Chapter 1

Smart Grids Enabled By Edge Computing

Alem Fitwi[1], Zekun Yang[2], Yu Chen[3] and Xuheng Lin [4]

A smart grid is the nervous system of the power generation, transmission, and distribution systems that makes a great deal use of the information and communication technologies (ICT). The ICT enables the smart grid to timely detect, monitor, and react to local changes in usage and in the event of electrical faults of various types. The samrt grid is the nexus of distributed electrical sensors, smart energy meters, smart appliances often deployed in customer premises, transducers, network interfaces, remote terminals, servers, and a multiplexed communication system which transmits data and commands between parts installed across the entire power grid system components. The main power grid components include the power generation station, high voltage transmission system, distribution systems, and customer premises. The sensors that can be interconnected to one another using various network architectures and computing paradigms are the eyes and ears of the smart grid which provide information vital for efficient and timely fault detection, monitoring, and controlling the entire power grid system. Hence, the smart grid is derived from the general-purpose network architecture and computing models in a manner as to fit the purposes of the electrical grid system.

The main thing that distinguishes a smart grid from the general purpose computer network is that it is one specific application of it. The most striking characteristic of computer networks is their generality. They are not optimized for a specific application like the smart grid. They are built principally from general-purpose programmable hardware capable of carrying and supporting many different types of data, and a wide spectrum of ever-growing applications. Just like the general purpose computer network, the smart grid could be deployed in client-server, peer to peer, or distributed architecture. In a similar fashion, the computational paradigm of the smart grid could be cloud, fog, or edge based. But the smart grid is typically the embodiment of the Internet of Things or cyber physical systems; hence, the most suitable computing paradigm is one that brings the computation and data storage closer to the point where data is created and garnered.

[1]Binghamton University, USA
[2]Binghamton University, USA
[3]Binghamton University, USA
[4]Binghamton University,Binghamton, New York, USA

Thus, this chapter looks at the typical ways how the Edge Computing paradigm is applied to improve reliability, the load forecasting capability, security and privacy of the smart grid. To put it another way, this chapter focuses on four things. It, first, lays down the foundations and background knowledge about the power grid, smart grid, and edge computing paradigm. Second, it explains the factors that affect the reliability of the smart grid and explains the ways how the edge computing techniques can improve the reliability of the smart grid. Third, it explores the requirements and ways how power consumption prediction could be accurately performed at the edge using Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) methods coupled with advanced electrical signal processing techniques. Finally, it presents how the security and privacy issues of a smart grid enabled by edge computing could be addressed.

1.1 Introduction To Edge Computing Enabled Smart Grids

Electrical grid is one of the leading and greatest technological inventions of the twentieth century. The genesis of early power systems and electric power grids during the past 130 years was enabled by automation and control of electromechanical machinery and power delivery networks. It has delivered the life blood for the technological innovations and advancements in the computing and communication arenas. The demand, economic, technical, environmental, and political challenges have pressingly called for radical changes on how electricity is generated, transmitted, distributed, controlled, monitored, consumed, and managed ending the times the grid could be taken for granted. As the concepts and techniques energy is generated make continuous advancements, it has become a necessity to employ a modernized grid system capable of meeting the ever-increasing needs of the customers by efficiently addressing the problems associated with power outages and thefts. As a result, today's end-to-end power and energy systems fundamentally depend on embedded and often overlaid systems of sensors, computation, communication, control and optimization. There are even more opportunities and challenges in today's devices and systems, as well as in the emerging modern power systems – ranging from watts, emissions, standards, and more – at nearly every scale of sensing and control. Recent policies combined with potential for technological innovations and business opportunities have attracted a high level of interest in the electric grids [1, 2, 3]. Hence, the apropos employment of an intelligent grid management system called a smart grid [4] is of astronomical importance. Smart Grid is an electricity network that can efficiently integrate the behavior and actions of all generators, consumers and prosumers so as to guarantee economically efficient, sustainable power system with low losses, and high levels of quality and security of supply and safety. The smart grid is introduced in a bit more detailed manner in subsection 1.1.1. Besides, an introduction to edge computing paradigm and how it can help improve the load forecasting capability, reliability, resilience, availability, and intelligence of smart grid is briefly presented in subsection 1.1.2.

1.1.1 The Smart Grid

The potential for a highly distributed system with a high penetration of intermittent sources poses opportunities and challenges. Any complex dynamic infrastructure network typically has many layers, decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, and distributed control is required to enable parts of the networks to remain operational and to even automatically reconfigure in the event of local failures or threats of failures. Here is where the smart grid becomes so handy. That is, it is one of the major areas of applications of the Internet of things (IoT) that plays roles of paramount importance in improving the generation, transmission, distribution, and consumption of electricity in terms of reliability, resilience, availability, and cost [4, 3, 5].

The traditional electric grid has been engulfed with a plethora of problems including outages, lower availability due to elongated fixing times in the event of component failures, unpredictable power disturbances, unattractively fixed prices of electricity, and failures to detect fraudulent consumers. These drawbacks, in one way or another, contribute to the increasing consumption of fossil fuels and subsequent increase in utility costs. Correct estimation of demands and peak load duration plays very pronounced role in the wise utilization of resources while meeting customer demands. The smart grid addresses the inefficiencies and unreliability of the grid. It efficiently delivers electricity from suppliers or utilities to consumers and prosumers using two-way digital communications to control appliances at consumers' homes. This could save energy, reduce costs and increase reliability and transparency if the risks inherent in executing massive information are avoided. It overlays the ordinary electrical grid with an information and net metering system that includes smart meters [4, 3]. Smart grids are being promoted by many governments as a way of addressing energy independence, global warming and emergency resilience issues. The grid usually encompasses myriads of local area networks that use distributed energy resources to several loads to meet specific application requirements for remote power, municipal or district power, premium power, and critical loads protection. It has infinitely many benefits like performing dynamic pricing, enabling real-time exchange of information between providers and consumers through the use of smart meters, and interconnecting green energy sources (like micro-grid, solar panels, and bio-fuels) to the grid that increases the reliability of electricity distribution.

However, the many benefits of the smart grid come along with some costs. As stated in the previous paragraphs, it employs a myriad of computing and communication technologies; as a result, most of the security issues faced in the information technology networks still exist in the smart grid as well. What is more, the smart grid invades the privacy of consumers as it collects massive data via its smart sensors deployed in the customers' building area network (BAN) [6] and suffers from some reliability and availability issues as well. Hence, theses limitations necessitate improvements. That is, the employment of contemporary technologies like artificial intelligence, machine learning, or deep learning coupled with edge computing paradigm can help solve some of the problems faced by the cloud-centric smart grid deployment.

1.1.2 Edge Computing Paradigm

Big Organizations or information technology (IT) services providers make use of hierarchical computing paradigms similar to the one depicted in figure 1.1 depending on data size, computational needs, and applications they run. That is, this architecture of computing infrastructures enable organizations or applications like the Industrial Internet of Things (IIoT) to take advantage of a variety of computing and data storage resources. Cloud computing paradigm frees organizations from the requirement to keep expensive data-center infrastructure on site. It allows data to be collected from multiple *distant* sites and devices. It is accessible from anywhere around the globe. Fog computing and edge computing look similar for they both bring the intelligence and processing power closer to the point of data creation and collection. However, a fog environment places intelligence at the enterprise campus area network (CAN) where data is transmitted from endpoints to a gateway for processing. The edge computing places intelligence and processing power in devices such as embedded automation controllers and smart meters. That is, it allows the processing of data to be performed locally at multiple decision points for the purpose of enabling real-time communication and decision making by reducing network traffic, response time, and risk of security and privacy breaches.

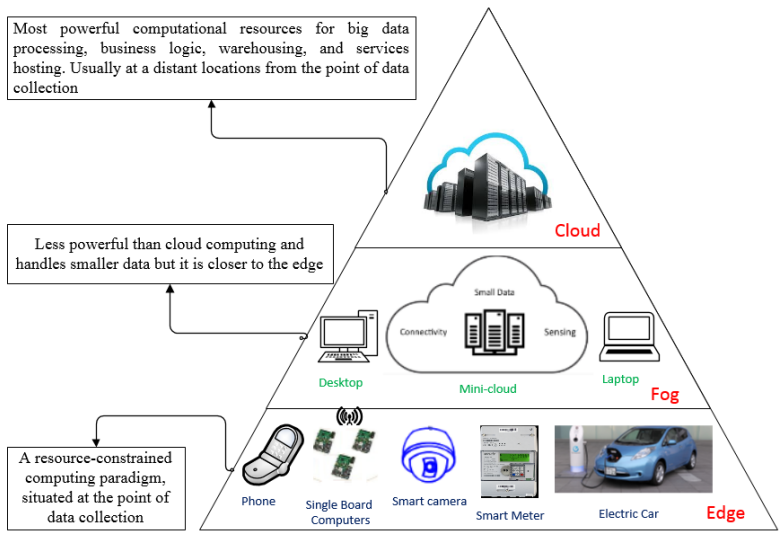

Figure 1.1 Hierarchical Computing Paradigm: Cloud, Fog, and Edge

The cloud-centric smart grids get data processed in distant cloud centers and suffer from network congestion, unpredictable response time, and security and privacy issues. These shortcomings have the potential to undercut the reliability, availability, and resilience of the smart grid [7, 5]. In lieu of sending data from IoT devices to the cloud inefficiently, fog nodes analyse the data on the network relatively closer to the edge avoiding the need to transfer data back to the distant center of the network.

But the edge computing paradigm directly addresses most of these issues by pushing computing power, and intelligence away from centralized clouds to sites closer to consumers, producers and prosumers [8]. In such a way, it drastically reduces the volumes of data transported to cloud centers thereby cutting down on the latency and the transmission costs. As a result, edge computing enabled smart grids outperforms the cloud-centric smart grids.

1.2 Availability and Reliability of Edge-Enabled Smart Grids

The fast and continued advancement in IT networks, and computing paradigms like distributed, cloud, fog and edge computing have drastically revolutionized the way electrical power is generated, transmitted, distributed, controlled and billed. The electrical grid that takes full advantage of these technologies and methods is called a "smart grid" [4, 2]. They play very pronounced roles in making the smart grid more reliable, more available, more efficient, and more secure. However smart grids are capable of breaking down that could cause power blackout due to the fact that they comprise a great deal of components. Hence, analyzing factors and designs that affect the availability and reliability of smart grids is of paramount importance. The availability and reliability are required to be as higher as possible at all stages including the electricity generation stations, electric power transmissions, electricity distributions, and control and monitoring systems. This section presents how availability and reliability of smart grids are affected and how edge computing could help improve these important attributes of the smart grid. The respective details are provided in subsections 1.2.1, 1.2.2, and 1.2.3.

1.2.1 The Availability of Smart Grids

Given a specified observation period which could be in hours, days, weeks, months or years, the availability is the ratio of the uptime (time during which it is in operation) of the smart grid to the observation period as stated in equation (1.1). In other words, it can be defined as the ratio of observation period minus its downtime to the observation period, stated in equation (1.2).

$$Availability(\%) = (\frac{Uptime}{Observation\_Period}) * 100 \tag{1.1}$$

$$Availability(\%) = (\frac{Observation\_Period - Downtime}{Observation\_Period}) * 100 \tag{1.2}$$

In a more realistic way, availability can be expressed using exponential distribution so as to provide a good measure for identifying the prospect that the grid is operational. This is modeled using the time until a component of the smart grid breaks down and the time taken to fix it. Equation (1.3) gives the time until the component of a smart grid breaks which is modeled using exponentially distributed function. Given the failure rate λ, the mean time of failure (MTF) is $1/\lambda$. In a similar fashion, the average downtime or the time required to fix the broken component can

be modeled with parameter μ using the exponential distribution. Hence, the mean time to repair (MTR) is equal to 1/μ.

$$f(t) = \begin{cases} \lambda e^{-\lambda t} & if\ \lambda\ >\ 0\ and\ t\ >\ 0 \\ 0 & else \end{cases} \tag{1.3}$$

The availability of the smart grid is therefore computed in terms of mean uptime (MTF) and mean downtime (MTR) as depicted in equation (1.4). In principle, there is no difference among equations (1.1), (1.2), and (1.4), but equation (1.4) is more realistic for it takes the probabilistic nature of failures into account.

$$Availability(\%) = (\frac{MTF}{MTF\ +\ MTR}) * 100 \tag{1.4}$$

The smart grid often comprises components connected in both series and parallel. Assuming that there are n redundant components that are in parallel in the smart grid, the overall availability can be computed using equation (1.6) which gives a better result than (1.4) when n is at least greater than one. As the degree of redundancy, n, increases, the exponential term decays to zero giving an availability of 100%. Hence, the major takeaway here is that availability is improved when there are more redundant devices and communication links in the smart grid. The total availability of components connected in tandem, given in equation (1.5), is much smaller than the availability of a single device given in equation (1.4) clearly indicating that the probability of failure is much higher. We know that a smart grid comprising a single series connection components is prone to a single point failure that substantially affect the availability of electricity. Simply, all the mathematical models emphasize how much pronounced roles the distributed and edge computing architectures can play in improving the availability of a smart grid [9].

$$\prod_{i=1}^{n} Availability_i \tag{1.5}$$

$$\prod_{i=1}^{n} (1 - (1 - Availability_i)^i) \tag{1.6}$$

For instance, as portrayed in figure 1.1, the computational power and distance from the point of data creation increase as we move up along the pyramid. However, the number of devices (of smaller computational power) and communication links increase as we move downwards. The former affects the redundancy which in turn impacts the availability as stated in equation (1.6). That is, in the event of a failure, it takes relatively increased MTR affecting the MTF. This lowers the availability. On the other hand, the edge computing comprises many devices with some computational power and intelligence installed at least per BAN basis. This approach cuts off the reliance on few distant cloud-centers. That is, the failure of an edge device at one point of data collection doesn't affect others. The downtime is much smaller that keeps the MTF higher which in turn gives higher service availability. Let us consider a BAN connected to three sources of energy making use of the edge devices computational power and intelligence where the observation period is assumed to be a day and the downtime is about 0.0101 day. The availability is computed to be about

99%. But in the absence of edge computing where the connection is one way series, the availability goes down to 97%. The calculations were performed according to equations (1.1) through (1.6).

1.2.2 The Reliability of Smart Grids

One of the noble goals of the electric power industry is creating a reliable and resilient grid operations. The reliability and resilience refers to the ability of the smart grid to recover as quickly as possible in the face of failures that might be caused by both man-made and natural disasters [10, 11]. The natural weather events are liable for the lion share of power outages in the USA and their frequency has been rising for long. But the impact of cyber attacks cannot be underestimated as well [12]. It is worth noting. Hence, it is important to invest in technologies that can empower the smart grid to have the ability to respond to power outages inflicted by natural disasters and to proactively deter potential cyber attacks. The underpinning concept of reliability is that even when stricken or attacked, the grid should be able to reroute power flows quickly and automatically thereby reducing the number of affected customers from downed power lines or from parts of the grid disabled by cyber attacks [13, 10, 11, 12].

Just like the availability, the reliability of electronic components of the smart grid can be modeled using the exponential distribution which is scaled up to compute the overall reliability of the smart grid. Given the hazard rate of a component to be λ and the mean time between failures (MTBF) to $1/\lambda$, the reliability at a specific point in time (t) can computed using equation (1.7).

$$\int_t^{\infty} f(t)dt \; = \; e^{-\lambda t} \tag{1.7}$$

Reliability, another important attribute of smart grids, is the probability of a failure occurring at some component of it or whole part of it as stated in equation (1.7). It refers to the ability of the smart grid to continuously and consistently operate as designed. As equation (1.7) shows, the smart grid components wear out with time. A reliable smart grid is completely free from any technical errors theoretically. In practice, that is not the case; it is expressed as a percentage and it is the capacity of the smart grid to continuously offer the same services amid component failure or partial failures. It should be designed in such a way that a single failure wouldn't bring it down on its knees. A perfectly reliable smart grid relishes 100% availability; however, when failures occur at any part of the grid, the availability might be affected in various ways depending on the nature of the problem and whether the smart grid has redundant design. A centralized smart grid is less reliable and liable to single point failure and the availability could be severely affected whenever a failure takes place. But an edge enabled smart grid, where there are distributed edge devices and fog servers, has a better reliability and availability than the one that relies on fewer cloud servers. That is, reliability of the smart grid affects its availability. But if the smart grid no matter how redundant is severely affected by cyber-attack, its reliability and efficiency are diminished which in turn affects its availability. Details about how

the availability of smart grids is affected by cyber attacks are provided in section 1.4 and subsection 1.4.1.1 methodically and profoundly.

1.2.3 Edge Computing Enabled Solutions For Smart Grids

Grids designed based on a centralized architecture (client-server) and cloud computing paradigms have a number of limitations. Hence, an improvement is needed in the way the smart grid carries out such tasks as measurement, data processing, communication, and controlling. The smart grid has a huge number of devices and sensors capable of continuously creating and garnering massive data. The centralized and cloud computing paradigms, which are often placed in distant locations from the points where data are collected, incur a lot of latency, bandwidth congestion, and privacy problems [5, 8, 13, 7]. That is, the server-client and cloud computing architecture have powerful computational powers at distant locations but the tremendous amount of data produced by the many sensors that constitute the smart-grid have the potential to cause some unpredictability in the response time. They consume a lot of bandwidth [14, 15]. Besides, they are prone to a number of cyber attacks including interruption, eavesdropping, and tampering. These limitations make such computing architectures less reliable and greatly affects the availability of the grid to both consumers and prosumers. Here is where edge computing paradigm becomes so handy. In other words, the smart grid needs to have mini-brains at the edge of its networks on top of its ears and eyes (the sensors) to improve its reliability and availability by reducing latency, by avoiding traffic congestion, by dropping the probability of cyber attacks, and by addressing the privacy concerns of customers and prosumers alike.

The edge computing keeps the computing tasks at the edge of the smart grid, in the BAN, where the smart sensors equipped with edge computing capabilities reside. That is to say, the data processing tasks, the data analytics, and the partial storage of the data generated by the smart sensors are performed within closer proximity of the points where data are generated and collected. The majority of the tasks that used to be processed by clouds or central data-centers after data have been sent by the edge sensors are now being acted upon locally at the edge nodes of the grid's network. As a result, edge computing provides a number of benefits to smart grids. First, it greatly cuts down on the latency by reducing the network traffic. That is, the edge computing performs the data processing and storage closer to where the data are collected that eschews unnecessarily bandwidth congestion, processing queues, and risk of privacy breaches. The reduction in latency creates an auspicious situation for real-time data exchange, monitoring and control. Furthermore, it provides a better platform for addressing the privacy problems by enforcing privacy conserving measures closer to the point of data collection. The central and cloud computing architectures endanger the privacy of customers. Huge amount of data are transported over communication networks, which are prone to several cyber attacks, to distant central locations for processing and storage. These heaps of data could help easily deduce the behavior and patterns of customers [16].

The edge computing has also the potential to bring intelligence closer to the consumers and prosumers that empowers BANs to implement energy management, supply prediction, and demand management methods locally using both supervised

and unsupervised learning methods [17]. It enables data analysis and decisions to be made at the edge of the network, where significant impacts could be made, in lieu of exclusively doing those tasks in the servers sitting in the back office of the utilities that incurs latency on top of being vulnerable interceptions. The machine learning based methods added to the edge can perform many a task including data mining, information processing, regression for supply prediction from green energy sources like solar panels, classification for determining operating and non-operating appliances or for identifying individual power consumption of appliances, clustering for putting data into different groups, conserving privacy, and decision making. Besides, it creates markets for prosumers who both consumes and produces electricity. The edge computing enables customers, who produce excess green energy from solar panels, bio-fuels, and micro-dams, to sell their excessive energies to other customer back through the smart grid [5, 8].

In summary, edge computing aims to deliver compute, storage, intelligence, and bandwidth much closer to the data input points and end costumers of the smart grid. This computing paradigm has a great potential to improve the reliability, resilience, and availability of the smart grid in many ways. Some of the benefits it provides are precisely outlined in what ensues.

- It allows the *bidirectional* flow of energy allowing customers to be both consumers and producers of energy. That is, customers can produce environment friendly energy from solar, bio-fuels, or micro-grids and sell back their excessive production to other consumers in the easy market created by the edge computing enabled smart grid. Increasing the energy generation stations enhances the reliability and availability of the electric power grid. Besides, it promotes the production of clean energy.
- It lowers the *latency*, brought about due to reliance on distant cloud computing, by avoiding the back and forth transportation of massive data collected by the sensors between the edge and cloud computing centers.
- It enables *real-time* processing and communication of refined information, not bulky raw data.
- It provides intelligent energy management, consumption and supply prediction, appliance classification based on their power consumption, and clustering of data based on their sensitivities or other criteria.
- It greatly enhances *reliability and availability*. The world of electrical grid includes some pretty remote rural territories with less optimal environments concerning internet connectivity. Hence, that fact that edge devices can locally store and process ensuing data improves the reliability. That is, temporary disruptions in intermittent connectivity will not impact the operation of the edge device merely due loss connection to the cloud.
- It improves the *quality of power* delivered to consumers. The power quality at customers' premises or places of business can have a tremendous effect on their daily works. Hence, the edge devices installed nearer to the customer premises make sure the power coming in is of the right quality that can meet the settings of the customers' machines and appliances. That is, the edge computing creates an enabling situation for fast and proactive handling of issues that affect the

power quality. The factors that affect the quality of power includes momentary power interruptions, electrical noises, grounding loops, voltage sags and surges, extended power interruptions, harmonic distortion, lightning damage, and high-speed transients.

- It improves the *security and privacy breaches* by enforcing pertinent measures right at the point of data collection. The chance of cyber attacks being realized while massive raw data is being exchanged between sensors and clouds without good security measures in place is higher. And the same is true with the privacy. The edge computing creates an enabling environment for enforcing security and privacy conserving mechanisms at the point of data creation where the details are explained in section 1.4.

1.3 Edge Enabled Power Consumption Forecasting

The smart grid technologies coupled with the edge computing paradigm improve the traditional power grids in many ways. One way, on top of the many ways mentioned in the previous sections, is improving the efficiency of the grid system by performing in-advance prediction of load. In the premises of customers who own households or industrial companies/factories, there are a number of appliances, and machines that have varying power consumption rates at different times of the day. They are connected one another by means of the smart grid. That is, the smart grid has become one of the major components of smart cities by exploiting the fast advancing IT and IoT technologies for reliably interweaving the cities' buildings and factories. It, therefore, needs to be equipped with the capabilities of intelligent scheduling and planning of electricity delivery based on robust and efficient power consumption forecasting and analysis.

Having appropriate methods for accurate power consumption prediction and customer demand management at the edge of an electrical grid is very vital. It creates an enabling environment for carrying out a comprehensive analysis and evaluation of the power consumption of every BAN by continuously monitoring both non-commercial and commercial buildings connected to that network for their respective energy consumptions. The data continuously garnered from the electric meters is used for monitoring and analyzing energy consumption. The result is, then, employed to formulate strategies vital for improving energy efficiency by reducing wastage, answering future demands with no more ado, and performing real-time pricing. Besides, good techniques for power consumption prediction enable utility companies to plan their future well on short, medium, and long term basis with minimized risks thereby increasing their revenues.

These days, the accurate prediction of power consumption is done through the application of computational intelligence techniques like artificial neural networks, machine learning, or deep learning in conjunction with the right choice of computing paradigms like centralized, cloud or edge. Regression and clustering methods, for instance, can be employed to perform the prediction of power consumption continuously as a function of time and environmental factors like temperature in real-time using data from the BANs of many commercial and non-commercial buildings.

In subsections 1.3.1 and 1.3.2, the different methods of energy disaggregation and load monitoring methods, and machine learning based power consumption prediction methods are discussed, respectively.

1.3.1 Intrusive And Non-intrusive Analysis of Load Monitoring

Nowadays, electricity load monitoring of customer appliances has a very important task of utility companies in an effort to study the power consumption behaviours of customers. For long, the operational status of the appliances in customer buildings has been traditionally addressed either by installing sensors on every appliance, or through the use of an intermediate monitoring system in order to record the appliance's operational dynamics and power consumption histories. That is to say, the power consumption by consumers can be traced intrusively or non-intrusively using automated methods. The Intrusive Load Monitoring (ILM) is a distributed method of sensing loads that requires the installation of a sensor or meter for every appliance in a customer premises [18]; whereas Non-Intrusive Load Monitoring (NILM) techniques require only a single smart meter per BAN or per customer. As a result, the ILM method provides a better accuracy in measuring energy consumption of every appliance in the customer BAN in comparison to the NILM where a single smart meter capable of performing sophisticated signal processing is employed per BAN and the accuracy is relatively lower. The ILM method, However, suffers from some critical practical issues including high costs due to its requirement for higher number of sensors and accessories, multiple sensor set-up, and higher complexity of sensor installations unlike the NILM where a single smart meter is employed per BAN that drastically reduces both initial and operation costs. Besides, NILM has less installation complexity and is convenient for large scale deployments where scalability is a key factor. For that matter, the inception of the NILM can be traced back to the late 1980's at MIT in the US. By then George Hart proposed a method to automatically track the operation of individual home appliances based on changes in real and reactive power consumption measured at the utility meter [19].

In other words, the NILM entirely relies on a unique point of measurement called the smart meter whereas the ILM relies on low-end electricity meter devices spread inside the customer premises [20, 21]. In both approaches, feature extraction and machine learning algorithms can be employed at edge, closer to the points where data is created and collected. The NILM equipped with feature extraction and machine learning algorithms is capable of analyzing the changes in electrical quantities (the voltage and current) going into a customer BAN and deducing what types of appliances are deployed in the customer premises and their individual energy consumption. The utility companies integrate NILM technology into their electric meters so as to survey the specific uses of electric power in different customer homes which is vital for better future scheduling and planning. The NILM is considered to be a low cost alternative to intrusively attaching individual monitors on each appliance which increases the complexity of installation that impacts the cost and maintenance process. That is, the NILM method is much more economical than the ILM method in terms of initial and running costs, and network complexity. Furthermore, it can enhance smart meters, save energy and money by reducing waste. The

NILM requires only a single meter and disaggregates the measured power consumption of the customer BAN into individual contributing loads of the appliances based on some peculiar features using advanced signal processing coupled with machine learning algorithms. That is, it determines how much energy is being consumed by each connected appliance in the customer premises. For instance, NILM does a good job for smart home applications which are based on the concept of monitoring and control of the low voltage (LV) loads. They require the knowledge of the operational status of each LV appliance within an installation of the home. This information can therefore be used in the context of demand side management programs towards energy savings and efficiency through the implementation of personalized incentives for overall consumed energy reduction and peak shaving.

Even though the NILM approach leads to a lower implementation cost, there has been a challenge of correctly disaggregating the load from aggregated voltage and current signals measured at a single point. The NILM algorithms often rely on the utilization of the electrical and functional characteristics of the loads towards the formulation of distinct and robust data fingerprints, also known as Load Signatures (LS). The higher the uniqueness of these load signatures, the easier the identification procedure. This eventually led to the development of Nonintrusive appliance load monitoring technique by Hart, George Williamled [19]. Nowadays, thanks to the advancement of the artificial intelligience, machine learning, and deep learning fields, the load disaggregation task has become more simplified. Some of the trending machine-learning based methods employed for power consumption prediction at the edge are presented in subsection 1.3.2. However, the NILM, ILM, and the methods discussed in 1.3.2 are not the perfect solutions yet. Their uses pose privacy concerns. The personal data processed at the NILM point in the BAN and exchanged with the utility servers can potentially be accessed by unauthorized parties causing a lot of information about the behavior of customers and other sensitive personal information to be divulged into the wider cyber space. The security and privacy challenges, along with their proposed solutions, are discussed in section 1.4.

1.3.2 Power Consumption Prediction

As a result of the ever-growing energy consumption and technological advancement, there are various concomitant critical economic and environmental challenges like maintenance and planning costs, and carbon emissions from energy generation. A multitude of research works have been carried out since the early 1990s in the design of non-intrusive algorithms capable of extracting useful information about the individual power consumption of electrical devices in a domestic environment only from an aggregated load measured at single point in order to significantly improve the efficacy of energy usage and accurately predict future consumption and peak load times [18, 20, 21]. The energy disaggregation process, as described in section 1.3.1, refers to non-intrusive load monitoring. Through the employment of a set of techniques based on advanced signal processing and machine-learning, it can be used to estimate the electrical power consumption of individual appliances from measurements of voltage and/or current taken at a fewer locations in the power distribution system of a building area network. It often requires only a single smart energy meter

which is installed at the main feeding panel of a BAN so as to effectively monitor and identify the status of every appliance within the BAN. As a result, this approach coupled with the state-of-the-art machine-learning algorithms and the edge computing paradigm has gained tremendous attention from the electrical utilities. It meets the interest of electrical utilities and systems by providing load profile details at nodes of electrical grid and commercial buildings. Given this characteristics, the computing paradigm that fits well to it is the edge computing, described in section 1.1.2, which pushes most of the computational processes closer to the customer premises relieving the network from unnecessarily higher and chatty traffics.

One of the premises and bases for the design of a contemporary, more robust and efficient smart grid is the capability to obtain an accurate evaluation of the power consumed by customers of all kinds. Besides, it must have a reliable forecasting model integrated into it that can inform utility owners about the power consumption change effectively and timely. Predicting the electricity consumption based on machine learning or lightweight convenlutional neural networks (CNN) has been a hot research topic during the last decade that considers a number of factors like weather conditions, holidays, weekdays, and the weekend. They are designed with the capability to assess the impact of every factor for more profound insight. The edge computing architecture drastically reduces the delays, latencies, and traffic congestions incurred during the processing of data in a centralized and cloud computing architectures thereby improving the timeliness and quality of communication. Performing the power consumption evaluation and prediction at the edge creates an auspicious environment for enforcing security and privacy measures closer to the source where data is created and collected. Some of the upsides of performing load forecasting at the edge are enumerated in what ensues:

- It improves the computational times by reducing the latencies. In the cloud or centralized datacenter based smart grids, the data collected from the distributed sensors must be sent over the network to the servers for processing which has a lot of problems like higher latency, traffic congestion, security and privacy issues, and reliability problem. But performing the computational processes nearer to the points where data are generated and collected drastically improves the response time.
- The accurate prediction of power consumption improves the return of investment (ROI) through the maximum utilization of power generating plants with minimum wastage. That is, the prediction creates an enabling environment for the plant owners and/or utilities to produce and distribute only the required amount of energy at the right times by avoiding both under and over generation.
- It has paramount importance in determining the amount of logistics and resources required to smoothly run the power generation plant in advance. It equips the power grid with the ability to determine the fuels, mobilization of human resources, and other resources that are needed to ensure economical and uninterrupted generation and distribution of the power to the consumers in time. Moreover, forecasting provides utilities better information to craft sound short,

medium, and long term plans to improve their operation and management of the supply to their customers.

- It plays very pronounced roles in helping decide and plan the right times for performing preventive maintenance of the power grid systems. In other words, prior knowledge of the demands enable the utilities to decide the right time during which the maintenance must be carried out with minimum impact on the consumers. It is advisable do the maintenance during the part of the day when most customers are out of their homes(or at work) and the demand is very low. And the low demand period is determined by the load prediction system in use.
- Electrical power consumption prediction techniques increase the efficiency and revenues of companies engaged in the generating and distribution of electrical power. It enables them to plan on their capacity and operations well ahead so as to sustainabily supply all consumers with the right amount of energy at the right time.
- It important in planning the size, location and type of a generating plant that must be built in the future to meet the growing demands of customers . The predictions collected from different edges or BANs can be used to determine the customer regions with higher and growing demands thereby enabling the utilities to build a power generation station nearer to the area with higher demand to minimize transmission and distribution infrastructures and associated losses. As a result, energy can be availed to customers at reasonable prices.
- It helps minimize the risks for the utility companies. Putting it another way, knowledge of the future long term load creates an enabling situation for the companies to plan and make economically viable decisions with respect to their future investments.
- It enables the implementation of new reconfigurable security framework based on edge computing to fix the security and privacy issues of smart grids. It includes measures against availability, integrity, and confidentiality attacks. Besides, the BANs equipped with edge devices tantamount to Raspberry PI 3, Tinker Board, or Jetson Nano, are capable of performing cryptographic functions and simplified key managements.

Summing it up, good power consumption prediction enables electric utility owners to make insightful and data-driven decisions on the generation and purchasing of electrical power, the switching of loads from region to region , the planning of maintenance, and the development of new power plant infrastructure. Depending on the duration of the period over which the prediction is made, load forecasting can be short term, medium term, or long term. The short-term load forecasting is usually done over a period of one hour to one week. It helps to estimate the power flows that provide insightful information to make decisions that prevent overloading. The medium load forecasting spans over a period of a week to a year while the long term load prediction spans over a period longer than a year. In a number of research outputs including research articles and textbooks, and other literature, many load forecasting techniques have been presented and implemented. Some of them are multiple regressions, knowledge based expert systems, stochastic time series, iterative reweighted least squares, exponential smoothing, Fuzzy logic, Neural Network,

Machine Learning, Deep Learning, and the ARMAX model based on genetic algorithm. However, load forecasting is yet a challenging task. That is to say, it is sometimes challenging to exhaustively consider and accurately fit the great deal of complex factors that affect the demand for electricity into the forecasting models. In addition, it may not be easy to obtain an accurate demand forecast based on parameters such as change in temperature, humidity, and other factors that influence the power consumption. As a result, the tendency to employ a deep neural network capable of taking all the factors that impact the power consumption has been growing.

1.4 Security of Smart Grids Enabled by Edge Computing

A smart grid that employs the state-of-the-art technologies promotes energy and cost efficacy. An edge computing enabled smart energy network automatically reads and reacts to supply and demand changes without waiting for computational support from a central server. This offers the potential for much improved security of supply through efficiency. When this is coupled with the deployment of edge enabled smart meters capable of performing non-intrusive appliance load monitoring (NIALM), it encourages consumers to adjust their own real-time demands and facilitate the integration of renewable energy like private wind turbines into the grid. This has a great potential to improve efficiency of the power grid system. That is, the NIALM is the technique for analyzing changes in electrical quantities like voltage, current, and operating frequencies when energy is consumed in customer houses. It is capable of deducing what kind of appliances are used in a customer premises and the individual energy consumption of every appliance. Furthermore, edge enabled electric meters are fitted with machine learning based algorithms and technologies for precise survey and prediction of the specific uses of electric power in different customer premises or houses. This is less prone to failure and low-cost solution to detect, and monitor the power consumption of each customer appliances and alert them so as to take corrective measures. However, on top of the chronic security problems of the old and centralized smart grid, this enhanced smart grid presents privacy concerns [6, 16]. It has the potential to divulge a lot of personal information of customers to the wider cyber space.

In general, the smart grid is a subset of the vast cyber physical system and inherits many of the security problems that the cyber physical system suffers. In other words, to effectively control and monitor the power plant along with its transmission and distribution systems, as portrayed in figure 1.2, the smart grid combines the powers of three vital components, namely communication network, Computational systems, and Control systems. As a result, it is vulnerable to a multitude of attacks described in subsection 1.4.1.

1.4.1 Security Challenges Of Smart Grids

Distributed sensors and edge devices are the eyes, ears, and brains of a smart grid which provide information and computational power vital for fault detection, analyzing the individual power consumption of home appliances, monitoring and control-

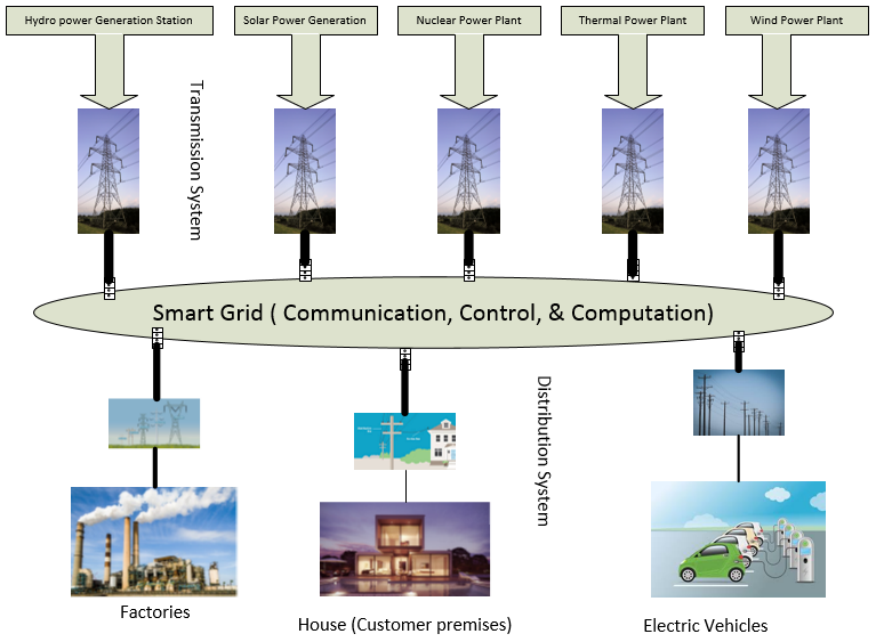

Figure 1.2 Major Components of a smart grid

ling the entire power generation, transmission, and distribution systems. Therefore, secure exchange of information among the sensing and decision-making entities is essential as security breaches may bring the entire system on its knees [22]. Smart grid technologies are designed to take advantage of the benefits of the information and communication technologies and incorporate them into the old and traditional physical networks of Electrical power grid for efficient and smart operation, and accurate billing of energy. In other words, the smart grid is a digital technology, like IT networks, that allows a bidirectional or duplex traffic flows between the utility and its customers equipped with smart sensing capability along the transmission and distribution lines, and various substations. More like the IT networks or the Internet, it comprises such important components as computers, automation, controls, protocols, and new technologies and equipment working in unison. It is known that the transmission control protocol/Internet protocol (TCP/IP) has become the most widely used network interconnection protocol; there was insufficient security concerns at the beginning of the design, though. Since then, IT engineers and researchers have been dealing successfully with Enterprise network securities. Today there are many security products in daily use in Enterprises which are never the cases in the operational networks where the smart grid is extensively employed. Networks like Industrial Control Systems (ICS) and Supervisory Control And Data Acquisition (SCADA) have a lot of security problems.In general, cyber security has been a challenge on control networks for the same techniques and tools used to secure IT

networks cannot be directly applied. That is to say, smart grid networks have unique requirements. They have different operational, security focus, vulnerability management, and interoperability requirements. Besides, highly sophisticated attacks, probably the first of their kinds, have been perpetrated on SCADA networks during the last two decades that have a potential of causing power network disruption and total power blackout.

Furthermore, in the case of the smart grid, the technologies are proprietary and specifically designed to work with the electrical grid with the ability to digitally respond to the quickly and dynamically changing demand of electricity. It is more of a cyber-physical nature that makes is more vulnerable to tones of attacks that could be perpetrated at various levels including the physical layer or communication links, Media Access Layer, and networking. Eavesdropping, Jamming, and replay attacks are the typical examples of attacks often launched on the smart grid. The security of IT networks primarily focuses on the protection/privacy of information whereas that of the smart grid focuses on the protection/safety of the the plant or process. Hence, the security goals of smart grid are Availability, Integrity, and confidentiality, the priority of Availability being the highest and that of confidentiality being the lowest. The converse is true in the case of the IT networks in that the highest priority is affixed to confidentiality/privacy and the lowest one is affixed to availability. All efforts to remedy the security problems of smart grids are, therefore, tuned this way. Hence, not with standing the fact that there are a lot of security products and solutions for IT networks on the market and a number of researches pertinent to smart grid security have been conducted especially following the discovery of the most threatening SCADA network attack perpetrated on the Iranian Nuclear Facilities where control and monitoring center crews were faked by replay attacks, there still exists a gaping hole begging for bridging. Hence, the subsections that ensue discuss the security and privacy issues of a smart grid system. The various types of security challenges and attacks directed on smart grid which include availability, integrity, and confidentiality attacks, and privacy issues are discussed in subsections 1.4.1.1 through 1.4.1.3, and the privacy issues of the smart grid are explained in subsection 1.4.1.4. Adversaries manage to realize these attacks often by exploiting the vulnerabilities in the generation system, transmission system, distribution system, and telemetry infrastructures.

1.4.1.1 Availability Attacks On Smart Grids

Availability attack is often realized when an authorized personnel or an adversary manages to gain an access or a control of the grid system. It also involves interruption caused by physical damage or electrocution of smart grid components. Following such type of attack, authorized personnel are denied of access to the smart grid; hence, it is also known as a denial of service attack (DoS). When the DoS attack is escalated and applied in a distributed manner using bot-nets, it is known as distributed denial of service (DDoS) attack. Both the DoS and DDoS attacks have the potential to interrupt, delay or corrupt data and command information flow causing unavailability of information exchange in the smart grid or power. On top of a service interruption in a smart grid system where billing is computed centrally based

on meter readings received via the smart grid network, the availability attack could cause substantial loss of revenues. Jamming is a type of availability attack. It is an active attack that can disruptively interrupt the transmission of data often achieved by transmitting simultaneously whenever the target transmits or receives data. This overwhelms the target and causes an availability attack or Dos. It occurs at the media access control (MAC) layer and the adversary can deliberately corrupt the control packets or exhaust the whole available channel causing DoS. That is, the legitimate nodes will not be able to access the channel or medium as a result of which their throughput goes down and eventually becomes zero. MAC and address resolution protocol (ARP) flooding are, for instance, DoS attacks directed on the Medium Access Layer [6, 22].

The most devastating availability attack recently launched on a smart grid is the cyberattack on Ukraine power grid in December 2015. It caused extensive power supply interruptions. The attack temporarily cuts off electricity supply from three energy distribution companies to a number of consumers' premises in Ukrain. The exploited security loopholes have been made public yet but the adversaries managed to gain access to the control and information systems of these suppliers. Then, they successfully compromised the power grids and brought down thirty substations across the nation that had left more than 230 thousand people without electricity for a quarter of a day [12].

1.4.1.2 Integrity Attacks on Smart Grids

It is the unauthorized and malicious modification of data and critical information of the control and command center, the sensory devices, computers, smart meters, and software [6, 22]. This could result in the provision of wrong information or command to the decision making components of the smart grid; that is, the exchange of corrupted data starts to take place in the smart grid following an integrity attack that could potentially impair its decision making capability. One way of compromising the integrity of the smart grid is through the injection of bad data during state estimation that could inflict power mismanagement. Besides, unless the integrity of whatever software running in the smart integrity is maintained at all times, it could open a door for an adversary who can employ compromised software to gain access to the critical sections of the smart grid. In today's smart grid system, SCADA is the heart of any load dispatching centers. In the old days, the SCADA system used to be a LAN or wide area network (WAN) on its own isolated from the Internet. However, today many a company who transmits and distributes power have integrated their SCADA communication network into the Internet for cost-effectiveness, improved efficiency and reliability. But this approach has its own cost. It gives the opportunity for any adversary, who has an access to the Internet, to look for loopholes in the SCADA system which increases the risk of infiltration and compromise of data and control information that can bring down the entire system on its knees.

The inter-communication systems of the major components of the SCADA system like master terminal units (MTU), remote terminal units (RTUs) and programmable logic controllers (PLCs) are said to have vulnerabilities that could be exploited to compromise the integrity of data and information. Most of the attacks perpetrated on

the IT network can also be launched on the smart grid. Due to its proprietary nature, the smart grid has not many available solutions unlike the IT networks. For instance, a malicious Cross-Site Request Forgery (CSRF) could be launched. That is, uniform resource locator (URL) scripts could be broadcast to the SCADA network and when they happens to be opened at any of the Human Machine Interfaces (HMI), they can detect and invade the PLCs and other components. This attack can be launched on both types of smart grids, the cloud-centric and edge enabled one. But the effect is less in case of the edge enabled smart grid.

1.4.1.3 Confidentiality Attacks on Smart Grids

An attack on the confidentiality of data and control commands is a hazardous intrusion into the smart grid network. It refers to the the unauthorized access of sensitive power usage data, price information and control commands that have the potential to invade the security of the power grid and the privacy of customers. It could also expose a lot of proprietary information about the power utilities. Intercepting the data and control commands exchanged between the various smart grid components is so easy for adversaries. For instance, it is next to impossible to prevent adversaries from eavesdropping the smart grid network. Eavesdropping is a passive attack where the adversary stealthily listens to the private communications of the smart grid communicating parties without their knowledge and consent. Putting it another way, unauthorized parties listen to the smart grid network with the help of wiretapping without any traceable or detectable interactions. Then, they conduct analysis on the the captured data to uncover the data and commands being communicated. Hence, the success of the confidentiality attack lies on whether the information is exchanged in strongly encrypted-text form or clear-text form. Hence, the smart grid should be able support end-to-end encryption and germane key exchange protocols for secured exchange of information.

As part of the smart grid systems, the SCADA system is installed and deployed in almost all power generation plants for continuous monitoring and controlling of the complex processes of the plant. The HMI's of the SCADA system serve as a dashboard that visually tracks, analyzes and displays measures, feed-backs, statuses, and alerts to monitor the health of the plant in which thousands of processes are concurrently running. One common problem that had repeatedly compromised the confidentiality of generation plats is the use of default manufacturer passwords after first login. Exploiting this weakness, an adversary could gain access to the plant SCADA system LAN and tamper with some parameters. For example, they could change the frequency measurements provided to the automatic governor control (AGC) and destabilize the plant. This is the case of a confidentiality attack leading to availability attack. That is, once the adversary gains an access to confidential data, keys, passwords or commands, they can perpetrate any kind of attack on the system. The Stuxnet is the most popular example of a sophisticated attack that combines confidentiality, replay and availability attacks [23]. This attack is believed to have been perpetrated on the Natanz uranium enrichment plant in Iran. It is believed to have managed to destroy more about one thousand centrifuges in the Iranian Nuclear facilities thereby causing a delay in the uranium enrichment process. Once it somehow

gained access to one of the SCADA computers in the nuclear facility, it is believed to have gained access to the SCADA server using the default/factory password of the server exploiting the IT experts negligence to change the password after first login following the commissioning of the network. Using relatively big-size most complicated ever computer virus or malware (Stuxnet), the adversaries had adeptly recorded the system dynamics for quite sometime and later replayed it to deceive human operators or programs while covertly perpetrating damage on the centrifuges by changing the operating frequencies.

The smart grid advanced metering infrastructure may employ such communication technologies as power line communication (PoLC), Wireless LAN (WLAN), ZigBee, Worldwide Interoperability for Microwave Access (WiMax), Ethernet Passive Optical Networks (EPON), and Mobile Radio Frequency (RF) mesh. All of these technologies don't have default security and authentication mechanisms [6, 16, 24]. The PoLC is an open wire communication technology that supports the sending of data over existing power cables. However, it is prone to misguiding. The WLAN which follows the IEEE 802.11 standards is also susceptible to such attacks as eavesdropping, traffic analysis and session hijacking. The ZigBee (IEEE 802.15.4 standards) can be jammed easily and suffers from delays caused by the cluster-tree based routing strategy. What is more, the WiMax, which works based on the IEEE 802.16 standard, is liable to replay and scrambling attacks. Similarly, the EPON is susceptible to eavesdropping, DoS, and spoofing attacks. The mobile communication system could also be employed but it is unprotected medium that could potentially cause the invasion of customers' privacy through the disclosure of their energy consumption data. Hence, unless additional measures are enforced into the grid system, the communication technologies employed in grid system don't have default means for ensuring confidentiality.

1.4.1.4 Privacy Concerns in Smart Grids

The smart grid represents a new era in the electrical sector and has a spectrum of advantages including efficient energy generation, transmission and distribution, accurate bill calculation, balancing cost, and support of green energies. Notably it can keep customers apprised about their daily energy consumption, the individual consumption of their appliances, and measures they should take to keep their bills lower. However, it has remarkable impact on the privacy of customers' data. It has the capability to garner a lot of detailed information on individual energy consumption usage and the patterns within consumers' premises. If all these data are divulged into the wider cyberspace, they have the potential to disclose about what kind of appliances the customer has, which appliance they frequently use, from which providers they have tapped electricity, personal information like names and addresses, and their billing information. Hence, unless smart grid technologies are designed to inherently incorporate a robust customer privacy conserving mechanism by design, they can potentially sacrifice the privacy of consumers.

Privacy is the number one concern of consumers and distribution utilities. A smart grid that increases the confidence of distribution utilities and customer alike is badly in need. But why are customers so concerned about their personal data ending

up in the hands of third parties or in the wider cyberspace? Why are the customers so paranoid about privacy? Well, we could look into the potential threats that could be posed to answer these questions. It is known that the smart meters installed at the consumers' premises exchange customer energy usage data and control signals with the respective customers' BAN gateway which is connected to the smart grid WAN in turn. But the networks could have exploitable flaws in that they could cause data leakage when eavesdropped. This could reveal a lot information about customers including account numbers, plug-in electric vehicles information,personal behavior as inferred from social networking activities, whether a residence or facility is occupied, what people are doing, technologies used, manufacturing output, sale events, and et cetera. For customers who own factories or manufacturing industries, this could amount to technological espionage that could be transferred to foes or competitors. Hence, this calls for a serious endeavor to address the issues of privacy caused by smart grids. Edge computing technologies provide better opportunities to address the privacy concerns at the customer premises. The possible edge enabled solutions are presented in subsection 1.4.2.

1.4.2 Edge Enabled Solutions To The Smart Grid Security Problems

Following the most sophisticated stuxnet malware attack on SCADA system, many utilities have started to look for better security solutions for their power grids. In addition to preventing potential security attacks, there are stringent requirements for the cyber security mechanisms of smart grids to be robust and resilient enough to address natural disasters, inadvertent compromises of the information infrastructure due to user errors, and equipment failures. The state-of-the-art security solutions of Enterprise IT networks like intrusion detection systems, firewall, antivirus, virtual private networks, and public key infrastructure cannot be employed as they are in the smart grid. This is because the two networks have intrinsic differences as explained at the outset of section 1.4.1. Hence, enhancement is required to bridge the differences. But the security objectives are the same in both cases; the priorities of their importance are conversely related, though. That is, the prime focus is plant availability in the smart grid; whereas privacy of information is the top priority in IT networks.

In general, any network including the smart grid is said to be secure only if it can ensure the three basic cyber security goals; availability, integrity, and confidentiality (AIC). As depicted in figure 1.3, only the intersection of the three security objectives is said to be secure which implies that all objectives must be achieved to have a secure network. Any failure to do so has a negative impact on the generation, transmission, and delivery of electricity. In other words, the three cyber security objectives form an AIC triad which is the foundation for all security models. The triad serves as the basic guide in formulating policies for information security within the premises of an organization. For data exchanged over a certain network to be completely secure, all of these security goals must be ensured inseparably. Besides, figure 1.4 depicts specific security requirements that must be met to achieve the three security goals. Having a mechanism for identity and security authentication and access control, re-

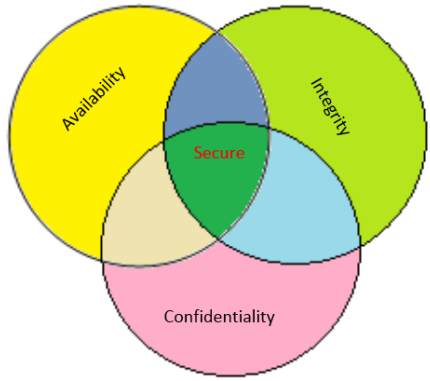

Figure 1.3 Security Goals

source access authorization, conserving privacy, and establishing trusted system are vital for preventing the availability, integrity, and confidentiality attacks.

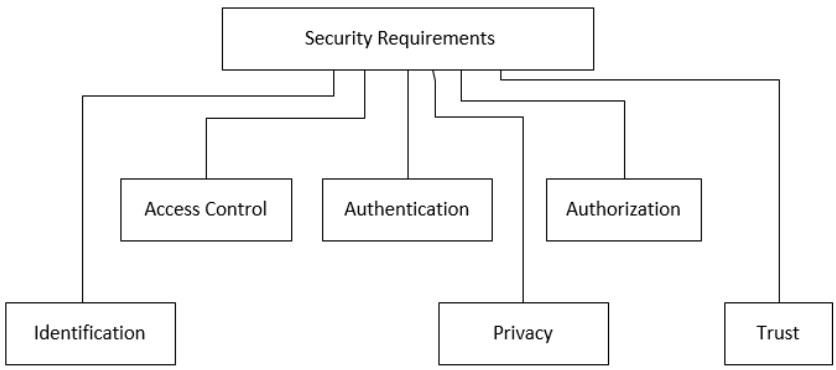

Figure 1.4 Security Requirements

The Edge Enabled smart grid allows the dynamic bidirectional flow of power and sharing of information among nodes. Unlike the conventional power grid where power flows in one direction from main generation stations to customer premises, the edge computing enabled smart grid supports two-way flow of energy. That is to say, the smart edge devices installed at customer premises have the capability to smoothly connect electricity generated by green sources like micro dams, solar panels, and wind station at customer sites back to the main grid. This gives the power grid a good energy mix and balance. To Put it another way, customers are not only consumers in an edge computing enabled smart grid but also producers of energy. They produce environment friendly green energy and contribute to the wider power grid system. In a similar fashion, the edge computing contributes a lot in providing better security and privacy solutions as compared to the conventional grid system.

For instance, it enables us to enforce intrusion detection and prevention systems, and many other security and privacy measures at the edge of the smart grid network to thwart attacks or potential threats before they can cause substantial damages to the grid system. Consistent scanning and monitoring of the security statuses is made at the edge not at a central location; that is, computing and security enforcement are performed right at the part of the network, where the data is generated. Hence, all security measures and policies enforced to prevent and detect any potential attack directed on the smart grid are enumerated in this subsection in what ensues. The edge computing enabled security measures principally focus on mechanisms that can prevent potential availability, integrity, and confidentiality attacks and privacy invasion from being realized. Attacks are warded off at the edge, at every customer premises and other major nodes.

- ***Preventing Availability attacks***: Availability is one of the three major objectives of a sound security service or mechanism. In cyber physical systems like the smart grid, availability of a plant is the top priority that makes sure that the plant is available 24/7 and information or services is accessible to authorized parties at the right time [22]. In other words, service or information is invaluable only if it can be accessed by the right/authorized people at the right times . But cyber physical systems liker power plants and information websites are attacked by adversaries. They are often taken down by DoS or DDoS attacks. Physical damage or interruption, ping flood, smurf attack, SYN Attack, jamming, and buffer overflow are some of the common methods of attack that might render the smart grid, information or services unavailable to legitimate users. They have the potential to deny the legitimate users access to the smart grid by degrading the performance of the system to the point of complete service disruption. That is, physically damaging some components of the smart grid or by hitting the target machine with simultaneous superfluous requests disrupts the normal functionality of the system. Hence, the solutions enforced to deter such attacks must have the capability of analyzing and authenticating incoming requests to identify whether the source is legitimate or not. Besides, it should be smart enough to detect superfluous requests coming from a single or multiple sources and be able to stop them before they could exhaust resources.

  The best strategy for security enforcement in an edge enabled environment is to equip the edge devices in every BAN with lightweight identity and security authentication mechanism with pre-configured but dynamic access control list (ACL)[22]. That is, an ACL, initially created by the utility owner, is stored in every edge device connected to every BAN to ensure authentic and secure access to the BAN components. It contains details about authorized users, unique node identifications, MAC addresses, system program attributes, and application program attributes which can be securely updated whenever change takes place. Hence, using the mini-ACL, the edge device can make identity and security authentication of request sources and share any presumed security risks with peers in the same or different neighboring BAN and the server. It can stop any unauthorized access or superfluous requests before potentially resulting into DoS attack. The edge devices periodically report the incidents they have expe-

rienced to the nearest utility server. Hence, threats or attacks are thwarted at the entry point in an edge computing enabled smart grid without much support from a central powerful server or firewall.

- ***Preserving Integrity of Data and control commands***: Phasor measurement units (PMUs), phasor data concentrators (PDCs), and control centers (CC) of a smart grid can be compromised [6, 25]. That is, adversaries can inject and send forged PMU frames with manufactured data to a PDC or CC which can cause a potential havoc in the system. Hence, preserving the integrity of data, and software is of paramount importance. Integrity of information refers to the mechanism of conserving information from being tampered or altered by unauthorized parties. It ensures that that information or command signal is exchanged over the communication channel between authorized parties intact; it can be altered only by legitimate users. Besides, the integrity of all sorts of software running in the smart grid must be maintained at all times by means of check-sums or equivalent methods to make sure that no compromised software is in the system that could serve as a gateway to adversaries. The fundamental thing here is that information or a software has value if and only if it is not tampered by illicit users.

  The integrity of data, and software can be checked using hash functions where the integrity of data is authenticated before every decision to use or access that data. Besides, the edge device in every BAN is equipped with a software integrity checker that reports manipulations or changes on any software running on the BAN. The attributes of the system programs and applications are compared against a database of initially generated hashes and check-sums residing in every edge device. Hash or check-sum mismatches imply that software was probably tampered and appropriate actions must be enforced with no more ado. The edge devices with computational power equivalent to tiny single board computers like Tinker Board, Raspberry PI 3, or NVIDIA Jetson Nano can perform any of the hashing functions with great ease. In addition, the edge devices support such mitigation scheme as dynamic state estimation (DSE) to dynamically deduce the state of the smart grid components based on measurements collected BAN wise to guard against replay attack by injection of recorded states. The DSE covers the progressive development of the state over a series of measurement instants so as to produce an accurate dynamic states of the system [6]. Summing it up, the edge computing enables the smart grid to have a platform for collaborative prevention against integrity attacks and injection of forged frames.

- ***Ensuring Confidentiality of Smart Grids***: The confidentiality here refers to the secrecy of the information exchanged over the smart grid communication network or the information stored in every utility server and BAN edge device. In the eyes of confidentiality, information is the most valued asset. Hence, all confidentiality assurance methods are therefore designed with this in consideration. Confidentiality ensures that a robust mechanism is in place to prevent the information from any disclosure to unauthorized parties; often cryptographic methods are used. Unlike the conventional grid where enforcing encryption

mechanisms is not possible due to the fact that the end devices lack the computation power required to perform decryption and the inverse process, the edge computing enabled smart grids can enforce cryptographic methods to ensure secure exchange of data. That is, in a setting where the smart grid has edge devices at every BAN, standard cryptographic methods like advanced encryption standards (AES)-128, AES-192, AES-256, or other singanl processing-based schemes [24] can be employed to create encrypted duplex communication. For key management, the Diffie-Hellman key exchange protocol or other public key methods could be employed.

- ***Conserving customer privacy at the edge***: The many upsides of smart Grid systems come with huge privacy risks. In other words, even though the smart grids components like smart meters and edge devices installed in customer premises or BANs have positively impacted the way power is generated, transmitted and distributed, and the way revenues are collected, they have the potential to invade the privacy of customers. The privacy concerns of the power grid customers include identity theft, determination of personal behavior patterns, deducing the specific appliances used, and carrying out real-time surveillance. The smart grid garners such sensitive private data and could end up in the bad hands of adversaries when its weaknesses are exploited and attacked. The smart grid industry still lacks transparently defined privacy principles and mechanisms. Government agencies may enact laws and impose regulations on utility owners but they lack the means to reflect the realities of a smart Grid where consumers actively contributes sensitive personal data on daily basis. That is, instructing or requiring distribution utilities by law alone lacks the means to prevent privacy breaches.The utilities may strive hard to obey the laws and regulations to protect customers' privacy; however, the edge devices, smart meters, sensors, communication networks, or storage devices can be compromised and intruded resulting in the private data ending up in the hands of hackers or adversaries.

  Edge computing provides convenience for enforcing privacy conserving mechanisms at the point of customer data collection unlike the cloud-based smart grid where account information, billing amount, appliance types, energy meter reading, frequency meter reading, et cetera are transported to the cloud location for computational processing and decision making which likely increases the chance of privacy breaches. Hence, the most feasible solution is to design and manufacture smart grid edge devices which are privacy aware. That is, privacy by design is the best solution for the smart grid enabled by edge computing. The edge devices can compute the bills based on the meter readings and they can only send the amount of bill to the utility server attached to unique customer ID via an encrypted channel. All other customer-specific data like the individual power consumption of appliances are solely provided to the customer for future decisions. Hence, the edge device can be further made more intelligent to perform robust classification of data into sensitive and non-sensitive through the incorporation of lightweight machine learning algorithms(LWMLAs) that can effectively run in a resource constrained environment. That is, edge devices equipped with LWMLA are capable of anonymizing and aggregating customer

data required for research and analysis uses to improve services and the technologies. They can effectively identify sensitive personal data and household identity and obscure them to prevent the exposure of customers' privacy.

1.5 Summary

This chapter has covered the major problems in the electrical grid and explained how the smart grid addresses many of the issues. Besides, it discusses the impact of the computing architectures on the reliability, resilience, security, and privacy of the grid and details the upsides of employing edge computing enabled smart grids. The electrical grid is the greatest technological inventions of the twentieth century that has paved the ways for the advancement of other technologies like computing and communication systems. However, it lacks smart means for efficient generation, transmission, distribution, and management of electricity. This has served as a push factor for the invention of an intelligent grid management system called a smart grid. It efficiently integrates the behavior and actions of all generators, consumers and prosumers in ways that guarantee economically efficient and sustainable power system with low losses, and high levels of quality and security of supply and safety. It solves most of the problems that had been beleaguering the traditional electric grid. That is, the smart grid addresses the inefficiencies and unreliability of the grid. It can efficiently deliver electricity from suppliers or utilities to consumers and prosumers using two-way digital communications to control appliances at consumers' homes and enable the interconnection of green energies produced by prosumers. It is, however, not an impeccable solution. It has a number of issues including reliability, resilience, availability, security and privacy issues. These problems can be solved by employing contemporary technologies and appropriate computing paradigms. The edge Computing is one that stands out as the best computing paradigm for smart grid. It processes the data at the edge of the IoT network closer to the embedded devices where the data is created and collected. It cuts down on the volumes of data transported to cloud centers for processing by handling it at the point of creation, and pushes intelligence to smart devices of the smart grid installed in the customers' premises. Hence, it improves the response time, enables real-time communication and decision-making, creates a facilitated environment for effective enforcement of security and privacy preserving measures, and promotes green energy production by prosumers.

References

[1] Gungor VC, Sahin D, Kocak T, et al. A survey on smart grid potential applications and communication requirements. IEEE Transactions on industrial informatics. 2012;9(1):28–42.

[2] Momoh JA. Smart grid: fundamentals of design and analysis. vol. 63. John Wiley & Sons; 2012.

[3] Yan Y, Qian Y, Sharif H, et al. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE communications surveys & tutorials. 2012;15(1):5–20.

[4] Ipakchi A, Albuyeh F. Grid of the future. IEEE power and energy magazine. 2009;7(2):52–62.

[5] Samie F, Bauer L, Henkel J. Edge Computing for Smart Grid: An Overview on Architectures and Solutions. In: IoT for Smart Grids. Springer; 2019. p. 21–42.

[6] Pandey RK, Misra M. Cyber security threats—Smart grid infrastructure. In: 2016 National Power Systems Conference (NPSC). IEEE; 2016. p. 1–6.

[7] Varghese B, Buyya R. Next generation cloud computing: New trends and research directions. Future Generation Computer Systems. 2018;79:849–861.

[8] Boccadoro P. Smart Grids empowerment with Edge Computing: An Overview. arXiv preprint arXiv:180910060. 2018;.

[9] Van Roy J, Leemput N, De Breucker S, et al. An availability analysis and energy consumption model for a flemish fleet of electric vehicles. In: European Electric Vehicle Congress (EEVC), Date: 2011/10/26-2011/10/28, Location: Brussels, Belgium; 2011. .

[10] Niyato D, Wang P, Hossain E. Reliability analysis and redundancy design of smart grid wireless communications system for demand side management. IEEE Wireless Communications. 2012;19(3):38–46.

[11] Islam A, Domijan A, Damnjanovic A. Assessment of the reliability of a dynamic smart grid system. International Journal of Power and Energy Systems. 2011;31(4):198.

[12] Zetter K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', Wired, 3 March 2016; 2017.

[13] Wang W, Xu Y, Khanna M. A survey on the communication architectures in smart grid. Computer networks. 2011;55(15):3604–3629.

[14] Fitwi A, Chen Y, Zhu S. No Peeking through My Windows: Conserving Privacy in Personal Drones. arXiv preprint arXiv:190809935. 2019;.

[15] Fitwi A, Chen Y, Zhu S. A Lightweight Blockchain-based Privacy Protection for Smart Surveillance at the Edge. 1st International Workshop on Lightweight Blockchain for Edge Intelligence and Security (LightChain, colocated with IEEE BlockChain Conference). 2019;.

[16] El Mrabet Z, Kaabouch N, El Ghazi H, et al. Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering. 2018;67:469–482.

[17] Khan S, Paul D, Momtahan P, et al. Artificial intelligence framework for smart city microgrids: State of the art, challenges, and opportunities. In: 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC). IEEE; 2018. p. 283–288.

[18] Ridi A, Gisler C, Hennebert J. A survey on intrusive load monitoring for appliance recognition. In: 2014 22nd International Conference on Pattern Recognition. IEEE; 2014. p. 3702–3707.

[19] Hart GW. Nonintrusive appliance load monitoring. Proceedings of the IEEE. 1992;80(12):1870–1891.

[20] Chang HH. Non-intrusive demand monitoring and load identification for energy management systems based on transient feature analyses. Energies. 2012;5(11):4569–4589.

[21] Norford LK, Leeb SB. Non-intrusive electrical load monitoring in commercial buildings based on steady-state and transient load-detection algorithms. Energy and Buildings. 1996;24(1):51–64.

[22] Fitwi A, Chen Y, Zhou N. An agent-administrator-based security mechanism for distributed sensors and drones for smart grid monitoring. In: Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII. vol. 11018. International Society for Optics and Photonics; 2019. p. 110180L.

[23] Langner R. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy. 2011;9(3):49–51.

[24] Fitwi AH, Nouh S. Performance analysis of chaotic encryption using a shared image as a key. Zede Journal. 2011;28:17–29.

[25] Paudel S, Smith P, Zseby T. Data Integrity Attacks in Smart Grid Wide Area Monitoring. In: ICS-CSR; 2016. .