energies

MDPI

Review

Cyber Attacks in Cyber-Physical Microgrid Systems: A Comprehensive Review

Sriranga Suprabhath Koduru, Venkata Siva Prasad Machina and Sreedhar Madichetty *

Department of Electrical and Computer Engineering, Ecole Centrale School of Engineering, Mahindra University, Hyderabad 500043, India; sriranga20peee002@mahindrauniversity.edu.in (S.S.K.); venkatasivaprasad20peee004@mahindrauniversity.edu.in (V.S.P.M.)
* Correspondence: sreedhar.803@gmail.com

Abstract: The importance of and need for cyber security have increased in the last decade. The critical infrastructure of the country, modeled with cyber-physical systems (CPS), is becoming vulnerable because of a lack of efficient safety measures. Attackers are becoming more innovative, and attacks are becoming undetectable, thereby causing huge risks to these systems. In this scenario, intelligent and evolving detection methods should be introduced to replace basic and outworn methods. The ability of artificial intelligence (AI) to analyze data and predict outcomes has created an opportunity for researchers to explore the power of AI in cyber security. This article discusses new-age intelligence and smart techniques such as pattern recognition models, deep neural networks, generative adversarial networks, and reinforcement learning for cyber security in CPS. The differences between the traditional security methods used in information technology and the security methods used in CPS are analyzed, and the need for a transition into intelligent methods is discussed in detail. A deep neural network-based controller that detects and mitigates cyber attacks is designed for microgrid systems. As a case study, a stealthy local covert attack that overcomes the existing microgrid protection is modeled. The ability of the DNN controller to detect and mitigate the SLCA is observed. The experiment is performed in a simulation and also in real-time to analyze the effectiveness of AI in cyber security.

Keywords: cyber physical systems; cyber attacks; artificial intelligence; machine learning; deep learning

Citation: Suprabhath Koduru, S.; Machina, V.S.P.; Madichetty, S. Cyber Attacks in Cyber-Physical Microgrid Systems: A Comprehensive Review. *Energies* **2023**, *16*, 4573. https://doi.org/10.3390/en16124573

Academic Editor: Elhoussin Elbouchikhi

Received: 3 May 2023
Revised: 1 June 2023
Accepted: 5 June 2023
Published: 7 June 2023

1. Introduction

Microgrids, the new-age form of power grid architecture, are gaining increasing attention from researchers and industries. The possibility of integrating renewable generations, electric vehicles (EV), energy storage, and distributed energy resources into the power grid and coupling them with effective communication links presents an opportunity to improve the efficiency of the power grid [1]. Additionally, microgrids are capable of powering localized loads by operating in an isolated mode [2].

With the aim of reducing carbon emissions, renewable energy generation is encouraged in the power sector, and the transportation sector is moving towards the electrification of vehicles. To achieve sustainable development goals, by 2030, there exists a target to integrate 8000 GW of renewables (compared to the 2800 GW integrated at present). By 2025, at least 100 countries will aim to transition to 100% renewable generation. At present, Norway has achieved the most renewable power integration, with 99%; New Zealand (81%), Brazil (79%), Colombia (74%), Canada (68%), Sweden (67%), and Portugal (65.5%) follow. Saudi Arabia has achieved the least integration (0.1%).

The renewable energy share globally increased from 26.30% to 28.1% from 2020 to 2021. It has been observed that 17% of global CO_2 emissions are due to the transport sector; the global EV market has received huge support, which has led to over 16.5 million EVs on

the road. By 2030, 2% of global electrical demand is expected to be due to EVs. Microgrids are the best alternative to conventional grids in terms of grid integration with RES and EVs [3]; the variety of sources and loads that can be integrated into a microgrid is shown in Figure 1.

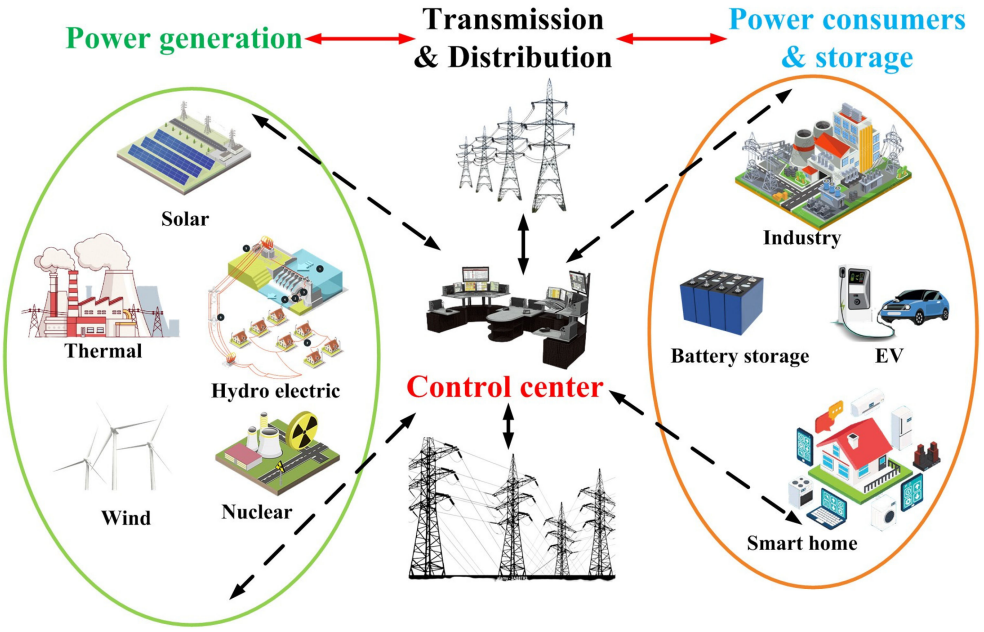

Figure 1. Overview of a microgrid.

With the variety of intermittent distributed energy resources that exists, information regarding load availability and demand on the grid should be continuously monitored and communicated to the controller for effective operation and control. The communication network is established based on the open system interconnection (OSI) model, transfer control protocol/internet protocol (TCP/IP) model, extensible authentication protocol (EAP), and microgrid communication [4,5]. Figure 2 denotes the different protocol structures. The development of Internet of Things (IoT) devices and architectures makes it viable to utilize the services of smart meters, smart health, smart transport, and smart grid [6]. IoT architecture is preferred on the demand side, whereas the EAP model is implemented on the supply side. The battlegrounds between countries have constantly been shifting. Intruding upon a country's cyberspace and attacking the communication channels of the enemy, thereby interrupting their information transfer, is the war strategy likely to be followed in the near future. This kind of war strategy is termed cyber warfare [7], and even the strongest and most developed countries are vulnerable to it. To overcome this, countries are focusing on building cyber security and creating cyber awareness [8–10]. According to the crunch base cyber security report [11], over the last decade, there has been an almost 700% increase in cyber security funding. The USA holds the greatest share (76%) of global cyber security funding, and Israel and the UK stand next with 13% and 3%, respectively; all the other countries account for 8%. There are seven different types of attacks, as shown in Figure 3, through which an attacker can create havoc in a country.

Espionage is a form of gentle cyber attack, where an attacking country tries to monitor and steal sensitive information by phishing attacks or botnets [12]. Sabotage attacks or cyber sabotage deliberately destroy critical infrastructure by introducing a malfunction into the system [13]. These attacks are frequently observed in the introduction of a software update bug. Flooding the communication channel with multiple requests, causing the channel to be irresponsive to legitimate users, is defined as a denial of service attack [14]. This attack is dangerous, and causes communication delays or interruptions, thereby affecting military bodies and research bodies. Cyber attacks on power grids are the most dangerous and

impactful phenomenon. They can cause interruptions in information sharing, disruption to critical services, and huge economic losses [15].

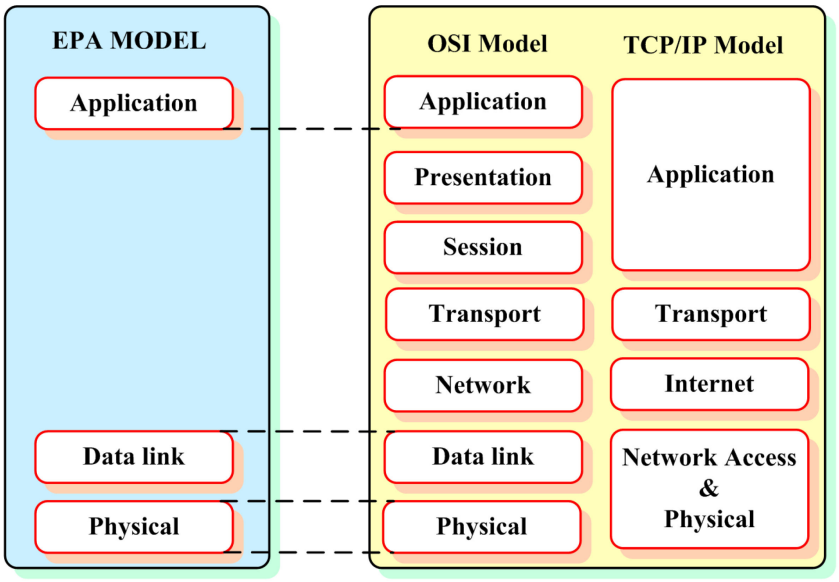

Figure 2. Communication models for microgrid communication.

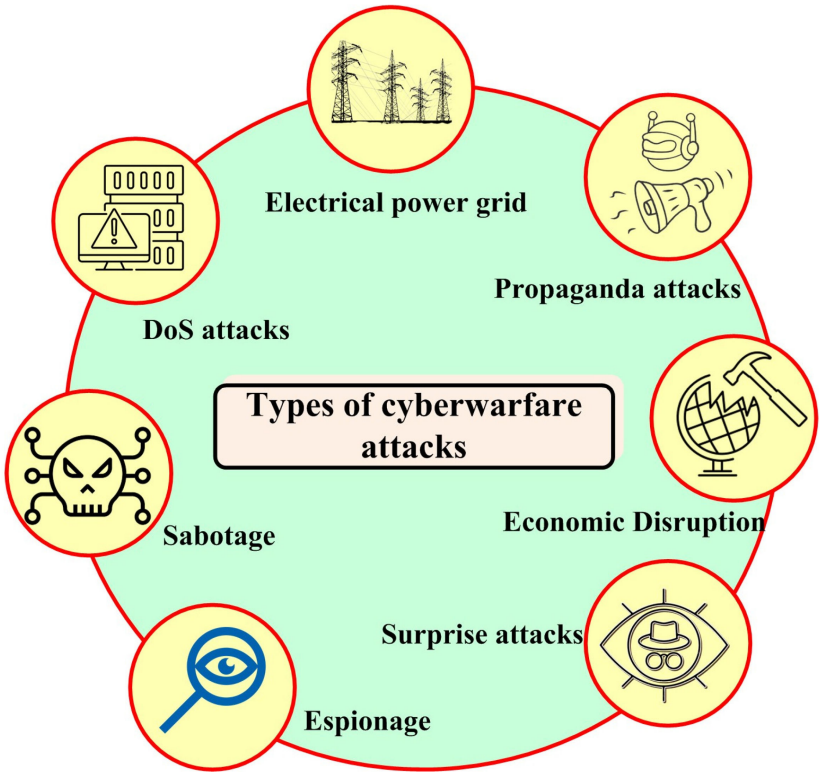

Figure 3. Different attack methodologies used for cyber warfare.

Propaganda attacks are largely used to influence the audience and their perspective by spreading false news that makes people lose faith and creates agitations in a country; these kinds of attacks look simple, but are effective [16]. Economic disruption attacks target the economic pillars of the country; these attacks try to take down financial systems such as the stock market and the banking sector by stealing money or blocking people's access

available funds [17]. Surprise attacks are performed to create a massive impact in less time, thereby weakening the country's defense systems.

2. Real-World Cyber Attack Scenarios

The most notable and successful cyber attack was the 2010 Iran nuclear plant attack; this attack targeted the programmable logical controllers (PLCs) in a nuclear plant. The Stuxnet virus used in this attack had an impact on 200,000 computers, and caused damage to almost 1000 machines [18]. The 2012 Aramco cyber attack used the Shamoon virus; this attack was intended to destroy confidential files in Aramco workstations. Some 30,000 Saudi Aramco workstations were affected by this attack [19].

The best examples of cyber warfare are the attacks that took place in the context of the Russia–Ukraine war. These cyber attacks have made the world realize the importance of cyber security. The 2015 cyber attack on Ukraine's power grid caused a blackout and led to a power outage affecting 2,300,000 people [20]. The attack group, known as Sandworm, used BlackEnergy 3 malware to compromise the information systems of energy distribution companies [21]. A spear-phishing [22] method was used to implement the attack. Following the 2015 attack, less than a year later, one more attack from Russia targeted Ukraine's capital Kyiv. Industroyer malware [23] was used in this attack to adversely affect protective relays, meaning the data packets of relays were diverted to the wrong IP address. This attack caused a blackout of 1 h. Some of the most notable cyberwarfare incidents are presented in Table 1.

Table 1. Real-world examples of cyber warfare.

Ref.	Cyber Attack	Target	Attack Type
[24]	Estonian cyber attacks (27 April 2007)	Estonian websites, parliament, banks, ministers	DDoS attacks through ping folds and botnets
[25,26]	Russo–Georgian War (20 July 2008)	Websites of Georgia, Russia, South Osettin and Azerbaijani	DoS
[27]	South Korea cyber attacks (2009)	Websites of major media, financial websites of South Korea and US	DDoS, activation of botnets
[28]	Attacks on the US Department of Defence (2008)	US military computers	Malware
[29]	GhostNet (March 2009)	Spying on political and economic locations of India, Indonesia, Romania and many South Asian countries	Cyber espionage, Advanced, persistent threat
[30]	Titan rain (2003)	US defense contractor computer networks	State-sponsored advance persistent threat
[31]	Shadow network	Targeting classified information of India gov ernment	Malware, cyber spying
[18]	Iran nuclear power plant attack (2010)	200,000 computers and 1000 machines are affected	Stuxnet
[19]	Aramco cyber attack (2012)	30,000 Aramco workstations are affected	Shamoon
[20–22]	Ukraine power grid attack (2015)	Power outage for 230,000 people	BlackEnergy 3 malware
[23]	Kyiv energy distribution network (2016)	Blackout for 1 h	Industroyer malware
[32]	US oil resource attack (2021)	Halted working of oil pipelines for 17 states in US	Darkside malware
[33]	Natanz nuclear plant attack (2021)	Destruction of centrifuges	Stuxnet

One of the biggest cyber attacks on oil resources took place in the US on 7 May 2021. This ransomware cyber attack halted the working of oil pipelines in nearly 17 states of the USA. Darkside malware was used in this attack [32]. A similar attack happened in Iran in

2021, where 4300 gas stations could not process payments. The 2021 Natanz cyber attack is one more example of cyber warfare; it is speculated that Israel is responsible for an attack on a nuclear power plant as a part of the Iran and Israel war [33].

These cyber attacks on cyber-physical systems are implemented by accessing information from communication links. Depending on the protocol used for communication, there are several possible different attacks, which are shown in Figure 4.

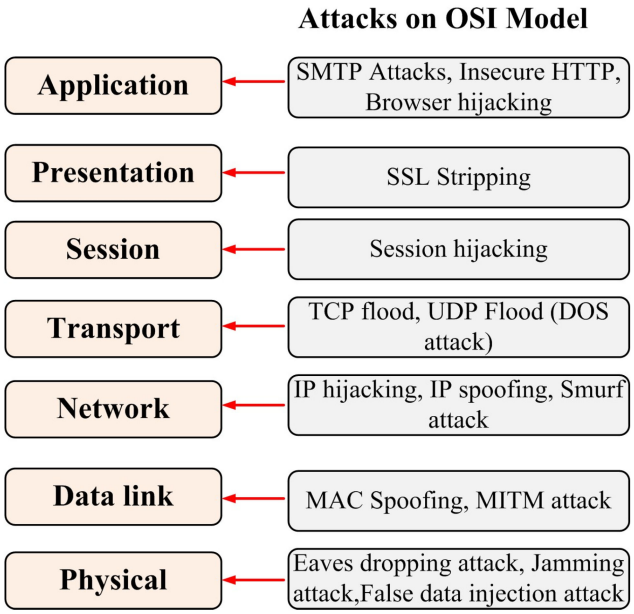

Figure 4. Cyber attacks in different layers of the OSI model.

In the information security domain, data protection is evaluated using the CIA triad and the AAA triad, with C indicating the confidentiality of the data, I indicating the integrity of the data, and *A* indicating availability in the CIA triad. Authentication, authorization and accountability are the parameters of the AAA triad. Data security is ensured if all the parameters in the CIA triad and AAA triad are satisfied. Cyber attacks target cyber-physical systems such that they disrupt the parameters of the CIA triad. Table 2 gives information on the different cyber attacks affecting the CIA triad.

Table 2. Cyber attacks' impact on the CIA triad.

Cyber Attack	Confidentiality	Integrity	Availability
Data injection	×	✓	✓
Eavesdropping	×	✓	✓
Masquerading	×	✓	✓
Sniffing	×	✓	✓
Social engineering	×	✓	✓
Traffic analysis	×	✓	✓
Unauthorized access	×	✓	✓
False data injection	✓	×	✓
Load drop attacks	✓	×	✓
Replay attacks	✓	×	✓
Spoofing	✓	×	✓
Time synchronization	✓	×	✓

Table 2. *Cont.*

Cyber Attack	Confidentiality	Integrity	Availability
Worm hole	✓	×	✓
Buffer overflow	✓	✓	×
Denial of service	✓	✓	×
Low rate DoS	✓	✓	×
Smurf	✓	✓	×
Teardrop	✓	✓	×

3. Cyber Attacks in Cyber-Physical Systems

There are various cyber attacks targeted towards CPS; the most prominent, frequent, and effective cyber attacks preferred by attackers are false data injection (FDI) attacks, man-in-the-middle (MITM) attacks, and denial of service (DoS) attacks.

3.1. False Data Injection Attacks

False data injection attacks are the most frequently occurring cyber attacks in DC microgrid systems. FDI attacks are targeted towards physical sensors or towards communication links [34]. Intruding into the network and hacking communication links is a more feasible method than gaining physical access to sensors. The primary aim of false data injection attacks is to modify the sensor values transmitted through the communication links [35]. FDI attacks increase the computational burden on the controllers, causing revenue losses and mismanagement of control devices, and lead to load dysfunction and power imbalance. The adversary targets the vulnerabilities in the communication links and injects false data into the existing sensor values using different injection techniques. Structured query language (SQL) injection and cross-site scripting attacks are the most common. In SQL injection attacks, the attacker tries to inject the commands that exploit the authenticity and authorization of the application [36]. The attacker can read, modify, and delete the data using this injection technique. The cross-site scripting technique inserts malicious code into the web application; this attack tries to manage the cookies, hijack the sessions and change the user settings [37]. Some other types of injection techniques are code injection, command injection and change cipher spec (CCS) injection. Figure 5 represents an FDI attack on the sensor values.

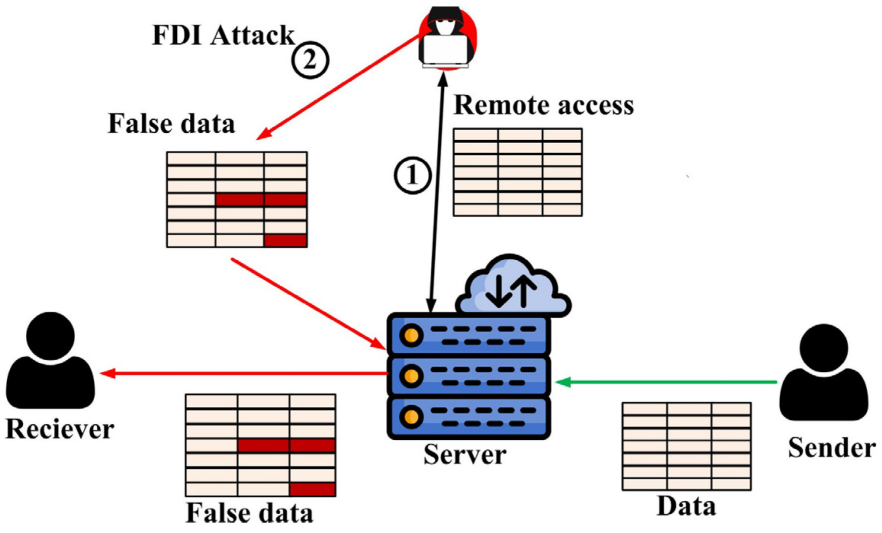

Figure 5. Representation of a false data injection attack.

Depending upon the knowledge and accessibility of the attacker, FDI attacks are further classified into two types: internal FDI attacks, and external FDI attacks. In the scenario that the attacker possesses complete knowledge of the system and has access to the critical infrastructure, the FDI attack is considered an internal FDI attack. Internal FDI attacks are considered as most effective and dangerous attacks. As the attacker is aware of the system working, the designed FDI attacks are more constructive and stealthy, which makes them difficult to identify. External FDI attacks are performed by an external agent who has limited knowledge of the system's workings; in this scenario, the attacker completely depends on the vulnerabilities of the communication network.

Depending on the attacker's knowledge and motive, FDI attacks can be classified as continuous FDI attacks, interim FDI attacks, stealthy FDI attacks, constrained FDI attacks, unconstrained FDI attacks, and time-varying FDI attacks [38].

Let us consider A_i the input vector with n samples, $A_i = [a_1, a_2, a_3, \ldots \ldots, a_n]$. The attacker injects the false data F_i into the input vector. Where $F_i = [f_1, f_2, f_3, \ldots \ldots, f_n]$ (1) represents the input vector after the FDI attack.

$$C_i = A_i + F_i \tag{1}$$

An attack is considered a continuous FDI attack when the attack continues till the end of the vector from its start. For instance, if the attack is initiated at the third sample, it propagates until the nth sample. (2) denotes the input vector after a continuous FDI attack. C_{cont} denotes the input vector, where $C_1 = a_1$ and $C_2 = a_2$, and other samples are the attacked samples. In a continuous FDI attack, $attack_{start} > 1$ and $attack_{end} = n$. In the interim FDI attack, the attacker ends the attack within the range of the vector. Here, $attack_{start} > 1$ and $attack_{end} < n$.

$$C_{cont} = [c_1, c_2, c_3, \ldots \ldots, c_n] \tag{2}$$

A stealthy FDI attack is the most deceptive attack, where the attacker hides the attack from the defense mechanism. In a stealth attack, the attacker injects false data within the stability range. An attacker who has complete knowledge of the system injects data, such that the value is within the limits of stability, as shown in (3). Another method of stealth attack consists of two parts; the first is to perform the attack on the controller outputs, and the second is to stealthily hide the attack's impact from the controller.

$$A_{min} < C_i < A_{max} \tag{3}$$

Unconstrained and constrained FDI attacks are the other types of FDI attacks. In unconstrained FDI attacks, the attacker has access to all the variables in the communication links, whereas in constrained FDI attacks, the attacker gains only limited access.

3.2. Man-in-the-Middle Attack

In a man-in-the-middle attack, the attacker tries to steal information between two parties that should be secure and private. A man-in-the-middle attack has two steps. Step 1 is intruding into the communication channel or intercepting the data traffic, and step 2 is decrypting the information that is transmitted through the channel [39], as shown in Figure 6. The motivations for a MITM attack can be several, but may include stealing the authorized parties' identity, modifying the parties' login credentials, and taking control of financial transactions, etc.

There are certain methods through which an attacker tries to intrude into the network: IP spoofing [40], address resolution protocol (ARP) spoofing [41], and domain name server (DNS) spoofing [42]. In IP spoofing, the attacker, who stands in the middle of the communication between the authorized parties, spoofs the IP address of the sender and receiver. To the sender, the attacker appears as the receiver by spoofing the IP address of the receiver, and vice versa, making the operation look legitimate. ARP is the address

resolution protocol used to map the device's IP address into the media access control (MAC) address.

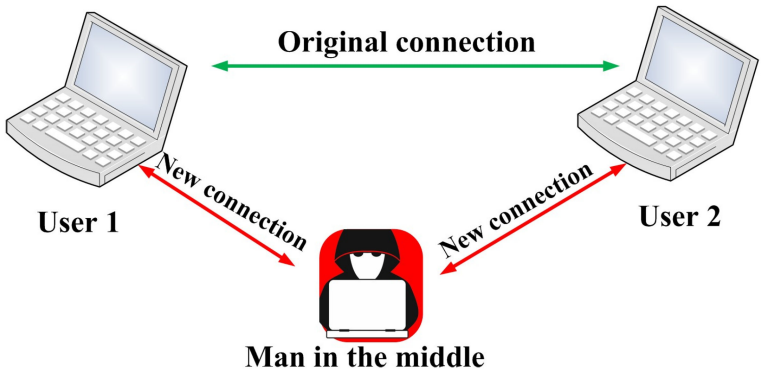

Figure 6. Representation of a man-in-the-middle attack.

When an ARP request is sent by one device, an ARP response is obtained by the device matching the request; these responses and requests are formed as an ARP cache. When the attacker gains access to the ARP cache, the attacker tries to match his MAC address with the device's IP address in the network. This allows the attacker to access the data transfer between the parties. DNS spoofing is a type of attack technique in which the user is directed to a fake account chosen by the attacker; this results from altered domain names in the server. When the user tries to enter confidential information, such as their login credentials, the information is stolen by the attacker.

After intruding into the network using any of the methods mentioned above, the attacker should find a way to decrypt the messages transmitted between the parties. Hypertext transfer protocol secure (HTTPS) spoofing, secure socket layer (SSL) hijacking, SSL stripping, and SSL beast are the methods often used to decrypt messages [43].

3.3. Denial of Service Attack

A denial of service (DoS) attack aims to make the service unavailable to the authorized user by flooding the server with false requests [44,45]. This attack disrupts the availability factor in the CIA triad. CIA stands for confidentiality, integrity and availability; these are the guidelines and policies followed to ensure information security. Disruption to any one of these factors indicates a cyber attack on the system. However, DoS attacks do not cause a breach of confidentiality or integrity, but cause a loss of time and computational resources. Attackers often use DoS attacks to halt the system's performance and cause financial losses. Sometimes this attack is also carried out to expose the vulnerability of the system. A DoS attack in which an attacker gains access to multiple devices and floods the server with requests is pictorially represented in Figure 7.

DoS attacks are distinguished based on the point of attack in the communication system. If the attack targets a specific application, it is defined as an application layer attack. In this kind of attack, the application is flooded with multiple HTTP requests; this attack is measured in requests per second (RPS). If a DoS attack is performed by exploiting the vulnerabilities in communication protocols, it is defined as a network layer attack; this attack disrupts the entire network and is measured in bits per second (BPS). Finally, the most common form of DoS attack is the volumetric attack, which targets the bandwidth of the communication channel. The bandwidth of the communication channel is flooded, creating congestion in network traffic; this attack is measured in BPS. Different techniques for implementing DoS attacks are SYN scan, smurf attack, teardrop attack, ARP attack, and fraggle attack. Another variant of the DoS attack is the distributed denial of service (DDoS) attack [46]. In this attack, a group of devices are used to attack the network; in the DoS attack, the attacker uses a single device.

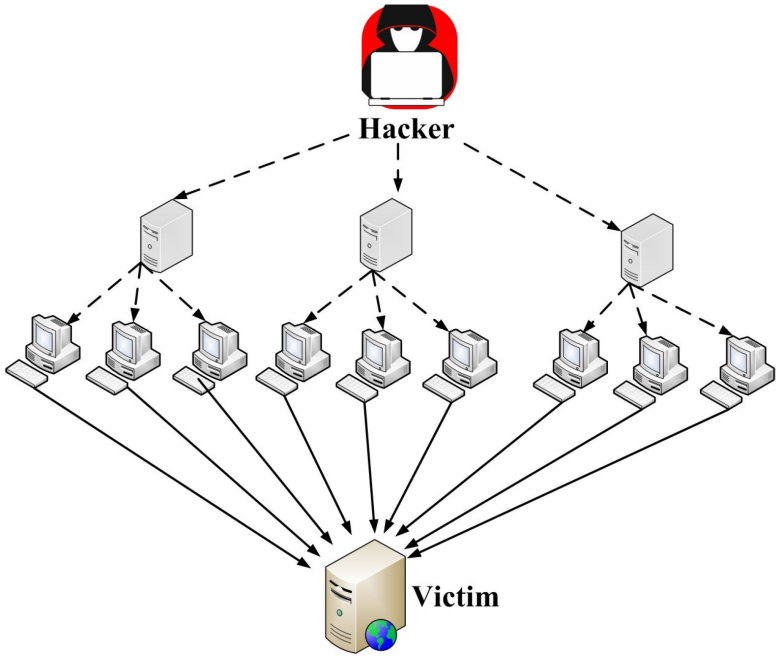

Figure 7. Representation of a denial of service attack.

In CPS, there are two different ways the attacker can destabilize the system using DoS attacks. One is by completely blocking the channel bandwidth by flooding it with false information; another is by introducing a buffer in the communication flow. For a brief amount of time, the communication between the two nodes is halted by the attacker, thereby introducing some delay in the information flow. This delay in the information flow disrupts the control operation of the microgrid and creates instability. The introduction of a buffer is even more dangerous, as it cannot be identified easily. There are different methods proposed in the literature to overcome DoS attacks on CPS. The packet marking scheme is used in [47], wherein the packets are traced back using probabilistic packet marking to identify the packet source address. In [48], a policy reinforcement learning method is used; this includes event-triggering control, robust control theory, and game theory approaches. Within this approach, a relationship between the cyber system and the physical system is established in order to detect DoS attacks.

4. Defense Mechanisms

In the process of achieving data security, information security and protection of the critical assets of the infrastructure, two types of security mechanisms are implemented: network-level security and device-level security. Information transfer in cyber-physical systems often occurs between the sensors and controllers. Multiple defense mechanisms are implemented at the networking level to defend against cyber attacks. If the defense mechanisms are implemented in the controller and control algorithm to analyze the incoming data, both for detection and to mitigate the effects of the attack on the system, the scenario is considered a device-level cyber attack.

4.1. Network-Level Cyber Security

Networking infrastructure is equipped with basic-level securities such as user authentications, firewall [49], anti-virus, data encryption, and cryptography. User authentication comes under application-level security; here, the client is asked to enter confidential credentials to access information [50]. Anti-virus software is an external software installed into the client system to monitor the incoming data packets through the network [51]. This comes under perimeter security.

Cryptography is one of the oldest yet most effective techniques used in network security; it is considered the data security method. Cryptography hides the actual data from intermediate intrusions by changing the plain text into cipher text; this process is known as encryption. Based on the level of confidentiality required, cryptography is implemented in two ways: symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography has a lower security level than asymmetric key cryptography. Data transmitted by the sender are encrypted with a key before transmission [52]. If the key is the same for both sender and receiver, it is known as symmetric key cryptography; however, there is a possibility of a breach in confidentiality as the key is public. In asymmetric key cryptography, the decryption key at the receiver end is different from that at the sender end; the message can only be decrypted through the private key of the receiver [53]. Within this cryptography method, the transmission is secured with a key, and the data are secured with encryption. Still, there is a chance of cyber attacks if the attacker gains access to the key or the attacker decodes the decryption algorithm.

Firewall security is an age-old technique invented in 1989 and used to protect networks from malicious data and cyber attacks. Depending upon the perimeter that needs to be secured, the firewall is placed on the perimeter's border to continuously monitor the incoming and outgoing data packets. A firewall can be used for perimeter security; this is referred to as the "perimeter firewall". Firewalls can also be used in network security, termed the "enclave firewall", and can be used as end point security, termed the "desktop firewall". Depending on their role, firewalls are classified either as a packet-filtering firewall, proxy service firewall, stateful inspection firewall, next-generation firewall or a unified threat management firewall [54]. Packet-filtering firewalls filter the incoming data based on the source address, destination address and the other fields present in the data packet [55]. Proxy service firewalls are used in the application layer to filter the malicious data entering into the system. Stateful inspection firewalls monitor the network traffic based on the protocol, port and state of the network traffic. Next-generation firewalls perform deep packet inspection that includes intrusion prevention and application-level inspection.

Intrusion detection systems (IDS) and intrusion prevention systems are specifically designed to detect and mitigate cyber attacks caused by unauthorized intrusions into the network. IDS are placed after the firewall and monitor for any malicious activities present in the network traffic; they alert the network administrator if any threat is detected [56,57]. An IDS is classified as a network intrusion detection system (NIDS) or a host intrusion detection system (HIDS). An NIDS is a software-defined system that monitors, captures and analyses network traffic. It detects malicious data packets by comparing them with already-known attack patterns. However, the operation of an NIDS is very difficult in busy and complex networks. An HIDS is a host-based system installed on individual devices; it monitors the information received on the particular device and generates alerts for any malicious packets found. Depending on the operation, an IDS is classified as a signature-based IDS [58] or an anomaly-based IDS [59].

A signature-based IDS works on detecting the patterns in the data packets. The signature-based IDS searches the database for attack patterns; if there is any similarity with the attack patterns, it sends an alert. The drawback of this system is it only detects known attack patterns, and there is a possibility of false negatives for new and unknown attacks. An anomaly-based IDS monitors the deviation from the normal, and a confidence interval creates a boundary that it marks as an anomaly. The disadvantage of this method is the high possibility of false positives for policy changes and new authentic intrusions. A hybrid IDS is introduced to overcome the disadvantages of the signature and anomaly-based IDS; it uses both techniques. Signature-based IDS detect known attacks, and anomaly-based IDS detect unknown attacks. The intrusion prevention system (IPS) is an extension of IDS which not only detects intrusions, but is also capable of blocking malicious data from entering the network [60].

Still, these security systems are not strong enough to address the present, innovative cyber attacks that are rapidly evolving. CPS systems are complex, and network-level defense

mechanisms must be continuously modified to secure communication links; this is not feasible. Additionally, adversaries are implementing attacks that can go undetected. Therefore, in addition to network-level security, device-level security should be implemented.

4.2. Device-Level Cyber Security

Device-level security analyzes a system's parameters, and its ability to detect and mitigate cyber attacks. In [61], the authors propose an adversarial perturbation method that protects the system from model-stealing attacks. The adversary tries to steal the model structure and rebuild the structure, using reverse engineering to perform stealth attacks. A dynamic event-triggered protocol is designed with a model predictive control approach in [62] to mitigate deception attacks and packet dropouts. In [63], the authors propose a blockchain method of protection to protect the data in an unmanned aerial vehicle. Ref. [64] proposes a heterogenous improved risk analysis model to detect the risk of intrusions in large engineering projects. Within this method, large projects are divided into stakeholder networks and project schedule networks, and then the relationship between these network layers is assessed in order to carry out the risk assessment. A distributed state-estimated algorithm is proposed in [65], where the bad data or fault data are detected by performing a weighted least-square method on every estimated sample. In [66], a signal temporal logic method is designed to detect the FDI attacks and also to quantify them; the threshold value is determined such that the parameter's value is always higher than the threshold in normal operating conditions, and above this value it is deemed a faulty scenario. Software-defined networking (SDN) is proposed in [67]; a separate networking model is designed based on the system performance. The incoming threats to the system are detected using this method. Additionally, SDN is used to design a routing algorithm for video conferences [68]. In [69], a multiagent system is proposed to detect the malicious data present in the system due to a load curtailment FDI attack. Batteries are used to temporarily compensate the curtailed loads due to attacks. Refs. [70,71] discuss an innovative game theory approach to detecting and analyzing cyber attacks. A distributed control approach is demonstrated in [72], which analyzes the effect of a DoS attack in the system. Wireless underground sensors, used in the areas such as mining and other underground applications, are highly prone to cyber attacks and reliability issues. Magnetic induction-based wireless underground sensors are proposed in [73] to increase the reliability of the sensors. Although multiple device-level cyber attack detection mechanisms are proposed in the literature, all of them are model-dependent and highly sensitive toward parametric changes. When there is an increase in system complexity, a change in system architecture, and during transient conditions, the performance of the model-dependent detection mechanisms reduces. Artificial intelligence methods are proposed to avoid model dependency and increase the system's performance. AI algorithms for cyber security and their applications are discussed in the following sections.

4.3. Cyber Security for CPS

Traditional IT security often focuses on network-level cyber attacks. There are a few security measures that are designed to detect and mitigate the basic security threats caused by network breaching. However, the advent of cyber-physical systems has led to the amalgamation of cyber systems and physical systems, giving rise to an entirely new problem statement. This advent of CPS led to the design of industrial network infrastructures, such as generic object-oriented system-wide events (GOOSE), international electrotechnical commission IEC61850, and distributed network protocol DNP3. Additionally, there the possibility of cyber attacks occurring at the device level; these are carried out by manipulating the information received by the controller or the information sent by sensors. The defense mechanisms developed in the information technology (IT) system are implemented at the network level by analyzing only the network parameters. Additionally, adversaries are smart enough to bypass the existing security measures with innovative attack methods. Therefore, CPS security is designed by analyzing the physical parameters using intelligent

attack detection and mitigation methods. The security mechanism developed for the CPS is embedded inside the plant controller, making it difficult to breach and manipulate. As there are various applications in CPS, the common security approach for all the systems will not ensure reliability. CPS security is flexible depending on the system's operation and control, making it more reliable and robust.

5. Artificial Intelligence in Cyber-Physical Systems

Artificial intelligence models' classification and predictive capability have produced diversified applications among cyber-physical systems. The evolution of AI has made it possible to estimate the remaining useful life (RUL) of the CPS, which makes it very important for the maintenance of the plant. [74] uses recurrent neural networks for predicting the RUL of the aero engine. AI is also used in study of earth and environmental sciences; [75] uses deep learning (DL)-based methods to identify subsurface sedimentary structures. AI is also used for designing automatic ground-penetrating radar, which detects the presence of underground pipelines; deep learning models are used in this article [76]. Image processing and image colorization is one of the applications of AI that is popularly used. [77] proposes the cycleGAN method to regenerate color image replicas of actual images. Traffic flow prediction is performed in [78], using spatial-temporal recurrent neural networks based on human mobility.

5.1. Artificial Intelligence for Cyber Security

With the introduction of CPS and smart systems, the attack surface is rapidly growing, making it very difficult for traditional methods to provide reliable security. Additionally, adversaries are opting for innovative methods to outfox security mechanisms. Therefore, there is a need to adopt intelligent and advanced mechanisms to provide efficient cyber security for systems. Artificial intelligence's ability to analyze billions of data (and identify patterns in the data) and its precise predictive ability makes it very effective in cyber security applications [79]. AI methods provide many advantages compared to traditional methods. With the rapid increase in the variety of cyber threats, traditional software-based systems have failed to identify these threats and upgrade accordingly, whereas AI's ability to learn from past experiences helps it to adapt to the new incoming threats. By using sophisticated techniques, AI can detect attack patterns in incoming data and anomalies in the data, and predict incoming threats. Other advantages that AI possesses compared to existing techniques are battling botnets, better endpoint protection, and breaching risk prediction.

When using AI for cyber security or any other application, the dataset plays a major role. The preparation of the dataset lays the foundation for the efficient performance of the AI system, as the AI model is trained on the dataset provided. Generally, for traditional systems, a historical dataset is considered, which includes all the malware data, attack patterns, and event occurrences. However, historical data are difficult to acquire, expensive, and can also be misleading in some cases. Therefore, CPS and particularly microgrid systems follow synthetic dataset creation methods. A synthetic dataset is created using simulation and using mathematical models; the advantages of synthetic dataset creation are that the data are easy to obtain, there is flexibility in the scaling of datasets, and edge cases can be created to train the model for outlier identification. Mathematical models are used for dataset creation for simple systems, and systems with more complexity use simulation for data creation.

Initially, basic machine learning algorithms, also called shallow models, are used for cyber security; later, deep learning techniques that are capable of dealing with complex networks are introduced, and further reinforcement learning methods, which are futuristic and claim to be self-learning methods, are proposed. Figure 8 presents the classification of various ML models used for cyber security.

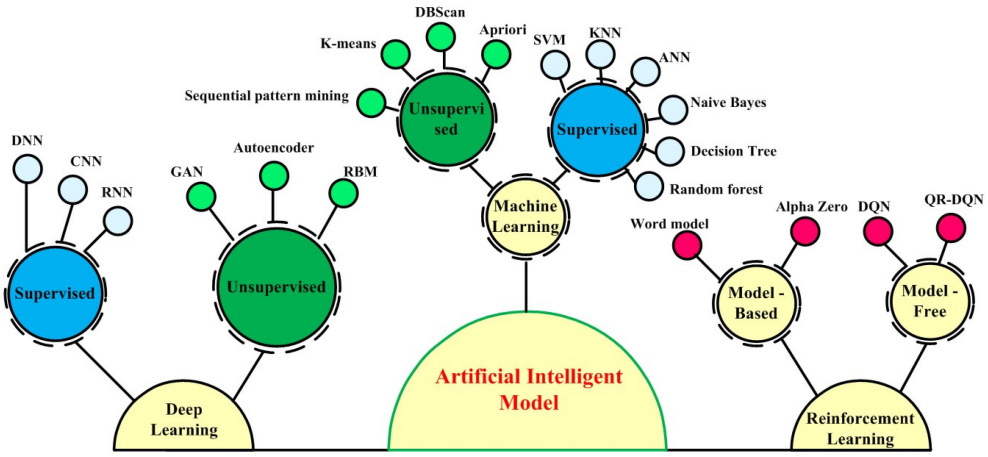

Figure 8. Taxonomy of artificial intelligence models for cyber security.

Machine learning models, referred to as shallow models, are further classified into supervised learning and unsupervised learning, based on their learning procedure. In unsupervised learning, the classified outputs are formed into clusters; these algorithms mostly depend on the internal pattern of the data. The k-means algorithm detects malicious entries into the network [80]; the k-means algorithm groups the unlabeled data into clusters. The value of K indicates the no. of clusters. This technique divides the data into different groups, which gives insights into data analysis on unknown and known attack patterns. Sequential pattern mining [81], a subset of data mining, is another data analysis method which unearths knowledge of the attack patterns; this method will send an alert if any malicious activity or abnormal activity is registered. Another data mining method used to detect web intrusion is the a priori algorithm [82]; the a priori method, which runs on the specific rule set, will keep track of frequently occurring data patterns and indicate if any new pattern is detected.

Supervised learning methods are already specified with class labels in order to verify model classification or predictions. The k-nearest neighbor (KNN) method is used to classify incoming entries as normal or malicious entries [83]. Naïve Bayes is a statistical method that uses a probabilistic method based on Bayesian theory; the probability of a field prone to attack can thus be calculated [84]. Support vector machine (SVM) is a classification method that separates the intrusions and normal entries from the dataset. SVM uses a kernel that facilitates the classification of even complex and nonlinear data; SVMs can transform the data into the next dimension if the decision boundary cannot be determined in this dimension [85]. Decision trees and random forests are tree-based classifiers [86]. Based on the training data, a tree-like structure is created in a decision tree; predictions can be made based on the tree's structure, and any unknown entities can be sorted out [87,88]. The random forest also follows a similar method, but instead of a single tree, a large group of trees are created, and the final structure of the tree for classification is decided using a voting process [89–91].

Deep learning (DL) models are designed to handle complex and non-linear systems; DL models are considered superior to ML models in terms of system-handling capability. The architecture of DL models also differs from that of ML models; there is no fixed algorithm for this model [92]. The DL model consists of neurons placed in different layers; the working of neurons in the DL model is inspired by the working of the human brain, and the neurons of each layer are interconnected. Information is transmitted from the input layer to the output through multiple hidden layers. The DL model consists of two stages: the training stage and the testing stage. The training stage consists of modifying weights for each connection during multiple iterations, making the DL model learn the patterns of the data feeding into the network.

Later, the efficiency of the trained model is tested on the testing data. Deep neural networks (DNN) have the structure discussed above, with multiple hidden layers; an increase in the depth of the network gives the model the ability to classify the nonlinear data [93,94]. Convolution neural networks (CNN) are widely used for image classification; the data to be classified is converted into image format, and the malicious data is identified [95,96]. Recurrent neural networks (RNN) are used for time series data; this network model predicts the occurrence of the next data sample based on the previous output and the present inputs [97]. However, this model suffers from memory issues; often, the outliers and extreme cases are considered attack vectors.

To overcome this, models such as long short-term memory (LSTM) and gated recurrent unit (GRU) are introduced; these contain the memory element, and their network architecture also differs from that of the classical RNN [98]. Generative adversarial networks (GaN) and autoencoders are unsupervised techniques in deep learning, where the outputs are not specified. The GaN model consists of two networks, namely the generator and discriminator. The generator takes the input data sample and generates a sample of data; the generated sample is compared with the training data or real sample using a discriminator. The discriminator, after comparison, decides whether the incoming data sample is real or fake [99,100]. An autoencoder is a neural network architecture, and this technique is often used for video and image classification [101]. The input data are compressed to the lower dimension, which is referred to as latent space; the latent space consists of data containing the most prominent features. From the latent space, the autoencoder tries to recreate the input data at the output; normal and fake data are classified by comparing the autoencoder output. During the training phase, autoencoders are trained to recreate the input near the output; a higher variation in the output and input indicates the attacked data.

Reinforcement learning is the advanced and futuristic architecture proposed to practice self-learning [102]. RL, also known as reward-based learning, works on the reward obtained by the action it performed in the previous iteration. The agent is present in a customized environment with predefined rules, goals and reward criteria. The model reaching the goal with high reward points is considered the optimized model; the RL model continuously updates its decision-making or policy based on the rewards.

5.2. Cyber Security Databases

There are some repositories specifically dedicated to the collection of data to perform security analysis. Readily available datasets on multiple domains provide researchers with a great platform to implement the designed mitigation mechanisms. IMPACT is a repository that produces the network operations data of cyber defense technology [103]. KYOTO is a traffic-related dataset generated by Kyoto University [104]. KDD'99CUP is the most popular dataset, which contains 41 features; this dataset contains the threat combinations of DoS, remote-to-local, user-to-remote, and probing [105]. The KDD'99CUP dataset has a class imbalance issue and more redundant samples; these issues are resolved in the NSL–KDD dataset [106]. The DARPA dataset is prepared in MIT Lincoln laboratory with authenticated IDS. LLDOS 1.0 and LLDOS 2.0.2 attacks are considered [107]. UNSW–NB15 is a large dataset that includes nine threat types; this dataset was collected from a cyber security lab at the University of New South Wales [108]. This data set is often used in anomaly detection. To validate the threat of insider attacks, the CERT dataset was designed, and detection algorithms track the user behavior [109]. The *Bot–IoT* dataset is used to evaluate the reliability issues of IoT data; it is a collection of simulated and authentic IoT data that includes various attack scenarios [110]. MAWI is a Japanese-designed dataset used to identify DDoS threats; this dataset is regulated by Japanese educational and research institutions [111]. The EnronSpam dataset is a collection of ham and spam emails; it is used to identify phishing and spear-phishing attacks [112]. Malware is a combination of multiple malicious files created from different projects; this dataset is used for malware analysis and malware detection [113]. DREBIN is a dataset created by the Drebin project to further research on Android malware; this dataset contains 179 malware categories [114]. The

CAIDA dataset was prepared to study DDoS and DoS attacks; machine learning models can be assessed for their performance in DDoS detection using the CAIDA'07 and CAIDA'08 datasets [115]. Further, there are many more created datasets that aid the detection of cyber attacks; detection of these attacks becomes much easier when using data-driven methods. Some existing works related to cyber attack detection using AI techniques are given below.

Popular real-time datasets such as KDD99 and DARPA are considered to evaluate the deep learning and machine learning algorithms' performance. Initially, machine learning algorithms were implemented on the KDD99 dataset, and the performances obtained are as follows. Naïve Bayes had a 97% accuracy [116], SVM a 93% accuracy [117], decision tree a 94.3% accuracy [118], random forest a 98.9% accuracy, [119] and deep belief networks a 96.5% accuracy [120]. Further, the same KDD99 dataset was classified using deep learning models, and performances were as follows: GRU with 99.42% [121], and CNN-LSTM with 99.7% [122–124]. A c-supported SVM technique was designed in [125] to improve industrial and operational safety. The KDD CUP 99 dataset was used for the simulation and for training the algorithm in the virtual reality environment, achieving an 86.7% accuracy and a 2.3% false positive rate. In [126], lightweight neural networks were developed for fault detection in hybrid smart grids; this method reduces the computational burden and increases the system's throughput. Table 3 shows the details of AI algorithms used for cyber security, and their detection accuracy.

Table 3. Cyber attack detection using AI algorithms.

Ref.	Algorithm	Objective	Accuracy
[127]	Deep Neural Network	Anomaly detection for DoS attacks, deception attacks and injection attacks	Dos attack: 98%, Deception attack: 91.76%, Injection attack: 96.75%
[128]	Artificial Neural Network	Cyber attack detection from NSL-KDD dataset and UNSW- NB15	NSL-KDD: 91%, UNSW-NB15: 96%
[129]	LSTM and GRU	Sensor attack detection using deep neural net work	LSTM: 97.3%, GRU: 97.1%
[130]	Artificial Neural Network	Intrusion detection	MLP: 90.18%, Linear regression: 89.5%
[131]	Deep Neural Network	Detection of FDI attack	90%
[132]	Random forest	Network traffic threat classification using KDD99 dataset	99%
[133]	Gated recurrent unit	Network traffic threat classification using KDD99 dataset	98.6%
[134]	Deep Belief Network	Anomaly detection using KYOTO dataset	98%
[135]	Support Vector Machines	Detection of distributed denial of service attack using DARPA dataset	95.1%
[136]	XGBOOST	Classification of spam emails using ENRON spam	98.6%
[137]	Decision tree	Botnet traffic identification using TCP dataset from Dartmouth University	97%
[138]	DBSCAN	Identify the outliers from KDD-99 dataset and separation of high density clusters from normal clusters	98%
[139]	Sequential Pattern Mining	Identification of attack patterns from DARPA dataset	93%
[140]	Deep belief networks	Malware detection	96%

5.3. Challenges for AI in Cyber Security

One of the major limitations of the use of AI in cyber security is the availability of datasets. Datasets play a major role in AI model training and its workings. Normally, historical datasets are used to train an AI model; these datasets contain all the malware details, attack patterns, and attack events. Using the signatures of the events in the dataset, AI will be able to detect cyber attacks. However, this historical dataset will not contain the new attack patterns and will not be readily available; in some cases, these data can be misleading, as the attacker is aware of the historical datasets. To avoid this, synthetic dataset creation is adapted; the advantages of this method are mentioned above. The disadvantage of this method is the complexity of creating the dataset; complex and nonlinear systems are difficult to simulate and model mathematically. Therefore, dataset preparation is considered the preliminary hurdle for AI in cyber security, and should be addressed before implementation. AI is considered an intelligent and adaptive system; therefore, cyber security experts prefer its design of security measures. However, the hard fact is that the adversaries also may be using AI to overcome security mechanisms. Therefore, security experts should be aware of both the advantages as well as the threats posed by AI in the field of cyber security.

6. Role of AI in Microgrid Control and Safety

Microgrid systems, considered the application of cyber-physical systems, are more complex and critical in their operation compared to the classical CPS. The characteristics of microgrids include energy management, demand-side management, generation, load scheduling, and interoperability. To achieve these characteristics, industrial IoT is implemented, and network frameworks such as GOOSE, DNP3, and IEC 61850 are used. The applications of artificial intelligence in DC microgrid systems are shown in Figure 9. The energy management system is important in DC microgrid systems' control and operation. Due to the presence of multiple distributed generations and a variety of loads on the microgrid system, energy management becomes crucial to attaining optimized power consumption. As the level of importance is high for EMS, it becomes the target of adversaries, who attempt to disrupt its operation. EMS basically collects the data from the variable sensors and gives them to various meta-heuristic methods, math heuristic methods, and state estimation for optimization. State estimation is considered one of the most effective energy management strategies of microgrid systems. The estimated state variables are used to monitor and control various aspects of the microgrid, such as load forecasting, stability analysis, contingency analysis, bad data detection, and optimal power dispatch [141,142]. Voltage control is one of the objectives of the microgrid system; in microgrids, voltage control is performed through the distribution generators controlled by power electronic devices. In such cases, the attackers try to breach the control layers and modify the sensor variables, causing a change in the reference voltage levels of the microgrid [143,144]. Additionally, the cyber attacks target the microgrid frequency control [145,146] and the protection systems [147]. Several attack mitigation strategies for cyber attacks on microgrid energy systems are proposed in the literature, based on the analysis of measured data. Detection schemes are classified into static and dynamic detection. Detection mechanisms used for attack detection in the steady state are known as static detection methods; meanwhile, dynamic detection schemes utilize systems dynamics for attack detection. The Bayesian detection method [148], discrete wavelet transform method with DNN [149], Kulback–Leibler distance method [150], and transmission line variations techniques [151] are used to detect FDIA within state estimation methods. Detection of cyber attacks on the load frequency control of power systems is discussed in [152,153], in which dynamic detection methods are used. An image-processing method based on parameter variations is used for FDIA detection in [154].

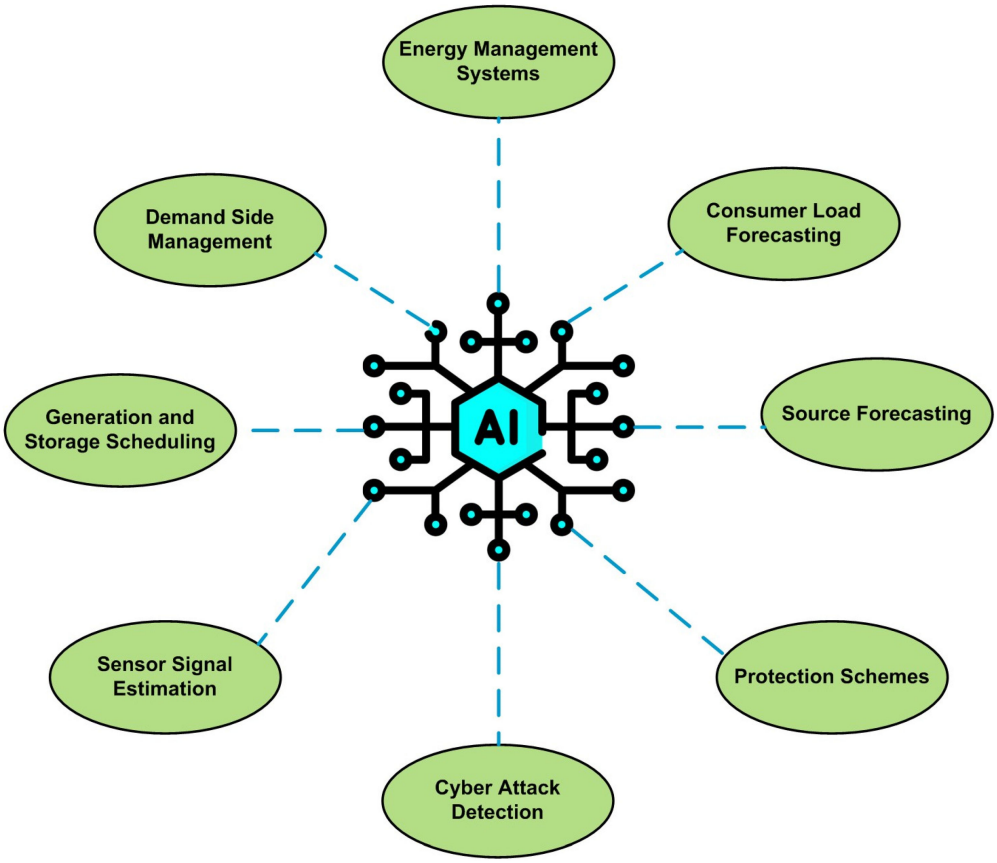

Figure 9. Applications of AI in DC microgrid systems.

Traditionally implemented model-based methods require complete domain expertise to design energy management systems (EMS). Moreover, the unpredictability and uncertainty in the microgrid often leads to the redesigning of EMS, leading to high design costs and maintenance costs. To overcome this, a model-free-based methodology is proposed, using AI to design EMS. In [155,156] GAN is used to model the uncertainties in the output power of RES in a DC microgrid, and to achieve optimal energy management. Load and source forecasting has become the most important part of DC microgrid control. Due to the integration of various RES in DC microgrid systems and dynamic loading scenarios, source forecasting and load forecasting is performed. Based on the time window of forecasting, it is differentiated into short-term, mid-term, and long-term forecasting methods. [157,158] explain the load forecasting and source forecasting methods; SVM, ANN, and self-organizing maps are also discussed. Fault detection in microgrids differs from distributed systems because of RES. In [159], fault detection is performed using machine learning techniques such as SVM, Naïve Bayes, KNN and decision trees. Demand-side management is one of the characteristics of a smart grid. Demand-side management (DSM) is implemented mainly in areas wherein there is a time-based pricing mechanism; depending on the time of the day, the tariff is varied by the utility. In such scenarios, to achieve cost optimization, the DSM mechanism is used, which schedules the operation of loads in order to reduce the overall cost of the end user. Ref. [160] demonstrates the DSM using ANN in smart grid environments.

Figure 10 shows the control architecture of the distributed control DC microgrid [161,162]. This architecture consists of four nodes, which communicate with neighboring nodes. There are two control layers: the primary control layer and the secondary control layer. The sensor value information from the neighboring converters is transferred to the particular converter through the secondary control layer. The received information is processed and passed through the control algorithm, and the control outputs are sent to the plant; the control

outputs are sent to the plant through the primary layer communication. Given the presence of multiple source and loads in the microgrid systems, the control and optimization plays a crucial role. Different control and optimization techniques of microgrids are proposed in the literature. In [163], the optimization and analysis of microgrid operation are performed using distributed algorithms; the initialization-free algorithm focuses on generation cost optimization in economic dispatch problems. To develop a safe consensus algorithm for the distributed control of microgrids, a differential privacy-based consensus algorithm is designed in [164]. This study shows that the privacy policy directly correlates to the number of neighbors; thus, each node decides its privacy level.

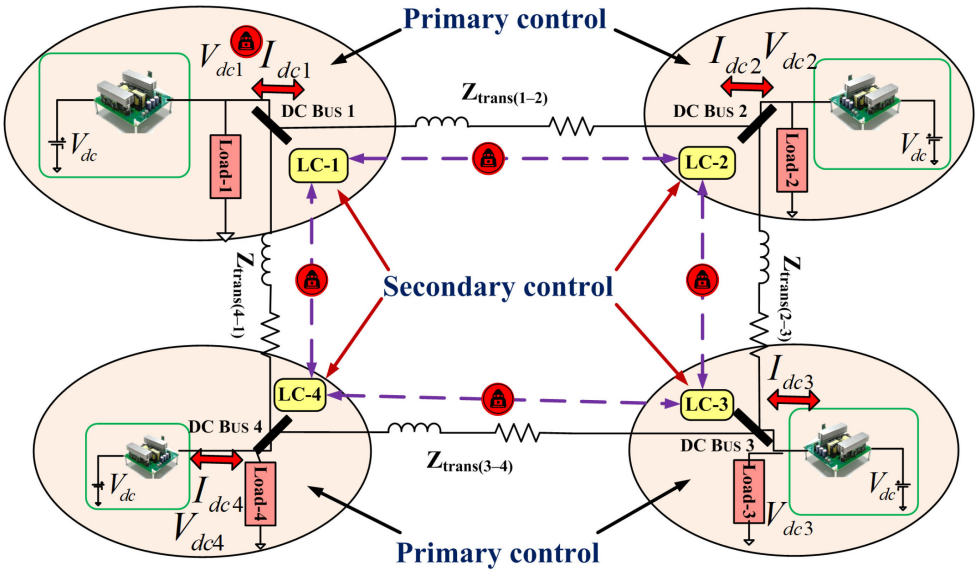

Figure 10. Control architecture of a distributed DC microgrid.

The present literature consists of different model-dependent control and optimization mechanisms. The inclusion of AI in microgrid control can improve the system's efficiency. The estimating ability and adaptive capability of the AI and DL methods should be utilized as much as possible.

Microgrid Cyber Security Using AI

Cyber attacks in microgrid systems not only cause issues with data integrity and confidentiality, but cause huge economic losses. Communication of sensor and operational data between each node is essential to attain the efficient operation of microgrid systems. Therefore, monitoring and analyzing the data continuously plays a major role in attaining data integrity. This becomes challenging when the attack is made at the device level rather than the network level. In this scenario, the basic network-level security used in the classical CPS fails to identify the attacks. Therefore, there is a need to develop a cyber security algorithm that is capable of detecting and mitigating device-level and network-level cyber attacks.

The secondary and primary layers, which carry critical sensor information, are prone to cyber attacks. The attack on the communication layers leads to the disruption in the control technique, and causes the maloperation of the DC microgrid. As discussed in the above sections, AI can detect and mitigate cyber attacks. In [165] an ANN-based FDI attack mitigation mechanism is proposed; an FDI attack is performed on the bus voltage sensors. Reference value estimation is performed using ANN, and compared with the bus voltage. The error from the comparison results in a correction factor when passed through a proportional-integral (PI) controller. This correction factor is added to the bus voltage value before passing to the secondary control to nullify the attack. In [166], model predictive control (MPC) along with an artificial neural network (ANN) was used to generate the

attack mitigation factor when there is an FDI attack on the bus voltage sensor. An ANN with a PI controller is used in [167] to detect and mitigate the FDI attack on the voltage sensors. A non-linear autoregressive network with an exogenous inputs (NARX) network is used in [168] to train the actual data and the attack data of the voltage sensors; when there is a difference between the NARX model output and the actual output, an FDI attack is detected.

In all the above articles studied, the attacker created a virtual attack layer just before the secondary layer. This attack layer manipulates the sensor values by injecting false data. Therefore, mitigation is also proposed before the secondary layer. In the whole process, the actual control algorithm is not disturbed. However, the proposed control algorithms, along with the mitigation mechanism, combine model-dependent and model-free parameters. Model-dependent parameters such as PI controllers should be integrated with model-free techniques such as the ANN model. This combination often results in high design complexity and increased computational burden. Additionally, the reduction in the efficiency of the PI controllers during parametric change affects the operation of the detection and mitigation mechanism. Therefore, a unified AI-based mechanism is needed to achieve microgrid control and mitigate cyber attacks.

The following section presents the design of a unified controller based on DL models to detect and mitigate stealth FDI attacks on DC microgrids. A stealth FDI attack is made on the DC-DC converter in one of the nodes of the DC microgrid. Manipulating the operation of DC-DC converter destabilizes the DC microgrid system.

7. Case Study of Stealth FDI Attack on DC-DC Converter

From the looming threat of cyber attacks, researchers and engineers have built efficient detection and mitigation strategies to protect the CPS from attackers [169]. However, the covert attack strategy implemented by attackers makes it difficult to find the presence of the attack in the system. The adversary tries to mimic the system's behavior and tries to prevent the effect of the attack from reaching the controller; this causes the controller to assume normal operation. These attack types demand the adversary to know the system's working, making it even more difficult to detect and mitigate. This article proposes a strategy to detect and mitigate covert attacks on DC-DC converters, the major component in CPS, such as microgrids and smart grids.

Covert attacks, or stealth attacks, are studied in the literature based on the type of attack and their criticality. In [170], the authors discussed stealth attacks and their effects on critical infrastructure; a taxonomy is proposed to discuss the risk posed by stealth attacks for each stage of the system. Stealthy covert attacks in cyber-physical systems are discussed in [171]; the study discusses modeling different types of stealth attacks from an adversary's perspective. The decoupling and zero dynamics methods are discussed, which make attacks completely stealthy. In [172], a steal attack methodology for a smart grid is proposed, in which the attack detection probability is reduced by minimizing the Kulback–Leibler (KL) divergence. The KL divergence term is reduced by obtaining a proper tradeoff between the loss of mutual information and the reduction in attack detection. An attack index is introduced in [173] to detect a stealth attack on current sensor information in a distributed controlled DC microgrid. In [174], a man-in-the-middle stealth attack is performed on battery energy storage systems with the help of an artificial neural network. Two ANNs are used: one to estimate the power of BESS, and the other to estimate the state of charge of the BESS for the adversary. The above-discussed literature discusses the effective implementation of stealth attacks with various techniques, and proposes some detection mechanisms. This article performs a false data injection-based stealth attack on the artificial intelligence-controlled DC-DC converter.

7.1. Proposed Methodology

The criticality and the level of stealthiness of the covert attacks depend on the knowledge of the adversary. If the adversary has complete knowledge and access to the system,

the attack is very dangerous; however, this is usually not the case. An adversary will have limited knowledge of the system, and will usually try to attack the nodes that are more vulnerable and critical to the system (but not every node). This type of attack is referred to in the literature as a local covert attack. The impact of a local covert attack depends on the amount of stealthiness in the attack. The proposed DC-DC converter contains an input voltage sensor (V_{in}), an output voltage sensor (V_o), an input current sensor (I_{in}) and the output current sensor (I_o). These sensor values are fed to the controller through the communication channel. An adversary located in the communication layer tries to gain access to the output variables. As shown in Figure 11, the controller receives the plant input variables (V_{in}, I_{in}) and plant output variables (V_o, I_o). Voltage controller and current controller are the deep neural networks with circles in the figure indicating neurons in each layer.

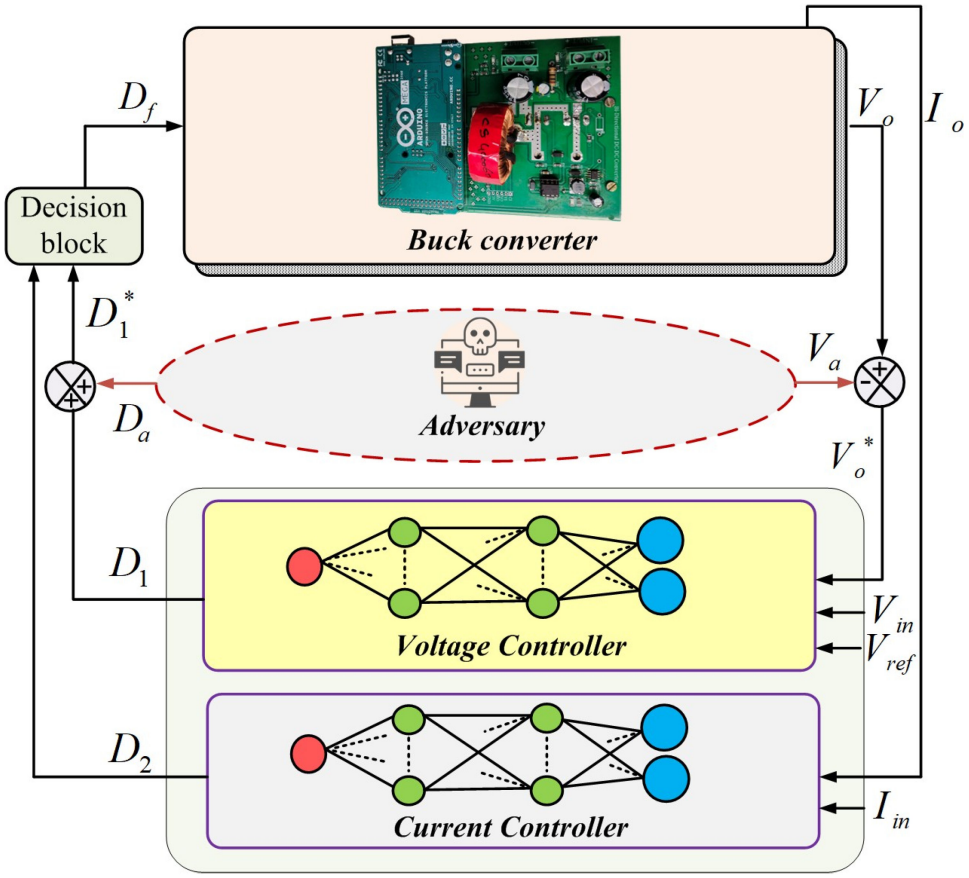

Figure 11. Proposed control mechanism for stealthy local covert FDI attack on buck converter.

7.1.1. Modelling of Stealth Local Covert FDI Attack (SLCA-FDIA)

In general, a microgrid protection system consists of the security measures which are embedded in a controller that tracks the system parameters that reach the controller as feedback variables. The traditional security measures might be equipped to deal with the FDI attacks that destabilize the system. However, the adversary aims to carry out a stealthy local covert attack on the converter by hiding the impact of the attack on to the controller. In this case, the device-level security fails to identify the presence of an attack.

In this case, the attack is performed beyond the controller. If no stealthification happens, the impact of the stealth attack reaches the controller, and the controller detects and mitigates the attack. However, the adversary hides the attack by removing the impact of the FDI attack on the feedback variables received by the controller. Therefore, during a stealth attack, the microgrid protection system assumes it to be the normal operating condition, thereby failing to identify the presence of an attack. Therefore, a special deep

learning-designed controller with a decision block is implemented to detect and mitigate the SLCA-FDIA.

The adversary tends to inject FDI attacks on the plant output sensors and finely tune their action, so detecting the attack is difficult for the protection devices. A stealth local covert attack is modeled such that the adversary has partial writing access to the output variables, and partial writing access to the control inputs. The adversary designs a plant model $B_a(s)$ that is similar to the actual plant model $B(s)$. The modified output vector and the control input vector after the SLCA are shown in (4) and (5).

$$y^* = \begin{bmatrix} V_O(t) \\ I_o(t) \end{bmatrix} \rightarrow \begin{bmatrix} V_o(t) - V_a(t) \\ I_o(t) \end{bmatrix} \tag{4}$$

$$D^* = \begin{bmatrix} D_1 \\ D_2 \end{bmatrix} \rightarrow \begin{bmatrix} D_1 + a \\ D_2 \end{bmatrix} \tag{5}$$

If there is no SLCA on the converter, i.e., $D_a = 0$ the output vector is given as (6)

$$y^*(t) = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} \begin{bmatrix} D_1 \\ D_2 \end{bmatrix} \tag{6}$$

B_{11}, B_{12}, B_{21} and B_{22} are the plant transfer function matrices If there is an SLCA on the converter, i.e., $D_a \neq 0$, the output vector is given as (7) and (8).

$$y_s^*(t) = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} \begin{bmatrix} D_1 + D_a \\ D_2 \end{bmatrix} - \begin{bmatrix} V_a(t) \\ 0 \end{bmatrix} \tag{7}$$

$$y_s^*(t) = \begin{bmatrix} y^*(t) + B_{11}D_a - V_a(t) \\ y^*(t) + B_{21}D_a \end{bmatrix} \tag{8}$$

For an attack to be completely stealthy,

$$\begin{gathered} B_{21}D_a = 0 \\ and\ B_{11}D_a = V_a(t) \end{gathered} \tag{9}$$

(9) indicates that the adversary plant design should be such that the attack should not propagate to the controller.

7.1.2. Deep Learning Controller Design

An artificial neural network-based controller using deep learning is designed to control the DC-DC converter and detect and mitigate the SLCA. The proposed SLCA mitigation controller consists of two controllers: a voltage controller and a current controller. The voltage controller is the deep learning controller which takes V_{in}, V_o and V_{ref} as inputs, giving the output as duty D_1. Similarly, the current controller also consists of a deep learning controller with I_{in} and I_o as inputs, giving the output as duty D_2.

A stepwise detailed explanation of the deep learning workflow is given below.

1. A set of training examples d_t is collected.
2. The deep learning model architecture is designed by determining the hyperparameters, such as the number of hidden layers, the number of hidden neurons in each layer, and the learning rate.
3. The initialization of weights and biases is carried out.
4. The training parameters of the model, such as activation function, optimizer and loss function, are determined.
5. The model is trained with training data.
6. The deep learning model is evaluated with testing data.
7. The trained deep learning model is deployed.

A generalized working model of the deep neural network is explained below. A set of training samples d_t is considered. After applying the random search algorithm using the Keras tuner, the structure of the neural network with x_n input nodes and two hidden layers α_i^1, α_i^2 and output node $\hat{y}$ is considered. Each hidden layer consists of 10 neurons each, and the learning rate (η) 0.1 is taken for training the deep learning model. To initialize the weights and biases, the Xavier uniform method is implemented, and its mathematical representation is given in (10).

$$w_{i,j} \sim \mathrm{U}\left[\frac{-\sqrt{6}}{\sqrt{n_{in}+n_{out}}}, \frac{\sqrt{6}}{\sqrt{n_{in}+n_{out}}}\right] \tag{10}$$

n_{in} are the no. of input connections to the neuron, and n_{out} are the no. of output connections of the neuron. Root mean square error (RMSE), as shown in (11), is the evaluation metric considered for model training as well as evaluation.

$$RMSE = \left[\frac{1}{2d_t}\sum_{i=1}^{d_t}\left|\hat{\mathrm{y}} - y\right|^2\right]^{\frac{1}{2}} \tag{11}$$

Various combinations of training parameters are applied to the deep learning model to finalize the best fit for the model. RMSE is the evaluation metric used for training parameter optimization. The sigmoid activation function with Adam optimizer, run for 100 epochs, gives the desirable RMSE value. The deep learning model's training process is shown below in (12)–(14).

$$\begin{aligned} \phi_1 &= \omega^1 * x + \beta^1 \\ \alpha^1 &= f\,(\phi_1) \end{aligned} \tag{12}$$

$$\begin{aligned} \phi_2 &= \omega^2 * \alpha^1 + \beta^2 \\ \alpha^2 &= f\,(\phi_2) \end{aligned} \tag{13}$$

$$\phi_3 = \omega^3 * \alpha^2 + \beta^3\alpha^3 = f(\phi_3) = \hat{y} \tag{14}$$

Here, ϕ denotes the weighted sum of inputs and bias, α denotes the output of the neuron, and f denotes the activation function. The training process continues until the error value converges to the performance goal specified, or the model reaches the specified epochs. Training parameters for deep neural network are specified in Table 4.

Table 4. Deep neural network controller training parameters.

Specification	Deep Learning Controller
Network type	FFBP
Activation function	Sigmoid
Optimizer	Adam
No. of hidden layers	2
Neurons in each hidden layer	10
Weight initialization method	Xavier uniform
Evaluation metric	RMSE
Learning rate	0.1
No. of epochs	100

In this article, it is considered that the adversary is attacking the duty D_1 obtained from the voltage controller, and to make the attack stealthy, the output voltage of the plant is modified to remove the effect of the FDI attack on the control input.

7.1.3. Detection and Mitigation of SLCA-FDIA

The decision block is placed before the plant, where it takes the control inputs generated from the controller. If there is no SLCA, the decision block receives D_1 and D_2. If there is an SLCA, the decision block receives D_1^* and D_2. In the decision block, the control logic is built to detect and mitigate the FDI attack. The duty D_1 is compared with D_2 with some threshold value ε; the ε value accounts for small noises and errors that occur within the controller. It is ensured that the ε value will not destabilize the system. (15) denotes the decision block logic.

$$D_2 - \varepsilon < D_1 < D_2 + \varepsilon \quad (15)$$

During no SLCA, $D_1^* = D_1$, and the condition (15) satisfies. If there is an SLCA, $D_1^* > D_1$, and the condition (15) fails. If (15) fails, it indicates the attack on the voltage controller input; during this case, D_2 is sent as the control input to the plant. In normal scenarios, if (15) satisfies, D_1 is considered the control input.

7.2. Simulation Results

The proposed methodology for the detection and mitigation of stealthy local covert FDI attacks is primarily implemented in MATLAB Simulink, and further evaluated using a real-time hardware setup. A DC-DC buck converter is simulated in MATLAB 2022a, and the control logic is designed using a deep learning toolbox. DC-DC converter specifications are given in Table 5.

Table 5. Buck converter component ratings.

Component	Rating
Inductor L	100 µH
Capacitor C	10 µF
Input voltage V_{in}	50 V
Output voltage V_o	20–40 V
Voltage ripple	1% of V_o
Current ripple	15% of I_o (peak)
Load range	50 W of 200 W

A deep learning controller taking the plant input variables V_{in} and I_{in} and the plant output variables V_o and Io as its inputs provides the output D_1 and D_2. In the no attack condition, the DL controller output is as shown in Figure 12, where the input voltage is given as 50 V, and the reference voltage is considered to be 25 V. The output duty generated by both the voltage controller and the current controller is 0.5.

An FDI attack is performed on the output of the voltage controller before reaching the decision block. False data D_a is injected into the voltage controller output D_1. Figure 13 shows the voltage controller output and current controller output at 0.25 s, where false data of 0.2 is injected. The output of the current controller is not affected by the FDI attack on the voltage controller output; it is constant at 0.5, whereas the voltage controller output is increased to 0.7. Figure 13 shows the attack on voltage controller duty. Figure 14a indicates voltage controller duty, and Figure 14b indicates the FDI attack on the duty at 0.25 s. Figure 14c shows the final duty D_1^* sent to the decision block. After performing the FDI attack on the voltage controller output, the adversary tries to hide the attack by performing a stealth local covert attack and making the controller assume it is in a normal operating condition. Figure 15a shows the output voltage of the converter at 2.5 s; when the FDI attack is made, an increase in output voltage is observed from 25 V to 35 V. To hide this attack, −10 V (a calculated value from the adversary plant model) is added to the output voltage at 2.5 s, as shown in Figure 15b. It can be observed from Figure 15c that the controller receives an unattacked and steady-state reference value of 25 V.

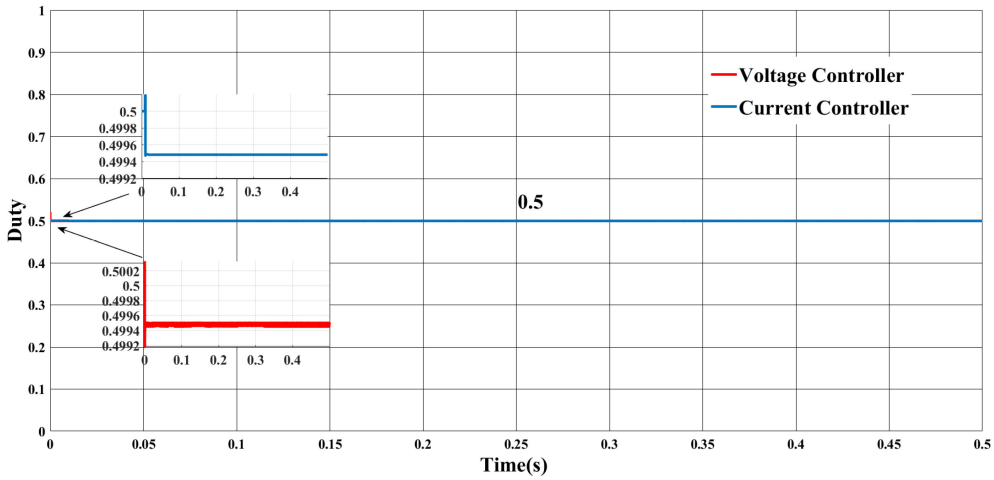

Figure 12. Deep learning controller outputs in the no attack condition.

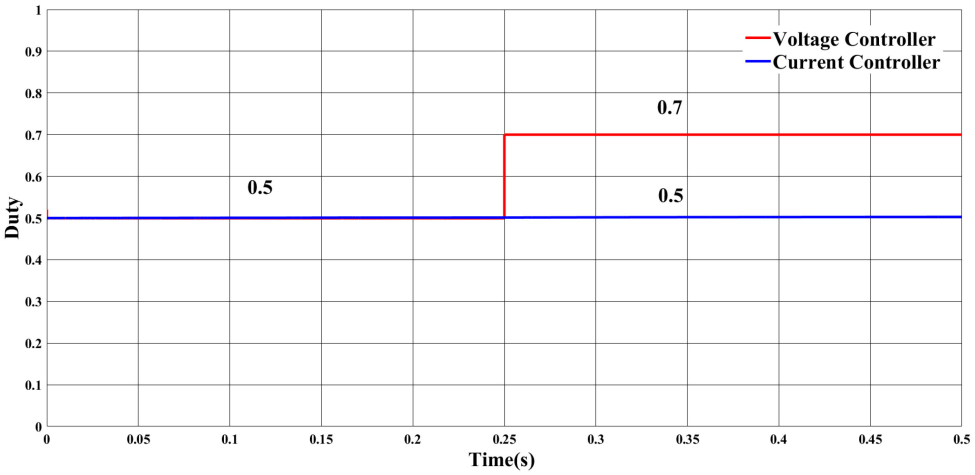

Figure 13. Deep learning controller outputs in the FDI attack condition.

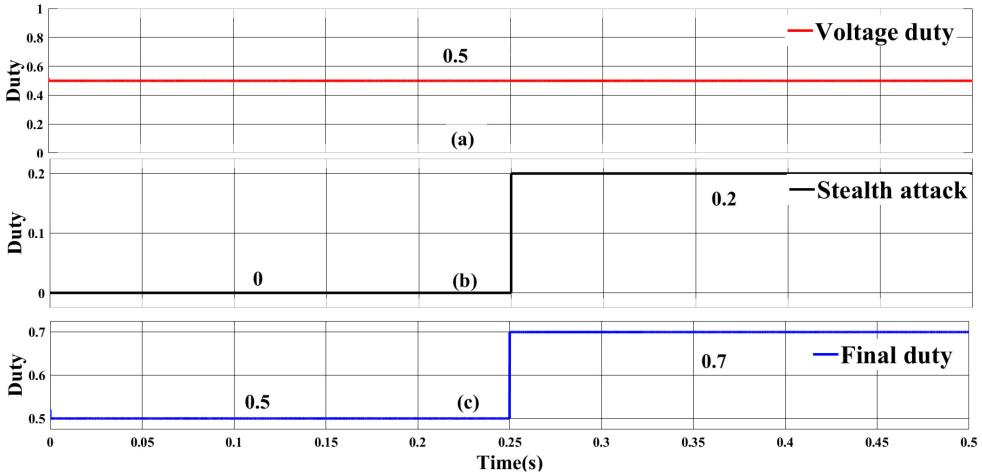

Figure 14. FDI attack on the voltage controller output. (**a**) voltage controller duty (**b**) FDI attack on duty (**c**) Final duty D_1^*.

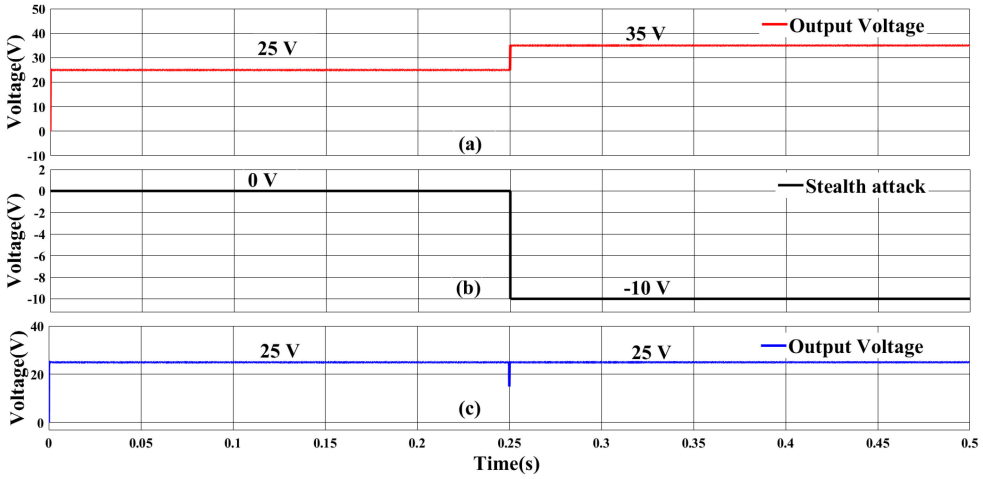

Figure 15. Stealthy local covert attack versus the FDI attack. (**a**) Output voltage of converter (**b**) stealth attack on output voltage sensor (**c**) Sensor voltage to controller after stealth attack.

To overcome the SLCA of an FDI attack, the generated control inputs are passed through the decision block. As shown in Figure 16a, the attacked voltage controller output and current controller output are passed through the decision block. The decision block gives an output of 0.5, as shown in Figure 16b; this represents the final duty, which is the current controller output that corresponds to the reference voltage. The duty received from the decision block is given to the DC-DC buck converter to obtain the reference value of 25 V.

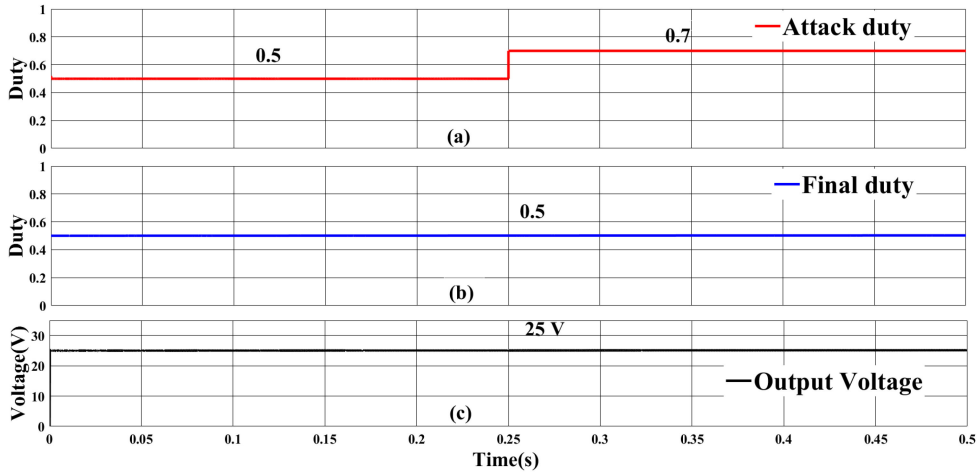

Figure 16. Overcoming the stealth attack. (**a**) Attacked voltage controller duty (**b**) Final duty to plant (**c**) Output voltage after stealth attack mitigation.

7.2.1. FDI Attack on the Output Voltage Sensor

In this case, the performance of the proposed algorithm is evaluated when there is an FDI attack on the output voltage sensor. Figure 17a shows the FDI attack on the output voltage sensor, where the adversary tries to manipulate the sensor data by changing the values from 25 V to 35 V at 0.22 s, 35 V to 40 V at 0.41 s, 40 V to 45 V at 0.62 s, 45 V to 35 V at 0.73 s and back to 25 V at 0.85 s. During all these sensor data manipulations, the actual output voltage of the converter remains stable at the reference value.

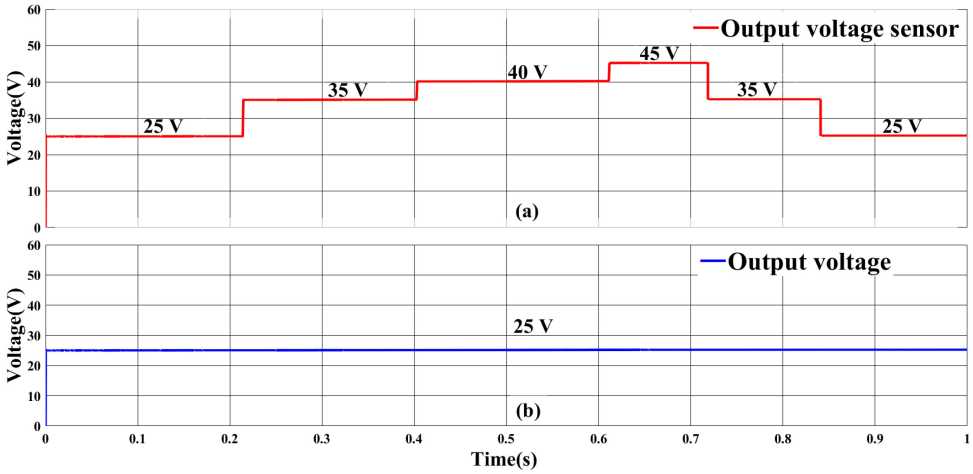

Figure 17. FDI attack on the output voltage sensor. (**a**) FDI attack on output voltage sensor (**b**) Output voltage of the plant.

7.2.2. FDI Attack on the Input Voltage Sensor

An FDI attack is performed on the input voltage sensor by injecting the false data into the sensor values. The input voltage is changed from 50 V to 65 V at 0.35 s, and back to 50 V at 0.7 s, as shown in Figure 18a. The designed control scheme efficiently mitigates the attack and keeps the output voltage constant at a reference value of 25 V, as shown in Figure 18b.

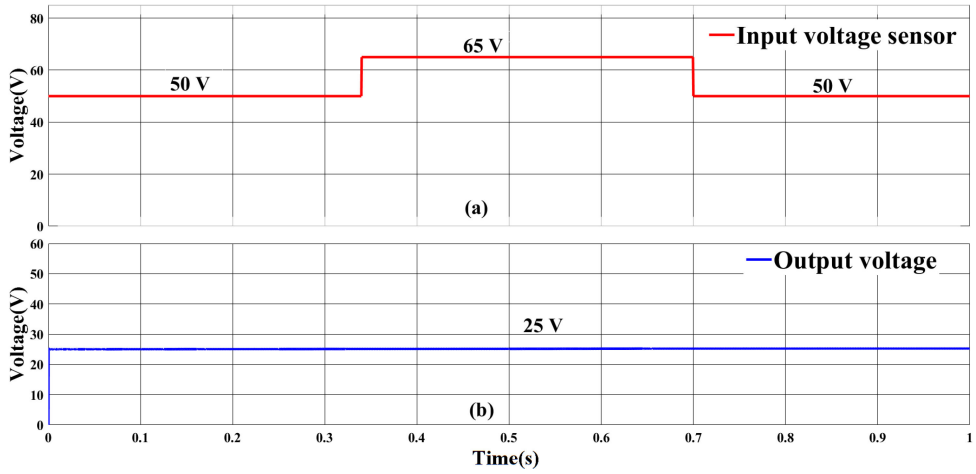

Figure 18. FDI attack on the input voltage sensor. (**a**) FDI attack on input voltage sensor (**b**) Output voltage of the plant.

7.2.3. FDI Attack on the Input Voltage Sensor and Stealth Attack

In this case, a complex scenario, in which the adversary tries to perform a stealth FDI attack on the voltage controller output and an FDI attack on the input voltage sensor, is considered. The robustness of the designed control mechanism is verified by implementing both attacks simultaneously. From Figure 19a, we observe that the D_1 is manipulated by injecting false data and changing the value from 0.5 to 0.39 at 0.35 s, and 0.39 to 0.6 at 0.5 s, before finally settling to 0.7 at 0.7 s. At the same time, the input voltage sensor data are also falsified by changing the value from 50 V to 65 V at 0.35 s, and back to 50 V at 0.7 s, as shown in Figure 19b. Figure 19c shows the output voltage of the converter which remains unchanged and maintained at a reference level of 25 V. This shows that the designed control scheme is effectively designed to handle multiple attacks with a wide range of false data values.

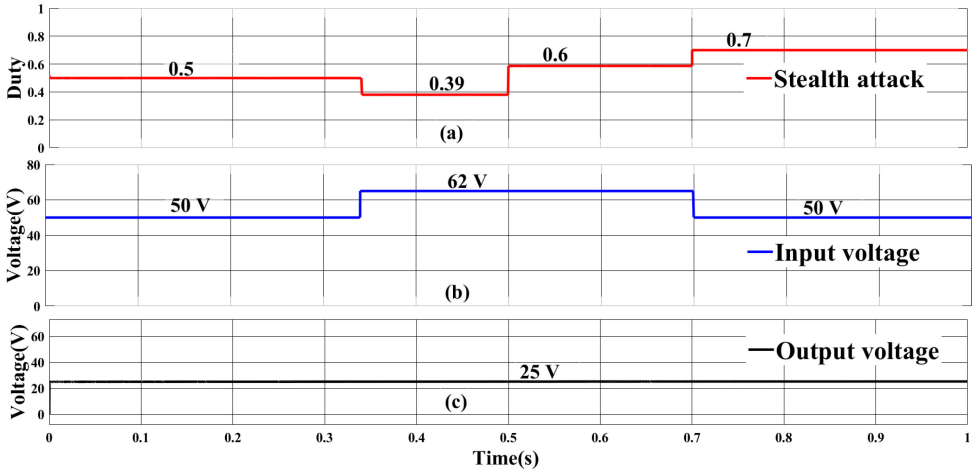

Figure 19. FDI attack on the input voltage sensor and stealth attack. (**a**) Stealth attack on voltage controller duty (**b**) FDI attack on input voltage sensor (**c**) Output voltage of the plant.

7.3. Hardware Implementation

To test the applicability and accuracy of the proposed control scheme in real-world scenarios, a real-time hardware setup was built in a laboratory environment, as shown in Figure 20. Initially, the designed control scheme's ability to control the DC-DC buck converter is analyzed. The converter's reference voltage is varied from 25 V to 35 V. Figure 21a shows the change in the pulse width corresponding to the change in the output of the control algorithm. From Figure 21b, we can observe that the converter's output voltage changes from 25 V to 35 V, and it takes approximately 10 ms for the transition to occur.

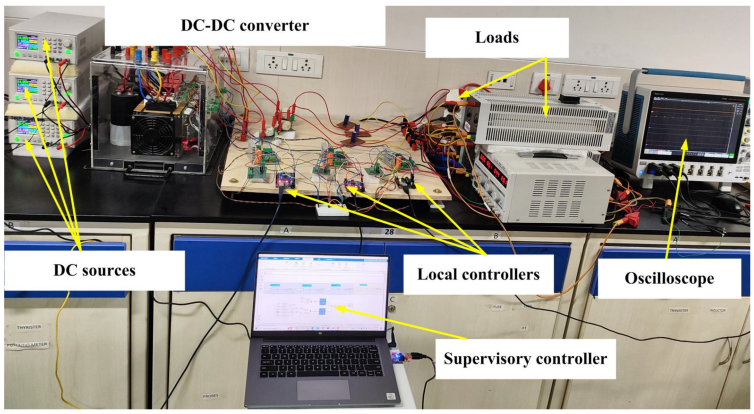

Figure 20. Realtime hardware setup of parallel DC-DC converters.

The predicted control inputs from the voltage controller and current controller and the adversary's FDI attack on the voltage control input is shown in Figure 22. The DL controller produces the controller inputs D_1 and D_2 by considering input voltages and currents, and output voltages and currents. During normal operation, a duty of 0.5 is obtained for both the voltage and current controller, as shown in Figure 22a,c. The adversary performs an FDI attack (D_a) of 0.2 on the controller input D_1; it is modified to D_1^*, which is 0.7, as shown in Figure 22b. The decision block receives the attacked voltage duty D_1^* and the normal current duty (D_1). The decision block decides on the duty that should be passed to the plant, based on the objective function specified in (15).

The performance of the designed control algorithm during the SLCA of the FDIA attack can be observed in Figure 23. Figure 23a gives the output voltage controller duty, and Figure 23b shows the FDI attack. Even though a stealth attack is performed by manipulating the output voltage sensor before reaching the controller, the proposed technique mitigates

the attack. Figure 23c shows the output voltage of the converter, which is the desired reference value.

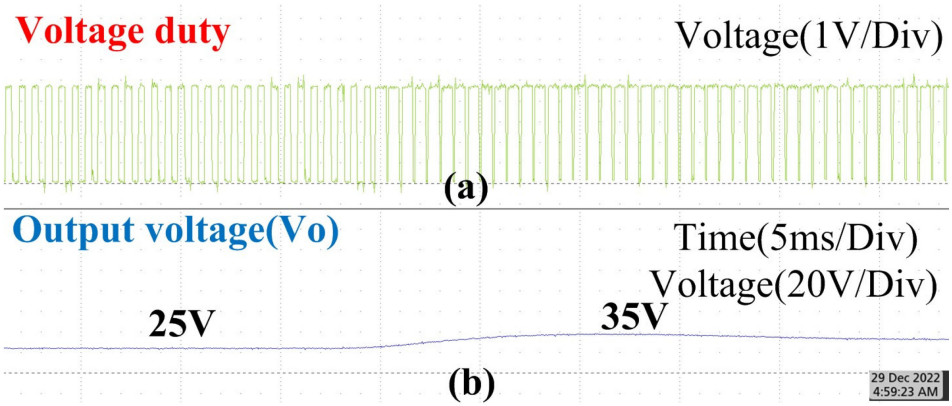

Figure 21. Reference change in the DC-DC converter. (**a**) Change in controller duty according to reference voltage change (**b**) Output voltage change according to reference change.

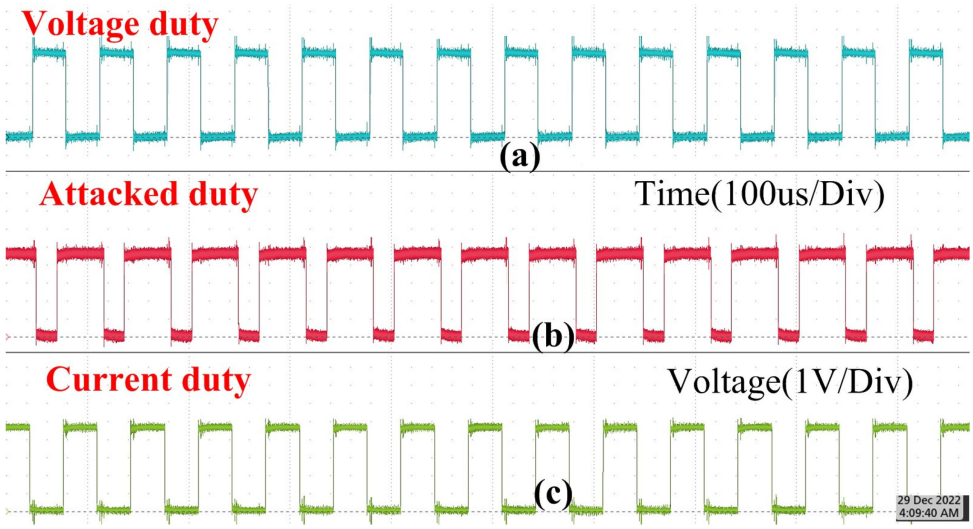

Figure 22. Deep learning controller output with FDI attack. (**a**) Voltage controller duty during normal operation (**b**) Attacked voltage controller duty (**c**) Current controller duty during attack and normal condition.

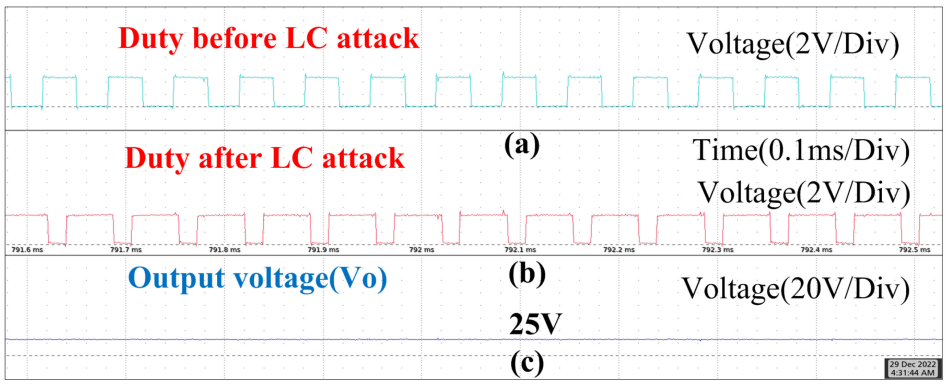

Figure 23. SLCA-FDIA attack mitigation. (**a**) Duty before local covert attack (**b**) Duty after local covert attack (**c**) Output voltage of the plant.

8. Conclusions and Future Scope

This article reviews different cyber threats that adversaries pose toward critical cyber-physical systems, and the transition of cyber security towards AI. The attacks on CPS are performed on a large scale, resulting in disasters, such as the failure of the entire critical infrastructure of a country. The cyberwarfare methods needed to do so are discussed in detail. To overcome cyber attacks from adversaries, various defense mechanisms are employed at the network level and device level. After studying the basic defense mechanisms and their shortcomings in attack detection in CPS, we can conclude that there is a need for intelligent attack detection and mitigation mechanisms. The general network infrastructure used in microgrids is discussed, and the cyber attacks targeting the network framework are represented. The most common and effective cyber attacks, such as FDIA, DoS, and MITM attacks, are discussed in detail. Additionally, the difference between normal IT security and CPS security is studied by analyzing the challenges involved in detecting and mitigating cyber attacks. Artificial intelligence provides effective methods for cyber attack detection that are studied elaborately.

After identifying the advantages of AI in cyber attack detection, some of the literature on AI as an attack detection mechanism is studied. We found that the complex control structure of CPS becomes even more complex with the inclusion of a data-driven attack detection mechanism. To reduce complexity and increase operational efficiency, a complete data-driven methodology should be proposed for CPS control and for cyber attack detection. To illustrate the importance of this methodology, a case study is performed, in which a stealth FDI attack is formulated and its mitigation is performed using deep neural networks. Further, real-time hardware implementation is performed to prove the method's effective operation. Further, AI techniques can be implemented on the most complicated CPS for mitigating different types of cyber attacks.

Funding: This work is supported by Science and Engineering Research Board (SERB) under start-up research grant SRG/2020/000269, sponsoring Dr. Sreedhar Madichetty.

Data Availability Statement: No new data is created.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The abbreviations used in this article are given below:

ARP	Address resolution protocol
CCS	Change cipher spec
CPS	Cyber-physical systems
DARPA	Defense Advanced Research Projects Agency
DNS	Domain name server
EAP	Extensible authentication protocol
EV	Electric vehicle
HTTP	Hypertext transfer protocol
HTTPS	Hypertext transfer protocol secure
IP	Internet protocol
KDD99	Knowledge Discovery in Databases 1999
MAC	Media access control
OSI	Open system interconnection
PLC	Programmable logical controller
RES	Renewable energy sources
SSL	Secure socket layer
TCP	Transfer control protocol
FDI	False data injection
SLCA	Stealthy local covert attack
FFBP	Feedforward back propagation

RMSE	Root mean squared error
GOOSE	Generic object-oriented system-wide events
DNP	Distributed network protocol
IEC	International Electrotechnical Commission
IDS	Intrusion detection system
LDOS	Low rate denial of service
NARX	Nonlinear autoregressive network with exogenous inputs
MPC	Model predictive control
ANN	Artificial neural network
PI	Proportional integral
LSTM	Long short-term memory
XGBOOST	Extreme gradient boosting
GRU	Gated recurrent unit

References

1. Bong, C.P.; Hashim, H.; Ho, W.S.; Ab Muis, Z.B.; Yunus, N.A.B.; Demoral, A.; Tirta, A.; Kresnawan, M.R.; Safrina, R.; Rosalia, S.A. Integration of Variable Renewable Energy, Electric Vehicle, and Smart Microgrid in ASEAN: A Focus Group Discussion Approach. In Proceedings of the IOP Conference Series: Earth and Environmental Science, Online, 14 September 2021; IOP Publishing: Bristol, UK, 2022; Volume 997, p. 012013.
2. Kulkarni, S.V.; Gaonkar, D.N. Operation and control of a microgrid in isolated mode with multiple distributed generation systems. In Proceedings of the 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), Kollam, India, 21–23 December 2017; pp. 1–6. [CrossRef]
3. Hossain, E.; Kabalcı, E.; Bayindir, R.; Perez, R. A comprehensive study on microgrid technology. *Int. J. Renew. Energy Res.* **2014**, *4*, 1094–1104.
4. Bani-Ahmed, S.; Weber, L.; Nasiri, A.; Hosseini, H. Microgrid communications: State of the art and future trends. In Proceedings of the 2014 International Conference on Renewable Energy Research and Application (ICRERA), Milwaukee, WI, USA, 19–22 October 2014; pp. 780–785. [CrossRef]
5. Kumar, S.; Islam, S.; Jolfaei, A. Microgrid communications—Protocols and standards. *Var. Scalability Stab. Microgr.* **2019**, *139*, 291–326. [CrossRef]
6. Serban, I.; Céspedes, S.; Marinescu, C.; Azurdia-Meza, C.A.; Gómez, J.S.; Hueichapan, D.S. Communication Requirements in Microgrids: A Practical Survey. *IEEE Access* **2020**, *8*, 47694–47712. [CrossRef]
7. Robinson, M.; Jones, K.; Janicke, H. Cyber warfare: Issues and challenges. *Comput. Secur.* **2015**, *49*, 70–94. [CrossRef]
8. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97. [CrossRef]
9. Chasanah, B.; Candiwan, C. Analysis of College Students' Cybersecurity Awareness in Indonesia. *SISFORMA* **2020**, *7*, 49. [CrossRef]
10. Hong, W.C.H.; Chi, C.; Liu, J.; Zhang, Y.; Lei, V.N.L.; Xu, X. The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Educ. Inf. Technol.* **2023**, *28*, 439–470. [CrossRef]
11. *Cyber Security Research Report 2020*; National Technology Security Coalition: Atlanta, GA, USA, 2021.
12. Freet, D.; Agrawal, R. *Cyber Espionage*; Springer: Cham, Switzerland, 2017. [CrossRef]
13. Schaefer, T.; Brown, B.; Graessle, F.; Salzsieder, L. Cybersecurity: Common risks: A dynamic set of internal and external threats includes loss of data and revenue, sabotage at the hands of current or former employees, and a PR nightmare. *Strateg. Financ.* **2017**, *99*, 54–62.
14. Hamid, A. Denial of Service Attacks: Tools and Categories. *Int. J. Eng. Res.* **2020**, *9*, 631–636. [CrossRef]
15. Nguyen, T.; Wang, S.; Alhazmi, M.; Nazemi, M.; Estebsari, A.; Dehghanian, P. Electric Power Grid Resilience to Cyber Adversaries: State of the Art. *IEEE Access* **2020**, *8*, 87592–87608. [CrossRef]
16. Goswami, M. Fake News and Cyber Propaganda: A Study of Manipulation and Abuses on Social Media. In *Mediascape in 21st Century: Emerging Perspectives*; Kanishka Publishers: Delhi, India, 2018; pp. 535–544.
17. Eling, M.; Elvedi, M.; Falco, G. The economic impact of extreme cyber risk scenarios. *N. Am. Actuar. J.* **2022**, 1–15. [CrossRef]
18. Collins, S.; McCombie, S. Stuxnet: The emergence of a new cyber weapon and its implications. *J. Polic. Intell. Count. Terror.* **2012**, *7*, 80–91. [CrossRef]
19. Dehlawi, Z.; Abokhodair, N. Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. In Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics, Seattle, WA, USA, 4–7 June 2013; pp. 73–75. [CrossRef]
20. Guo, Q.; Xin, S.; Wang, J. Comprehensive security assessment for a cyber physical energy system: A lesson from Ukraine's blackout. *Dianli Xitong Zidonghua/Autom. Electr. Power Syst.* **2016**, *40*, 145–147. [CrossRef]
21. Cherepanov, A.; Lipovsky, R. Blackenergy–What We Really Know about the Notorious Cyber Attacks. *Virus Bulletin* **2016**, 1–8.
22. Halevi, T.; Memon, N.; Nov, O. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN Electron. J.* **2015**. [CrossRef]

23. Cherepanov, A.; Lipovsky, R. *Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet*; WeLiveSecurity, ESET: San Diego, CA, USA, 2017; Volume 12.
24. Herzog, S. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *J. Strateg. Secur.* **2011**, *4*, 49–60. [CrossRef]
25. Lazar, M. The Russian Cyber Campaign against Georgia (2008). *Int. Annu. Sci. Sess. Strateg.* **2012**, *21*, 500–505.
26. Keizer, G. Cyberattacks Knock out Georgia's Internet Presence. *Computerworld* **2008**, *24*, 2010.
27. Sang-Hun, C.; Markoff, J. Cyberattacks Jam Government and Commercial Web Sites in US and South Korea. *New York Times*, 9 July 2009.
28. Sanger, D.E.; Barboza, D.; Perlroth, N. Chinese army unit is seen as tied to hacking against US. *New York Times*, 19 February 2013; p. 18.
29. Deibert, R.J.; Rohozinski, R.; Manchanda, A.; Villeneuve, N.; Walton, G. *Tracking Ghostnet: Investigating a Cyber Espionage Network*; University of Oxford: Oxford, UK, 2009.
30. Norton-Taylor, R. Titan Rain: How Chinese Hackers Targeted Whitehall. *Guardian* **2007**, 5.
31. Espionage, I.C. Shadows in the Cloud. 2010. Available online: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/shadows-in-the-cloud.pdf (accessed on 2 May 2023).
32. Dudley, R.; Golden, D. *The Colonial Pipeline Ransomware Hackers Had a Secret Weapon: Self-Promoting Cybersecurity Firms*; MIT Technology Review and ProPublica: Cambridge, MA, USA, 2021.
33. Khoshnood, A. *The Attack on Natanz and the JCPOA*; BESA Center Perspectives Paper; BESA Center: Ramat Gan, Israel, 2021.
34. Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A.V. False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey. *IEEE Trans. Ind. Inform.* **2016**, *13*, 411–423. [CrossRef]
35. Liang, G.; Zhao, J.; Luo, F.; Weller, S.; Dong, Z. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1630–1638. [CrossRef]
36. Halfond, W.G.; Viegas, J.; Orso, A. A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE International Symposium on Secure Software Engineering, Washington, DC, USA, 13–15 March 2006; Volume 1, pp. 13–15.
37. Endler, D. *The Evolution of Cross Site Scripting Attacks*; Technical Report; iDEFENSE Labs: Botany, Australia, 2002.
38. Mode, G.R.; Calyam, P.; Hoque, K.A. False data injection attacks in internet of things and deep learning enabled predictive analytics. *arXiv* **2019**, arXiv:1910.01716.
39. Wlazlo, P.; Sahu, A.; Mao, Z.; Huang, H.; Goulart, A.; Davis, K.; Zonouz, S. Man-in-the-middle attacks and defence in a power system cyber-physical testbed. *IET Cyber-Phys. Syst. Theory Appl.* **2021**, *6*, 164–177. [CrossRef]
40. Ali, F. IP spoofing. *Internet Protoc. J.* **2007**, *10*, 1–9.
41. Whalen, S. An Introduction to arp Spoofing. Node99 [Online Document] 2001. Available online: https://www.cavalcantetreinamentos.com.br/blog/material-sala-de-aula/Seguranca%20em%20Redes/Outros/arp_spoofing_slides.pdf (accessed on 2 May 2023).
42. Steinhoff, U.; Wiesmaier, A.; Araújo, R. The state of the art in DNS spoofing. In Proceedings of the 4th International Conference on Applied Cryptography and Network Security (ACNS), Singapore, 6–9 June 2006.
43. Gangan, S. A review of man-in-the-middle attacks. *arXiv* **2015**, arXiv:1504.02115.
44. Elleithy, K.M.; Blagovic, D.; Cheng, W.K.; Sideleau, P. *Denial of Service Attack Techniques: Analysis, Implementation and Comparison*; Sacred Heart University: Fairfield, Connecticut, 2005.
45. Long, N.; Thomas, R. *Trends in Denial of Service Attack Technology*; CERT Coordination Center: Pittsburgh, PA, USA, 2001; Volume 648, p. 651.
46. Lau, F.; Rubin, S.H.; Smith, M.H.; Trajkovic, L. Distributed denial of service attacks. In Proceedings of the SMC 2000 Conference, 2000 IEEE International Conference on Systems, Man and Cybernetics. 'Cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions' (Cat. No. 0), Nashville, TN, USA, 8–11 October 2000; Volume 3, pp. 2275–2280.
47. Nur, A.Y.; Tozal, M.E. Defending cyber-physical systems against dos attacks. In Proceedings of the 2016 IEEE International Conference on Smart Computing (SMARTCOMP), St Louis, MO, USA, 18–20 May 2016; pp. 1–3.
48. Liu, S.; Li, S.; Xu, B. Event-triggered resilient control for cyber physical system under denial-of-service attacks. *Int. J. Control* **2018**, *93*, 1907–1919. [CrossRef]
49. Neupane, K.; Haddad, R.; Chen, L. Next generation firewall for network security: A survey. In Proceedings of the IEEE SoutheastCon 2018, St. Petersburg, FL, USA, 19–22 April 2018; pp. 1–6.
50. Lal, N.A.; Prasad, S.; Farik, M. A review of authentication methods. *Int. J. Sci. Technol. Res.* **2016**, *5*, 246–249.
51. Post, G.; Kagan, A. Management tradeoffs in anti-virus strategies. *Inf. Manag.* **2000**, *37*, 13–24. [CrossRef]
52. Delfs, H.; Knebl, H.; Delfs, H.; Knebl, H. Symmetric-Key Cryptography. In *Introduction to Cryptography: Principles and Application*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 11–48.
53. Chandra, S.; Paira, S.; Alam, S.S.; Sanyal, G. A comparative survey of symmetric and asymmetric key cryptography. In Proceedings of the 2014 IEEE International Conference on Electronics, Communication and Computational Engineering (ICECCE), Tamilnadu, India, 17–18 November 2014; pp. 83–93.
54. Mukkamala, P.P.; Rajendran, S. A survey on the different firewall technologies. *Int. J. Eng. Appl. Sci. Technol.* **2020**, *5*, 363–365. [CrossRef]

55. El-Atawy, A.; Al-Shaer, E.; Tran, T.; Boutaba, R. Adaptive early packet filtering for defending firewalls against DoS attacks. In Proceedings of the IEEE INFOCOM 2009, Rio De Janeiro, Brazil, 24 April 2009; pp. 2437–2445.
56. Liao, H.J.; Lin, C.H.R.; Lin, Y.C.; Tung, K.Y. Intrusion detection system: A comprehensive review. *J. Netw. Comput. Appl.* **2013**, *36*, 16–24. [CrossRef]
57. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 1–22. [CrossRef]
58. Ioulianou, P.; Vasilakis, V.; Moscholios, I.; Logothetis, M. A signature-based intrusion detection system for the internet of things. In Proceedings of the Information and Communication Technology Form, Heslington, UK, 11–13 July 2018.
59. Gyanchandani, M.; Rana, J.; Yadav, R. Taxonomy of anomaly based intrusion detection system: A review. *Int. J. Sci. Res. Publ.* **2012**, *2*, 1–13.
60. Wang, Z.; Li, X. Intrusion prevention system design. In Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012, Chongqing, China, 26–28 October 2012; Springer: Berlin, Germany, 2013; Volume 3, pp. 375–382.
61. Zhang, J.; Peng, S.; Gao, Y.; Zhang, Z.; Hong, Q. APMSA: Adversarial Perturbation Against Model Stealing Attacks. *IEEE Trans. Inf. Secur.* **2023**, *18*, 1667–1679. [CrossRef]
62. Li, B.; Zhou, X.; Ning, Z.; Guan, X.; Yiu, K.F.C. Dynamic event-triggered security control for networked control systems with cyber-attacks: A model predictive control approach. *Inf. Sci.* **2022**, *612*, 384–398. [CrossRef]
63. Lv, Z.; Qiao, L.; Hossain, M.S.; Choi, B.J. Analysis of using blockchain to protect the privacy of drone big data. *IEEE Netw.* **2021**, *35*, 44–49. [CrossRef]
64. Chen, Y.; Zhu, L.; Hu, Z.; Chen, S.; Zheng, X. Risk propagation in multilayer heterogeneous network of coupled system of large engineering project. *J. Manag. Eng.* **2022**, *38*, 04022003. [CrossRef]
65. Schweppe, F.C.; Wildes, J. Power system static-state estimation, Part I: Exact model. *IEEE Trans. Power Appar. Syst.* **1970**, *PAS-89*, 120–125. [CrossRef]
66. Beg, O.A.; Nguyen, L.V.; Johnson, T.T.; Davoudi, A. Signal temporal logic-based attack detection in DC microgrids. *IEEE Trans. Smart Grid* **2018**, *10*, 3585–3595. [CrossRef]
67. Jin, D.; Li, Z.; Hannon, C.; Chen, C.; Wang, J.; Shahidehpour, M.; Lee, C.W. Toward a cyber resilient and secure microgrid using software-defined networking. *IEEE Trans. Smart Grid* **2017**, *8*, 2494–2504. [CrossRef]
68. Gong, J.; Rezaeipanah, A. A fuzzy delay-bandwidth guaranteed routing algorithm for video conferencing services over SDN networks. *Multimed. Tools Appl.* **2023**, 1–30. [CrossRef]
69. Kushal, T.R.B.; Lai, K.; Illindala, M.S. Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system. *IEEE Trans. Smart Grid* **2018**, *10*, 4741–4750. [CrossRef]
70. Nikmehr, N.; Moradi Moghadam, S. Game-theoretic cybersecurity analysis for false data injection attack on networked microgrids. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 365–373. [CrossRef]
71. Cai, W.; Shea, R.; Huang, C.Y.; Chen, K.T.; Liu, J.; Leung, V.C.; Hsu, C.H. A survey on cloud gaming: Future of computer games. *IEEE Access* **2016**, *4*, 7605–7620. [CrossRef]
72. Chlela, M.; Mascarella, D.; Joos, G.; Kassouf, M. Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks. *IEEE Trans. Smart Grid* **2017**, *9*, 4702–4711. [CrossRef]
73. Liu, G. Data collection in mi-assisted wireless powered underground sensor networks: Directions, recent advances, and challenges. *IEEE Commun. Mag.* **2021**, *59*, 132–138. [CrossRef]
74. Zhao, K.; Jia, Z.; Jia, F.; Shao, H. Multi-scale integrated deep self-attention network for predicting remaining useful life of aero-engine. *Eng. Appl. Artif. Intell.* **2023**, *120*, 105860. [CrossRef]
75. Zhan, C.; Dai, Z.; Yang, Z.; Zhang, X.; Ma, Z.; Thanh, H.V.; Soltanian, M.R. Subsurface sedimentary structure identification using deep learning: A review. *Earth-Sci. Rev.* **2023**, *239*, 104370. [CrossRef]
76. Liu, H.; Yue, Y.; Liu, C.; Spencer, B.; Cui, J. Automatic recognition and localization of underground pipelines in GPR B-scans using a deep learning model. *Tunn. Undergr. Space Technol.* **2023**, *134*, 104861. [CrossRef]
77. Li, B.; Lu, Y.; Pang, W.; Xu, H. Image Colorization using CycleGAN with semantic and spatial rationality. *Multimed. Tools Appl.* **2023**, *82*, 21641–21655. [CrossRef]
78. Zhang, X.; Wen, S.; Yan, L.; Feng, J.; Xia, Y. A Hybrid-Convolution Spatial–Temporal Recurrent Network for Traffic Flow Prediction. *Comput. J.* **2022**, bxac171. [CrossRef]
79. Zhang, Z.; Ning, H.; Shi, F.; Farha, F.; Xu, Y.; Xu, J.; Zhang, F.; Choo, K.K.R. Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artif. Intell. Rev.* **2022**, *55*, 1029–1053. [CrossRef]
80. Shrestha Chitrakar, A.; Petrović, S. Efficient k-means using triangle inequality on spark for cyber security analytics. In Proceedings of the ACM International Workshop on Security and Privacy Analytics, Dallas, TX, USA, 27 March 2019; pp. 37–45.
81. Husák, M.; Kašpar, J.; Bou-Harb, E.; Čeleda, P. On the sequential pattern and rule mining in the analysis of cyber security alerts. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017; pp. 1–10.
82. Azeez, N.A.; Ayemobola, T.J.; Misra, S.; Maskeliūnas, R.; Damaševičius, R. Network intrusion detection with a hashing based apriori algorithm using Hadoop MapReduce. *Computers* **2019**, *8*, 86. [CrossRef]

83. Aung, Y.Y.; Min, M.M. Hybrid intrusion detection system using K-means and K-nearest neighbors algorithms. In Proceedings of the 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), Singapore, 6–8 June 2018; pp. 34–38.
84. Majeed, R.; Abdullah, N.A.; Mushtaq, M.F. IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 7. [CrossRef]
85. Meyer, D.; Wien, F. Support Vector Machines. In *The Interface to Libsvm in Package e1071*; Technische Universit: Wien, Austria, 2015; Volume 28, p. 20.
86. Al-Omari, M.; Rawashdeh, M.; Qutaishat, F.; Alshira'H, M.; Ababneh, N. An intelligent tree-based intrusion detection model for cyber security. *J. Netw. Syst. Manag.* **2021**, *29*, 20. [CrossRef]
87. Rahman, C.M.; Farid, D.M.; Harbi, N.; Bahri, E.; Rahman, M.Z. Attacks Classification in Adaptive Intrusion Detection Using Decision Tree. 2010. Available online: http://dspace.uiu.ac.bd/handle/52243/73 (accessed on 2 May 2023).
88. Ferrag, M.A.; Maglaras, L.; Ahmim, A.; Derdour, M.; Janicke, H. Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. *Future Internet* **2020**, *12*, 44. [CrossRef]
89. Choubisa, M.; Doshi, R.; Khatri, N.; Hiran, K.K. A simple and robust approach of random forest for intrusion detection system in cyber security. In Proceedings of the 2022 IEEE International Conference on IoT and Blockchain Technology (ICIBT), Ranchi, India, 6–8 May 2022; pp. 1–5.
90. Chen, Z.; Zhou, L.; Yu, W. ADASYN- Random Forest Based Intrusion Detection Model. In Proceedings of the 2021 4th International Conference on Signal Processing and Machine Learning, Beijing, China, 18–20 August 2021; pp. 152–159.
91. Apruzzese, G.; Andreolini, M.; Colajanni, M.; Marchetti, M. Hardening random forest cyber detectors against adversarial attacks. *IEEE Trans. Emerg. Top. Comput. Intell.* **2020**, *4*, 427–439. [CrossRef]
92. Shrestha, A.; Mahmood, A. Review of deep learning algorithms and architectures. *IEEE Access* **2019**, *7*, 53040–53065. [CrossRef]
93. Bapiyev, I.M.; Aitchanov, B.H.; Tereikovskyi, I.A.; Tereikovska, L.A.; Korchenko, A.A. Deep neural networks in cyber attack detection systems. *Int. J. Civ. Eng. Technol. (IJCIET)* **2017**, *8*, 1086–1092.
94. Zhou, L.; Ouyang, X.; Ying, H.; Han, L.; Cheng, Y.; Zhang, T. Cyber-attack classification in smart grid via deep neural network. In Proceedings of the 2nd International Conference on Computer Science and Application Engineering, Hohhot, China, 22–24 October 2018; pp. 1–5.
95. Jemal, I.; Haddar, M.A.; Cheikhrouhou, O.; Mahfoudhi, A. Performance evaluation of Convolutional Neural Network for web security. *Comput. Commun.* **2021**, *175*, 58–67. [CrossRef]
96. Alabadi, M.; Celik, Y. Anomaly detection for cyber-security based on convolution neural network: A survey. In Proceedings of the IEEE 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 26–27 June 2020; pp. 1–14.
97. Tang, T.A.; McLernon, D.; Mhamdi, L.; Zaidi, S.A.R.; Ghogho, M. Intrusion Detection in Sdn-Based Networks: Deep Recurrent Neural Network Approach. In *Deep Learning Applications for Cyber Security*; Springer: Cham, Switzerland, 2019; pp. 175–195.
98. Feltus, C. Learning algorithm recommendation framework for IS and CPS security: Analysis of the RNN, LSTM, and GRU contributions. *Int. J. Syst. Softw. Secur. Prot. (IJSSSP)* **2022**, *13*, 1–23. [CrossRef]
99. Tasneem, S.; Gupta, K.D.; Roy, A.; Dasgupta, D. Generative Adversarial Networks (GAN) for Cyber Security: Challenges and Opportunities. In Proceedings of the 2022 IEEE Symposium Series on Computational Intelligence, Singapore, 4–7 December 2022.
100. Chen, D.; Wawrzynski, P.; Lv, Z. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustain. Cities Soc.* **2021**, *66*, 102655. [CrossRef]
101. Yousefi-Azar, M.; Varadharajan, V.; Hamey, L.; Tupakula, U. Autoencoder-based feature learning for cyber security applications. In Proceedings of the 2017 IEEE International Joint Conference on Neural Networks (IJCNN), Anchorage, AK, USA, 14–19 May 2017; pp. 3854–3861.
102. Li, C.; Qiu, M.; Li, C. Reinforcement Learning for Cybersecurity. *Reinf. Learn. Cyber-Phys. Syst* **2019**, 155–168.
103. IMPACT. Available online: https://www.impactcybertrust.org/ (accessed on 2 May 2023).
104. Traffic Data from Kyoto University's Honeypots. Available online: http://www.takakura.com/Kyoto_data/ (accessed on 2 May 2023).
105. KDD Cup 1999 Data. Available online: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed on 2 May 2023).
106. NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB. Available online: https://www.unb.ca/cic/datasets/nsl.html (accessed on 2 May 2023).
107. 1998 DARPA Intrusion Detection Evaluation Dataset | MIT Lincoln Laboratory. Available online: https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset (accessed on 2 May 2023).
108. The UNSW-NB15 Dataset | UNSW Research. Available online: https://research.unsw.edu.au/projects/unsw-nb15-dataset (accessed on 2 May 2023).
109. Insider Threat Test Dataset. Available online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099 (accessed on 2 May 2023).
110. The Bot-IoT Dataset | UNSW Research. Available online: https://research.unsw.edu.au/projects/bot-iot-dataset (accessed on 2 May 2023).
111. MAWIWorking Group Traffic Archive. Available online: https://mawi.wide.ad.jp/mawi/ (accessed on 2 May 2023).

112. Keila, P.; Skillicorn, D. Structure in the Enron email dataset. In Proceedings of the Workshop on Link Analysis, Security and Counterterrorism, SIAM International Conference on Data Mining, Newport Beach, CA, USA, 21–23 April 2005; pp. 55–64.
113. Yang, L.; Ciptadi, A.; Laziuk, I.; Ahmadzadeh, A.; Wang, G. BODMAS: An open dataset for learning based temporal analysis of PE malware. In Proceedings of the 2021 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 27 May 2021; pp. 78–84.
114. Kumar, R.; Zhang, X.; Khan, R.U.; Kumar, J.; Ahad, I. Effective and explainable detection of android malware based on machine learning algorithms. In Proceedings of the 2018 International Conference on Computing and Artificial Intelligence, Sanya, China, 21–23 December 2018; pp. 35–40.
115. CAIDA Data—Completed Datasets—CAIDA. Available online: https://www.caida.org/catalog/datasets/completed-datasets/ (accessed on 2 May 2023).
116. Amor, N.B.; Benferhat, S.; Elouedi, Z. Naive bayes vs decision trees in intrusion detection systems. In Proceedings of the 2004 ACM Symposium on Applied Computing, Nicosia, Cyprus, 14–17 March 2004; pp. 420–424.
117. Amiri, F.; Yousefi, M.R.; Lucas, C.; Shakery, A.; Yazdani, N. Mutual information-based feature selection for intrusion detection systems. *J. Netw. Comput. Appl.* **2011**, *34*, 1184–1199. [CrossRef]
118. Zhang, J.; Zulkernine, M.; Haque, A. Random-forests-based network intrusion detection systems. *IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.)* **2008**, *38*, 649–659. [CrossRef]
119. Hasan, M.A.M.; Nasser, M.; Ahmad, S.; Molla, K.I. Feature selection for intrusion detection using random forest. *J. Inf. Secur.* **2016**, *7*, 129–140. [CrossRef]
120. Gao, N.; Gao, L.; Gao, Q.; Wang, H. An intrusion detection model based on deep belief networks. In Proceedings of the 2014 IEEE Second International Conference on Advanced Cloud and Big Data, Huangshan, China, 20–22 November 2014; pp. 247–252.
121. Xu, C.; Shen, J.; Du, X.; Zhang, F. An Intrusion Detection System Using a Deep Neural Network With Gated Recurrent Units. *IEEE Access* **2018**, *6*, 48697–48707. [CrossRef]
122. Ahsan, M.; Nygard, K.E. Convolutional Neural Networks with LSTM for Intrusion Detection. In Proceedings of the 35th International Conference on Computers and Their Applications, San Francisco, CA, USA, 23–25 March 2020; Volume 69, pp. 69–79.
123. Gurung, S.; Ghose, M.K.; Subedi, A. Deep learning approach on network intrusion detection system using NSL-KDD dataset. *Int. J. Comput. Netw. Inf. Secur.* **2019**, *11*, 8–14. [CrossRef]
124. Ding, Y.; Zhai, Y. Intrusion detection system for NSL-KDD dataset using convolutional neural networks. In Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence, Shenzhen, China, 8–10 December 2018; pp. 81–85.
125. Lv, Z.; Chen, D.; Lou, R.; Song, H. Industrial Security Solution for Virtual Reality. *IEEE Internet Things J.* **2021**, *8*, 6273–6281. [CrossRef]
126. Li, J.; Deng, Y.; Sun, W.; Li, W.; Li, R.; Li, Q.; Liu, Z. Resource Orchestration of Cloud-Edge–Based Smart Grid Fault Detection. *ACM Trans. Sensor Netw. (TOSN)* **2022**, *18*, 1–26. [CrossRef]
127. Shi, D.; Guo, Z.; Johansson, K.H.; Shi, L. Causality Countermeasures for Anomaly Detection in Cyber-Physical Systems. *IEEE Trans. Autom. Control* **2018**, *63*, 386–401. [CrossRef]
128. Nguyen, K.K.; Hoang, D.T.; Niyato, D.; Wang, P.; Nguyen, D.; Dutkiewicz, E. Cyberattack detection in mobile cloud computing: A deep learning approach. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
129. Shin, J.; Baek, Y.; Eun, Y.; Son, S.H. Intelligent sensor attack detection and identification for automotive cyber-physical systems. In Proceedings of the 2017 IEEE Symposium Series on Computational Intelligence (SSCI), Honolulu, HI, USA, 27 November–1 December 2017; pp. 1–8.
130. Hodo, E.; Bellekens, X.; Hamilton, A.; Dubouilh, P.L.; Iorkyase, E.; Tachtatzis, C.; Atkinson, R. Threat analysis of IoT networks using artificial neural network intrusion detection system. In Proceedings of the 2016 IEEE International Symposium on Networks, Computers and Communications (ISNCC), Hammamet, Tunisia, 11–13 May 2016; pp. 1–6.
131. Niu, X.; Li, J.; Sun, J.; Tomsovic, K. Dynamic detection of false data injection attack in smart grid using deep learning. In Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–21 February 2019; pp. 1–6.
132. Ravipati, R.D.; Abualkibash, M. Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets-a review paper. *Int. J. Comput. Sci. Inf. Technol. (IJCSIT)* **2019**, *11*. [CrossRef]
133. Choudhary, S.; Kesswani, N. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. *Procedia Comput. Sci.* **2020**, *167*, 1561–1573. [CrossRef]
134. Alrawashdeh, K.; Goldsmith, S. Optimizing Deep Learning Based Intrusion Detection Systems Defense Against White-Box and Backdoor Adversarial Attacks Through a Genetic Algorithm. In Proceedings of the 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), Washington, DC, USA, 13–15 October 2020; pp. 1–8.
135. Kokila, R.; Selvi, S.T.; Govindarajan, K. DDoS detection and analysis in SDN-based environment using support vector machine classifier. In Proceedings of the 2014 IEEE Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, 17–19 December 2014; pp. 205–210.

136. Singh, M. *User-Centered Spam Detection Using Linear and Non-Linear Machine Learning Models*; University of Victoria: Victoria, BC, Canada, 2019.
137. Livadas, C.; Walsh, R.; Lapsley, D.; Strayer, W.T. Usilng machine learning technliques to identify botnet traffic. In Proceedings of the 2006 31st IEEE Conference on Local Computer Networks, Tampa, FL, USA, 14–16 November 2006; pp. 967–974.
138. Blowers, M.; Williams, J. Machine Learning Applied to Cyber Operations. In *Network Science and Cybersecurity*; Springer: New York, NY, USA, 2013; pp. 155–175.
139. Li, Z.; Zhang, A.; Lei, J.; Wang, L. Real-time correlation of network security alerts. In Proceedings of the 2007 IEEE International Conference on e-Business Engineering (ICEBE'07), Hong Kong, China, 24–26 October 2007; pp. 73–80.
140. Ding, Y.; Chen, S.; Xu, J. Application of deep belief networks for opcode based malware detection. In Proceedings of the 2016 IEEE International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 24–29 July 2016; pp. 3901–3908.
141. Sou, K.C.; Sandberg, H.; Johansson, K.H. On the exact solution to a smart grid cyber-security analysis problem. *IEEE Trans. Smart Grid* **2013**, *4*, 856–865. [CrossRef]
142. Abur, A.; Exposito, A.G. *Power System State Estimation: Theory and Implementation*; CRC Press: Boca Raton, FL, USA, 2004.
143. Isozaki, Y.; Yoshizawa, S.; Fujimoto, Y.; Ishii, H.; Ono, I.; Onoda, T.; Hayashi, Y. Detection of cyber attacks against voltage control in distribution power grids with PVs. *IEEE Trans. Smart Grid* **2015**, *7*, 1824–1835. [CrossRef]
144. Qi, J.; Hahn, A.; Lu, X.; Wang, J.; Liu, C.C. Cybersecurity for distributed energy resources and smart inverters. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 28–39. [CrossRef]
145. Sargolzaei, A.; Yen, K.; Abdelghani, M.N. Delayed inputs attack on load frequency control in smart grid. In Proceedings of the IEEE ISGT 2014, Washington, DC, USA, 19–22 February 2014; pp. 1–5.
146. Esfahani, P.M.; Vrakopoulou, M.; Margellos, K.; Lygeros, J.; Andersson, G. Cyber attack in a two-area power system: Impact identification using reachability. In Proceedings of the 2010 IEEE American Control Conference, Baltimore, MD, USA, 30 June–2 July 2010; pp. 962–967.
147. Manson, S.; Anderson, D. Cybersecurity for protection and control systems: An overview of proven design solutions. *IEEE Ind. Appl. Mag.* **2019**, *25*, 14–23. [CrossRef]
148. Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious data attacks on the smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 645–658. [CrossRef]
149. James, J.; Hou, Y.; Li, V.O. Online false data injection attack detection with wavelet transform and deep neural networks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3271–3280.
150. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting false data injection attacks in AC state estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. [CrossRef]
151. Tian, J.; Tan, R.; Guan, X.; Liu, T. Enhanced hidden moving target defense in smart grids. *IEEE Trans. Smart Grid* **2018**, *10*, 2208–2223. [CrossRef]
152. Tan, R.; Nguyen, H.H.; Foo, E.Y.; Dong, X.; Yau, D.K.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Optimal false data injection attack against automatic generation control in power grids. In Proceedings of the 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, 11–14 April 2016; pp. 1–10.
153. Liu, S.; Liu, X.P.; El Saddik, A. Denial-of-Service (dos) attacks on load frequency control in smart grids. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.
154. Singh, S.K.; Khanna, K.; Bose, R.; Panigrahi, B.K.; Joshi, A. Joint-transformation-based detection of false data injection attacks in smart grid. *IEEE Trans. Ind. Inform.* **2017**, *14*, 89–97. [CrossRef]
155. Sadek, S.M.; Omran, W.A.; Hassan, M.A.M.; Talaat, H.E.A. Data Driven Stochastic Energy Management for Isolated Microgrids Based on Generative Adversarial Networks Considering Reactive Power Capabilities of Distributed Energy Resources and Reactive Power Costs. *IEEE Access* **2021**, *9*, 5397–5411. [CrossRef]
156. Tang, Z.; Lin, Y.; Vosoogh, M.; Parsa, N.; Baziar, A.; Khan, B. Securing Microgrid Optimal Energy Management Using Deep Generative Model. *IEEE Access* **2021**, *9*, 63377–63387. [CrossRef]
157. Zor, K.; Timur, O.; Teke, A. A state-of-the-art review of artificial intelligence techniques for short-term electric load forecasting. In Proceedings of the 2017 6th International Youth Conference on Energy (IYCE), Budapest, Hungary, 21–24 June 2017; pp. 1–7. [CrossRef]
158. Baliyan, A.; Gaurav, K.; Mishra, S.K. A Review of Short Term Load Forecasting using Artificial Neural Network Models. *Procedia Comput. Sci.* **2015**, *48*, 121–125. [CrossRef]
159. Abdelgayed, T.S.; Morsi, W.G.; Sidhu, T.S. A New Approach for Fault Classification in Microgrids Using Optimal Wavelet Functions Matching Pursuit. *IEEE Trans. Smart Grid* **2018**, *9*, 4838–4846. [CrossRef]
160. Macedo, M.N.; Galo, J.J.; De Almeida, L.A.L.; Lima, A.D.C. Demand side management using artificial neural networks in a smart grid environment. *Renew. Sustain. Energy Rev.* **2015**, *41*, 128–133. [CrossRef]
161. Espina, E.; Llanos, J.; Burgos-Mellado, C.; Cárdenas-Dobson, R.; Martínez-Gómez, M.; Sáez, D. Distributed Control Strategies for Microgrids: An Overview. *IEEE Access* **2020**, *8*, 193412–193448. [CrossRef]
162. Tan, S.; Wu, Y.; Xie, P.; Guerrero, J.M. New challenges in the design of microgrid systems: Communication. *IEEE Electrif. Mag.* **2020**, *8*, 98–106. [CrossRef]
163. Duan, Y.; Zhao, Y.; Hu, J. An initialization-free distributed algorithm for dynamic economic dispatch problems in microgrid: Modeling, optimization and analysis. *Sustain. Energy Grids Netw.* **2023**, *34*, 101004. [CrossRef]

164. Ma, J.; Hu, J. Safe consensus control of cooperative-competitive multi-agent systems via differential privacy. *Kybernetika* **2022**, *58*, 426–439. [CrossRef]
165. Habibi, M.R.; Baghaee, H.R.; Blaabjerg, F.; Dragičević, T. Secure mpc/ann-based false data injection cyber-attack detection and mitigation in dc microgrids. *IEEE Syst. J.* **2021**, *16*, 1487–1498. [CrossRef]
166. Habibi, M.R.; Sahoo, S.; Rivera, S.; Dragičević, T.; Blaabjerg, F. Decentralized coordinated cyberattack detection and mitigation strategy in DC microgrids based on artificial neural networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 4629–4638. [CrossRef]
167. Habibi, M.R.; Baghaee, H.R.; Blaabjerg, F.; Dragičević, T. Secure control of DC microgrids for instant detection and mitigation of cyber-attacks based on artificial intelligence. *IEEE Syst. J.* **2021**, *16*, 2580–2591. [CrossRef]
168. Habibi, M.R.; Baghaee, H.R.; Dragičević, T.; Blaabjerg, F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *9*, 5294–5310. [CrossRef]
169. Amin, M.; El-Sousy, F.F.; Aziz, G.A.A.; Gaber, K.; Mohammed, O.A. CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review. *IEEE Access* **2021**, *9*, 38571–38601. [CrossRef]
170. Cazorla, L.; Alcaraz, C.; Lopez, J. Cyber stealth attacks in critical information infrastructures. *IEEE Syst. J.* **2016**, *12*, 1778–1792. [CrossRef]
171. Mikhaylenko, D.; Zhang, P. Stealthy local covert attacks on cyber-physical systems. *IEEE Trans. Autom. Control* **2021**, *67*, 6778–6785. [CrossRef]
172. Sun, K.; Esnaola, I.; Perlaza, S.M.; Poor, H.V. Stealth attacks on the smart grid. *IEEE Trans. Smart Grid* **2019**, *11*, 1276–1285. [CrossRef]
173. Annavaram, D.; Sahoo, S.; Mishra, S. Stealth Attacks in Microgrids: Modeling Principles and Detection. In Proceedings of the 2021 9th IEEE International Conference on Power Systems (ICPS), Kharagpur, India, 16–18 December 2021; pp. 1–6.
174. Pasetti, M.; Ferrari, P.; Bellagente, P.; Sisinni, E.; de Sá, A.O.; do Prado, C.B.; David, R.P.; Machado, R.C.S. Artificial neural network-based stealth attack on battery energy storage systems. *IEEE Trans. Smart Grid* **2021**, *12*, 5310–5321. [CrossRef]