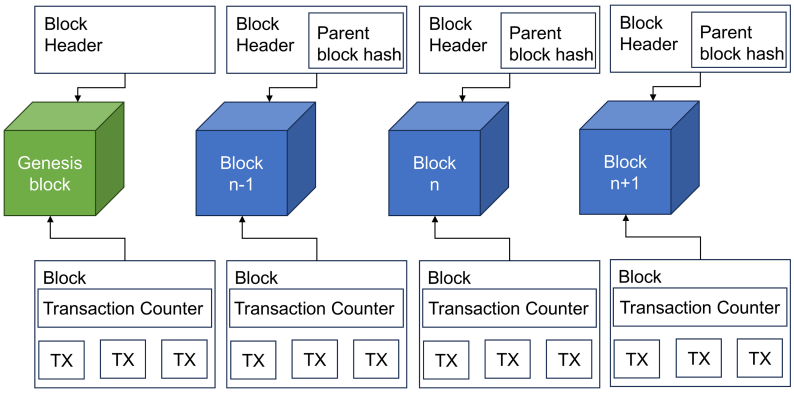

Figure 3 **The blockchain structure contains a sequence of blocks.**
Full-size DOI: 10.7717/peerj-cs.3237/fig-3

FOUNDATIONS OF BLOCKCHAIN

Modern blockchain technology was proposed and developed by Satoshi Nakamoto, whose identity remains unknown, in a white paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Nakamoto, 2008*). Originally, the main goal was to solve the problem of double spending in digital payment systems by proposing and developing a digital signature, namely Bitcoin. However, its entire system architecture gained attention and paved the way to a new application and research field.

System architecture of blockchain

The structure of a blockchain consists of a sequence of blocks, as shown in Fig. 3. Each block contains two groups of information: (1) block header and (2) transaction records. The block header consists of six types of information: (1) Block version, (2) Merkle tree root hash, (3) Timestamps, (4) n-bits, (5) Nonce, and (6) Parent block hash, as shown in Fig. 4 (*Haber & Stornetta, 1991*).

In the blockchain, the first block is referred to as the genesis block. Within a block, the block header contains the hash of the previous block, and there is only one parent block, the genesis block is the only one that does not have a parent block hash. Table 3 listed the individual composition of the information stored in the block header of a single block (*Zheng et al., 2017*).

Transaction records are stored in the main part of the block, including a transaction counter and a list of transactions, whereby the number of transactions varies depending on the block and transaction size. The authenticity of each transaction is verified with a digital signature based on asymmetric cryptography in an untrusted environment (*Gad et al., 2022*). With the digital signature, each party has a private key for signing transactions, which must be kept secret, and a public key, which is distributed openly across the blockchain. The algorithm used for the digital signature in a blockchain is usually the Elliptic Curve Digital Signature Algorithm (ECDSA) (*Johnson, Menezes & Vanstone, 2001*). The encryption algorithm can differ depending on the cryptocurrency and its

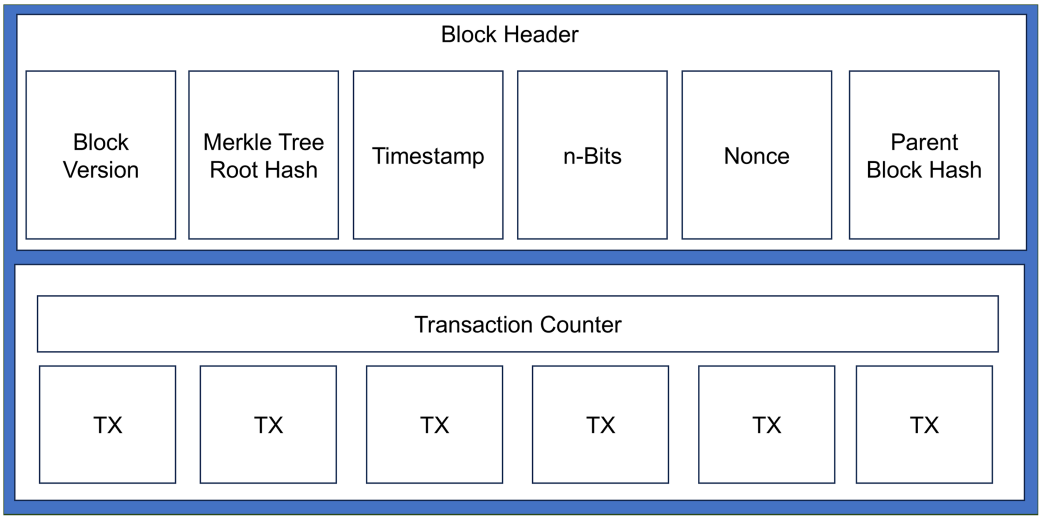

Figure 4 **A detailed illustration of a single block structure.**
Full-size DOI: 10.7717/peerj-cs.3237/fig-4

Table 3 **Listed definition of individual composition block header of a single block.**

Composition	Definition
Block version	Shows the set of block validation guidelines to adhere to.
Merkle tree root hash	The entire block's hash value of all transactions.
Timestamp	Present universal time as seconds since 1970-01-01.
n-Bits	The hashing target of a valid block hash.
Nonce	A 4-byte field that typically begins with 0 and increases for each hash calculation.
Parent block hash	A 256-bit hash value that points to the previous block.

version. The current version of Bitcoin, for example, uses the SHA-256 (*FIPS Pub, 2012*) hashing algorithm for data encryption.

Types of blockchain

The study categorizes blockchain technology into five different types: firstly the public blockchain, secondly the private blockchain, thirdly the consortium blockchain, fourthly the permissioned (fully private) blockchain and fifthly the hybrid blockchain, which we explain comprehensively and in detail in Table 4 (*Paul et al., 2021*; *IBM, 2021*).

Components and features of blockchain

There are three main elements of the blockchain: (1) distributed ledger (*AWS, 2023*); (2) smart contract (*Taherdoost, 2023*), and (3) consensus (*Lashkari & Musilek, 2021*). The distributed ledger is of crucial importance for the blockchain, as it stores data publicly and for everyone to view and read, but is unchangeable once it has been written. Smart contracts can be thought of as tiny applications that can be stored in the blockchain (distributed ledger). There is a special programming language for this called Solidity (*Wood, 2024*). It is a rule-based agreement that, once written to the blockchain, is

Table 4 Summary of five types of blockchain.

Type	Description
Public	The public blockchain, exemplified by Bitcoin (*Nakamoto, 2008*), is a decentralized system that anyone can participate in and read, with transparency increasing as more users join.
Private	The key difference between public and private blockchains is that private blockchains are managed by an organization or administrator, making them less decentralized and typically used internally rather than openly.
Consortium	Similar to private blockchains, consortium blockchains are managed by selected members, but unlike private blockchains, they are governed by multiple organizations or members with shared goals.
Permissioned	A permissioned blockchain network requires additional permissions for writing access, while read access may remain public, and currently, only Ethereum (*Buterin, 2014*) can extend into such a system (*The Investopedia Team, 2024*).
Hybrid	A hybrid blockchain combines elements of both public and private blockchains, allowing controlled data access and storage while maintaining public accessibility and keeping certain data private.

Table 5 Summary of proof-based consensus mechanism.

Type	Description
Proof-of-Work (PoW)	In proof-of-work, new blocks compete to solve difficult cryptographic problems (mining) to be added to the blockchain, requiring high computation and energy, with verification being easier than solving; this method is mainly used by Bitcoin (*Mololoth, Saguna & Åhlund, 2023*; *Nakamoto, 2008*).
Proof-of-Stake (PoS)	PoS, introduced by PPCoin (*King & Nadal, 2012*), is energy-efficient and doesn't require high computation power, using coin age (value multiplied by holding time) to reduce attack likelihood and grant more rights, while proposing accounting rights for mining.
Delegated Proof-of-Stake (DPoS)	DPoS lets stakeholders choose representatives for block validation, ensuring efficiency, with representatives adjusting block size and interval, and voting eliminating dishonest delegates to prevent malicious activity.
Proof-of-Authority (PoA)/Proof-of-Identity (PoI)	The PoA/PoI consensus mechanism uses trusted nodes with verified identities to create blocks, staking their reputation influenced by user behavior, essential for high-trust, permissioned blockchains (*Yaga et al., 2018*).
Proof-of-Elapsed-Time (PoET)	In permissioned blockchains, authenticated participants are identified before joining. PoET uses Intel SGX to ensure fair block creation by verifying waiting times and generating tamper-proof attestations, enhancing security and fairness (*Masood & Faridi, 2018*).

automatically executed and immutable, although updates are possible but difficult to implement. The consensus mechanism/algorithm is the security system of the blockchain that determines whether a new block can be safely added to the chain and protects against potential attackers and threats. There are two main categories of consensus mechanisms: (1) proof-based and (2) voting-based (*Jain & Jat, 2022*; *Khan et al., 2020*). In proof-based consensus algorithms, which are common in public blockchains, a proof of work is provided to compete for the addition of blocks. Private permissioned blockchains and consortium blockchains use voting-based consensus, where blocks collectively verify transactions before new ones are added. Table 5 summarizes the proof-based mechanisms and Table 6 summarizes the voting-based mechanisms. Table 7 (*Viriyasitavat & Hoonsopon, 2019*) summarizes the characteristics of blockchain in three categories: (1) decentralization, (2) immutability, and (3) consensus.

Machine learning techniques

A common method for developing adaptive algorithms is to combine ML (*Obulesu, Mahendra & ThrilokReddy, 2018*) with reinforcement learning (RL). ML and RL can

Table 6 Summary of voting-based consensus mechanism.

Type	Description
Practical byzantine fault tolerance (PBFT)	PBFT, used in private and permissioned blockchains, handles up to 33% malicious nodes with Byzantine fault tolerance but has limited scalability due to increased message complexity with more nodes (*Mololoth, Saguna & Åhlund, 2023*).
Ripple consensus	In the Ripple network, nodes generate a Unique Node List (UNL) of reliable nodes, achieving consensus through rounds of transaction validation and voting, with 80% agreement required for ledger acceptance and 40% UNL overlap between nodes (*Khan et al., 2020*).
Tendermind consensus	In Tendermind consensus, clients directly create and broadcast transactions to validating block nodes *via* the gossip protocol, which must gather and validate transactions before including them in the block (*Jain & Jat, 2022*; *Khan et al., 2020*).

Table 7 Summary of characteristics of blockchain in three categories.

Characteristics	Description
Decentralization	Decentralization shifts control from a central system to a distributed network, reducing costs, increasing efficiency, and enhancing transparency by spreading trust among participants.
Immutability	Immutability means blockchain data cannot be altered, making transaction records tamper-proof; errors can only be corrected by adding new transactions or blocks.
Consensus	The consensus mechanism sets rules for participants to agree on recording transactions and storing data, requiring majority consent for new entries.

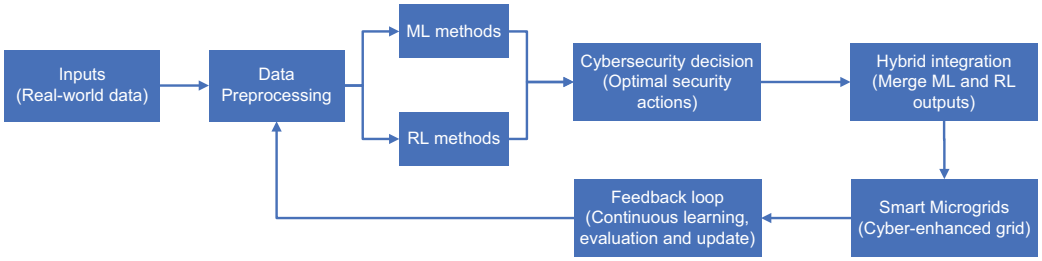

Figure 5 Hybrid RL methods integrate various ML strategies to enhance the cybersecurity of MGs.
Full-size DOI: 10.7717/peerj-cs.3237/fig-5

improve real-world problem solving by identifying the best solutions to specific problems. In the following sections, the features of this algorithm and the changes made to improve the cybersecurity of MG are explained. The ML, RL and hybrid models used in this study have been explained in detail as shown in Fig. 5.

Supervised learning

In supervised learning (*Muhammad & Yan, 2015*), learning models are created by labeling data to solve classification and regression problems. Regression methods including linear, polynomial and exponential techniques - extract attributes for independent and dependent variables. Among these, techniques based on Gaussian Process Regression (GPR) are becoming increasingly popular. Unlike parametric schemes, which define the shape of samples based on their mean and variance functions, GPR adheres to a Gaussian random process distribution, as shown in Eqs. (1) to (3).

$$f(x) = G_p(m(x), k(x, x')) \tag{1}$$

where,

$$m(x) = E\{f(x)\} \tag{2}$$

and

$$k(x, x') = G_p\left[\{\langle f(x) - m(x)\rangle\langle f(x) - m(x)\rangle\}^T\right]. \tag{3}$$

The input vectors in Eqs. (1) to (3) are denoted by x and x', the mean function is specified by $m(x)$ and the covariance function by $k(x, x')$. Linear kernels, square exponential kernels, Matern kernels, periodic kernels or various types of complex qualified equations can be used as covariance functions (also called kernel functions). When training with the labeled sample dataset, the hyperparameters in Eq. (1) are optimized. The accuracy of GPR in dealing with nonlinear relationships is one of its advantages over LR methods.

One of the most commonly used kernel-based supervised learning methods is the Support Vector Machine (SVM). By using the SVM to separate the data from the input pattern vector (x) and the labeled target vector (y), the linearly separable dataset (x, y) can be clearly represented by two hyperplanes (edges). The form of the decision area for two parallel hyperplanes is explained by Eq. (4), where w stands for the weights and b for the vector of bias factors. If you use normalized or standardized datasets, the decision area and each hyperplane are $1/\|w\|$ away from each other. SVM reduces classification errors by applying a hinge loss algorithm to a hyperplane of classification targets on linearly indivisible datasets.

$$w^T x + b = 0. \tag{4}$$

The goal is to minimize the function L in Eq. (5), where L is the regularization parameter and n is the number of modes.

$$L = \left[\frac{1}{n}\sum_{i=1}^{n} \max\left(0,\ 1 - y\left(w^T x_i + b\right)\right)\right] + \lambda\|w\|^2. \tag{5}$$

By using kernel functions (such as those in Table 8 (*Patle & Chouhan, 2013*)) to convert input states into wide-dimensional feature regions and then applying hyperplanes to delineate the input data, SVM can also be used to determine decision boundaries (decision boundaries are defined in Eqs. (6) and (7) where φ denotes the mapping function).

$$w^T \varphi(x) + b = 0. \tag{6}$$

$$k\left(x_i,\ x_j\right) = \varphi(x_i)^T \varphi\left(x_j\right). \tag{7}$$

Kernel functions (see Table 8) first transform the input state into a wide-dimensional feature space, and hyperplanes delimit the input data. Support Vector Machines (SVM) optimize the parameters for these hyperplanes using methods such as stochastic gradient descent (SGD), sequential minimal optimization (SMO) and interior point techniques (IPT), which makes them effective for regression tasks. Common SVM variants also

Table 8 Frequently used kernel functions of vector machines.

Kernel function	Mathematical formulation
Linear	$k(x_i,\ x_j) = \langle x_i^T,\ x_j \rangle$
Polynomial	$k(x_i,\ x_j) = \langle x_i^T,\ x_j \rangle^n$
Radial basis function (RBF)	$k(x_i,\ x_j) = \exp\left(-\gamma \|x_i - x_j\|^2\right),\ \gamma > 0$
Sigmoid	$k(x_i,\ x_j) = \tanh\left(\gamma \langle x_i - x_j \rangle + r\right)$

Two samples of vectors are x_i and x_j.

Parameter r is specified by initial coefficient (*coef0*).

include Bayesian SVM and Support Vector Clustering (SVC). From the point of view of sparse Bayesian learning theory, Relevance Vector Machines (RVM) (*Tipping, 2001*, *1999*, *2003*) are also known as kernel-based models. There are real-time intrusion detection systems using RVMs that are similar to SVMs in the cybersecurity domain, including MGs (*Naveen, 2012*).

Decision Trees (DT), another approach to supervised learning, begin by selecting a root node based on the feature with the highest information gain rate. While the main node has the greatest information gain, the sub-nodes rank the data according to the different attribute values of the main node. This process is repeated until there are no more attributes or additional information in the new sub-nodes. To maximize information gain, DT algorithms such as ID3, C4.5 and Classification and Regression Trees (CART) use information entropy. Random Forest, an ensemble learning method that combines multiple DT models, improves the flexibility of tree-based algorithms. After evaluating the predictions of all DT models, the RF algorithm selects the model with the highest majority vote.

Unsupervised learning

Unsupervised learning (*Usama et al., 2019*), which works with unlabeled data, is often used to solve clustering problems. Common techniques include k-means clustering algorithms (*e.g.*, k-Nearest Neighbor), where k cluster centers are randomly initialized and then each data point is assigned to the nearest center. The algorithm iteratively adjusts these centers to minimize an objective function based on the distance between the clusters and the data points and stops when the cost function stabilizes or a maximum iteration limit is reached. Another approach is hierarchical clustering, which groups the data according to their similarity (measured by linkage methods or Euclidean distance) and stops once a predefined number of clusters has been formed. Density-based spatial clustering, introduced by *Ester et al. (1996)*, identifies dense regions based on parameters such as scan radius (ε) and minimum points labeling outliers in low-density areas. It concludes by processing all data points. Alternative strategies include mean-shift or Gaussian mixture models, which adaptively refine cluster positions based on data density or probabilistic distributions.

Deep learning

Artificial neural networks (ANN) (*Uhrig, 1995*) form the backbone of DL systems and operate in both supervised and unsupervised modes. They use non-linear functions to

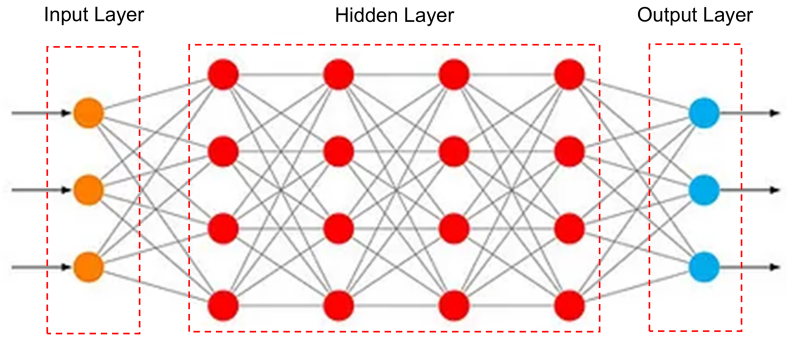

Figure 6 **An illustration depicts the architecture of DNNs.**
Full-size DOI: 10.7717/peerj-cs.3237/fig-6

model relationships between input and target variables while optimizing their parameters. Advances in big data mining and computer technologies are driving the growing popularity of DL. Figure 6 illustrates the architecture of deep neural networks (DNN). DNNs mainly contain several hidden layers.

Backpropagation is not only used for training DNNs, but is also considered as an optimization method that uses gradient descent to determine the weights and biases of the neural network (NN). The mathematical formulation is shown in Eq. (8). Another popular type of ANN is the deep belief network (DBN) (*Hinton, Osindero & Teh, 2006*).

$$f(x) = f_a\left[W_i^T f_a\left(W_{i-1}^T \cdots f_a\left(W_0^T x + b_0\right)\right) + b_i\right]. \tag{8}$$

CNNs (*O'Shea & Nash, 2015*) are advanced DL models that learn hierarchical representations and extract features and excel at tasks such as image and object recognition. Their convolutional layers achieve this by applying convolutional kernels to process the input tensor and the outputs of the previous layers. Fully connected layers and pooling layers are used to further identify features, as shown in Fig. 7. The format of the convolutional layers is shown in Eqs. (9) and (10) (*Goodfellow, Bengio & Courville, 2016*), where $Z^{l+1}(i,j)$ denotes the (i-th, j-th) output pixel from the $(l+1)^{th}$ feature map of the convolutional layer, Z_k^l denotes the input to the $(l+1)^{th}$ convolutional layer (the k-th channel), K is the number of channels in the first convolution layer, L_{l+1} is the size of Z^{l+1}, $w_k^{l+1}(x,y)$ is the weight of the (x-th, y-th) element in the convolution kernel in the $(l+1)^{th}$ convolution layer, b is the bias vector, f is the size of the convolution kernel, s_0 is the stride number and p is the padding number.

$$Z^{l+1}(i,j) = \sum_{k=1}^{K}\sum_{x=1}^{f}\sum_{y=1}^{f}\left[Z_k^l(s_0 i + x, s_0 j + y)w_k^{l+1}(x,y)\right] + b, (i,j) \in \{0,1,\cdots L_{l+1}\}. \tag{9}$$

$$L_{l+1} = \frac{L_l + 2p - f}{s_0 + 1}. \tag{10}$$

The process of selecting features and filtering information is called pooling and it usually takes the form of Eq. (11) (*Estrach, Szlam & LeCun, 2014*), where a is the parameter that defines the pooling strategy (a = 1 indicates the average pooling; $a \to \infty$ indicates the

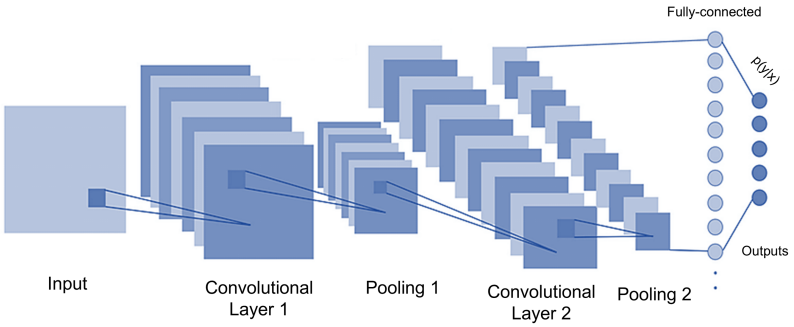

Figure 7 **A 2D CNN architecture.** Full-size DOI: 10.7717/peerj-cs.3237/fig-7

maximum pooling), and $P_k^{l+1}(i,j)$ is the output. Maximum or average values are common pooling algorithms.

$$P_k^{l+1}(i,j) = \left[\sum_{x=1}^{f}\sum_{y=1}^{f} Z_k^l(s_0 i + x, s_0 j + y)^a\right]^{\frac{1}{a}}. \tag{11}$$

Combining the convolutional layer with the pooling layer usually improves the performance of data exploration. CNNs are usually trained with a backpropagation algorithm, similar to DNNs. The extracted functions are aggregated by the fully linked layer in (8) and then sent to the output layer and optimized for DNNs. To improve training performance and flexibility, some DNN and CNN models can benefit from ensemble learning (EL) and transfer learning (TL) methods. TL uses tiny training datasets to train complex NNs. Basically, the accuracy and flexibility of an NN increases when it contains multiple learning systems.

As shown in Fig. 8, recurrent neural networks (RNN) have become increasingly popular for processing time series data. Each RNN block receives an input variable $x(t)$ at each time t. The input variable $x(t)$ is the same as the input variable $x(t)$. The output of each block is $y(t)$ and its hidden state is $h(t)$. The output $y(t+1)$ is obtained by importing $h(t)$ and combining it with $x(t+1)$ to form $h(t+1)$. During this process, a time series memory is created. The trained RNN can predict the input time series variables. Hochreiter originally proposed the LSTM framework, which is a representative RNN framework (*Hochreiter & Schmidhuber, 1997*). By forgetting inputs that are irrelevant to the block and strengthening key inputs, the forgetting gates in LSTM solve the problems of gradient vanishing and explosion problems. It is well known that reservoir computing (RC) algorithms, Bidirectional RNNs and Stacked RNNs outperform traditional RNN algorithms in terms of training performance. One of the variants of the RNN architecture is the Gate Recurrent Unit (GRU). It is also considered an improved architecture of RNN and is a mutation form of LSTM (*Cho et al., 2014*).

Reinforcement learning

A unique branch within machine learning is RL. It is based on the principle of mimicking human learning and development through trial and error, which was originally proposed

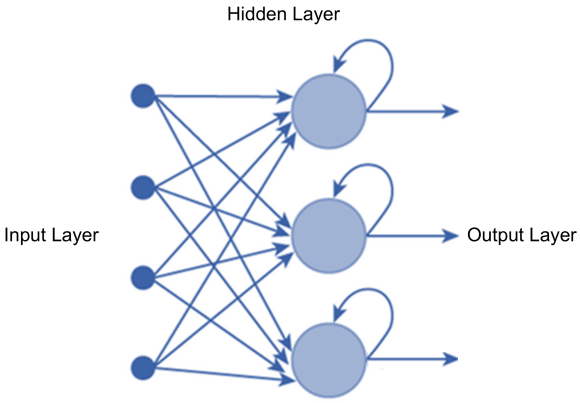

Figure 8 **An RNN architecture.** Full-size DOI: 10.7717/peerj-cs.3237/fig-8

by *Sutton & Barto (2018)*. In RL, agents interact with their environment by observing states, performing actions, and receiving rewards that include both positive incentives and negative punishments. Agents choose actions from a finite set of possibilities in their environment, and we measure their success by evaluating these rewards. To balance long-term goals, discounting factors adjust the weight of future incentives over immediate rewards, preventing an excessive focus on short-term gains. Agents primarily engage with their environment through this iterative process and refine their behavior based on reward-driven feedback. Rewards are given to the agent based on their behavior. A typical reinforcement learning process is shown in Fig. 9. Here, the states and actions are $S = \{1, \ldots, n\}$ and $A = \{1, \ldots, n\}$ Which of these value sets are continuous and which are discrete depends on the problem. This strategy was then defined for this function. The next goal for the reinforcement learning agent was to maximize the reward and obtain it by acting appropriately according to its current condition. Since this method is a closed loop, it requires an initial condition. To achieve the desired results, the RL must be set correctly. If the condition is simplified, the RL condition is not properly designed. The result is poor performance and an inability to respond positively to rewards.

When the agent interacts with its environment, RL is mainly used to identify the activities that will generate the highest cumulative rewards. The Markov Decision Process (MDP) principle is used for this. It usually consists of an agent and an environment. Depending on whether the environment needs to be explicitly modeled or not, RL can be divided into two categories: model-based and model-free, as Fig. 9 shows. Agents derive their behavior from their environment and this environment motivates them. Standard RL methods are used:

- Q-learning (*Watkins & Dayan, 1992*): using the combination between Q-values $Q(s,\ a)$ and the Q-table to create the next action. This results in a new Q-value that is generated using Eq. (12), where R stands for rewards, a and s for the following steps α and γ for learning rates.

$$Q(s,\ a) \leftarrow Q(s,\ a) + \alpha[R + \gamma max_{a'} Q(s',\ a') - Q(s, a)], s \leftarrow s'. \tag{12}$$

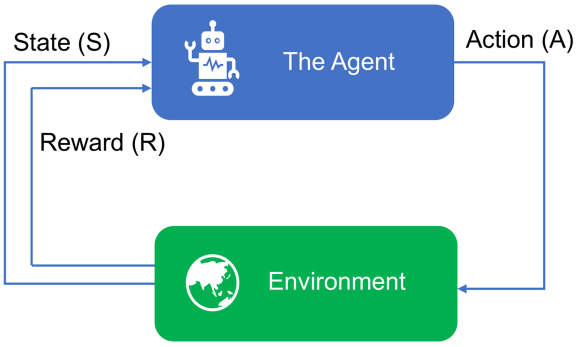

Figure 9 **An illustration of the RL process.** Full-size DOI: 10.7717/peerj-cs.3237/fig-9

- Deep Q-networks (DQN) (*Mnih et al., 2013*): the goal is to use DL techniques (*e.g.*, DNN, CNN, LSTM) to overcome the exponentially increasing computational cost of Q learning.
- Policy gradient methods (*Sutton et al., 1999*): instead of using Q-values, build post-test steps using policy functions, which are measures of the state and operational behavior in the current step.
- Actor-Critic (A2C) algorithms (*Konda & Tsitsiklis, 1999*): in order to modify its scoring policy based on the score of the critic, the actor creates the posterior-step action using the current-step state. The critic then assigns the actor a score at the current step.

Q-learning

Q-learning is a reinforcement learning technique that enables agents to learn optimal decision-making strategies by maximizing cumulative rewards through trial-and-error interactions with an environment. The agent can use Q-learning to learn the optimal policy that maximizes the long-term rewards and leads it to achieve its goal. Random variations and incentive alignment challenges can be effectively addressed without changing the existing framework of the environment. This technique identifies an optimal policy for a finite Markov decision process (FMDP) by maximizing the expected cumulative reward across all future time steps. Q-learning aims to identify the optimal policy for an FMDP by maximizing the cumulative expected future rewards from the current state, rather than focusing only on immediate or stage-specific gains. The Q-function evaluates the long-term utility of an action by iteratively updating its value estimates using reward feedback, thus reinforcing the learning process of the agent. The value-based model-free reinforcement learning approach uses approximation functions (*e.g.*, NNs) to estimate action values. One-step Q-learning for training action-valued variables is based on iterative minimization of the loss function, which is how DNNs work. This off-policy learning technique uses current conditions to determine the best course of action. In Q-learning, decision making that deviates from the current policy, such as randomly exploring small actions, is classified as "off-policy" because the process does not rely on the existing policy at every step. In addition, Q-learning attempts to optimize its overall reward through execution. Through this feedback loop, the learning process

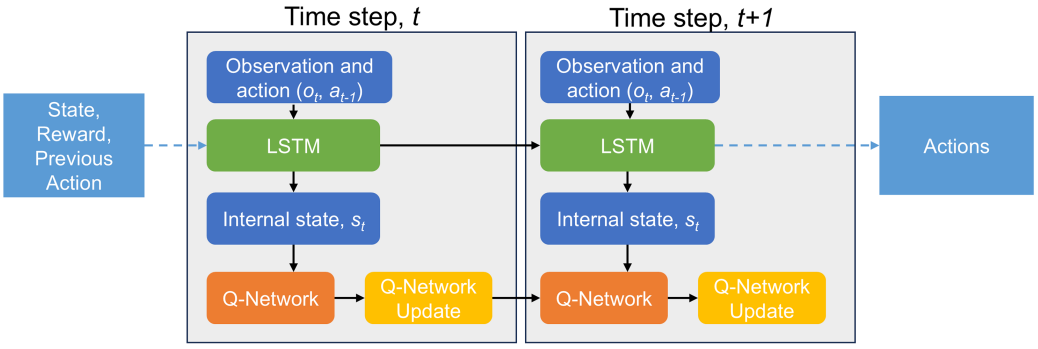

Figure 10 **LSTM-based Q-Network agent.** Full-size DOI: 10.7717/peerj-cs.3237/fig-10

becomes more accurate and the rewards are optimized. The input can be categorized by an agent that has time series analysis capability and the output is delivered in a timely manner. By training the DL LSTM agent, the memory component within the DNN layer can recognize the actions and states of the time series-based elements. With the developed deep Q-learning model, a variety of optimization tasks can be solved. Figure 10 shows an agent based on the architecture of the LSTM model. The input vectors consist of the prior action, the current state and the reward received. To mitigate overfitting and reduce the inaccuracy of the model in the current ensemble, the architecture includes additional LSTM layers paired with a batch normalization layer. Subsequently, the data was processed through the fully connected layer, a fundamental component of DL architectures. The entire layers and nodes of the architecture dynamically adapt to variations in input variables coming from real circuit signals or simulation data. The selection process can be efficiently performed by a straightforward grid search in combination with representative data samples, as shown in Fig. 11.

Perspective on the application of ML techniques in microgrids

The selection of an appropriate ML model is not arbitrary but must be tailored to the specific cybersecurity challenge within an MG. The choice depends critically on the requirements of the application, such as real-time performance, data availability, and the specific nature of the protected assets.

Suitability for real-time threat detection

Real-time threat detection is arguably the most critical application of ML for MG cybersecurity, necessary to preempt system instability. For this purpose, DL models that can analyze time-series data are exceptionally well-suited. RNNs, including LSTM and GRU models are prime candidates. Their inherent ability to process sequential data allows them to learn the normal temporal patterns of voltage, current, and frequency signals within an MG. An attack, such as an FDIA, would create anomalies in these patterns that a well-trained RNN could detect with high accuracy. However, the computational complexity of these DL models presents a significant trade-off. Deploying a complex LSTM model on resource-constrained devices like smart inverters or remote terminal units

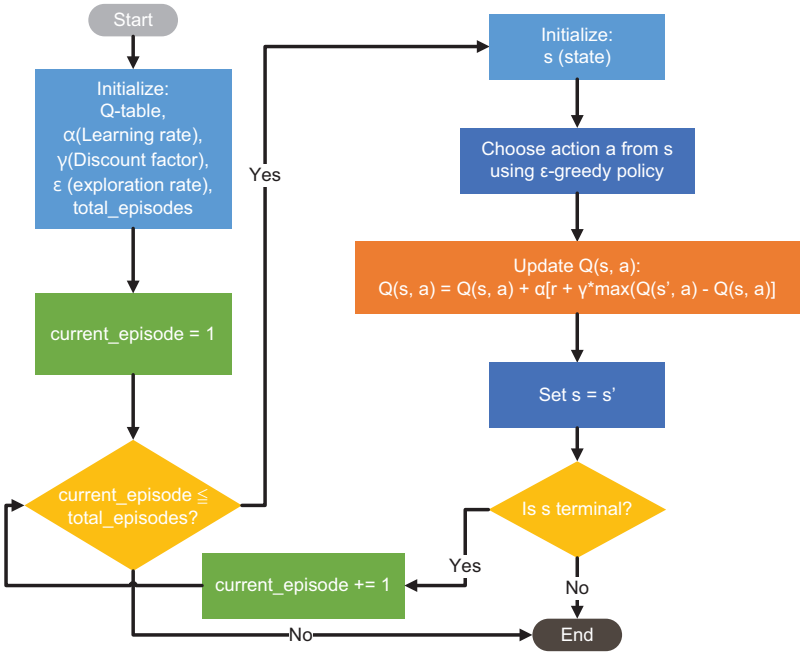

Figure 11 **Visual representation workflow of the Q-learning.**
Full-size DOI: 10.7717/peerj-cs.3237/fig-11

may be infeasible. In these scenarios, less computationally intensive algorithms like SVMs or RVMs offer a more practical solution. While perhaps offering slightly lower accuracy than a deep DL model, their speed makes them better suited for initial, rapid threat detection at the edge of the network. Furthermore, in real-world MGs, obtaining large, accurately labeled datasets of cyberattacks is a major challenge. This limitation makes a strong case for unsupervised learning approaches. Clustering algorithms can identify deviations from normal operating clusters without prior knowledge of attack signatures, making them invaluable for detecting novel or zero-day attacks that would evade supervised models.

Suitability for energy transactions

For securing energy transactions, the primary security mechanism is blockchain itself, which ensures integrity and non-repudiation. However, ML can serve as a vital secondary defense layer. The most suitable ML techniques for this application are supervised classification models. DT, Random Forests, and SVMs are well-suited for analyzing transactional data to detect fraudulent or anomalous patterns. For instance, a model could be trained on historical data to identify transactions that deviate from a typical energy consumption of a user or trading behavior, flagging them for review. This is not a real-time control application, so the slight latency of these models is acceptable. The key is their ability to classify transactions based on learned features, adding an intelligent monitoring layer to the structural security of blockchain.

A robust cybersecurity framework for MGs requires a hybrid approach, as no single ML technique is universally optimal. Such a framework integrates lightweight, real-time

models (*e.g.*, SVM) at the edge, sophisticated time-series deep learning models (*e.g.*, LSTM) at the central control level, and unsupervised models for novel threat detection. This entire architecture leverages a blockchain to ensure an immutable data record.

CYBERATTACK TYPES IN MICROGRIDS

The integration of advanced technologies and complex networks increases the cybersecurity vulnerabilities of MGs and exposes them to various cyberattack vectors. Attackers exploit vulnerabilities in critical components to compromise the intelligent MG infrastructure. Each type of cyberattack has unique characteristics and has different consequences. This section examines the main cyberattacks on MGs, including FDIA, DoS, adversarial attacks, Time Delay Attack (TDA), Replay Attack (RA), Man-in-the-Middle (MiTM), Switching Attacks (SA), malware and malicious command injection.

Our literature analysis reveals that FDIAs and Denial-of-Service (DoS) attacks constitute the most researched and potent threats to microgrid security. The focus on FDIAs arises from their capacity to directly corrupt the data governing critical MG functions, such as SE, frequency control, and economic dispatch. Stealthy FDIAs can emulate normal system fluctuations to bypass traditional bad data detectors that use simple thresholds, which poses a significant challenge to detection systems. Similarly, DoS attacks present a severe threat by exploiting the heavy reliance of MGs on ICT for real-time control. A DoS attack can overwhelm communication channels, incapacitating the EMS, severing control over DERs, and potentially initiating cascading failures. The proliferation of IoT devices continually expands the attack surface, making DoS and its distributed variant (DDoS) persistent and scalable threats. Although other attack types like Switching Attacks can cause catastrophic damage, they often demand specialized knowledge of the physical system topology and present greater difficulty for remote execution. These factors likely account for the greater emphasis on research on data-centric attacks like FDIAs and DoS.

False data injection attacks

FDIAs occur in various forms, including deceptive tactics that compromise the reliability of control systems or manipulate measurement data (*Pasqualetti, Dörfler & Bullo, 2013*). The most well-known variants of FDIAs include random, pulse, ramp, scaling, and Additive White Gaussian Noise (AWGN) attacks (*Prasad, 2020*; *Ali et al., 2024*; *Elsisi, Su & Ali, 2024*). In this section, we review common FDIA types and analyze their intended targets and the resulting consequences. The attacks start at time t_{atk} and interfere with the original transmission signal S_{tx}, resulting in the formation of mixed data S_R, a mixture of real and manipulated information at time t.

1. **Random attack**: the random attack aims to corrupt the measurement signal by injecting random data, which obscures the transmission signal as shown in Eq. (13). S_{rnd} represents the vector of random values introduced by the attacker.

$$S_{tx} = \begin{cases} S_R + S_{rnd}, & t_{atk} \\ S_R, & otherwise \end{cases}. \tag{13}$$

2. **Pulse attack**: the pulse attack interferes with and alters measurement signals by introducing a pulse signal into the normal signal. S_{pul} refers to the pulse signal that is deliberately introduced by an attacker. As Eq. (14) shows.

$$S_{tx} = \begin{cases} S_R + S_{pul}, & t_{begin} < t < t_{end} \\ S_R, & otherwise \end{cases}. \tag{14}$$

3. **Ramp attack**: the attacker alters the transmitted signal by integrating ramp signals and thus changes the true measurement by means of a ramp attack. S_{ram} stands for the ramp signal that the attacker intentionally injects. As Eq. (15) shows.

$$S_{tx} = \begin{cases} S_R + S_{ram}, & t_{begin} < t < t_{end} \\ S_R, & otherwise \end{cases}. \tag{15}$$

4. **Scaling attack**: the scaling attack manipulates the measurement signal *via* a scaling variable or function, resulting in unstable and inconsistent measurement data. As Eq. (16) shows. S_{scal} stands for the scaling attack, while e_s stands for the scaling factor.

$$S_{scal} = \begin{cases} S_R, & \forall t \notin t_{atk} \\ (1 + e_s)S_R, & \forall t \in t_{atk} \end{cases}. \tag{16}$$

5. **AWGN attack**: the AWGN attack works subtly by injecting Gaussian noise into the signals and disguising the interference as natural disturbances to avoid detection. The name reflects the mechanics: additive combines the noise with the signal, white distributes it evenly across the frequencies, and Gaussian follows a normal distribution. As Eq. (17) shows. S_{awgn} refers to a signal that has been compromised by an AWGN attack, where an attacker maliciously injects noise.

$$S_{tx} = \begin{cases} S_R + S_{awgn}, & t_{begin} < t < t_{end} \\ S_R, & otherwise \end{cases}. \tag{17}$$

6. **Load redistribution attack (LRA)**: *Yuan, Li & Ren (2011)* developed the LRA, a targeted FDIA that disrupts smart MGs by compromising the economic dispatch (ED) system, a system designed to minimize operational costs (*e.g.*, generation expenses, load shedding penalties) through strategic adjustments to power generation. As Eq. (18) shows. Here, ΔP_L represents the attack on power flow metering, $-S_F$ represents the shift factor matrix, K_D represents the bus load incidence matrix, and ΔD represents the attack on metering.

$$\Delta P_L = -S_F \cdot K_D \cdot \Delta D. \tag{18}$$

Denial of service

In a DoS attack, the attacker floods the system with excessive data packets, overwhelming communication channels between measuring devices and the control center for a predetermined timeframe. This disruption forces the system to drop any signals transmitted during the attack. As shown in Eq. (19).

$$S_{tx} = \begin{cases} 0, & t_{begin} < t < t_{end} \\ S_R, & otherwise \end{cases}. \tag{19}$$

In addition to flooding the system and overloading it with data packets, a DoS attack can also take the form of protocol manipulation, weak spots, jamming and routing attacks (*Wenyuan et al., 2006*; *Jhaveri, Patel & Jinwala, 2012*; *Liang et al., 2017*). *Yi et al. (2014)* characterize the Puppet attack, a novel DoS tactic, as an intrusion that transforms regular nodes in Advanced Metering Infrastructure (AMI) networks into puppet nodes. The attackers instruct these hijacked nodes to flood the network with attack packets, overloading communication capacity and draining energy reserves through excessive traffic. In contrast to conventional DoS attacks with a single source, Distributed Denial-of-Service (DDoS) attacks, a variation of DoS in MGs, are executed simultaneously from multiple geographically dispersed systems (*Raja et al., 2022*).

Adversarial attack

The primary goal of attacks is to compromise analytical models (*Elsisi et al., 2024*; *Liu et al., 2019*). The Fast Gradient Sign Method (FGSM) exploits the vulnerabilities of a pre-trained model by generating adversarial noise over the gradient of the input signal, thus intentionally maximizing the classification errors. As defined in Eq. (20) (*Goodfellow, Shlens & Szegedy, 2014*), the FGSM attack generates adversarial examples by modifying the original input data.

$$\eta_{adv_x} = x + \epsilon sign\left(\nabla_x \mathcal{J}\left(\theta, x, y\right)\right) \tag{20}$$

where η_{adv_x} is the perturbed image, x is the original image, y is the target (victim) image, $\mathcal{J}$ denotes the loss function of the model, θ represents the parameters of the model, and ϵ defines the perturbation magnitude.

The Projected Gradient Descent (PGD) attack derives from the single-step FGSM, originally proposed by *Madry et al. (2017)*. The PGD attack is a method designed to fortify classifiers against first-order adversarial threats, as shown in Eq. (21) (*Madry et al., 2017*; *Elsisi et al., 2024*). The iterative method produces a sequence of adversarial examples: $\left\{x_{adv}^{0},\ x_{adv}^{1},\ \cdots x_{adv}^{N+1}\right\}$.

$$\begin{aligned} x_0^{adv} &= x, \\ x_{N+1}^{adv} &= Clip_{x,\epsilon}\left\{x_N^{adv} + \alpha \cdot \frac{\nabla_x L(\theta, x)}{\|\nabla_x L\left(\theta, x, y\right)\|_2}\right\} \end{aligned} \tag{21}$$

where, the hyperparameter α, typically defined as ϵ/N for a given ϵ, is applied iteratively. The $Clip_{x,\epsilon}$ operation ensures per-pixel constraints on the adversarial image.

Kurakin, Goodfellow & Bengio (2018) proposed the Basic Iterative Method (BIM), which extends the FGSM framework by iteratively refining adversarial perturbations. Unlike single-step noise application of the FGSM, BIM applies incremental adjustments through a multi-step process, generating small perturbations that cumulatively maximize errors, as formalized in Eq. (22).

$$\begin{aligned} x_0^{adv} &= x, \\ x_{N+1}^{adv} &= Clip_{x,\epsilon}\left\{x_N^{adv} + \alpha \cdot sign\left(\nabla_x \mathcal{J}\left(x_N^{adv}, y\right)\right)\right\}. \end{aligned} \tag{22}$$

Time delay attack

The TDA influences the system by introducing random delays in both the transmission and reception of packets (*Wu et al., 2019*). Receiving the control signal at the right time is crucial for effective system management. This attack interrupts the transmission of signals from the remote terminal units (RTU) to the control center over the communication channel as described in Eq. (23).

$$S_{tx} = S_R(t - \tau(t)) \tag{23}$$

where $\tau(t)$ represents the time delay encountered in the reception of plant states at the control center location. Uncertainty in time delay attacks can result in varied patterns.

Replay attack

The RA strategy operates by capturing sensor data over a specific time window and substituting genuine measurements to corrupt control signals, or by maliciously passing operator-generated commands to actuators to disrupt normal operation (*Zhu & Martínez, 2014*).

Man in the middle

MiTM attacks threaten MGs by intercepting and manipulating communications between devices to secretly monitor data (eavesdropping) or impersonate devices (spoofing), all while mimicking the normal flow of data (*Conti, Dragoni & Lesyk, 2016*). *Kulkarni et al. (2020)* analyzed these attacks and pointed out the risks associated with the vulnerabilities of the Modbus TCP/IP protocol, while *Fritz et al. (2019)* demonstrated a prototype MiTM attack on an emulation platform and showed practical exploitation methods.

Switching attack

SAs destabilize MGs by targeting circuit breakers to disturb the phase angles and frequencies of generators and eventually force disconnection (*Liberati, Garone & Giorgio, 2021*). *Liu et al. (2011a*, *2011b)* demonstrated this using a Single-Machine Infinite Bus (SMIB) model that simulates transmission systems with a generator and a load connected *via* a circuit breaker. Attackers execute SAs by disconnecting devices in substations such as transformers, transmission lines or busses *via* compromised local networks. These actions risk grid congestion, instability, and cascading failures such as blackouts (*Yamashita et al., 2020*). Researchers warn that attackers can exploit IP-connected substations by hijacking local computers with breaker access to breakers or digital relays with partial control, enabling cascading trips. *Yamashita, Ten & Wang (2020)* describe how attackers use IP-based intelligent electronic devices (IED), commonly used in MGs, to remotely open circuit breakers during SAs.

Malware attacks and malicious command injection

Malware attacks such as logic bombs, Trojan horses and botnets threaten systems in different ways. Logic bombs remain inactive until certain conditions trigger their payload, causing systems to crash, data to be corrupted or hard disks to be irrevocably erased (*Dusane & Pavithra, 2020*). Trojan horses disguise malicious code as legitimate software to

trick users into running it (*Namanya et al., 2018*), while botnets use networks of compromised devices to spread malware, send spam or intercept communications (*Liu et al., 2009*). Malicious command injection attacks infiltrate systems to seize unauthorized control, as shown by *Lin, Kalbarczyk & Iyer (2018)*, who simulate adversarial command sequences to study their destabilizing effects on MG dynamics.

Perspective on cyberattack landscape in microgrids

While the literature describes a wide array of cyberattacks, a critical analysis from the perspective of MG operations reveals why certain threats receive more attention and are considered more probable. The extensive focus on FDIAs in research is not arbitrary; it stems from their unique potential to compromise the cyber-physical nature of MGs stealthily. Unlike DoS attacks that overtly disrupt communication, FDIAs subtly alter sensor measurements and control signals. This allows them to directly manipulate critical MG functions like SE and economic dispatch, potentially causing physical damage or widespread instability before detection. The challenge of distinguishing malicious data from legitimate operational fluctuations makes FDIA a particularly insidious and academically compelling problem.

From a practical standpoint, the most plausible attacks on current and future MGs exploit the expanding digital footprint created by ICT and the IoT. Therefore, FDIAs, MiTM attacks, and RAs are highly probable threats. These attacks target the communication channels between DERs, smart inverters, and control centers, essential for smart grid functionality. Their feasibility is heightened because they often do not require overwhelming force but exploit common communication vulnerabilities of protocols. In contrast, attacks like coordinated large-scale SAs may be less probable as they often require more system knowledge and synchronized access to multiple physical devices. However, the increasing interconnection of substation automation systems means their potential impact cannot be overlooked. Thus, the focus of the literature reflects a risk matrix where both the likelihood and the potential impact of an attack are considered. FDIAs represent a critical intersection of high likelihood (due to ICT vulnerabilities) and severe impact (due to physical system manipulation).

CYBERSECURITY APPLICATIONS IN MICROGRIDS

Advanced communication networks, IoT devices, and automated control systems expose MGs to significant cyber threats (*Gaggero, Girdinio & Marchese, 2021*). To counter these risks, experts have developed sophisticated protective measures, including AI-driven intrusion detection systems (IDS), blockchain protocols, and real-time anomaly monitoring. However, attacks such as FDIA, DDoS, and ransomware continue to destabilize MGs, risking widespread outages and underscoring the urgency of robust security measures (*Dai et al., 2024*).

Blockchain-based framework

Blockchain is mainly used in MGs to solve the problem of energy trading in energy sharing. Leveraging the decentralized nature of blockchain for peer-to-peer (P2P) energy

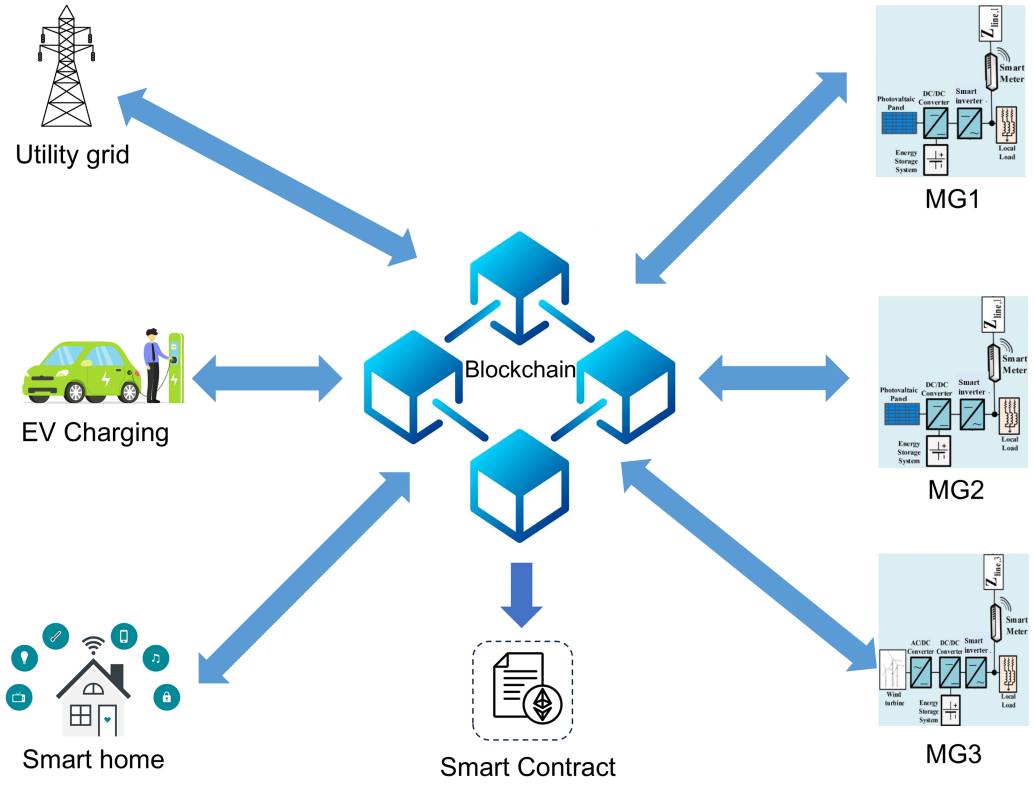

Figure 12 **The application of blockchain in between MGs and buyers.**
Full-size DOI: 10.7717/peerj-cs.3237/fig-12

transmission not only reduces energy loss, but also ensures secure energy transmission. Figure 12 illustrates the blockchain application between MGs and buyers.

Coordinating energy trading between multiple buyers is a complex challenge for MG operations. The authors of *Košťál, Khilenko & Hunák (2024)* introduce a two-level hierarchical blockchain framework to optimize P2P energy trading and demand management. The platform employs game algorithms to help participants make cost-efficient decisions while maintaining grid stability, and implements cryptographic protocols to block fraudulent transactions. The simulation results show that the integration of recommendation algorithms for buyers and sellers reduces the peak-to-average ratio (PAR), reduces network congestion and increases overall efficiency. A real world case study on P2P energy trading in the MG system is conducted by the authors of *Khubrani & Alam (2023)*. In addition to P2P energy trading, they also proposed Renewable Energy Certificates (REC) management and secure billing. This ensures transparent, tamper-proof transactions, strengthens trust in energy trading and reduces security risks.

Despite the inherent security of the blockchain, the communication channels connecting the blockchain to MGs or buyers are still fraught with cybersecurity risks, prompting developers to deploy smart contracts as tailored communication protocols with predefined rules and functions to secure these connections. The authors of *Faheem et al. (2024)* propose an Advanced Solana Blockchain (ASB) framework that utilizes smart

contracts to monitor and control DERs in real time. By minimizing communication overhead and increasing efficiency, the ASB framework ensures data integrity and authentication mechanisms, thus increasing the resilience of smart grids against cyberattacks. The authors (*Zhang et al., 2024*) propose a blockchain-based security architecture for scalable IoT-integrated microgrids that use multi-layer smart contracts to secure authentication and interactions between components. They introduce a Computing Balance-based Exchange (CBE) algorithm to optimize data exchange and reduce latency, while the framework ensures secure device communication and addresses trust/privacy concerns. Simulations show improved security and efficiency in large-scale smart grids.

The reliability of power distribution must be guaranteed, especially in medium voltage networks where power failures can lead to blackouts or serious operational disruptions. Using distributed ledger technology (DLT), the authors (*Hahn et al., 2024*) propose a Cyber Grid Guard (CGG) system that verifies and authenticates data received from electricity meters and protection relays. The system provides an additional layer of security for monitoring the power grid, detects faulty phases and immutably logs event data in the blockchain using IEC 61850 GOOSE messages. With the increasing penetration of solar energy in residential areas, smart inverters now play a crucial role in modern electricity grids. However, these IoT-enabled devices expose grids to cyber threats, jeopardizing stability. To address this issue, the authors (*Akkaoui et al., 2024*) introduce Resilient Authenticated Smart-inverter Secure Firmware *via* Auditable Blockchain (RASSIFAB), a blockchain framework that secures smart inverter firmware updates by increasing security, resilience, and auditability. By leveraging the immutability of blockchain, RASSIFAB guarantees authentic firmware over-the-air (FOTA) updates and prevents tampering, even against malicious insiders. *Appasani et al. (2022)* emphasize enhanced security, transparency, and decentralization in domains such as AMI, EVs, and synchrophasors. The discussion suggests that integrating blockchain with ML can strengthen MG cybersecurity by enabling secure data management and intelligent threat detection. Table 9 summarizes the blockchain-based framework for application of cybersecurity in MGs.

Machine learning-based framework

ML improves the cybersecurity of microgrids through real-time threat detection, adaptive anomaly monitoring and proactive risk mitigation. By analyzing IoT and sensor data to detect attacks such as FDIA and DoS, ML systems adapt to evolving threats, increase grid resilience and ensure reliable power distribution. Figure 13 shows the cyberattack path and critical targets that represent optimal locations for ML model deployment. FDIAs are the most widespread and effective cyberattack method, particularly targeting the transmission of signaling data. Numerous studies have dealt with the detection of FDIAs using different machine learning approaches. The authors of *Yu, Hou & Li (2018)* propose a real-time method for detecting FDIAs that integrates wavelet transforms (WTs) with DNNs and exploits temporal correlations in system states to overcome the one-point limitations of traditional approaches. Their DL model extracts hidden patterns from wavelet-transformed signals and can accurately distinguish cyberattacks from normal operations. One of the biggest challenges in identifying FDIA, besides detecting the attack

Table 9 Summary of blockchain-based cybersecurity applications in MGs.

Methods	Microgrid applications	Security approaches	Contributions	Critical insights
Hierarchical blockchain energy trading with game theory (*Košťál, Khilenko & Hunák, 2024*).	Optimizing energy trading and load balancing in microgrids.	Blockchain with cryptographic security measures and game theory optimization.	Developed a hierarchical blockchain system for optimized microgrid energy management.	The integration enhances microgrid efficiency, security, and scalability by reducing PAR and ensuring transparent trading; however, it introduces design complexity, relies on accurate user modeling, and may incur computational overhead.
Blockchain-based decentralized MG framework (*Khubrani & Alam, 2023*).	Peer-to-peer energy trading and REC management.	Decentralized transactions with blockchain for security and transparency.	Proposed a blockchain-based decentralized microgrid for secure energy trading	The article proposes a secure blockchain-based microgrid for Saudi Arabia, enhancing transparency and decentralization, but lacks real-world validation and faces regulatory and scalability challenges.
Lightweight smart contracts on Solana blockchain (*Faheem et al., 2024*).	Secure communication for DERs.	Smart contracts for authentication, data integrity in DER communication,	Introduced an Advanced Solana Blockchain (ASB) framework for DER communication security.	The authors propose a lightweight Solana-based smart contract framework that enhances secure, low-latency DER communication, though its complexity and computational overhead may hinder practical scalability.
Multi-layer smart contracts and CBE algorithm (*Zhang et al., 2024*).	Secure identity authentication and data sharing in smart grids.	Multi-layer smart contracts with cryptographic authentication.	Designed a smart contract-based secure architecture for smart grid communication and data exchange.	The article presents a secure and efficient smart grid framework using blockchain and smart contracts, though its complexity limits practical scalability.
Cyber Grid Guard system with DLT (*Hahn et al., 2024*).	Fault detection in medium-voltage feeders.	DLT for data validation, fault detection and cyber resilience.	Implemented DLT for enhanced fault detection and power grid security	The CGG system with DLT enhances fault detection security by validating relay data, but it lacks fault-type distinction and may introduce detection delays.
Blockchain-based firmware update security (RASSIFAB) (*Akkaoui et al., 2024*).	Securing firmware updates for smart inverters.	Blockchain for immutable firmware updates, resistance against cyber threats.	Developed RASSIFAB, a secure blockchain-based firmware update framework for smart inverters.	The article introduces a blockchain-based FOTA framework that strengthens firmware security and auditability for smart inverters, but incurs overhead and depends on a trustworthy majority of OEM nodes.
Blockchain with smart contracts and distributed ledger (*Appasani et al., 2022*).	Synchrophasor systems, AMI, EVs, Home Automation.	Digital signatures, consensus algorithms, private/consortium chains.	Enables secure, decentralized data exchange and enhances resilience against cyberattacks.	The article highlights the potential of blockchain to secure and decentralize smart grid applications but provides limited practical validation and insufficient analysis of implementation challenges.

itself, is to find the exact origin of the attack. To address this problem, researchers use a multilabel classification strategy (*Wang, Bi & Zhang, 2020*). They combine CNNs with traditional bad data detectors (BDD) to accurately identify compromised nodes in microgrids. Location detection is critical for real-time threat defense as it enables targeted countermeasures. AC smart islands, where DERs operate in isolated grid configurations, provide a unique environment for viewing FDIA (*Dehghani et al., 2020*). Their method uses wavelet singular values as feature inputs to a DL model and utilizes wavelet transforms

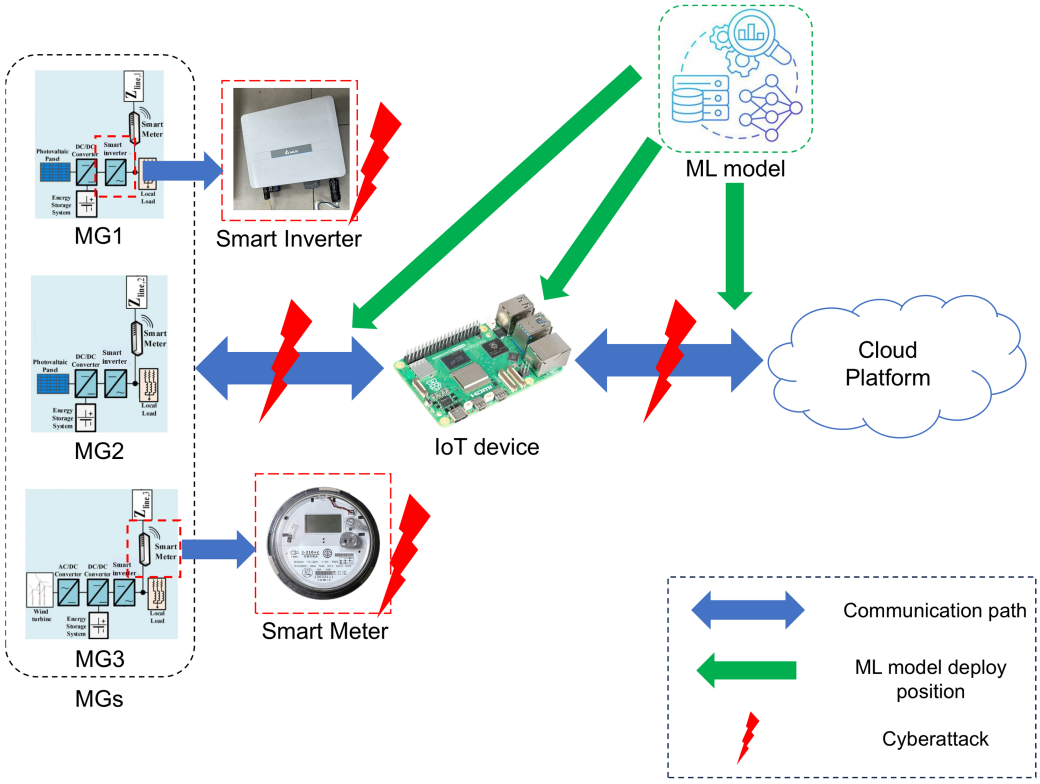

Figure 13 **The cyberattack attack path and targets with the viable position to deploy ML model.**
Full-size DOI: 10.7717/peerj-cs.3237/fig-13

to detect subtle anomalies in voltage and current signals and identify attacks early. The model has been trained on simulated attack scenarios and achieves exceptional accuracy in distinguishing between normal grid operation and compromised states. The researchers propose a federated learning (FL) system for detecting FDIAs in distribution networks that offsets the inefficiencies and privacy risks of centralized methods through an end-edge cloud collaboration that distributes the computational tasks (*Li et al., 2024*). Key innovations include temporal-spatial Graph Convolutional Networks (GCN) that analyze temporal-spatial data correlations, demonstrating the potential of FL to strengthen cybersecurity while preserving data privacy.

Increasing reliance on IoT and communication networks exposes smart grids to cyber threats such as DoS attacks and malware intrusions, prompting researchers to use ML and DL techniques for robust countermeasures (*Hasan et al., 2024*). However, challenges such as hyperparameter optimization, critical feature selection, privacy assurance, and real-time detection require special attention. Without proper feature selection techniques, the performance of ML models decreases and increases the attack effect. There are three main types of feature selection techniques: first, rule-based; second, signature-based; and third, anomaly-based (*Mohammed et al., 2024*). Using the right features can not only reduce the attack effect but also reduce the computational cost. Most studies using ML techniques are based on supervised learning. Supervised learning requires labeled datasets with high

Table 10 Summary of ML-based cybersecurity applications in MGs.

Methods	Microgrid applications	Security approaches	Contributions	Critical insights
DWT and deep neural networks for AC SE FDIA detection (*Yu, Hou & Li, 2018*)	FDIA detection in AC systems (large MGs).	Temporal-spatial feature learning, anomaly detection *via* DNN.	Introduces combined DWT and DNN for AC state FDIA detection.	The study proposes a DWT-DNN-based FDIA detection method that achieves high accuracy in AC systems but requires extensive training and careful parameter tuning.
CNN with BDD for multilabel locational FDIA detection (*Wang, Bi & Zhang, 2020*)	FDIA locational detection in smart grids (microgrid level detection).	Multilabel classification with CNN, no alteration to existing systems.	First multilabel CNN-based FDIA locational detection framework.	The article proposes an accurate and efficient CNN-based FDIA locational detector but limits generalizability due to reliance on synthetic data.
Wavelet singular value decomposition with DL (*Dehghani et al., 2020*)	FDIA detection in AC smart islands (MG scenarios)	Sliding mode control, feature extraction with wavelet singular values.	Novel FDIA detection model using wavelet SVD and deep learning.	The study develops a DL-based FDIA detection method with high accuracy, but its simulation-based validation limits practical applicability.
End-edge-cloud collaboration, FL, temporal–spatial GCN (*Li et al., 2024*)	FDIA detection in distribution networks using FL.	Privacy-preserving FL, distributed detection, edge-cloud aggregation.	First end-edge-cloud FDIA detection with FL and temporal–spatial GCN.	The article presents a federated TSGCN-based FDIA detection framework that enhances scalability and privacy but slightly compromises accuracy and struggles with subtle attacks.
Comprehensive ML and DL review for CPS security (*Hasan et al., 2024*)	Smart grid CPS cybersecurity (general overview including MGs).	Analyzes security protocols, attack mitigation, detection strategies.	Comprehensive ML-based security review, gaps and future directions.	The article offers a comprehensive ML-based review for smart grid cyber-physical systems security but lacks real-world validation and deployment insights.
Feature selection evaluation with ML methods (*Mohammed et al., 2024*)	Smart grid cyberattacks detection (includes MG relevance).	Supervised, semi-supervised, ensemble ML with feature selection.	Evaluation of FS techniques for attack detection improvement.	Heuristic and embedded feature selection significantly improve the accuracy and efficiency of ML-based smart grid attack detection but face limited validation, scalability challenges, and reliance on synthetic datasets.
Unsupervised learning (clustering, association rule mining) (*Pinto, Siano & Parente, 2023*)	MG FDIA detection with unsupervised learning approaches.	Anomaly detection using clustering, association rule mining.	Highlights use of unsupervised learning for FDIA detection.	Clustering and association rule mining enable detection of novel false data injection attacks without labeled data but demand high computational resources and yield reduced accuracy under severe tampering.
ML challenges in MG attack detection, intrusion detection system (IDS) analysis (*Ramotsoela, Hancke & Abu-Mahfouz, 2023*)	Challenges and considerations of ML-based IDS for microgrids.	Practical IDS deployment challenges, behavior-based detection emphasis.	Generalizes IDS deployment challenges in microgrid applications.	The article shows that adaptive, ensemble, and context-aware ML intrusion detection effectively detects data integrity and DoS attacks in microgrids but induces high false positives and burdens resource-constrained devices with intensive preprocessing.

quality and large quantity, which are difficult to obtain in the real world. Therefore, unsupervised learning approaches that use clustering algorithms and data mining to detect anomalies without prior attack knowledge can be more effective compared to supervised learning approaches (*Pinto, Siano & Parente, 2023*). In practice, other constraints must be considered when adapting ML approaches for cybersecurity in MG environments, such as

computational limitations, communication overhead, and false positive rates (FPR). To mitigate this, hybrid approaches that combine signature-based detection with adaptive learning models can provide more flexibility and robust mechanisms (*Ramotsoela, Hancke & Abu-Mahfouz, 2023*). Table 10 summarizes the ML-based framework for cybersecurity application in MGs.

Based on our review, the choice of an ML technique should be directly tied to the specific cybersecurity challenge it aims to solve within the MG context. We offer the following perspective:

- **For Real-Time Attack Detection**: DL models, particularly RNNs like LSTM and GRU, are exceptionally well-suited. MG operations are inherently time-series-based (*e.g.*, voltage, current, frequency data). RNNs excel at learning temporal dependencies, allowing them to accurately model normal grid behavior and flag subtle deviations indicative of an attack. For attacks manifesting across multiple nodes, CNNs can be highly effective in learning spatial correlations from sensor data to pinpoint the attack location.
- **For Autonomous Resilience and Defense**: RL is the most promising approach for moving beyond passive detection to active defense. An RL agent can be trained to make optimal control decisions, such as isolating a compromised part of the grid or re-dispatching energy, to maintain stability during an attack. Its trial-and-error learning mechanism makes it adaptive to novel, zero-day threats without signatures.
- **For Privacy-Preserving Collaborative Security**: FL is the superior architecture in multi-stakeholder MG environments where data sharing is restricted. It allows multiple MGs to collaboratively train a robust detection model without sharing their sensitive raw data, sharing only anonymized model updates. This is crucial for building collective intelligence while respecting data privacy.
- **For Environments with Limited Data**: the challenge of obtaining large, labeled datasets of real-world attacks is significant. Unsupervised learning methods are invaluable for anomaly detection, as they do not require pre-labeled data. Furthermore, TL offers a practical solution by enabling the adaptation of models trained on extensive datasets from other domains to the MG context with minimal fine-tuning.

COMBINE BLOCKCHAIN AND MACHINE LEARNING

Blockchain secures data integrity in microgrids; ML detects FDIAs and malware. Their synergy enables decentralized trust, mitigates vulnerabilities and ensures scalable, privacy-preserving defenses for resilient energy systems. The integration of blockchain and ML establishes a robust cyber-defense framework, wherein each technology mutually mitigates the inherent limitations of the other. While powerful, ML models exhibit vulnerabilities to adversarial attacks and data poisoning, compromising the reliability of their decisions if the integrity of their training data is undermined. Blockchain technology addresses this vulnerability by providing a cryptographically secure and auditable trail. Storing ML training data, models, and real-time sensor readings on an immutable and

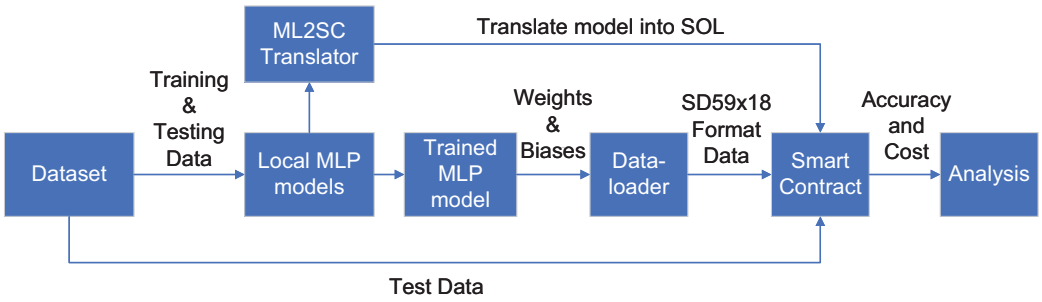

Figure 14 **Combining smart contract and ML model and deploying on the blockchain.**
Full-size DOI: 10.7717/peerj-cs.3237/fig-14

decentralized ledger ensures the trustworthiness of the data that informs ML-driven decisions. Conversely, ML models function as intelligent oracles for smart contracts. Upon detecting a threat, an ML model can initiate a defensive action codified within a smart contract, such as revoking device access credentials or isolating a microgrid segment. This process creates a secure, automated, and transparent response loop. Smart contracts are one of the most important and secure application implementations of blockchain. Since a smart contract has the property that once it is written, it cannot be changed or modified, combined with its tamper resistance and the detection sensitivity provided by ML models, it can detect and defend against cyberattacks. The author of *Li, Vott & Krishnamachar (2024)* suggested training the ML model with smart contracts as training data. Since a smart contract must be designed with its programming language, it can be translated. Figure 14 (*Li, Vott & Krishnamachar, 2024*) shows the combination of a smart contract and an ML model. Although the smart contract is immutable, it is not impossible to update it as the attack methods may evolve. The methods have been converted into an open-source tool and can be found on GitHub, as stated by the authors (*Vott, Li & Krishnamachari, 2023*).

The authors of *Albakri, Alabdullah & Alhayan (2023)* have developed a cryptocurrency-based framework that combines blockchain technology with DL models and optimizes them using a hybrid metacomputation method. They presented the Blockchain-assisted Hybrid Metaheuristics with Machine Learning-based Cyber Attack Detection and a Classification (BHMML-CADC) model, which uses the Ethereum blockchain to ensure transparency and prevent tampering in network attack detection records. The model integrates a quasi-recurrent neural network (QRNN) and applies Hunter-Prey optimization (HPO) to refine the parameters. To improve performance, the team has also used biologically inspired swarm optimization techniques, adding another layer of innovation to its approach. As EV become more widespread, the charging system for EVs with MGs faces further challenges. Two persistent challenges are trust and scalability. Researchers (*Kashyap et al., 2024*) have tackled both problems using blockchain and quantum RL approaches, categorizing them as energy trading optimization problems with cybersecurity. Their approach, Blockchain and quantum Machine learning driven Energy Trading model for EVs (B-MET), treats EVs and MGs as environments for the

Table 11 Summary of combined blockchain and ML cybersecurity applications in MGs.

Methods	Microgrid applications	Security approaches	Contributions	Critical insights
ML2SC Translator (PyTorch to Solidity), On-chain MLP models (*Li, Vott & Krishnamachar, 2024*).	Deploying ML models as smart contracts for verifiable inference.	On-chain computation using Solidity, fixed-point math, verifiable ML inference.	Built the first open-source translator for PyTorch models to Solidity smart contracts	The ML2SC framework accurately translates PyTorch MLPs into Solidity for on-chain execution while preserving off-chain accuracy, yet substantially elevates gas consumption and confines deployment to elementary architectures.
Blockchain, Hybrid Metaheuristics, QRNN, HPO (*Albakri, Alabdullah & Alhayan, 2023*).	Cyberattack detection and classification in MG with IoT.	Ethereum blockchain, optimization-based detection, feature selection.	Proposed blockchain-assisted hybrid metaheuristic DL detection framework.	The blockchain-enabled metaheuristic-driven QRNN attains up to 99.74% accuracy on the BoT-IoT dataset but its intricate feature-selection, hyperparameter-tuning, and blockchain overhead impede real-time deployment and wider applicability.
Blockchain, quantum RL, MDP formulation (*Kashyap et al., 2024*).	P2P energy trading for EVs.	Consortium blockchain, decentralized auditing, quantum RL optimization.	Designed quantum RL-based energy trading system with consortium blockchain.	The B-MET framework secures P2P energy trading *via* consortium blockchain with quantum RL achieving 0.92 utility in 160 episodes but its quantum virtual machines, Grover amplification, and Fabric dependencies incur heavy overhead.
Federated Learning (FL-XGB), Blockchain Smart Contracts (*Sundareswaran & Sasirekha, 2023*).	Intrusion analysis and secure communication in MGs.	Blockchain-based Federated Learning Smart Contracts.	Introduced FL-XGB with blockchain for intrusion detection in MGs.	The integration of federated XGBoost with blockchain achieves approximately 99% intrusion detection accuracy and immutable audit logs while imposing considerable computational and storage overhead.
DT, SDN, Blockchain Authentication, Deep Learning (Bi-GRU) (*Kumar et al., 2023*).	MG cybersecurity, intrusion detection, real-time monitoring.	Blockchain-based mutual authentication, SDN security, DL-based IDS.	Developed integrated digital twin-SDN-Blockchain system for grid security.	The proposed digital twin–driven SDN with blockchain authentication and self-attention Bi-GRU achieves 99.73% real-time intrusion detection accuracy but adds substantial complexity and scalability overhead

interaction of multiple agents that directly broking energy transactions. By using a consortium blockchain, the exposure to a single failure is avoided, while quantum RL interacts with complex, large-scale situations that would overwhelm typical ML models and conventional algorithms. The system learns the best trading strategies to encourage more MGs to participate in local energy trading by balancing loan amounts, shared energy quantities, and energy prices. The authors of *Sundareswaran & Sasirekha (2023)* have proposed a privacy-preserved approach to detect cyberattacks on multiple MGs. They present a combination of blockchain and FL and use Extreme Gradient Boosting (XGBoost) to classify the attacks. The participating nodes learn autonomously from local data in a decentralized environment and only share aggregated insights with the blockchain. This not only protects privacy, but also builds a collective intellect that is more powerful than the work of a single person. MGs with an increasing penetration of REs increase the complexity of connecting with different buyers, such as EVs and smart homes. Vulnerabilities lurk in this sophisticated network. This problem has been addressed by

researchers using Digital Twin (DT) technology to mirror the MG system with digital immunity and monitor MG behavior in real time (*Kumar et al., 2023*). At its core, it is a software-defined network (SDN) that redirects traffic securely, efficiently and dynamically. The framework combines blockchain-based authentication to secure the communication in between and its legitimacy and verification, with the bi-directional GRU (Bi-GRU) DL model as IDS detection that uncovers anomalies in communication patterns. Table 11 summarizes the combination of blockchain and ML for the framework for cybersecurity applications in MGs.

PROSPECTIVE INTEREST IN RESEARCH AND DEVELOPMENT

Interest in merging blockchain and ML to secure MGs is growing as cyberthreats become more sophisticated. Blockchain anchors trust by enshrining data integrity in decentralized networks, making tampering nearly impossible. Meanwhile, ML algorithms analyze real-time grid data to detect anomalies such as FDIA or DoS attacks before they escalate. Together, they form a dynamic defense: the immutable ledgers of the blockchain validate transactions *via* smart contracts, while ML adapts to new attack patterns by training on secure, decentralized datasets. This combination solves critical problems such as protecting solar inverters or defending against malware that disrupts the power grid without compromising privacy. There are still some challenges, such as balancing computing speed with ironclad security, but early breakthroughs point to a future where MGs heal themselves from attacks, maintain seamless energy flows and outpace hackers. By combining the transparency of blockchain with the predictive power of ML, researchers are not only fixing vulnerabilities but redefining the resilience of future energy grids.

Complex MG systems with high dependencies and high data requirements need advanced methods that combine blockchain and machine learning technologies for improved cybersecurity (*Ghadi et al., 2024*). Several possible future research directions can be derived from the results of current research.

- DL holds great potential when integrated with blockchain-based data integrity capabilities (*Dong, Li & Kamruzzaman, 2023*). Together, the integration can enable both accurate forecasting and immutable, verifiable audit trails in microgrid security designs.
- Hybrid RL models deployed on IoT devices offer promising paths to decentralized management and energy conservation. However, future study will attempt to address the inherent security challenges of such RL models by utilizing blockchain technologies to protect the data from tampering, unwanted interferences, complexity and economic prohibitions during computations.
- The diversity of future experimental conditions limits the applicability of machine learning algorithms to microgrid environments. This limitation underscores the need for standardized blockchain-based collaboration and data sharing platforms that would facilitate reproducible research, systematic testing of algorithms, and consensus-based identification of the most effective machine learning methods tailored to specific microgrid environments.

- In addition, the establishment of secure, blockchain-based cloud platforms for interdisciplinary collaboration between researchers, industry stakeholders, and policymakers is recommended. These platforms would accelerate the development and deployment of ML solutions in the MG industry and also promote transparency, trust and immunity to emerging cyberthreats.

OPEN CHALLENGES AND QUESTIONS

- **Interoperability and standardization**: the integration of blockchain and ML technologies into microgrid systems offers promising improvements in security, efficiency and resilience. These technologies individually contribute to improved data integrity, real-time analytics and automated decision making. However, the lack of uniform standards for integrating these technologies across different platforms poses a major challenge, especially in hybrid AC/DC microgrid systems that use a variety of communication protocols, which could be considered an open question and challenge for the future.
- **Energy-computation trade-offs**: the energy overhead is always caused by consensus mechanisms (*e.g.*, Proof of Work (PoW), Proof of Stake (PoS)). Moreover, the use of ML/DL techniques always consumes a lot of energy during the training process in microgrids, especially when resources are limited and constrained. This is a major gap for large-scale deployment in practice for real-world scenarios.
- **Adversarial Robustness of Hybrid Systems**: the use of immutable blockchain ledgers for ML training data can ensure cryptographic audit trails, tamper-proof storage and decentralized consensus on the provenance of the data. However, this mechanism can lead to critical unresolved tensions with adversary robustness, such that some irrevocable datasets on the vulnerability of models to circumvention attacks are yet to be verified.
- **Human-Centric Security Governance**: this raises significant concerns about accountability, operational transparency and system reliability, as the autonomous blockchain ML systems operate without a human oversight framework for cyber incidents. It is necessary that a human is involved in the system and that resilience protocols are in place to overcome the issues related to system vulnerabilities, trust undermining and ethical and legal dilemmas in critical applications.

CONCLUSIONS

The integration of blockchain and ML represents a transformative approach to addressing cybersecurity challenges in MGs. As these energy systems become more complex and interconnected, their vulnerability to cyber threats increases, requiring innovative solutions. With its decentralized architecture, immutability and cryptographic security, blockchain technology ensures robust data integrity and secure transaction management. Meanwhile, ML improves threat detection and response through advanced anomaly identification, predictive analytics and adaptive learning from real-time data streams. Together, these technologies form a synergistic defense framework: blockchain enhances

trust and transparency in data sharing, while ML dynamically mitigates evolving threats, creating a resilient, layered security posture.

However, there are other challenges. The limited scalability and latency of the blockchain must be reconciled with the real-time requirements of MG operations, while ML faces hurdles in data quality, model robustness and vulnerability to adversarial attacks. Furthermore, the integration of these technologies requires efficient data interoperability and energy-efficient design to avoid increasing computational overhead. Future research should focus on scalable consensus algorithms, lightweight blockchain architectures and FL techniques to preserve data privacy. Integrated systems combining blockchain traceability with ML adaptability could strengthen resilience against advanced cyber-physical threats. Collaboration between policymakers, industry stakeholders and researchers is crucial to create standardized protocols and regulatory frameworks that support secure and sustainable deployment.

A focused cybersecurity strategy is essential for the practical implementation of ML and blockchain in MGs. Countering high-impact threats like FDIAs requires real-time ML analysis, necessitating a trade-off between the accuracy of complex models and the efficiency of lightweight algorithms for edge deployment. Furthermore, the scarcity of labeled attack data makes unsupervised learning critical for detecting novel zero-day threats. While these technical limitations must be overcome through interdisciplinary innovation, the immense potential of combining ML with blockchain for MG protection is clear. Through the simultaneous advancement of these technologies, the vision of safe, smart, and self-healing energy systems is becoming increasingly tangible.

LIST OF ABBREVIATIONS

A2C	Actor-Critic
AWGN	Additive White Gaussian Noise
AMI	Advanced metering infrastructure
ASB	Advanced Solana Blockchain
AVOA	African Vulture Optimization Algorithm
ANN	Artificial Neural Networks
BDD	Bad Data Detectors
BIM	Basic Iterative Method
Bi-GRU	Bi-Directional Gate Recurrent Unit
CBE	Computing Balance-Based Exchange
CNN	Convolutional Neural Networks
CGG	Cyber Grid Guard
DT	Decision Trees
DBN	Deep Belief Network
DL	Deep Learning
DNN	Deep Neural Networks
DQN	Deep Q-networks

DPoS	Delegated Proof-of-Stake
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DERs	Distributed Energy Resources
DLT	Distributed Ledger Technology
EV	Electric Vehicles
ECDSA	Elliptic Curve Digital Signature Algorithm
EMS	Energy Management System
ESS	Energy Storage Systems
EL	Ensemble Learning
FDIA	False Data Injection Attacks
FPR	False Positive Rates
FGSM	Fast Gradient Sign Method
FL	Federated Learning
FMDP	Finite Markov Decision Process
FOTA	Firmware Over-The-Air
GRU	Gate Recurrent Unit
GPR	Gaussian Process Regression
GCN	Graph Convolutional Networks
HPO	Hunter-Prey optimization
ICT	Information And Communication Technologies
IT	Information Technology
IED	Intelligent Electronic Devices
IPT	Interior Point Techniques
IoT	Internet Of Things
IDS	Intrusion Detection Systems
LSTM	Long Short Term Memory
ML	Machine Learning
MiTM	Man-in-the-Middle
MDP	Markov Decision Process
MG	Microgrids
NN	Neural Network
OT	Operational Technology
PAR	Peak-to-Average Ratio
P2P	Peer-to-Peer
PGD	Projected Gradient Descent
PoA	Proof-of-Authority
PoET	Proof-of-Elapsed-Time
PoI	Proof-of-Identity
PoS	Proof-of-Stake
PoW	Proof-of-Work

QRNN	Quasi-Recurrent Neural Network
RASSIFAB	Resilient Authenticated Smart-Inverter Secure Firmware *Via* Auditable Blockchain
RNN	Recurrent Neural Networks
RL	Reinforcement Learning
RVM	Relevance Vector Machines
RTU	Remote Terminal Units
RE	Renewable Energy
REC	Renewable Energy Certificates
REG	Renewable Energy Generation
RESs	Renewable Energy Sources
RA	Replay Attack
RC	Reservoir Computing
SMO	Sequential Minimal Optimization
SMIB	Single-Machine Infinite Bus
SDN	Software-Defined Network
SE	State Estimation
SGD	Stochastic Gradient Descent
SVM	Support Vector Machine
SVC	Support Vector Clustering
SA	Switching Attacks
TDA	Time Delay Attack
TL	Transfer Learning
WTs	Wavelet Transforms
XGBoost	eXtreme Gradient Boosting

ACKNOWLEDGEMENTS

In this article, AI tools were strategically utilized to enhance efficiency and rigor across research, writing, and editing phases. AI writing assistants, such as Grammarly, were used for grammar checking to ensure the correctness of grammar; QuillBot was used primarily for improving writing and grammar checking; ChatGPT was used to perform summarization on partial references; and EndNote was used for managing reference citations.

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

This work was supported by National Science and Technology Council of Taiwan under Grants MOST 110-2221-E-992-044-MY3, NSTC 113-2221-E-992-037, 113-2218-E-992-003, 113-2221-E-992 -086 -MY3. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Grant Disclosures

The following grant information was disclosed by the authors:
National Science and Technology Council of Taiwan: 110-2221-E-992-044-MY3, NSTC 113-2221-E-992-037, 113-2218-E-992-003 and 113-2221-E-992 -086 -MY3.

Competing Interests

The authors declare that they have no competing interests.

Author Contributions

- Chou-Mo Yang conceived and designed the experiments, performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.
- Chun-Lien Su analyzed the data, authored or reviewed drafts of the article, and approved the final draft.
- Mahmoud Elsisi conceived and designed the experiments, performed the experiments, analyzed the data, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

This is a literature review.

REFERENCES

Abdi N, Albaseer A, Abdallah M. 2024. The role of deep learning in advancing proactive cybersecurity measures for smart grid networks: a survey. *IEEE Internet of Things Journal* **11(9)**:16398–16421 DOI 10.1109/JIOT.2024.3354045.

Ahmad G, Hassan A, Islam A, Shafiullah M, Abido MA, Al-Dhaifallah M. 2025. Distributed control strategies for microgrids: a critical review of technologies and challenges. *IEEE Access* **13(4)**:60702–60719 DOI 10.1109/ACCESS.2025.3552940.

Ahmethodzic L, Music M. 2021. Comprehensive review of trends in microgrid control. *Renewable Energy Focus* **38(3)**:84–96 DOI 10.1016/j.ref.2021.07.003.

Akkaoui R, Stefanov A, Palensky P, Epema DHJ. 2024. Resilient, auditable, and secure iot-enabled smart inverter firmware amendments with blockchain. *IEEE Internet of Things Journal* **11(5)**:8945–8960 DOI 10.1109/JIOT.2023.3321954.

Albakri A, Alabdullah B, Alhayan F. 2023. Blockchain-assisted machine learning with hybrid metaheuristics-empowered cyber attack detection and classification model. *Sustainability* **15(18)**:13887 DOI 10.3390/su151813887.

Ali Z, Hussain T, Su CL, Sadiq M, Jurcut AD, Tsao SH, Lin PC, Terriche Y, Elsisi M. 2024. A new paradigm for adaptive cyber-resilience of DC shipboard microgrids using hybrid signal processing with deep learning method. *IEEE Transactions on Transportation Electrification* **11(1)**:4280 DOI 10.1109/TTE.2024.3459856.

Appasani B, Mishra SK, Jha AV, Mishra SK, Enescu FM, Sorlei IS, Bîrleanu FG, Takorabet N, Thounthong P, Bizon N. 2022. Blockchain-enabled smart grid applications: architecture, challenges, and solutions. *Sustainability* **14(14)**:8801 DOI 10.3390/su14148801.

AWS. 2023. What is blockchain?-Blockchain technology explained-AWS. *Available at https://aws.amazon.com/what-is/blockchain/* (accessed 19 July 2024).

Buterin V. 2014. A next-generation smart contract and decentralized application platform. *White Paper* **3(37)**:2-1.

Cagnano A, Tuglie EDe, Mancarella P. 2020. Microgrids: overview and guidelines for practical implementations and operation. *Applied Energy* **258(2)**:114039 DOI 10.1016/j.apenergy.2019.114039.

Canaan B, Colicchio B, Abdeslam DO. 2020. Microgrid cyber-security: review and challenges toward resilience. *Applied Sciences* **10(16)**:5649 DOI 10.3390/app10165649.

Chen J, Yan J, Kemmeugne A, Kassouf M, Debbabi M. 2025. Cybersecurity of distributed energy resource systems in the smart grid: a survey. *Applied Energy* **383(3)**:125364 DOI 10.1016/j.apenergy.2025.125364.

Cho K, van Merriënboer B, Gulcehre C, Bahdanau D, Bougares F, Schwenk H, Bengio Y. 2014. Learning phrase representations using RNN encoder-decoder for statistical machine translation. In: *Association for Computational Linguistics, in Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*. Doha, Qatar, 1724–1734 DOI 10.3115/v1/D14-1179.

Conti M, Dragoni N, Lesyk V. 2016. A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials* **18(3)**:2027–2051 DOI 10.1109/COMST.2016.2548426.

Dai J, Yang J, Wang Y, Xu Y. 2024. Blockchain-enabled cyber-resilience enhancement framework of microgrid distributed secondary control against false data injection attacks. *IEEE Transactions on Smart Grid* **15(2)**:2226–2236 DOI 10.1109/TSG.2023.3328383.

Dehghani M, Kavousi-Fard A, Dabbaghjamanesh M, Avatefipour O. 2020. Deep learning based method for false data injection attack detection in AC smart islands. *IET Generation, Transmission & Distribution* **14(24)**:5756–5765 DOI 10.1049/iet-gtd.2020.0391.

Dong KAS, Li M, Kamruzzaman J. 2023. Blockchain technology and application: an overview. *PeerJ Computer Science* **9**:1705 DOI 10.7717/peerj-cs.1705.

Dusane PS, Pavithra Y. 2020. Logic bomb: an insider attack. *International Journal of Advanced Trends in Computer Science and Engineering* **9(3)**:3662–3665 DOI 10.30534/ijatcse/2020/176932020.

Dutta SD, Prasad R. 2020. Cybersecurity for microgrid. In: *2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC), 19–26 Oct. 2020*, 1–5 DOI 10.1109/WPMC50192.2020.9309494.

Elsisi M, Rusidi AL, Tran MQ, Su CL, Ali MN. 2024. Robust indoor positioning of automated guided vehicles in internet of things networks with deep convolution neural network considering adversarial attacks. *IEEE Transactions on Vehicular Technology* **73(6)**:7748–7757 DOI 10.1109/TVT.2024.3357780.

Elsisi M, Su CL, Ali MN. 2024. Design of reliable IoT systems with deep learning to support resilient demand side management in smart grids against adversarial attacks. *IEEE Transactions on Industry Applications* **60(2)**:2095–2106 DOI 10.1109/TIA.2023.3297089.

Elsisi M, Yu JT, Lai CC, Su CL. 2024. A drone-assisted deep learning-based iot system for monitoring ship emissions in ports considering adversarial attacks. *IEEE Transactions on Instrumentation and Measurement* **73**:1–11 DOI 10.1109/TIM.2024.3374306.

Ester M, Kriegel H-P, Sander J, Xu X. 1996. A density-based algorithm for discovering clusters in large spatial databases with noise. In: *Proceedings of the Second International Conference on Knowledge Discovery and Data Mining*. Portland, Oregon.

Estrach JB, Szlam A, LeCun Y. 2014. Signal recovery from pooling representations. In: *Proceedings of the 31st International Conference on Machine Learning, Proceedings of Machine Learning Research*.

Faheem M, Kuusniemi H, Eltahawy B, Bhutta MS, Raza B. 2024. A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications. *IET Generation, Transmission & Distribution* **18(3)**:625–638 DOI 10.1049/gtd2.13103.

Fatima S, Arshad MJ. 2025. A comprehensive review of blockchain and machine learning integration for peer-to-peer energy trading in smart grids. *IEEE Access* **13(3)**:92756–92782 DOI 10.1109/ACCESS.2025.3572174.

FIPS Pub. 2012. Secure hash standard (shs). *FIPS Pub* **180(4)**:180–184 DOI 10.6028/NIST.FIPS.180-4.

Fritz JJ, Sagisi J, James J, Leger AS, King K, Duncan KJ. 2019. Simulation of man in the middle attack on smart grid testbed. In: *2019 SoutheastCon, 11–14 April 2019*, 1–6 DOI 10.1109/SoutheastCon42311.2019.9020426.

Gad AG, Mosa DT, Abualigah L, Abohany AA. 2022. Emerging trends in blockchain technology and applications: a review and outlook. *Journal of King Saud University-Computer and Information Sciences* **34(9)**:6719–6742 DOI 10.1016/j.jksuci.2022.03.007.

Gaggero GB, Girdinio P, Marchese M. 2021. Advancements and research trends in microgrids cybersecurity. *Applied Sciences* **11(16)**:7363 DOI 10.3390/app11167363.

Ghadi TMYY, Aurangzeb K, Haq I, Shahzad T, Laghari AA, Anwar MS. 2024. Security risk models against attacks in smart grid using big data and artificial intelligence. *PeerJ Computer Science* **10(1840)**:e1840 DOI 10.7717/peerj-cs.1840.

Goodfellow I, Bengio Y, Courville A. 2016. *Deep learning*. Cambridge, Massachusetts: MIT Press.

Goodfellow IJ, Shlens J, Szegedy C. 2014. Explaining and harnessing adversarial examples. ArXiv DOI 10.48550/arXiv.1412.6572.

Haber S, Stornetta WS. 1991. How to time-stamp a digital document. *Journal of Cryptology* **3(2)**:99–111 DOI 10.1007/BF00196791.

Hahn G, Piesciorovsky EC, Hink RB, Werth A. 2024. Detection of faulted phases in a medium-voltage main feeder using the cyber grid guard system with distributed ledger technology. *International Journal of Electrical Power & Energy Systems* **161(3)**:110162 DOI 10.1016/j.ijepes.2024.110162.

Halgamuge MN. 2024. Leveraging deep learning to strengthen the cyber-resilience of renewable energy supply chains: a survey. *IEEE Communications Surveys & Tutorials* **26(3)**:2146–2175 DOI 10.1109/COMST.2024.3365076.

Hasan MK, Abdulkadir RA, Islam S, Gadekallu TR, Safie N. 2024. A review on machine learning techniques for secured cyber-physical systems in smart grid networks. *Energy Reports* **11(May 2019)**:1268–1290 DOI 10.1016/j.egyr.2023.12.040.

Hasankhani A, Hakimi SM, Bisheh-Niasar M, Shafie-khah M, Asadolahi H. 2021. Blockchain technology in the future smart grids: a comprehensive review and frameworks. *International Journal of Electrical Power & Energy Systems* **129(22)**:106811 DOI 10.1016/j.ijepes.2021.106811.

Hinton GE, Osindero S, Teh Y-W. 2006. A fast learning algorithm for deep belief nets. *Neural Computation* **18(7)**:1527–1554 DOI 10.1162/neco.2006.18.7.1527.

Hochreiter S, Schmidhuber J. 1997. Long short-term memory. *Neural Computation* **9(8)**:1735–1780 DOI 10.1162/neco.1997.9.8.1735.

Hong YY, Alano FI, Lee YD, Jiang JL, Yeh JN. 2024. Digital twin-based blockchain for power support in networked microgrids. *IEEE Access* **12**:86675–86689 DOI 10.1109/ACCESS.2024.3416672.

IBM. 2021. What is blockchain? | IBM. *Available at https://www.ibm.com/topics/blockchain* (accessed 16 July 2024).

Irmak E, Kabalci E, Kabalci Y. 2023. Digital transformation of microgrids: a review of design, operation, optimization, and cybersecurity. *Energies* **16(12)**:4590 DOI 10.3390/en16124590.

Islam S, Schwarz K, Bollens K, Hartmann M, Creutzburg R. 2025. A review of cyber security and challenges associated with microgrid systems. *Electronic Imaging* **37**:1–10 DOI 10.2352/EI.2025.37.3.MOBMU-315.

Jain A, Jat DS. 2022. A review on consensus protocol of blockchain technology. In: Nagar AK, Jat DS, Marín-Raventós G, Mishra DK, eds. *Intelligent Sustainable Systems*. Singapore: Springer Nature, 813–829 DOI 10.1007/978-981-16-6369-7_72.

Jamil N, Qassim QS, Bohani FA, Mansor M, Ramachandaramurthy VK. 2021. *Cybersecurity of microgrid: state-of-the-art review and possible directions of future research. Applied Sciences.* Vol. 11**(21)**:9812 DOI 10.3390/app11219812.

Jhaveri RH, Patel SJ, Jinwala DC. 2012. DoS attacks in mobile ad hoc networks: a survey. In: *2012 Second International Conference on Advanced Computing & Communication Technologies, 7–8 Jan. 2012*, 535–541 DOI 10.1109/ACCT.2012.48.

Johnson D, Menezes A, Vanstone S. 2001. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security* **1(1)**:36–63 DOI 10.1007/s102070100002.

Kashyap PK, Dohare U, Kumar M, Kumar S. 2024. Blockchain and quantum machine learning driven energy trading for electric vehicles. *Ad Hoc Networks* **165(4)**:103632 DOI 10.1016/j.adhoc.2024.103632.

Khan D, Jung LT, Hashmani MA, Waqas A. 2020. A critical review of blockchain consensus model. In: *3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. Sukkur, Pakistan: IEEE, 1–6 DOI 10.1109/iCoMET48670.2020.9074107.

Khubrani MM, Alam S. 2023. Blockchain-based microgrid for safe and reliable power generation and distribution: a case study of Saudi Arabia. *Energies* **16(16)**:5963 DOI 10.3390/en16165963.

King S, Nadal S. 2012. PPcoin: peer-to-peer crypto-currency with proof-of-stake. Self-published paper.

Konda V, Tsitsiklis J. 1999. Actor-critic algorithms. In: *Advances in Neural Information Processing Systems*, Vol. 12.

Košťál K, Khilenko V, Hunák M. 2024. Hierarchical blockchain energy trading platform and microgrid management optimization. *Energies* **17(6)**:1333 DOI 10.3390/en17061333.

Kulkarni S, Rahul RK, Shreyas R, Nagasundari S, Honnavalli PB. 2020. MITM intrusion analysis for advanced metering infrastructure communication in a smart grid environment. In: *Trends in Computational Intelligence, Security and Internet of Things*. Cham: Springer International Publishing, 256–267 DOI 10.1007/978-3-030-66763-4_22.

Kumar P, Kumar R, Aljuhani A, Javeed D, Jolfaei A, Islam AKMN. 2023. Digital twin-driven SDN for smart grid: a deep learning integrated blockchain for cybersecurity. *Solar Energy* **263(10)**:111921 DOI 10.1016/j.solener.2023.111921.

Kurakin A, Goodfellow IJ, Bengio S. 2018. Adversarial examples in the physical world. In: *Artificial Intelligence Safety and Security*. Florida, USA: Chapman and Hall/CRC, 99–112.

Lashkari B, Musilek P. 2021. A comprehensive review of blockchain consensus mechanisms. *IEEE Access* **9**:43620–43652 DOI 10.1109/ACCESS.2021.3065880.

Li H, Dou C, Yue D, Hancke GP, Zeng Z, Guo W, Xu L. 2024. End-edge-cloud collaboration-based false data injection attack detection in distribution networks. *IEEE Transactions on Industrial Informatics* **20(2)**:1786–1797 DOI 10.1109/TII.2023.3281664.

Li Z, Vott S, Krishnamachar B. 2024. ML2SC: deploying machine learning models as smart contracts on the blockchain. ArXiv DOI 10.48550/arXiv.2404.16967.

Li Y, Yan J. 2023. Cybersecurity of smart inverters in the smart grid: a survey. *IEEE Transactions on Power Electronics* **38(2)**:2364–2383 DOI 10.1109/TPEL.2022.3206239.

Liang G, Zhao J, Luo F, Weller SR, Dong ZY. 2017. A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid* **8(4)**:1630–1638 DOI 10.1109/TSG.2015.2495133.

Liberati F, Garone E, Giorgio ADi. 2021. Review of cyber-physical attacks in smart grids: a system-theoretic perspective. *Electronics* **10(10)**:1153 DOI 10.3390/electronics10101153.

Lin H, Kalbarczyk Z, Iyer RK. 2018. Impact of malicious SCADA commands on power grids' dynamic responses. In: *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 29–31 Oct. 2018*, 1–7 DOI 10.1109/SmartGridComm.2018.8587462.

Liu S, Feng X, Kundur D, Zourntos T, Butler-Purry K. 2011a. A class of cyber-physical switching attacks for power system disruption. In: *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*. Oak Ridge, Tennessee, USA DOI 10.1145/2179298.2179316.

Liu S, Feng X, Kundur D, Zourntos T, Butler-Purry KL. 2011b. Switched system models for coordinated cyber-physical attack construction and simulation. In: *2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS),17-17 Oct. 2011*, 49–54 DOI 10.1109/SGMS.2011.6089026.

Liu Y, Mao S, Mei X, Yang T, Zhao X. 2019. Sensitivity of adversarial perturbation in fast gradient sign method. In: *2019 IEEE Symposium Series on Computational Intelligence (SSCI), 6–9 Dec. 2019*, 6–9 DOI 10.1109/SSCI44817.2019.9002856.

Liu J, Xiao Y, Ghaboosi K, Deng H, Zhang J. 2009. Botnet: classification, attacks, detection, tracing, and preventive measures. *EURASIP Journal on Wireless Communications and Networking* **2009(1)**:692654 DOI 10.1155/2009/692654.

Madry A, Makelov A, Schmidt L, Tsipras D, Vladu A. 2017. Towards deep learning models resistant to adversarial attacks. ArXiv DOI 10.48550/arXiv.1706.06083.

Mariam L, Basu M, Conlon MF. 2016. Microgrid: architecture, policy and future trends. *Renewable and Sustainable Energy Reviews* **64(3)**:477–489 DOI 10.1016/j.rser.2016.06.037.

Masood F, Faridi AR. 2018. Consensus algorithms in distributed ledger technology for open environment. In: *2018 4th International Conference on Computing Communication and Automation (ICCCA), 14–15 Dec. 2018*, 14–15 DOI 10.1109/CCAA.2018.8777695.

Meslouhi SE, Fadil HE, Lassioui A, Hasni A, Fhail A. 2025. Internet of energy in microgrids and smart grids: state-of-the-art. In: *2025 5th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), 15–6 May 2025*, 15–16 DOI 10.1109/IRASET64571.2025.11008259.

Mnih V, Kavukcuoglu K, Silver D, Graves A, Antonoglou I, Wierstra D, Riedmiller MA. 2013. Playing atari with deep reinforcement learning. ArXiv DOI 10.48550/arXiv.1312.5602.

Mohammed SH, Al-Jumaily A, Singh MSJ, Jiménez VPG, Jaber AS, Hussein YS, Al-Najjar MMAK, Al-Jumeily D. 2024. A review on the evaluation of feature selection using machine

learning for cyber-attack detection in smart grid. *IEEE Access* **12(1)**:44023–44042 DOI 10.1109/ACCESS.2024.3370911.

Mololoth VK, Saguna S, Åhlund C. 2023. Blockchain and machine learning for future smart grids: a review. *Energies* **16(1)**:528 DOI 10.3390/en16010528.

Muhammad M, Alshra'a AS, German R. 2024. Survey of cybersecurity in smart grids protocols and datasets. *Procedia Computer Science* **241(3)**:365–372 DOI 10.1016/j.procs.2024.08.049.

Muhammad I, Yan Z. 2015. Supervised machine learning approaches: a survey. *ICTACT Journal on Soft Computing* **5(3)**:946 DOI 10.21917/ijsc.2015.0133.

Mutluri RB, Saxena D. 2024. A comprehensive overview and future prospectives of networked microgrids for emerging power systems. *Smart Grids and Sustainable Energy* **9(2)**:45 DOI 10.1007/s40866-024-00218-0.

Nakamoto S. 2008. Bitcoin: a peer-to-peer electronic cash system. *Available at https://bitcoin.org/bitcoin.pdf*.

Namanya AP, Cullen A, Awan IU, Disso JP. 2018. The world of malware: an overview. In: *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), 6–8 Aug. 2018*, 420–427 DOI 10.1109/FiCloud.2018.00067.

Naveen N. 2012. Application of relevance vector machines in real time intrusion detection. *International Journal of Advanced Computer Science and Applications* **3(9)**:48–53 DOI 10.14569/IJACSA.2012.030907.

Nejabatkhah F, Li YW, Liang H, Ahrabi RR. 2021. Cyber-security of smart microgrids: a survey. *Energies* **14(1)**:27 DOI 10.3390/en14010027.

Obulesu O, Mahendra M, ThrilokReddy M. 2018. Machine learning techniques and tools: a survey. In: *2018 International Conference on Inventive Research in Computing Applications (ICIRCA),11–12 July 2018*, 11–12 DOI 10.1109/ICIRCA.2018.8597302.

O'Shea K, Nash R. 2015. An introduction to convolutional neural networks. ArXiv DOI 10.48550/arXiv.1511.08458.

Pasqualetti F, Dörfler F, Bullo F. 2013. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control* **58(11)**:2715–2729 DOI 10.1109/TAC.2013.2266831.

Patle A, Chouhan DS. 2013. SVM kernel functions for classification. In: *2013 International Conference on Advances in Technology and Engineering (ICATE), 23–25 Jan. 2013*, 1–9 DOI 10.1109/ICAdTE.2013.6524743.

Paul P, Aithal P, Saavedra R, Ghosh S. 2021. Blockchain technology and its types—a short review. *International Journal of Applied Science and Engineering (IJASE)* **9(2)**:189–200.

Paul B, Sarker A, Abhi SH, Das SK, Ali MF, Islam MM, Islam MR, Moyeen SI, Badal MFR, Ahamed MH, Sarker SK, Das P, Hasan MM, Saqib N. 2024. Potential smart grid vulnerabilities to cyber attacks: current threats and existing mitigation strategies. *Heliyon* **10(19)**: e37980 DOI 10.1016/j.heliyon.2024.e37980.

Pinto SJ, Siano P, Parente M. 2023. Review of cybersecurity analysis in smart distribution systems and future directions for using unsupervised learning methods for cyber detection. *Energies* **16(4)**:1651 DOI 10.3390/en16041651.

Prasad S. 2020. Counteractive control against cyber-attack uncertainties on frequency regulation in the power system. *IET Cyber-Physical Systems: Theory & Applications* **5(4)**:394–408 DOI 10.1049/iet-cps.2019.0097.

Raja DJS, Sriranjani R, Parvathy A, Hemavathi N. 2022. A review on distributed denial of service attack in smart grid. In: *2022 7th International Conference on Communication and Electronics Systems (ICCES), 22–24 June 2022*, 812–819 DOI 10.1109/ICCES54183.2022.9835859.

Rajeyyagari S, Saravanan M, Pandey PS, Devi A, Shankar SS. 2024. Convolutional Neural network-based African vulture optimization algorithm for the enhancement of cybersecurity in the blockchain-based Smart grid. *Multimedia Tools and Applications* **83(20)**:58527–58553 DOI 10.1007/s11042-023-17805-5.

Ramotsoela DT, Hancke GP, Abu-Mahfouz AM. 2023. Practical challenges of attack detection in microgrids using machine learning. *Journal of Sensor and Actuator Networks* **12(1)**:7 DOI 10.3390/jsan12010007.

Rouhani SH, Su C-L, Mobayen S, Razmjooy N, Elsisi M. 2024. Cyber resilience in renewable microgrids: a review of standards, challenges, and solutions. *Energy* **309(5)**:133081 DOI 10.1016/j.energy.2024.133081.

Soumya KT, Jadoun VK, NS J, S S. 2024. A systematic study on the intelligent cyber security for smart microgrid. In: *2024 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), 22–24 June 2022*, 18–19 DOI 10.1109/DISCOVER62353.2024.10750634.

Sundareswaran N, Sasirekha S. 2023. Federated blockchain model for cyber intrusion analysis in smart grid networks. *Intelligent Automation & Soft Computing* **36(2)**:2129–2143 DOI 10.32604/iasc.2023.034381.

Sutton RS, Barto AG. 2018. *Reinforcement learning: an introduction*. Second Edition. Cambridge, Massachusetts: MIT Press.

Sutton RS, McAllester D, Singh S, Mansour Y. 1999. Policy gradient methods for reinforcement learning with function approximation. In: *Proceedings of the 13th International Conference on Neural Information Processing Systems*. Denver, CO.

Swathika OVG, Karthikeyan A, Rout K, Hatkar S. 2024. Cybersecurity deployment in smart grids: critical review, applications, protection, and challenges. *IEEE Access* **12**:113618–113641 DOI 10.1109/ACCESS.2024.3443312.

Taherdoost H. 2023. Smart contracts in blockchain technology: a critical review. *Information* **14(2)**:117 (In English) DOI 10.3390/info14020117.

The Investopedia Team. 2024. Permissioned blockchain: definition, examples, vs. permissionless. *Available at https://www.investopedia.com/terms/p/permissioned-blockchains.asp* (accessed 22 July 2024).

Tipping M. 1999. The relevance vector machine. In: *Advances in Neural Information Processing Systems*Vol. 12.

Tipping ME. 2001. Sparse Bayesian learning and the relevance vector machine. *Journal of Machine Learning Research* **1(Jun)**:211–244 DOI 10.1162/15324430152748236.

Tipping ME. 2003. Bayesian inference: an introduction to principles and practice in machine learning. In: Bousquet O, Luxburg V, Rätsch G, eds. *Advanced Lectures on Machine Learning: ML Summer Schools 2003, Canberra, Australia, February 2-14, 2003, Tübingen, Germany, August 4–16, 2003, Revised Lectures*. Berlin, Heidelberg: Springer Berlin Heidelberg, 41–62.

Uhrig RE. 1995. Introduction to artificial neural networks. *Proceedings of IECON '95-21st Annual Conference on IEEE Industrial Electronics* **1**:33–37 DOI 10.1109/IECON.1995.483329.

Usama M, Qadir J, Raza A, Arif H, l. A. Yau K, Elkhatib Y, Hussain A, Al-Fuqaha A. 2019. Unsupervised machine learning for networking: techniques, applications and research challenges. *IEEE Access* **7**:65579–65615 DOI 10.1109/ACCESS.2019.2916648.

Viriyasitavat W, Hoonsopon D. 2019. Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration* **13(2)**:32–39 DOI 10.1016/j.jii.2018.07.004.

Vott S, Li L, Krishnamachari B. 2023. ML_onChain: a python-solidity translator that generates on-chain neural networks. *Available at https://github.com/ANRGUSC/ML_onChain* (accessed 18 March 2025).

Wang S, Bi S, Zhang YJA. 2020. Locational detection of the false data injection attack in a smart grid: a multilabel classification approach. *IEEE Internet of Things Journal* **7(9)**:8218–8227 DOI 10.1109/JIOT.2020.2983911.

Watkins CJCH, Dayan P. 1992. Q-learning. *Machine Learning* **8(3)**:279–292 DOI 10.1007/BF00992698.

Wenyuan X, Ke M, Trappe W, Yanyong Z. 2006. Jamming sensor networks: attack and defense strategies. *IEEE Network* **20(3)**:41–47 DOI 10.1109/MNET.2006.1637931.

Wood G. 2024. Solidity. *Available at https://docs.soliditylang.org/en/v0.8.29/* (accessed 28 July 2024).

Wu Y, Weng J, Qiu B, Wei Z, Qian F, Deng RH. 2019. Random delay attack and its applications on load frequency control of power systems. In: *2019 IEEE Conference on Dependable and Secure Computing (DSC, 18–20 Nov. 2019*, 18–20 DOI 10.1109/DSC47296.2019.8937611.

Xiao Z, Wu J, Jenkins N. 2010. An overview of microgrid control. *Intelligent Automation & Soft Computing* **16(2)**:199–212 DOI 10.1080/10798587.2010.10643076.

Yaga D, Mell P, Roby N, Scarfone K. 2018. "Blockchain technology overview", National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8202. *Available at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf* (accessed 28 July 2024).

Yaghoubi E, Yaghoubi E, Yusupov Z, Maghami MR. 2024. A real-time and online dynamic reconfiguration against cyber-attacks to enhance security and cost-efficiency in smart power microgrids using deep learning. *Technologies* **12(10)**:197 DOI 10.3390/technologies12100197.

Yamashita K, Ten CW, Rho Y, Wang L, Wei W, Ginter A. 2020. Measuring systemic risk of switching attacks based on cybersecurity technologies in substations. *IEEE Transactions on Power Systems* **35(6)**:4206–4219 DOI 10.1109/TPWRS.2020.2986452.

Yamashita K, Ten C-W, Wang L. 2020. Dynamical analysis of cyber-related contingencies initiated from substations. In: Karimipour H, Srikantha P, Farag H, Wei-Kocsis J, eds. *Security of Cyber-Physical Systems: Vulnerability and Impact*. Cham: Springer International Publishing, 223–246.

Yi P, Zhu T, Zhang Q, Wu Y, Li J. 2014. A denial of service attack in advanced metering infrastructure network. In: *2014 IEEE International Conference on Communications (ICC)*, 10–14 DOI 10.1109/ICC.2014.6883456.

Yu JJQ, Hou Y, Li VOK. 2018. Online false data injection attack detection with wavelet transform and deep neural networks. *IEEE Transactions on Industrial Informatics* **14(7)**:3271–3280 DOI 10.1109/TII.2018.2825243.

Yuan Y, Li Z, Ren K. 2011. Modeling load redistribution attacks in power systems. *IEEE Transactions on Smart Grid* **2(2)**:382–390 DOI 10.1109/TSG.2011.2123925.

Zhang M, Liu Y, Cheng Q, Li H, Liao D, Li H. 2024. Smart grid security based on blockchain and smart contract. *Peer-to-Peer Networking and Applications* **17(4)**:2167–2184 DOI 10.1007/s12083-024-01703-0.

Zheng Z, Xie S, Dai H, Chen X, Wang H. 2017. An overview of blockchain technology: architecture, consensus, and future trends. In: *2017 IEEE International Congress on Big Data (BigData Congress), 25–30 June 201*, 557–564 DOI 10.1109/BigDataCongress.2017.85.

Zhou X, Guo T, Ma Y. 2015. An overview on microgrid technology. In: *2015 IEEE International Conference on Mechatronics and Automation (ICMA), 2–5 Aug. 2015*, 76–81 DOI 10.1109/ICMA.2015.7237460.

Zhu M, Martínez S. 2014. On the performance analysis of resilient networked control systems under replay attacks. *IEEE Transactions on Automatic Control* **59(3)**:804–808 DOI 10.1109/TAC.2013.2279896.