applied sciences

Review

Technological Perspective of Cyber Secure Smart Inverters Used in Power Distribution System: State of the Art Review

Sumukh Surya [1,*], Mohan Krishna Srinivasan [2] and Sheldon Williamson [3,*]

[1] e-PowerTrain, Software Engineer, KPIT, Bangalore 560103, India
[2] Department of Electrical and Electronics Engineering, Alliance College of Engineering and Design, Alliance University, Bangalore 562106, India; smk87.genx@gmail.com
[3] Department of Electrical, Computer and Software Engineering, Faculty of Engineering and Applied Science, Ontario Tech. University, Oshawa, ON L1H 7K4, Canada
[*] Correspondence: sumukhsurya@gmail.com (S.S.); sheldon.williamson@uoit.ca (S.W.)

Abstract: The purpose of smart grid architecture as compared to the conventional grid is to ensure more stability, reliability and bi-directional communication between the utility and the consumer. The deployment of the same has succeeded in improving the efficiency of the distribution systems and effective co-ordination and interoperability among the different components of the grid. Smart inverters play a major role in seamless grid integration, control and conversion of power when the renewable energy sources are present. However, they come with several security challenges as well, which are of considerable concern. Certain cyber threats include physical and cyber attacks, natural phenomena which in turn can lead to grid failure, blackouts, commercial energy losses, privacy and safety issues, etc. Therefore, there is a need for critical examination of all these issues which must be considered for designing cyber secure smart inverters at the distribution level. In this comprehensive review, keeping the technological perspective in mind, the existing gaps and the necessity for the same are highlighted. The various topologies, IEEE protocols and the control strategy are presented in detail. This will enable prospective researchers to address the design issues of smart inverters with greater focus on security and reliability aspects.

Keywords: smart inverters; cyber security; distribution systems; grid integration; reliability

check for updates

Citation: Surya, S.; Srinivasan, M.K.; Williamson, S. Technological Perspective of Cyber Secure Smart Inverters Used in Power Distribution System: State of the Art Review. *Appl. Sci.* **2021**, *11*, 8780. https://doi.org/10.3390/app11188780

Academic Editor: Reinaldo Tonkoski

Received: 28 June 2021
Accepted: 17 September 2021
Published: 21 September 2021

1. Introduction

Smart grids are a revolutionary step toward a reliable, efficient and secure means of power transfer and delivery to the consumers. Technology evolution of smart grid has tried to amalgamate the information technology (IT) domain with the conventional grid structure. Smart grid architecture relies heavily on digital information and controls and also incorporates dynamic optimization of grid operations and resources. It also encourages the use of distributed resources and generation which includes renewable. The purpose of making the grid smart is to enforce greater responsibility toward energy use, energy consumption and efficiency. Keeping consistent with the concept, smart technologies (for the purpose of grid optimization, metering, communications as well as distributed automation) and smart appliances are integrated in the grid architecture. There is also considerable research on employing peak-shaving and energy storage technologies such as the plug-in hybrid and electric vehicles, thermal storage etc. Microgrids are an important subset of smart grids. While the former is confined to a smaller scale and operates independent of the larger utility grid, the latter operates at a larger utility level. Generally, microgrids are community based whereas smart grids are designed for the entire power system (from the generation to distribution stages). The block diagram representation of a smart grid is shown in Figure 1. The microgrid usually comprises multiple distributed generators (DGs) such as solar and wind along with linear and non-linear loads.

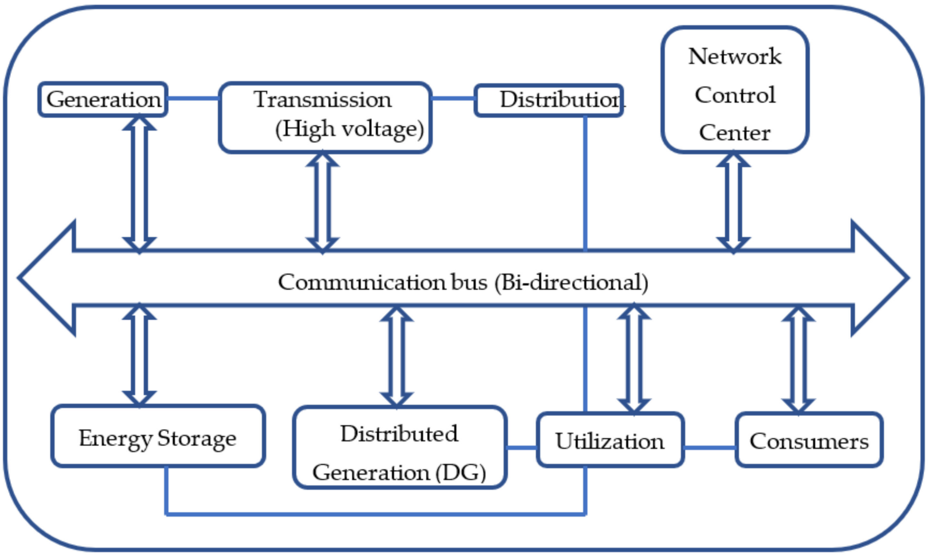

Generation
Transmission (High voltage)
Distribution
Network Control Center
Communication bus (Bi-directional)
Energy Storage
Distributed Generation (DG)
Utilization
Consumers

Figure 1. Schematic of a Smart Grid.

1.1. Literature Survey

The most significant area of concern in a microgrid is the power converters' control, Arbab-Zavar, Babak, et al. [1]. The converters act as links between the DGs and the microgrid bus. To enable an efficient level of power control, conversion and regulation, there is a necessity to equip the converters with "smart" features. The multi-functional aspect of smart inverters is provided in Figure 2.

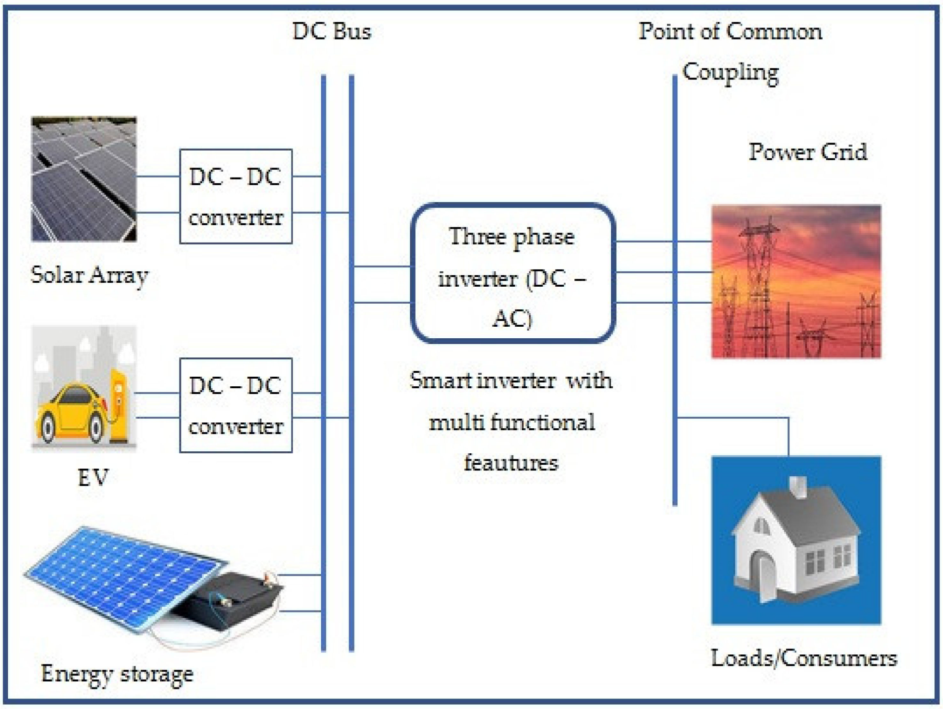


Figure 2. Smart inverter with multi-functional features.

These features are handled comprehensively in Arbab-Zavar, B. et al. [1]. The communication aspects are also discussed to incorporate several control schemes. The significant roles played by communication, networking and middleware technologies in the smart grid and the challenges faced in this particular field are critically examined. The feasibility of choosing a particular communication technology for grid applications are studied in

Ancillotti, E. et al. and Kuzlu, M. et al. [2,3]. The block chain technology-based co-operative control approach is applied for solar inverters in a photovoltaic system in Hadi, A.A. et al. [4]. Furthermore, feasibility studies of a co-simulation method for the block chain network and smart inverter are also conducted. The compatibility of employing power line communication (PLC) technologies for smart grid applications is investigated in Yigit, M. et al. [5]. A review of protocols and standards prescribed for PLC is performed for finding solutions to the problem of standardization. From the Internet of things (IoT) perspective, the effectiveness of long range communications is analyzed, which can be applied to a smart city scenario as shown in Centenaro, M. et al. [6], and the essence of wireless sensor networks for communications in a smart grid is also explored in Townsend, C. et al. [7]. Extending this concept further, several works by Angrisani, L. et al. and Thielemans S. et al. [8,9] have also reported the use of low-power wide-area networks (LPWANS) such as LoRa, which also combines the effects of the existing communication protocols to increase the diversity and reach of wireless sensor networks. The performance assessment of the same subjected to critical noise environment is also conducted. It is inferred that LPWAN extends battery life, decreases the cost and provides enhanced link budgets as compared to the conventional formats. There is also considerable research space linked to the cyber security aspects of smart grids. The vulnerabilities of the smart grid are highlighted in Nejabatkhah, F. et al. and Leszczyna, R. et al. [10,11] along with the economical and physical effects the cyber attacks may have on, particularly the power electronics intensive smart grid. Several standards shown in Barbara, L. et al. [12] have evolved over time for cyber security assessment of the smart grid. A method visualizing the National Institute of Standards and Technology Interagency Report (NISITR) 7628, which provides guidelines for cyber security of a smartgrid, is presented in Harvey, M. et al. [13]. It helps the stakeholders to produce effective smart grid-associated characteristics, risks, and vulnerabilities. In addition, the code of practice for security controls and enhancement of the same for cyber attacks on microgrid control are discussed in Schweizerische, S.N.V. etal. [14]. Stability of the smart grid is also discussed extensively in Chlela, M. et al. [15] by means of false data injection (FDI) in power systems based on state estimation. A comprehensive survey reveals the attacks, impacts and defenses against FDI. Control systems for distributed energy sources are designed to be resilient against cyber attacks in Deng, Ruilong, et al. and Liu, Xindong, et al. [16,17]. The impacts of such attacks are demonstrated, and a state observer is designed for the purpose of detection and estimation of such attacks. A risk analysis on the microgrids is also performed by considering the impact of such attacks. The challenges in the enhancement of the cyber security of the smart grid are effectively handled in Gholami, S. et al. [18]. It is important, as it is a key measure of the resilience of the smart grid. Three key parameters are adopted namely: accuracies, computational time, and robustness. However, an all-inclusive solution that suits all the requirements of the power system is yet to be established. To handle FDI attacks, an artificial intelligence-based detection method was proposed in Mohammadi, F. et.al. [19] to determine meters that have been compromised. The measurements are accurate when subjected to cyber attacks, and the faulty meters are identified. Photovoltaic (PV) farms are also vulnerable to such cyber threats. A framework is proposed in Khanna, K. et al. [20] to detect data integrity attacks for PV farms. Many such schemes have been proposed based on machine learning and computational intelligence in Zhang, J. et al. and Acosta, M.R.C. et al. and Acosta, and M.R.C. et al. [21–23] for detection of cyber threats in a smart grid. In all these works, state estimation of the power system is also assessed simultaneously without compromising on convergence speed. Decision-making approaches as well as game theory have also been employed for analysis, detection and prevention of cyber threats in Li, B. et al. and Hao, Y. et al. [24,25]. Intrusion-detection frameworks by means of state observer schemes and proactive intrusion-detection schemes have been incorporated for analytics and detection for smart inverters in Pilz, M. et al. and Zhang, Z. et al. [26,27]. Predictive control schemes for detection and mitigation of FDI on the inverter was discussed in Fard, A.Y. et al. [28]. The authors employed the k-nearest neighbors (KNN) algorithm for mitigating FDI attacks.

It was subjected to various types of attack signals. Results portrayed robust performance. In order to facilitate real-time monitoring and control of the electric grid, synchrophasor technologies were employed in Rao, R. et al. [29]. Phasor measurement units (PMUs) are used, owing to their enhanced situation-awareness capabilities. The amalgamation of block chain technologies in Hadi, Abdullah A. et al. and Makhdoom, I. et al. and Makhdoom, I. et al. [30–32] with IoT in Ghasempour, A. et al. [33] for co-ordination and control is investigated. Several challenges exist in the adoption of block chain in IoT; several include co-simulation and secondary control. The primary concerns of the existing literature on cyber secure smart inverters are highlighted below:

- Cyber threats pose a major hurdle to the operation and maintenance of smart grid;
- Sensors that form the most important interface in the cyber-physical systems in the smart grid are most susceptible to false data injection that can once again compromise the smart grid;
- Co-ordination and control of different components of a smart grid (particularly smart inverters) along with detection, analysis and mitigation of the cyber threats continue to occupy primary research space;
- Newer technologies such as block chain and IoT are increasingly being adopted for greater grid resilience and more reliable performance.

Our work is an attempt to provide a comprehensive overview of the existing and upcoming technological advancements in cyber secure smart inverters at the distribution level. The design aspects, topologies and control strategies of the same, along with communication aspects and standard cyber security protocols are addressed. The different techniques of cyber attack detection and identification are also provided for the benefit of the readers. The emergence of block chain, Synchrophasor and IoT technologies is also detailed in the work.

1.2. Article Structure

The work is organized as follows: Section 1 gives the background and motivation with respect to cyber secure smart inverters and its importance in smart grid. Section 2 details the different topological configuration of smart inverters with respect to wired and wireless communication. Section 3 addresses the standard cyber security protocols, and Section 4 emphasizes extensively on cyber attacks—classification, detection and identification. Section 5 outlines the role new technologies such as block chain and IoT play in the cyber secure smart grid system along with a general control strategy followed by conclusion and references.

2. Topologies in Smart Inverters

An inverter is considered smart if it can operate with high efficiency and requires little or no human intervention. Although the function of the inverter is to convert DC power to AC power, it should also sense the necessary faults, ensure power flow control and disconnect when faults occur. Concisely, a smart inverter should collect data from the microgrid and configure itself to work in a secure and effective environment. The features of a smart inverter are shown in Figure 3.

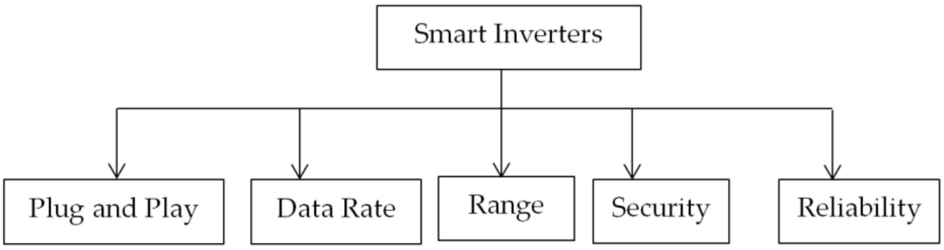


Figure 3. Features of a smart inverter.

2.1. Topologies under Wired Communication

The wired communication is vulnerable to electromagnetic interference and offers lesser operational dependency with batteries. The cost of implementation is high, and the signal quality declines over **PowerLine Communication (PLC)**. The main advantages include easy implementation for long distances and wide coverage. PLC can be classified as (a) narrow band (NB) PLC's and broadband (BB) frequencies. NB and BB PLCs operate at 500 kHz and 30 MHz, respectively. NB PLCs provide low-data rates but offer higher range. BB PLCs provide high-data rate but for a shorter duration with lower reliability. Hence, NB PLCs are preferred for smart grids or smart inverters and domestic applications. Comparative analyses between different wired technologies are shown in Table 1.

Table 1. Comparison between different wired topologies.

Type		Speed	Distance	Demerits
PLC	NB	100–500 kpbs	150 km	High bit rate not possible
	BB	10–200 Mbps	1.5 km	Issues with EMI
Fiber Optics	PON	100 Mbps–2.5 Gbps	10–60 km	Large investment cost
	AON	100 Mbps	10 km	Issues with update
DSL	HDSL	2 Mbps	3.6 km	Data Quality degradation
	ADSL	1.3–8 Mbps	5 km	
	VDSL	16–85 Mbps	1200 m	

2.1.1. Plug and Play

A standard protocol is required to be compatible with the microgrid. However, most of the modern microgrids do not have a standard protocol (droop based). Hence, for a smart inverter, a protocol valid for large distance is required. Major requirements for a microgrid or a smart inverter are illustrated below.

2.1.2. Data Rate

Data rate indicates the speed at which data is transmitted and plays an important role in terms of taking quick actions. Data rate is more than 10 Mbps for a wide area network (WAN) and can be less than 10 Mbps for home or industrial application.

2.1.3. Range

Several energy storage devices, power converters, and finally, the loads are present in a microgrid. Distance can range from several km to several tens of km depending on the size of the microgrid. Inverters are interfaced to the microgrid. Hence, communication protocol may not be possible.

2.1.4. Security

The system would be vulnerable to cyber and physical attacks if the security is poor. Hence, smart blockchain protocols such as Bitcoin are being used for security purpose. However, blockchain protocols cannot solve all physical and cyber security vulnerabilities. Limitations include high computation complexity and low probability of successful generation of the proof of work. It also creates a limitation on creation of new blocks to the blockchain network to roughly one at every 10 min.

2.1.5. Latency

Depending on the response time of each device, latency is set. This allowance is less than ten milliseconds for inverter control signals.

2.2. Topologies under Wireless Communication

Most common wireless systems are M2M, H2M communication, and Long Term Evolution (LTE) communication. However, the devices that can support these features are small. In addition, M2M communication is sensitive to delays. Extremely short range communication cannot be used for inverters as the range of the microgrid may vary from several km to tens of km. Hence, NFC (near field communication) cannot be used. Short-range active radio frequency systems can be used for shorter distance. Low-power wide area networks (LPWANs) are made suitable to smart inverter application. LoRa is popular due to its low operating cost and larger range.

ZigBee and LPWAN are well suited for M2M communication. Mesh topology is used in ZigBee systems, which provides advantages over fault tolerance. However, the routing process is complex and provides lower efficiency. Due to the multi-hop mesh structure, the data rate may decrease once the signal reaches the final destination.

Meanwhile, a network with star topology can be observed with central nodes connected to the internet in LPWANs and SIGFOX. Complexity as seen in ZigBee topology is reduced in LPWANs. At each node, power consumed is lower than that of ZigBee. The main disadvantage with LPWAN is low reliability. If the main or the principal node fails to operate, to keep the network active, other nodes cannot compensate. Figure 4a,b shows the schematic of ZigBee and LoRa. Figure 5 shows the comparison of different wireless topologies as a function of range and data rate.

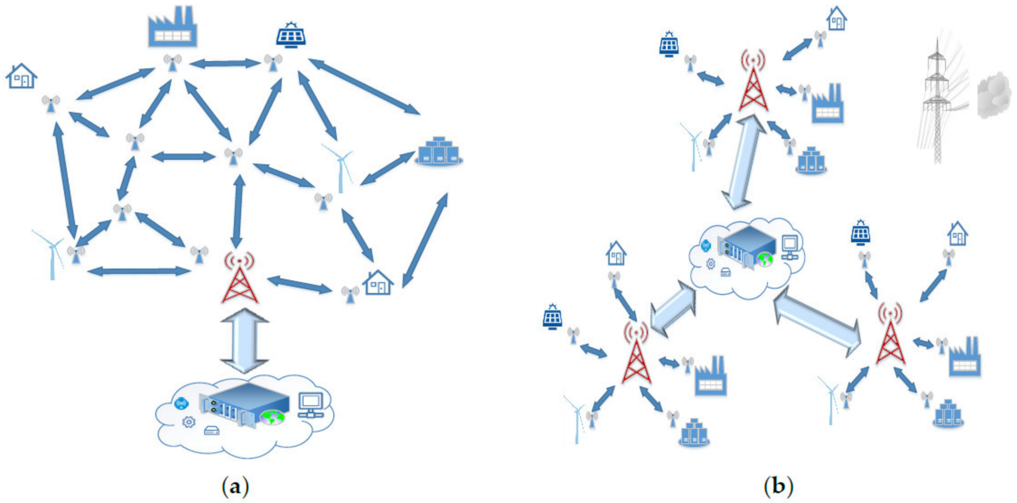


Figure 4. (**a**,**b**) shows the schematic of ZigBee (Mesh) and of LoRa (Star).

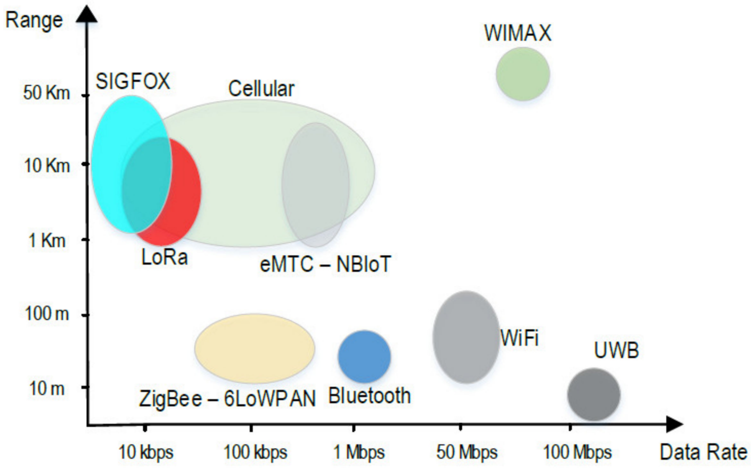


Figure 5. Comparison of different wireless topologies as a function of distance and speed.

A comparative analysis is shown in Table 2.

Table 2. Comparison between different wireless technologies.

Type		Speed	Distance	Demerits
Cellular Network	GSM	14.4 kbps	1–10 km	Poor speed
	GPRS	170 kbps	1–10 km	Poor speed
	3G	2 Mbps	1–10 km	Expensive
	WIMAX	75 Mbps	50 km	Limited stock
Short Range	ZigBee	250 kbps	50 m	Small distance and poor speed
	6LoWPAN	250 kbps	10–100 m	Small distance and poor speed
	Bluetooth	1–2 Mbps	15–30 m	Small distance
	Wi-Fi	54 Mb/s	100 m	Small distance
	UWB	110 Mb/s	10 km	Small distance
LPWAN	LoRa	0.3–37.5 kpbs	3–5 km	Low data range
	SIGFOX	0.1 kbps	3–10 km	Low data range
	eMTC	< 1 Mbps	5 km	Licensed network

3. Standard Cyber Security Protocols

Figure 6 shows a typical smart microgrid with cyber secure systems in which power electronic converters are used in Nejabatkhah, Farzam, et al. [10]. The cyber secure model consists of four important layers discussed below.

The physical power system layer consists of power electronic converters, transformers, etc. To implement the control decisions, sensor and actuator layers are used. The devices are used to measure voltage, frequency and to check the circuit breaker status. For enabling communication between different layers, communication layer is used.

As stated earlier, the communication can be either wired or wireless. The management layer is the central control layer and maintains the microgrid under varied conditions. This layer gathers the data from the measurement layer and generates control signals to the microgrid. These control signals are sent to the actuators for performing necessary actions.

To control the physical system, cyber security collects, transmits and processes the data. The flow of data should be based on certain secure protocols that are reliable and efficient. Certain cyber secure protocols are described below.

3.1. AMI System Security Requirements (AMI-SEC)

To develop a strong rule for the initial AMI (Advanced Metering Infrastructure) in a smart grid, UCA International Users Group (UCAIug) was implemented. This protocol can be used for a home area network, meter management and forecasting system.

3.2. NERC CIP

This was established for setting up safe operation of bulk electric systems in North America. This protocol involves nine standards and forty-five requirements. This protocol provides emphasis on identification of critical cyber asset, controls and security management systems.

3.3. GB/T 22239

This is setup for information security technology in China. For the information system, it contains five security protection abilities to protect from hackers and reinstate to the previous state.

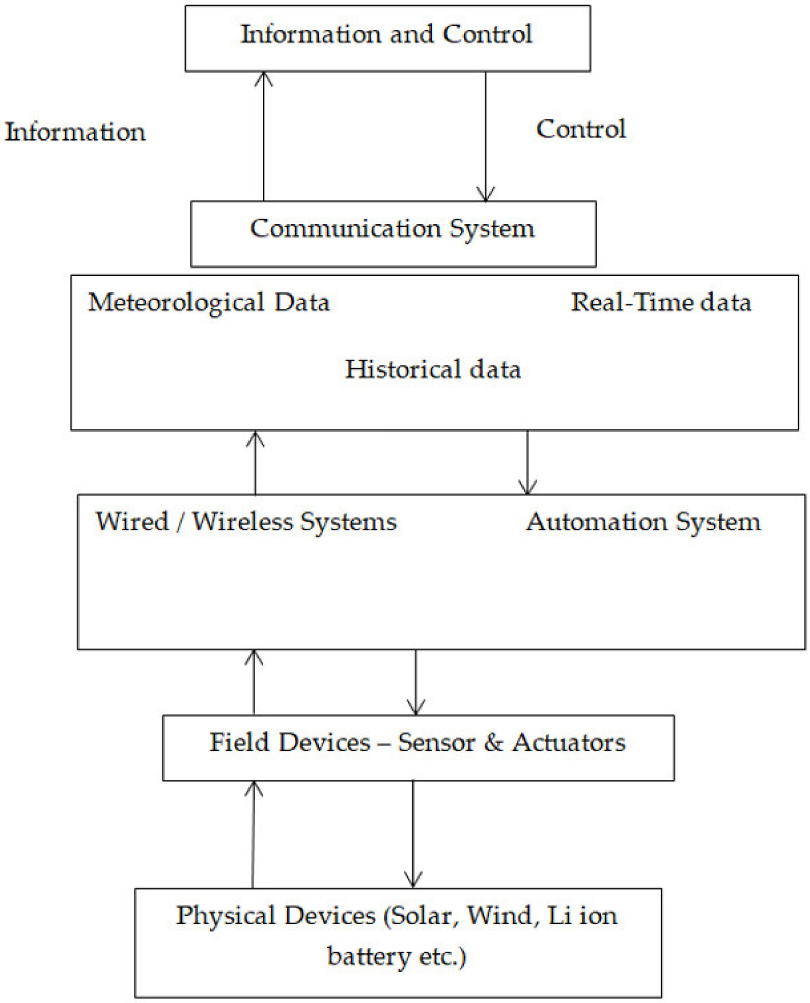


Figure 6. Typical smart microgrid with cyber secure systems.

3.4. NISTIR 7628

This was proposed by the National Institute of Standards and Technology Interagency Report (NISITR). The guideline consists of more than six hundred pages with three volumes. This information helps many organizations in terms of information support (vehicle charging stations).

3.5. ISO/IEC 27001 and 27002

In regard to security testing, compliance with security policies this protocol is used to ensure that the execution of hardware and software controls is precise. To all smart grid components, this protocol can be used.

3.6. NIST SP 800-82

In regard to security of the industrial control system that is used world-wide, this protocol is used. The validation and certification of security controls if implemented in the right manner are maintained. Vulnerability and penetration testing standards are provided by this protocol.

4. Classifications in Cyber Attacks

Different types of cyber attacks are: (a) attack on data availability; (b) attack on data integrity; (c) attack on confidential data.

4.1. Attack on Data Availability

During islanded mode and in transients, the behavior of the power electronic converters is important. A secure smart grid should make sure that the data should be available during these periods. The attacks made during these instances are called attack on data availability. Initiation of the attack can be from either one point or multiple points, by sending malicious packets to the host or by exceeding the routers' processing capacity, network bandwidth, or servers.

4.2. Attack on Data Integrity

By manipulating the measurements in the communication network, these attacks are made. This leads to the imbalance in voltage and frequency, and synchronization with the grid does not happen. Hence, under all operating conditions, the data should be accurate and trustworthy. False data injection (FDI) is the best example for attack on data integrity. These are also referred to as stealth attacks. In such attacks, the hackers enter the communication layer and system operators will be unaware of such attacks.

4.3. Attack on Confidential Data

The confidential data should be available only for authorized personals. Although this attack does not cause much effect on the smart grid, hackers access user data (identity and usage of power)

4.4. Types of Cyber Attacks

In smart microgrids the concept of outer supervisory control and inner primary control is followed. The supervisory control manages the overall operation effectively and efficiently and generates the control signals by receiving the information from power electronic converter. These control signals reach the inner control layer and perform necessary actions. The hackers target the steady state and the transient operations of the microgrid.

4.5. Cyber Attacks on State Estimation

Voltage and phase angle measurements and state estimation are used to decide the system operation. The state estimation also helps in an efficient and effective operation. The state estimation plays a major role in monitoring and controlling the smart grid. The estimated states are used for estimating the load flow, stability analysis, load forecasting and location pricing. Any attack by the hackers on the states will cause devastating effects on the performance and operation of the smart grid

State estimation can be classified as AC and DC state estimations. DC state estimations have studied more than AC, as analytical models are simple.

4.6. Cyber Attacks on Protection Schemes

The protection scheme is one of the most important components in a microgrid. This scheme should work during grid-connected and islanded mode of operation. The relay setting is made based on the type of operation and current level. This is based on standards provided by IEC (International Electrotechnical Commission) 61850. Hackers change the setting of the relay, leading to disastrous effects. Hence, a secure, reliable, and fast communication network-enabled protection scheme should be provided.

4.7. Cyber Attacks on Voltage Control

The power electronics interfaced distributed generations and diesel generators govern the voltage in a smart grid. The system voltage and the reactive power-measured control system provide the reference values for generation of power. Hackers attack the reference data and voltage regulation is impacted.

4.8. Detection and Identification Methods

Data driven techniques using artificial intelligence (AI) were pre-owned to predict the cyber attacks on meters. An IEEE 14-bus system was coupled to New York independent system operator load data. A comparison between AI and extreme machine learning was made to identify the cyber attacks on meters. It was observed that both the techniques were able to identify the attack with high precision. In AI-based method, the actual meter readings of estimated load and measurements were compared with that of the affected meter. To the existing model, an extra load estimator was added to effectively check for the tampered meters.

The historical data and log information were used to detect cyber attacks using supervised learning method. The accuracy and detection rates were 93.9% and 93.6%, respectively. The supervised learning method provided the highest accuracy and detection rates compared to the other models such as K-nearest neighbors (KNN) algorithm, Random Forest (RF) method, etc.

To capture deadly cyber attacks, supervisory learning methods were applied. The proposed method was robust, although noisy data was supplied to it. This computation time was less than that of traditional principal component analysis (PCA) and could precisely identify the cyber attacks.

State estimators help in safe and controlled operation of the smart grid. The hackers trap the estimators by bypassing the bad data detection (BDD) algorithms and creating a change in estimation.

An accurate and computational attractive approach for false data injection attacks (FDIA) detection was proposed. For FDIA to be composed as a matrix separation problem, characteristics of the low rank for matrix measurement and the sparsity of the attack matrix were used. To solve the matrix, the algorithms proposed were traditional augmented Lagrange multipliers (ALM), double-noise dual-problem ALM (DNDP-ALM), etc. Among all the algorithms, Go Dec provided the highest computation efficiency and showed good amount of tolerance toward measurement noise. This algorithm was scalable to larger attacks. However, complexity in terms of scalability was observed in ALM, DNDP-ALM and LMaFit.

By characterizing the work of the intruder in a dynamic environment, the likelihood of cyber attack is predicted. This prediction plays a crucial role to assess the vulnerability of the attack to the grid, with minimal knowledge. The model was developed based on an intruder's strategy. Based on the intruder's perspective, solution for the optimal attack policy is derived. Numerical data based on IEEE 14-bus and 30-bus systems were used to validate the algorithm.

Game theory was used to implement attacker–defender model to project the power system. In this approach, the attacker chronologically identifies the critical substations to create maximum damage. However, the intruder identifies the critical substations to protect such that the system damage can be minimized.

An observer-based attack prediction was proposed. The proposed framework is robust against attacks caused to the electromagnetic interference (EMI) on the hall effect sensors used in a power system. Different types of detection of attacks and solutions to such problems are proposed. Concisely, Table 3 shows a comparative analysis on detection of cyber attacks and identification techniques.

Table 3. Comparative analysis on attacks.

Attack	Tools Used
Malicious Meter Identification	AI
Detection and Prevention	Supervised learning Algorithm
Online Detection and Prevention	Reinforcement Learning Based Algorithm
Detection, Prevention and Identification	Game Theory

For monitoring purposes, state estimation, fault location and protection synchrophasor technology is used. To represent the magnitude and phase of the sinusoidal signals, synchrophasors based on electrical measurements are used. Phasor measurement units (PMUs) are used to account for monitoring time and control measures in the electrical grid. The principle of working is based on the equations shown below:

$$x(t) = X_m \cos(\omega t + \varphi) \tag{1}$$

Equation (1) can be represented as

$$X = \frac{X_m}{\sqrt{2}} e^{j\varphi} = \frac{X_m}{\sqrt{2}} (\cos\varphi + j\sin\varphi) = X_r + jX_i \tag{2}$$

where X_m isthe peak value of the waveform and φ is the phase angle depending on the timescale at t = 0.

A functional block diagram of a PMU is shown in Figure 7.

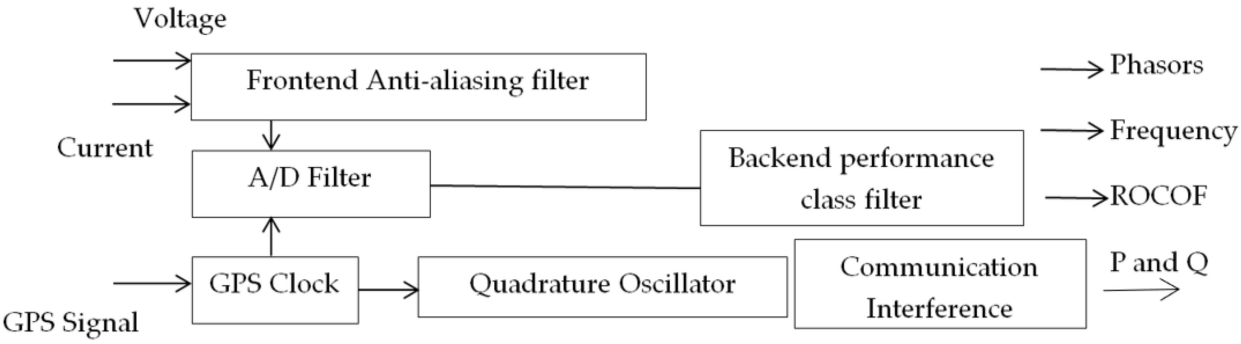


Figure 7. PMU block diagram.

For the three phase AC current or voltage waveforms, PMU (electronic device) provides synchrophasors and frequency measurements. PMU uses hybrid processors to capture signal phase and three phase voltages and currents. The captured signal is passed through the front end anti-aliasing filter and for the elimination of signals of high frequency and digitalized using A/D converter. A synchronized GPS clock provides a fixed sampling rate. The digitized signals and the carrier signal are multiplied to obtain the real and imaginary parts of the phasor. The resultant signal is passed through the backend performance class filter for proving the required accuracy during transient conditions. The final values are used to estimate the voltage, current, phase, frequency and rate of change of frequency (ROCF).

In earlier days, SCADA was used to effectively monitor a power system based on steady-state power flow analysis. However, with the help of ST, dynamic measurements can also be made. Table 4 shows the differences between SCADA and PMU.

Table 4. Differences between SCADA and PMU.

Features	Supervisory Control Aspects	PMU
Least Count	One sample every Two-Four/s	Ten-Sixty samples/s
Observability	Settled Condition	Transient
Measurement	Voltage and Current	Voltage, Current, Frequency and ROCOF
Synchronization	Not considered	Considered
Phase Angle	Not considered	Considered
Focus	Local monitoring and control	Large area monitoring and control

The architecture of ST is shown in Figure 8 and consists of measurement layer, data collection layer and energy management layer. Many critical measurements are used to communicate with the data of PMU and with the rest of the grid.

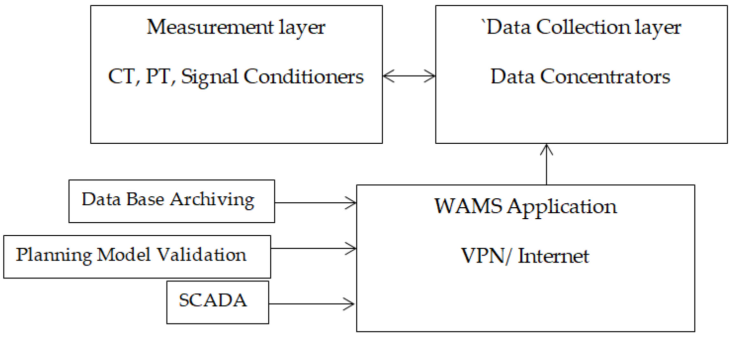


Figure 8. Basic architecture of ST.

The measurement layer consists of PMUs, current and potential transformers and analog units. GPS are installed in PMU in order to record the location of the transformers and store data. The Phasor data concentrators (PDC) receive the data from the PMU. PMU collates all data available from different measurements. Functions of PDC include data monitoring, synchronization, processing, and storage in the data collection layer. During normal operations, the major substation connected through PMU and the data transmission is performed using fiber optics. A locally available PDC collects the data and stores it in a database. It is through this channel that the PDC sends the data to a control room. Major applications of ST in a power system are large area recognition and observation of frequency, voltage stability and identification.

Several IEEE standards of synchrophasors are shown in Table 5.

Table 5. IEEE standards of synchrophasor.

IEEE Standards	Description	Features
C37.118-2005	Replaced IEEE 1344	Basis for current methods and standards
C37.118.1-2011	Synchrophasor measurement	Defines frequency and ROCF measurement under all operating conditions
C37.118.2-2011	Synchrophasor data transfer	Defines message types, data types, format and uses
C37.242-2013	Guide for synchronization	Guidance for synchronization and installation of PMUs
C37.244-2013	PDC Guide	Guide to terminology and operation of phasor data concentrators
C37.247-2013	PDC Standard	Standardize requirements from concepts of C37.244

4.9. Application of Smart Inverter in Photovoltaic Cells

The inverter used in solar applications can be made robust by implementing Internet of things (IoT) and cloud technologies using blockchain technology in them. This feature enables higher security, connectivity and decentralized power control. The main features are: (a) sending data to the main server and health monitoring; (b) decentralized control using shared data; (c) execute PV and inverter operation and record.

5. Blockchain Technology

One decade ago, blockchain technology was introduced as a distributed, protected and a combination of lengthening data structure. This was earlier used in crypto currency. However, this has been used in applications involving critical data. The important feature of this technology is to maintain data from multiple users and maintain it in a secured environment. This data would be made available only for a set of users. This is generally made decentralized such that the data can be shared globally.

In each block, continuous data is organized and the blocks are connected by a cryptographic hash address named "chain". The blocks are connected to each other creating a chain of blocks. Hence, the name blockchain is derived. There are three main types of blockchain platforms based on the accessibility viz, (a) public (b) consortium and (c) private.

In a public blockchain, information can be accessed by anyone without permission. Bitcoin and Ethereum are examples of a public blockchain. In a consortium and private blockchain, information cannot be shared or received without a key or permission. A classic example for such a blockchain is Hyperledger Fabric (HLF).

5.1. Architecture of IoT Enabled PV System

A schematic of the architecture of IoT-enabled PV system is shown in Figure 9. The IoT PV system consists of inverters with IoT technology. This acts as a primary node in the blockchain network. To pass on information to other inverters and battery systems, the IoT device contains SoC (System on Chip) and a pass-on system tied to the cloud server through the internet. The cloud management setup enables power and energy management, optimal control and health monitoring. The transaction and validation data are made available using miners used in the blockchain server.

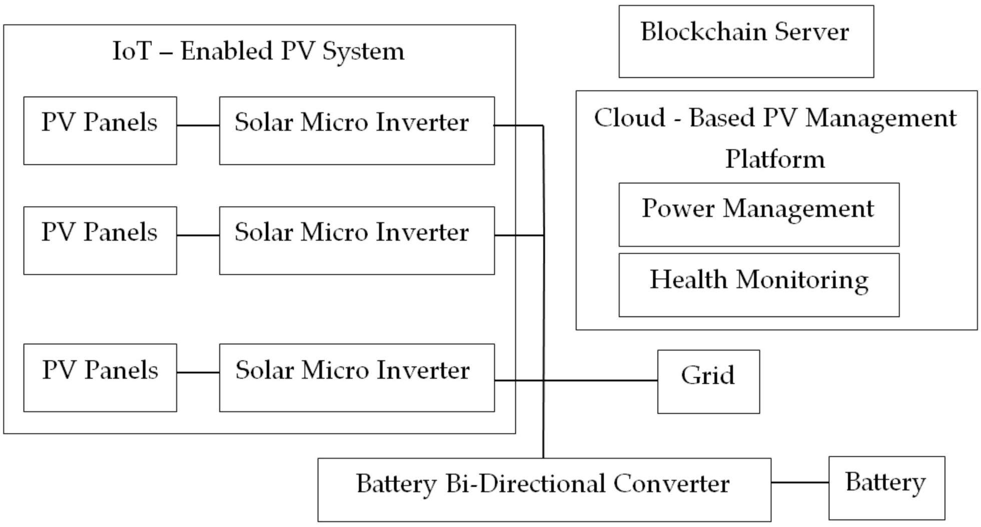


Figure 9. Architecture of IoT-enabled PV system.

5.2. Architecture of Blockchain Implementation in IoT

Figure 10 shows the architecture of blockchain implementation in IoT. The IoT peer-node performs: (a) remote control operation; (b) communication operation between nodes and cloud server; (c) data storage; and (d) smart action. IBM's Hyperledger Fabric was proposed for blockchain technology. This needs smaller energy and computation power and does not require transaction fees/coins.

Certain requirements of an IoT in a smart grid shown are: (a) operate in harsh environmental condition; (b) security; (c) reliability; (d) sensor technology; and (e) energy harvesting.

5.3. Control Strategy

Figure 11 depicts the topology and the control strategy of the IoT-enabled smart inverter by TI for 250 W. A Latte-Panda is used as an IoT device. To the inverter, input is provided by a Flyback DC–DC converter. The low voltage from the PV panel is stepped by the DC–DC converter. The reference current for the DC–DC converter is enabled by an MPPT controller. For the generation of PWM signals to the inverter, a Piccolo TMS302F28035 is used. This also collects data and executes MPPT algorithm.

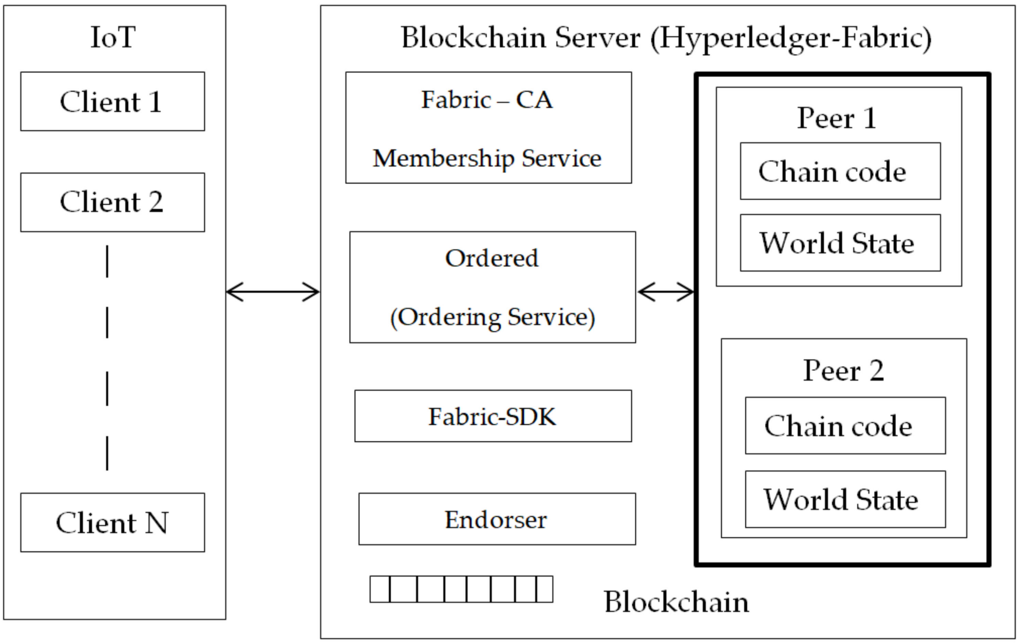


Figure 10. Architecture of blockchain implementation in IoT.

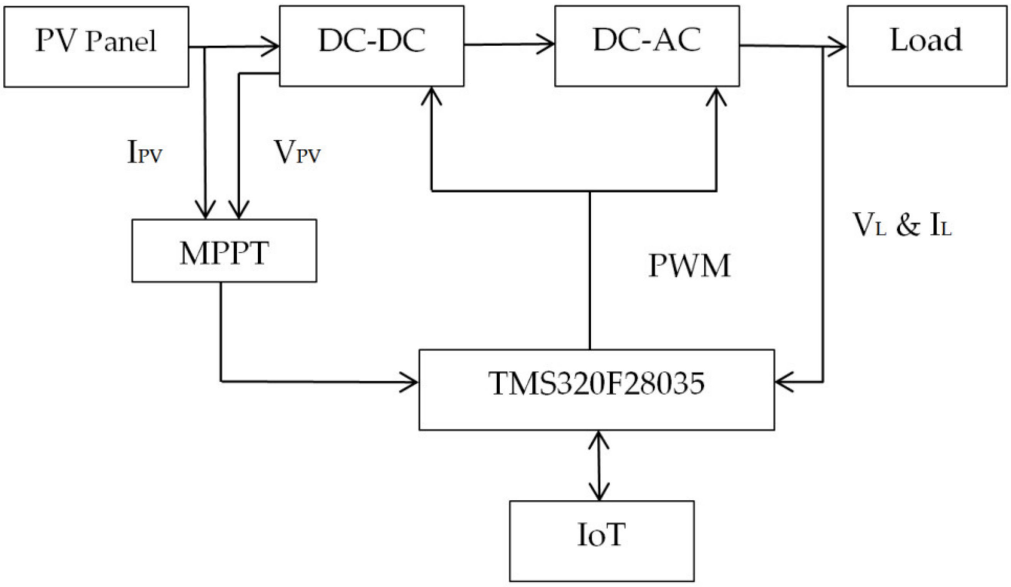
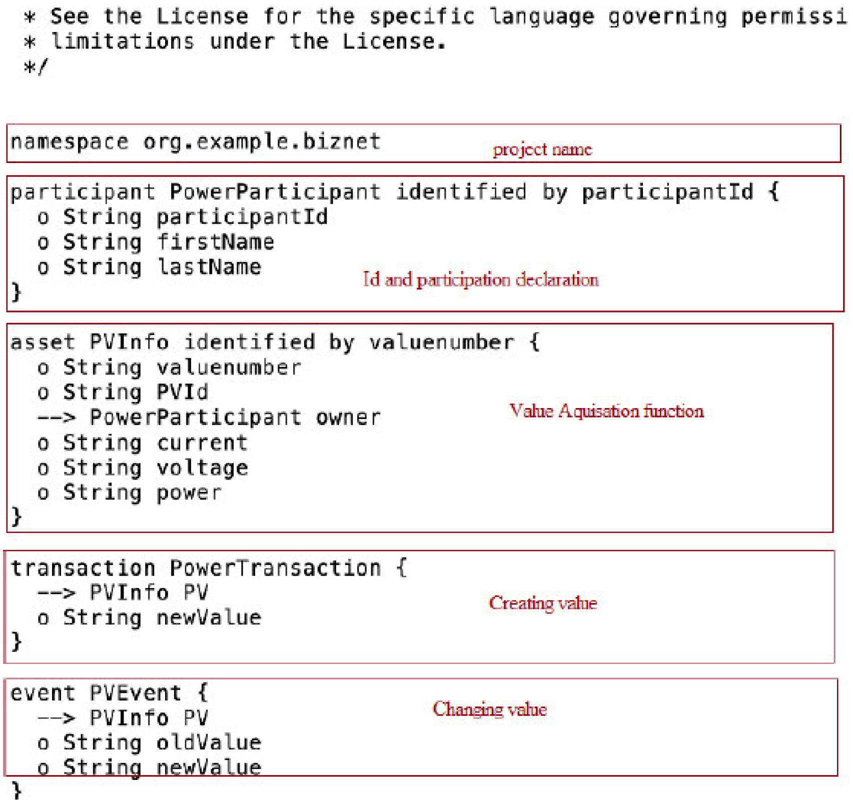


Figure 11. Topology and the control strategy of the IoT-enabled smart inverter.

As shown in Figure 10, to the blockchain network, smart contracts are applied, termed as fabric. It consists of IoT client nodes and a blockchain server. Hyperledger Fabric platform is used to create a blockchain network.The smart contract called "chaincode" in Hyperledger Fabric is executed by the IoT client node. A certificate is sent to the client when enrolled via membership, Fabric–CA. Using Fabric-Sdk-node, the communication with a peer node in the server is enabled. For a block to be created, the following steps were followed. Figure 12 shows a sample code chain.

(a) Using encrypted rest API, smart inverter transfers the data to the server;
(b) To validate the data with the chaincode, it transferred to the endorsement peers;
(c) The data after validation was transferred to a peer who would be ordered and sequences the data into a block.



```
* See the License for the specific language governing permissi
* limitations under the License.
*/

namespace org.example.biznet

participant PowerParticipant identified by participantId {
  o String participantId
  o String firstName
  o String lastName
}

asset PVInfo identified by valuenumber {
  o String valuenumber
  o String PVId
  --> PowerParticipant owner
  o String current
  o String voltage
  o String power
}

transaction PowerTransaction {
  --> PVInfo PV
  o String newValue
}

event PVEvent {
  --> PVInfo PV
  o String oldValue
  o String newValue
}
```

Figure 12. Sample chain code.

6. Cascading Failures, Co-Ordination and Cyber Security Issues in Smart Grids

Since a smart grid is a huge interconnected system, if there is any failure in any part of the grid, it can trigger the failure of other parts as well. This phenomenon, called the cascading failure occurs commonly in computer networks and power systems. The fundamental architecture of a smart grid is different from the conventional grid as many advanced technologies are incorporated into the smart grid. Distributed generation, which forms the crux of the smart grid, transforms it into a decentralized mechanism and at the same time. However, any failure occurring at any part of the grid, can propagate to other regions and give rise to massive scale black-outs and interruptions. This is more dangerous when the number of local generators is increased in the smart grid. Therefore, there is a necessity to equip the smart grids with infrastructure to predict, prevent, and mitigate the effects of cascading failures. This includes condition monitoring and intelligent control of the grid. In addition, the robustness and resilience of the smart grid can be improved by means of risk assessment models where, in the event of a cascading failure, the power network degradation is quantified and utilizing this disintegration state, the optimal dispatch and configuration is determined at every restoration stage.

There are several data driven approaches to risk assessment of cascading failures in smart grids. Several of them depend on historical and simulation-based data (statistical data), which define the features of the cascading effects. The smart power grid is considered as a multi-agent system and complex network. Data driven algorithms are developed for uncertain regions in the multi-agent network. Preventive control methods make use of reinforcement learning and artificial intelligence, which make use of the available data to overcome low accuracy. There are also instances where the time series data samples are utilized from time domain simulations. The data from dynamic behavior of the system and the sensitivity is used to determine the most effective set of generators for improving the power system security.

There are several deterministic and risk-based tools utilized in the power system operation and planning to analyze, mitigate and prevent cascading failures. Several are commercially available and several are available in the development stages. However, the complexity in risk evaluation of cascading failures is high. Any event which has occurred will generate a sequence of reactions that need to be modeled. Since the events may occur individually or as a combination, most of these risk-based tools adopt a probabilistic strategy. Table 6 provides a brief overview of certain popularly used commercial as well as research grade tools used for cascading failure analysis [34].

Table 6. Tools for Cascading failure analysis in smart power grids.

Cascading Tools	Developer	Availability	Description
ACCESS	RTE, France & National Grid, UK	Commercial	A single software environment is provided to the user for precise specification of Varieties of uncertainties, and for their impacts to be investigated.
CAT (Cascade Analysis Tool)	Commonwealth Associates, Inc., USA	Commercial	Contingency based analysis. Several of the most important parameters include thermal overload, low voltage and voltage change
HIDDEN FAILURE	Chen and Thorp	Research grade	Probabilistic analysis for identification of a relay/relay system which incorrectly reacts to disturbances.
Power System Analyzer (PSA)	Los Alamos National Laboratory	Research grade	Isolation and connectivity network analyses are performed. Considering both, base-case and component-failure conditions, the power-flow related effects are computed.

Grid inverters play a significant role in voltage regulation by modulating the real and reactive power components. Interfacing solar photovoltaic system (PV) with the smart grid creates challenges to the operation, owing to its seasonal and intermittent nature. The fluctuations in the voltage will result in grid-voltage violation beyond the operating limits. With the advent of PV smart inverters, which have a fast response to voltage regulation, the inherent problems have been partially addressed. However, there exist issues due to co-ordination as the existing control strategies for smart inverters are based on local information. Several algorithms based on deep learning and artificial intelligence has tried to address this sub-optimal performance and the co-ordination of multiple smart inverters. The reactive power of the smart inverters is effectively utilized for ensuring voltage operation limits. However, there exists several technical restrictions on the volt-var curves for grid-connected solar PV systems employing smart inverters. In certain cases, the set points of the volt–VAR curves are only optimized leading to limitations in performance enhancements. Besides, it is also not easy to change the optimal setting of the volt-var curve every hour. There also exits an option to optimize the volt-VAR curves by considering the PV output and system losses, however, the voltage (which is a significant factor) was not considered.

In a smart grid, there exists a tight coupling between information and communication technologies (ICT) and physical systems, which also comes with considerable concerns of security. The prevalent security strategies are not scalable and inadequate to address the complex nature of a smart grid. The smart grid cyber physical security remains a challenge with many questions raised related to the cyber components being compromised, robust grid topologies to withstand cyber attacks, the relation between information available and the security risk, etc. There are attacks on information accuracy, denial of information access and reconfiguration attacks. Therefore, a dynamic strategy must be explored that considers the modeling of cyber physical interactions of different sub systems in the smart grid. Cyber security must be a part of system design.

7. Future Developments in Network Science, Statistical Inference, Data Science and Deep Learning—Impact on Smart Grids

A smart grid as such has revolutionized the conventional grid structure since it is integrated with various distributed components, which includes advanced metering and communication infrastructure, distributed energy resources, and electric vehicles [35–37]. The objective is to provide more fool-proof features in terms of reliability, better control [38–41], improved energy efficiency and demand side management, as well as more security. Internet of things (IoT) continues to drive the different sub systems of the grid and plays a predominant role at the utility level. Therefore, considerable amounts of data would be processed, stored and analyzed for various subsystems of the smart grid. These energy data can be utilized for condition monitoring of the grid, energy management at the utility side, demand and generation forecasting, fault diagnosis, etc. Network and data science, statistical tools, and artificial intelligence (AI) can be incorporated into the smart grid for performing energy analytics, which will further improvise the performance of the grid and help in decision making. Certain popularly used AI techniques for the purpose of classifying information, demand forecasting, networking, optimizing, and formulating control strategies are the artificial neural network (ANN), reinforcement learning (RL), genetic algorithm (GA), and multi-agent systems. They have been primarily designed for renewable energy sources (RES) integration, energy storage systems (ESS) integration, demand response (DR) management, building and home energy management systems, and security. However, there are inherent challenges as well. Therefore, future developments must look into the limitations of scalability, user requirements and preferences, efficiency of the algorithm, stability, security and privacy issues, algorithm efficiency, user awareness of these intelligent algorithms, etc. The future directions and research developments in the statistical tools, data science and intelligent algorithms and their impacts on smart grids are highlighted in the Table 7.

Table 7. Future developments in smart grids—leveraging data science and statistical tools.

Future Developments	Role Expected—Data Science, AI and Statistical Tools
Self-learning mode	For enhancement of grid intelligence, the self-learning algorithms update the system configuration after the occurrence of each event. These algorithms must be supplemented with availability of data.
Automation of grid	AI approaches can provide better handling and management of distributed resources.
Self-healing mode	Real-time detection of data from sensors and controllers for isolating the faulty circuit from the healthy circuit. Online condition monitoring of the grid.
Cyber security	Adaptive security strategies exploring machine learning, knowledge detection and information theory methods.
Power quality enhancement	AI approaches to reduce power losses in the distribution side.

8. Challenges and Recommendation for Further Research

One of the major challenges with IoT device is its operation in different environmental conditions. Since, the IoT device is exposed to the environment; it should perform well under high/low temperatures, exposure to electromagnetic interference (EMI), etc., In addition, device-supported communication protocols and efficient and energy harvesting techniques should be used. The device should be reliable and secure.

Since the communication layer uses internet for transferring data, the internet connection must be secure as attackers can manipulate the sensor data. The data collected from IoT devices should be accessible only to the license holders, as it contains customers' private information. IoT devices possess limitation in storage and computation power.

Suitable protocols must be setup by such as "trust mechanism" for detecting attacks and stealing of power from the grid.

9. Conclusions

The technological advancements in the smart inverter technology were handled, comprehensively keeping the distribution level end user in mind. Since the smart inverter constitutes the most significant aspect of power conversion, control and regulation and acts as the interface between the utility and consumer, the vulnerabilities of the same when subjected to cyber attacks are highlighted in detail. Communication also forms a vital aspect as it is bi-directional (between the utility and consumer and vice-versa) in a smart grid platform. Therefore, the different standards of communication and rules along with the co-ordination aspects are elucidated in detail. The topological configuration of smart inverters under wired and wireless topologies are also handled, to give a better understanding with respect to the choice and selection of the same, keeping the end-user perspective in mind. Security being the key area of concern, the different types of cyber attacks that are prevalent and can be detected and identified is explained in detail. In addition, the role of the synchrophasor technology in state estimation, monitoring and detection of faults is demonstrated. Considering, the solar PV-based DER as an end-use application, the importance of newer technologies related to IoT and block chain with respect to the cyber security aspects of the smart grid is brought forth. This domain is of continuing importance and concern and still has several challenges to overcome. Keeping this in mind, the existing gaps and future directions are also presented.

Author Contributions: Concptualization, S.S.; methodology, M.K.S.; Formal Analyses, S.S. and M.K.S.; supervision, S.W.; project administration, S.W.; funding acquistion, S.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Arbab-Zavar, B.; Palacios-Garcia, E.J.; Vasquez, J.C.; Guerrero, J.M. Smart inverters for microgrid applications: A review. *Energies* **2019**, *12*, 840. [CrossRef]
2. Ancillotti, E.; Bruno, R.; Conti, M. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Comput. Commun.* **2013**, *36*, 1665–1697. [CrossRef]
3. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **2014**, *67*, 74–88. [CrossRef]
4. Hadi, A.A.; Bere, G.; Ahn, B.; Kim, T. Smart Contract-Defined Secondary Control and Co-Simulation for Smart Solar Inverters using Blockchain Technology. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; IEEE: Piscataway, NJ, USA, 2020.
5. Yigit, M.; Gungor, V.C.; Tuna, G.; Rangoussi, M.; Fadel, E. Power line communication technologies for smart grid applications: A review of advances and challenges. *Comput. Netw.* **2014**, *70*, 366–383. [CrossRef]
6. Centenaro, M.; Vangelista, L.; Zanella, A.; Zorzi, M. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wirel. Commun.* **2016**, *23*, 60–67. [CrossRef]
7. Townsend, C.; Arms, S. Wireless sensor networks: Principles and aplications. In *Sensor Technology Handbook*; Wilson, J.S., Ed.; Elsevier: Amsterdam, The Netherlands, 2005; pp. 575–589.
8. Thielemans, S.; Bezunartea, M.; Steenhaut, K. Establishing transparent IPv6 communication on LoRa based low power wide area networks (LPWANS). In Proceedings of the 2017 Wireless Telecommunications Symposium (WTS), Chicago, IL, USA, 26–28 April 2017; IEEE: Piscataway, NJ, USA, 2017.
9. Angrisani, L.; Arpaia, P.; Bonavolontà, F.; Conti, M.; Liccardo, A. LoRa protocol performance assessment in critical noise conditions. In Proceedings of the 2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI), Modena, Italy, 11–13 September 2017; IEEE: Piscataway, NJ, USA, 2017.
10. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Ahrabi, R.R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. [CrossRef]
11. Leszczyna, R. Standards on cyber security assessment of smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 70–89. [CrossRef]

12. Barbara, L.; Bohua, Y. *GB/T 22239:2008–Information Security Technology–Baseline for Classified Protection of Information System Security Technical Report*; National Standard of the People's Republic of China: Beijing, China, 2008.
13. Harvey, M.; Long, D.; Reinhard, K. Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security. In Proceedings of the 2014 Power and Energy Conference at Illinois (PECI), Champaign, IL, USA, 28 February–1 March 2014; pp. 1–8.
14. ISO/IEC. *ISO/IEC 27002:2013: Information Technology –Security Techniques –Code of Practice for Information Security Controls*; ISO: Geneva, Switzerland, 2013.
15. Chlela, M. Cyber Security Enhancement Against Cyber-Attacks on Microgrid Controllers. Ph.D. Thesis, McGill University, Montréal, QC, Canada, 2017.
16. 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]
17. Liu, X.; Shahidehpour, M.; Cao, Y.; Wu, L.; Wei, W.; Liu, X. Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1330–1339. [CrossRef]
18. Gholami, S.; Saha, S.; Aldeen, M. A cyber-attack resilient control for distributed energy resources. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conf. Europe (ISGT-Europe), Torino, Italy, 26–29 September 2017; pp. 1–6.
19. Mohammadi, F. Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies* **2021**, *14*, 1380. [CrossRef]
20. Khanna, K.; Panigrahi, B.K.; Joshi, A. AI-based approach to identify compromised meters in data integrity attacks on smart grid. *IET Gener. Transm. Distrib.* **2018**, *12*, 1052–1066. [CrossRef]
21. Zhang, J.; Li, Q.; Ye, J.; Guo, L. Cyber-physical security framework for Photovoltaic Farms. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; IEEE: Piscataway, NJ, USA, 2020.
22. Wang, D.; Wang, X.; Zhang, Y.; Jin, L. Detection of power grid disturbances and cyber-attacks based on machine learning. *J. Inf. Secur. Appl.* **2019**, *46*, 42–52. [CrossRef]
23. Acosta, M.R.C.; Ahmed, S.; Garcia, C.E.; Koo, I. Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks. *IEEE Access* **2020**, *8*, 19921–19933. [CrossRef]
24. Li, B.; Ding, T.; Huang, C.; Zhao, J.; Yang, Y.; Chen, Y. Detecting false data injection attacks against power system state estimation with fast go-decomposition approach. *IEEE Trans. Ind. Inform.* **2018**, *15*, 2892–2904. [CrossRef]
25. Hao, Y.; Wang, M.; Chow, J.H. Likelihood analysis of cyber data attacks to power systems with Markov decision processes. *IEEE Trans. Smart Grid* **2016**, *9*, 3191–3202. [CrossRef]
26. Pilz, M.; Naeini, F.B.; Grammont, K.; Smagghe, C.; Davis, M.; Nebel, J.-C.; Al-Fagih, L.; Pfluegel, E. Security attacks on smart grid scheduling and their defences: A game-theoretic approach. *Int. J. Inf. Secur.* **2019**, *19*, 427–443. [CrossRef]
27. Zhang, Z.; Easley, M.; Hosseinzadehtaher, M.; Amariucai, G.; Shadmand, M.B.; Abu-Rub, H. An Observer Based Intrusion Detection Framework for Smart Inverters at the Grid-Edge. In Proceedings of the 2020 IEEE Energy Conversion Congress and Exposition (ECCE), Detroit, MI, USA, 11–15 October 2020; IEEE: Piscataway, NJ, USA, 2020.
28. Fard, A.Y.; Easley, M.; Amariucai, G.T.; Shadmand, M.B.; Abu-Rub, H. Cybersecurity analytics using smart inverters in power distribution system: Proactive intrusion detection and corrective control framework. In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 5–6 November 2019; IEEE: Piscataway, NJ, USA, 2019.
29. Rao, R.; Liu, Z.; Wang, L.; Hou, S.; He, Y. Improved Model Predictive Control for Mitigating False Data Injection on Cascaded H-Bridge Inverters. In Proceedings of the 2019 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Macao, China, 1–4 December 2019; IEEE: Piscataway, NJ, USA, 2019.
30. Usman, M.U.; Faruque, M.O. Applications of synchrophasor technologies in power systems. *J. Mod. Power Syst. Clean Energy* **2019**, *7*, 211–226. [CrossRef]
31. Hadi, A.A.; Sinha, U.; Faika, T.; Kim, T.; Zeng, J.; Ryu, M.H. Internet of Things (IoT)-Enabled Solar Micro Inverter Using Blockchain Technology. In Proceedings of the 2019 IEEE Industry Applications Society Annual Meeting, Baltimore, MD, USA, 29 September–3 October 2019; IEEE: Piscataway, NJ, USA, 2019.
32. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *J. Netw. Comput. Appl.* **2019**, *125*, 251–279. [CrossRef]
33. Ghasempour, A. Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. *Inventions* **2019**, *4*, 22. [CrossRef]
34. Vaiman, M.; Bell, K.; Chen, Y.; Chowdhury, B.; Dobson, I.; Hines, P.; Papic, M.; Miller, S.; Zhang, P. Risk Assessment of Cascading Outages: Methodologies and Challenges. *IEEE Trans. Power Syst.* **2012**, *27*, 631–641. [CrossRef]
35. Krishna S., M.; Daya J.L., F.; Padmanaban, S.; Mihet-Popa, L. Real-Time Analysis of a Modified State Observer for Sensorless Induction Motor Drive Used in Electric Vehicle Applications. *Energies* **2017**, *10*, 1077. [CrossRef]
36. Krishna Srinivasan, M.; Daya John Lionel, F.; Subramaniam, U.; Blaabjerg, F.; Madurai Elavarasan, R.; Shafiullah, G.M.; Khan, I.; Padmanaban, S. Real-Time Processor-in-Loop Investigation of a Modified Non-Linear State Observer Using Sliding Modes for Speed Sensorless Induction Motor Drive in Electric Vehicles. *Energies* **2020**, *13*, 4212. [CrossRef]
37. Daya John Lionel, F.; Dias, J.; Krishna Srinivasan, M.; Parandhaman, B.; Prabhakaran, P. A Novel Non-Isolated Dual-Input DC-DC Boost Converter for Hybrid Electric Vehicle Application. *Int. J. Emerg. Electr. Power Syst.* **2021**, *22*, 191–204.
38. Sreelakshmi, S.; Krishna, M.; Deepa, K. Bidirectional Converter Using Fuzzy for Battery Charging of Electric Vehicle. In Proceedings of the 2019 IEEE Transportation Electrification Conference (ITEC-India), Bengaluru, India, 17–19 December 2019.

39. Prabhakaran, P.; Krishna, S.M.; Febin, D.J.L.; Perumal, T. A Novel PR Controller with Improved Performance for Single-Phase UPS Inverter. In Proceedings of the 2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), Mumbai, India, 15–16 January 2021.
40. John Lionel, F.D.; Jayan, J.; Srinivasan, M.K.; Prabhakaran, P. DC-Link Current Based Position Estimation and Speed Sensorless Control of a BLDC Motor Used for Electric Vehicle Applications. *Int. J. Emerg. Electr. Power Syst.* **2021**, *22*, 269–284.
41. Surya, S.; Singh, D.B. Comparative study of P, PI, PD and PID controllers for operation of a pressure regulating valve in a blow-down wind tunnel. In Proceedings of the 2019 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Manipal, India, 11–12 August 2019.