An IoT-enabled Smart Grid: Definitions, Characteristics, Challenges, and Future Directions

Abeer Akkad

*Dept. of Computer Science
University of Southampton
Southampton, UK*

Gary Wills
*Dept. of Computer Science
University of Southampton
Southampton, UK*

Abdolbaghi Rezazadeh
*Dept. of Computer Science
University of Southampton
Southampton, UK*

Abstract—The IoT-enabled Smart Grid (SG) could be viewed as a large Cyber-Physical-System (CPS). The Smart Grid is considered to be part of the vital critical infrastructure for many communities worldwide. Globally, the energy market is considered the biggest market for any country to grow economically and therefore Smart Grids are one of the biggest applications of IoT. The evolution of an Internet of Things-enabled Smart Grid affords better automation, communication, monitoring, and control of electricity consumption. It is now essential to supply and transmit the data required, to achieve better sensing, more accurate control, wider information communication and sharing, and more rational decision-making. However, the rapid growth in connected entities, accompanied by the increased demand for electricity, has resulted in several challenges to be addressed. This research helps better depicts and understand the challenges of Smart Grid implementation. Identifying the challenges is considered a pre-requisite pillar to understanding whether the applied implementation and design approach can be employed to foster the IoT-enabled Smart Grid. To the best of the author’s knowledge, no previous study addresses sufficiently and comprehensively the challenges of the IoT-enabled Smart Grid.

Keywords— Smart Grid, Smart energy, IoT, Internet of Things, IoT - enabled Smart Grid, Cyber-Physical-System, CPS.

# Introduction

As cities transform into smart cities, it is essential that they have sustainable green energy, and the implementation of the IoT-enabled Smart Grid is considered a way to achieve this goal. According to a study conducted by McKinsey Global Institute, the IoT will have a significant economic contribution from $3.9 to $11.1 trillion per year by 2025 (Manyika *et al.*, 2015) influencing (homes, factories, retail environments, offices, worksites, human health, outside environments, cities, and vehicles). The electric utility industry is currently developing an IoT-enabled Smart Grid (SG) which is envisioned as the largest installation of an IoT system, with billions of smart objects and things, such as smart meters, smart appliances, and other sensors (Reka and Dragicevic, 2018)(Reka and Dragicevic, 2018). This huge number of connected devices besides the increasing demand for electric energy results in many significant challenges that may face the Smart Grid. Although the Smart Grid could address the drawbacks of the traditional power system, it also contained some challenges of security, big data processing, cost, centralization, scalability, interoperability, heterogeneity, and latency. This research discusses the existent challenges of the IoT-enabled Smart Grid which could help practitioners and engineers in the energy sector for better implementation of the IoT-enabled Smart Grid.

This paper is organised as follows: Section II defines the Smart Grid, its importance, characteristics, and components. Then, it describes the link between IoT modules and Smart Grid. In section III the challenges of the IoT-enabled Smart Grid are investigated. Section IV looks at the future work directions in the context of IoT and Smart Grid. Then, the work is concluded in section V.

# Background

This part of the paper offers an overview of the IoT-enabled Smart Grid definitions, characteristics, components, as well as its benefits. Moreover, the role of IoT in the Smart Grid is explained.

## Definition of Smart Grid

The many definitions of SG vary between organisations and studies, as shown in , and there is no agreement; however, the common concept is that SG revolves around an information communication infrastructure. For instance, in the definition by the largest standardisation authority, IEEE, the SG describes a new age of electricity that features the use of ICT in the generation, delivery, and consumption of electricity and the electric system (IEEE, 2018). Likewise, the viewpoint of the Ontario Independent Electricity System Operator (IESO), the leader in SG, is that it involves the use of ICT in optimising all power system operations for the benefit of the consumer and the environment (Singer, 2009).

Both definitions focus on the SG component, which is specifically the communication infrastructure, whereas others focus on the outcomes that benefit from SG. For instance, the Energy Independence and Security Act of 2007 (EISA, 2007) produced the first official definition of SG (US Public Law, 2007; Al Khuffash, 2018), as given in a report to the US Congress: “*The modernization of the Nation’s electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve a set of requirements that together characterize the SG*” (US Public Law, 2007; U.S. Department of energy, 2018). It is worth pointing out that this definition describes SG from the perspective of its benefits. Within the IEEE and EISA definitions, SG domains are prominent, including electricity generation, transmission, distribution, and consumption (US Public Law, 2007; IEEE, 2018).

In the context of information technologies, other definitions focused on how information could be transferred through the SG. The bi-directional flow has given rise to the term “prosumers” in SG (Dalipi and Yayilgan, 2016), meaning customers who generate energy for the grid, as stressed by the European Union’s viewpoint as well as the UK Institution of Engineering and Technology (IET, 2013), also shown in Table 2-1. The IET’s definition of SG is based on that of the ETP (IET, 2013). From an environmental perspective, both Singer (2009) and the Electric Power Research Institute (2005) mention green energy and the environmental impact of SG in their definitions as the most important advantages of SG due to their contribution to a reduction in the CO2 footprint (EPRI, 2005; Singer, 2009).

From the above, the SG can be defined as the integration of ICT into the existing electrical network, consisting of renewable sources and involving its multiple domains (generation, transmission, distribution, and consumption) in the efficient automation and real-time demand management of a reliable, sustainable, bi-directional, and economic green electrical energy.

Table 1. A summary of some Smart Grid definitions.

|  |  |
| --- | --- |
| **Organisation** | **Definition** |
| IEEE  | Smart Grid describes a new age of electricity that features the use of Communications and Information Technology (CIT) in the generation, delivery, and consumption of the electrical system. (IEEE, 2018) |
| DOE/EISA(US Dept of Energy) | The modernization of the Nation’s electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve a set of requirements that together characterize a Smart Grid. (U.S. Department of energy, 2018) |
| IESO(Independent Electricity System Operator) | Smart Grid is the employment of ICT in optimizing all power system operations for the benefit of the consumer and the environment. (Singer, 2009)  |
| ETP(European Union) | Smart Grid is developed by the European Technology Platform, and it means the smart integration of all operations from the connected producer, consumers, and prosumersto supply sustainable, and secure power energy. (ETP, 2006) |
| EPRI(Electric Power Research Institute)  | A Smart Grid is one that incorporates information and communications technology into every aspect of electricity generation, delivery, and consumption in order to minimize environmental impact, enhance markets, improve reliability and service, reduce costs, and improve efficiency. (EPRI, 2005) |

There are two flows in the IoT-enabled Smart Grid:

* **Electricity flow** is the classic flow in a conventional electrical grid from generating stations to consumers, while in SG this flow is bi-directional (Bekara, 2014).
* **Information flow** is a bi-directional flow between utilities and all components of the SG, including smart meters, sensors, actuators, smart appliances, and electric vehicles. Consequently, this flow is a real-time Big Data flow, owing to the increase in the number of connected devices on the SG (Bekara, 2014).

## Why IoT-enabled Smart Grid?

Decarbonisation has become a goal worldwide for all countries, to address climate change and limit global warming by reducing CO2 emissions (Colak, 2016; Reka and Dragicevic, 2018). Over time, the exponential growth of demand and the variety of loads have become a burden on the electricity grid (Al Khuffash, 2018). For instance, electric vehicles require charging, and the United Kingdom is investing £30 million in supporting this charging infrastructure (Jenkins *et al.*, 2015). Consequently, there is a strong probability that the grid will be overwhelmed by increasing demand for electricity. Then, costs will rise due to operational expense and latency (Al Khuffash, 2018). Thus, Colak (2016) emphasised that the rapid growth in demand for electricity, and the variety of loads, must be managed and planned efficiently to secure cost containment or reduction.

In addition, transmission and distribution lines experience both losses and unauthorised consumption (Colak, 2016; Al Khuffash, 2018), so inevitably there has arisen a need to be smarter with the electricity grid to manage and monitor consumption effectively and to ensure power availability. The electricity supply could be managed efficiently by increased standardisation of the information system between utilities and consumers in the SG (DeBlasio and Tom, 2008; Sortomme *et al.*, 2011; Colak, 2016). In a SG, more monitoring and control could regulate power generation to respond to demand. By contrast, in a conventional power grid, the traditional meter readings provide insufficient information on grid conditions and consumption, with no real-time energy information (Al Khuffash, 2018). Consequently, consumers have no data on their usage, which, in turn, leads to rising costs. In addition, the centralised architecture of the conventional grid may represent a burden on its productivity. Therefore, the SG is considered to have the potential to solve the drawbacks of the old infrastructure on a conventional grid (Ghasempour, 2016).

Both Ghasempour (2019) and Al Khuffash (2018) argued that SG is essential to enable and integrate all the renewable energy sources in the system, such as solar, hydro, and wind. The SG can both handle the variability, and counterbalance the constant fluctuations in wind and solar.

From the above, the reasons why cities need an IoT-enabled SG can be summarised as: the SG ensures controllable automation, the integration of renewables, sustainable green energy solutions, and real-time awareness (IET, 2013; Colak, 2016; Kaur and Kalra, 2016). As a result, the development of the SG is looked on as the infrastructure to overcome the challenges of rising carbon emissions, rapid growth in demand, overloading, latency, transmission losses and outage, real-time information inadequacy, a centralised old architecture, and integrating the multiple forms of green energy.

## IoT-enabled SG Characteristics

The following 10 points characterise the IoT-enabled SG. This step will contribute to developing a proper model by assuring the functionality need to be accomplished in each characteristic. The characteristics issued by NIST and commonly used in the sector (NIST, 2014; U.S. Department of energy, 2018):

1. To increase the usage of ICT to enhance the reliability and efficiency of the power grid.
2. To optimise the operations and resources of the grid, with full cybersecurity.
3. To integrate distributed resources and generation, such as those of renewable resources.
4. To incorporate the demand response, demand-side resources, and energy-efficiency resources.
5. To deploy smart technologies such as real-time, automated, interactive technologies that improve the physical operation of appliances and consumer devices for metering, communicating, and reporting grid status.
6. To integrate smart appliances and consumer devices.
7. To integrate the advanced electricity storage and peak sharing technologies, including plug-in electric and hybrid electric vehicles and thermal-storage air conditioning.
8. To provide timely information and control services to consumers.
9. To standardise the communication and interoperability of appliances and devices connected to the power grid with the grid’s infrastructure.
10. To reduce unnecessary obstacles to the adoption of SG technologies, practices, and services.

## IoT Modules and SG

This section presents the background of the Internet of things (IoT) and IoT devices. To address the research goals, it discusses the main IoT modules of IoT devices. IEEE defines IoT as the integration of things, which are equipped with sensors, via the internet. The ITU Telecommunication Standardisation Sector (ITU-T) considers the IoT system as an infrastructure for information systems that connect physical and virtual entities. Cisco (2013) gave a definition for IoT as ‘the Internet of Everything’, with the ability to gather people, data, and things to construct a network capable of exchanging information (Cisco, 2013). Hewlett-Packard states that IoT is a system in which every object is connected to the internet. Shakerighadi et al. (2018) defined IoT as infrastructure, including sensors, communication systems, information systems, and objects connected to the internet, which are essentially standardised.

According to Rathke and Sassone (2010), an IoT device consists of the five main modules, shown in : (1) a sensing module, (2) a processing module, (3) an actuation module, (4) a communication module, and (5) an energy module. These are supported by storage and applications.

Mugunthan and Vijayakumar (2019) supported the claim that IoT technologies have afforded SG with the cloud, 5G, mobile wireless networks, application programming interfaces (APIs), machine learning, AI, predictive analytics, and Big Data management.

In SG, in the context of IoT, each device is connected to the internet. To facilitate communicating information and receiving control commands via the internet protocols, each must have a unique IP address (Al-Ali and Aburukba, 2015; Saleem *et al.*, 2019). Under the IP addressing schemas, IoT can offer **monitoring and control capabilities** for SG, as discussed by Kaur and Kalra (2016). This monitoring aspect can cover the generation plan, distribution, storage, and consumption to achieve efficiency management, demand management, renewable energy needed measurement, and CO2 emissions administration. Therefore, IoT devices contribute to the reduction of wasted energy and the accurate estimation of required energy.

Further, those devices exchange data in bi-directional flow via the SG communication layer, using several communication protocols, such as Wi-Fi, Zigbee, WiMax, LET, and GPRS. IoT standardises communication, reducing the number of these protocols relating to the SG components (Al-Ali and Aburukba, 2015). Both Saleem et al. (2019), and Al-Ali and Aburukba (2015), emphasised that IoT technologies enable SG to **communicate** across all its multiple subsystems of generation, transmission, distribution, and consumption. Al-Ali and Aburukba (2015) stated that each device can exchange data and commands from the control centres and utilities.

Both Kaur and Kalra (2016) and Al-Ali and Aburukba (2015) suggested that all objects in a SG can be represented as IoT devices distributed throughout the residential network, substations, and utilities. For instance, these devices could be:

* Smart home appliances with electric vehicle charging
* Substation devices (smart meters, actuators, circuit breakers, transformers, switches, routers, concentrators, voltage regulators, capacitors, or cameras)
* Renewable energy sources
* Utility and control data centres (servers or testing devices)

The conventional power grid relies on SCADA systems, which are built with a centralised architecture (Yang, 2019). Utilising IoT in such systems will increase their scalability, efficiency, and availability; however, there are serious risks. Similar to devices, on the control centre side, SCADA has its own IP address. Classical SCADA systems are renowned for having no proper security controls, in part because they were never designed to be open to the internet. With the integration of complex new architectures such as IoT, therefore, in deploying SCADA systems on the internet, security is an issue (Sajid *et al.*, 2016), especially since several types of malware have recently targeted SCADA systems owing to this lack of built-in security (Pour *et al.*, 2017; Kimani *et al.*, 2019). Centralisation and security issues are discussed in the challenges section.

Figure ‎II‑2: SG and IoT

In short, SG is considered as one of the biggest applications of IoT (Bekara, 2014; Reka and Dragicevic, 2018; Al-Turjman and Abujubbeh, 2019), as shown in Figure ‎2‑3. In other words, IoT technology is subsumed under the wider umbrella of SG. However, many studies considered IoT as a technology separate from the Smart Grid. From the cyber-physical systems point of view, this research considers IoT as part of the SG itself, enabling all those features that are discussed here.

According to the IoT Security Foundation (IoTSF, 2020), the term **Consumer IoT (CIoT)** concerns consumer usage, while **Industrial IoT (IIoT)** is about industrial purposes, including manufacturing, supply chains, monitoring, and controlling. Consumer IoT and Industrial IoT are discussed from the security viewpoint in the next section.

## Smart Grid components

By combining the views of the US DOE (2018), Al Khuffash (2018), and Bekara (2014), it can be seen that SG comprises two major elements: smart devices and Advanced Metering Infrastructure (AMI) (Bekara, 2014; Al Khuffash, 2018), although some studies consider smart meters to be a part of AMI (Mohassel *et al.*, 2014; Mrabet *et al.*, 2018).

### Smart Devices

represent the physical infrastructure of the SG and include smart meters, smart appliances, sensors, phasors, measuring units, and circuit breakers. Smart meters are digital meters consisting of a microprocessor and local memory, and they represent the fundamental blocks with which to build a SG (Rahman, 2009). They measure and collect energy consumption data with a timestamp, which is crucial to delivering electricity in a reliable manner. Also, on the utility side, smart meters transmit data in real-time to the AMI. The smart meters are installed on the consumer side and at other locations around the SG, and report information annually, monthly, daily, hourly, or even each second, for the purpose of management and control. Smart meters record other information, such as voltage and current for both consumers and utilities, due to their two-way capability. From the consumers’ perspective, smart meters raise consumption consciousness by informing them of their average usage, advising them of peak demand times, and alerting them when a specific usage limit is reached. Therefore, smart meters can contribute to an energy-efficient economy and energy conservation to manage the rapid growth in demand (Bekara, 2014; Al Khuffash, 2018; Ghasempour, 2019).

From the utility perspective, smart meters enable monitoring and the detection of power theft. They provide failure/shortage notifications, as well as real-time overviews on grid status to support decision-making on electricity generation, distribution, load balancing, and scheduling. Moreover, they assure a swift response to any controlling commands, including shortage management, software upgrade, on/off turns, and pricing systems. They enhance the planning process by capturing the information so that, with sophisticated analysis, utilities can predict future usage and demand patterns (Flick and Morehouse, 2011; Bekara, 2014; Al Khuffash, 2018; Ghasempour, 2019).

### Advanced Metering Infrastructure (AMI)

like a smart device, enables two-way communication between smart meters and utilities. Before the AMI, automatic meter readings (AMR) allowed only unidirectional communication, from smart meters to utilities (Ghasempour, 2019; Martins *et al.*, 2019). AMI collects, analyses, measures, and stores the energy data sent by the consumer’s smart meter to the utility’s information management systems. The AMI transmits requests, command signals, notifications, recommendations, pricing information, and software updates from the utilities back to the consumer’s smart meter (Bekara, 2014; Mohassel *et al.*, 2014; Al Khuffash, 2018; Ghasempour, 2019). It consists of three elements: (i) a smart meter; (ii) the AMI headend; and (iii) concentrators or collectors.

On the utility side, the **AMI headend** is an AMI server that includes meter data management system (MDMS). The communication with the smart meters is established using communication protocols such as Zigbee and Z-wave (Mrabet *et al.*, 2018).

### Communications network

The communications network aims to enable data sharing and exchange between IoT smart devices and the utility side (U.S. Department of energy, 2018). It includes the network itself and transmission and distribution devices such as switches, voltage regulators, capacitors, and transformers (PTI, 2011; Al Khuffash, 2018). The network collects information from smart meters and transmission and distribution devices to aid in diagnosing and monitoring network status, thereby providing supply distribution (Gungor *et al.*, 2010). The communication network is standardised by IoT to reduce the number of protocols that have to be used to communicate. Al-Ali and Aburukba (2015) proposed the 6LowPAN communication protocol as the backbone of the IoT communication layer in SG. SG employs ICT with a centralised architecture (Al-Omar *et al.*, 2012; Al-Ali and Aburukba, 2015; Yang, 2019). According to the DOE (2018), ICT is what makes the grid smart. As a CPS, SG uses ICT to monitor, manage, and control its processes and physical assets, including substations, transformers, circuit breakers, smart meters, and cables (Khan *et al.*, 2017). Thus, ICT is the most important characteristic of a SG, and it is the key factor in designing IoT systems.

### The supervisory control and data acquisition system (SCADA)

SCADA is the central system that controls the power grid. SCADA is situated on the control centre side, and is composed of three elements (Mrabet *et al.*, 2018):

* Remote terminal unit (RTU): a device consisting of three elements used, respectively, for data acquisition, instruction execution for the Master Terminal Unit (MTU), and communication.
* Master terminal unit (MTU): a device that controls the RTU.
* Human-Machine Interface (HMI): a graphic interface for the SCADA system.

###  Information systems

Information systems are essential for processing, computing, analysing, and accessing the data collected from digital devices in the SG. Information systems of SG can be classified into the following systems (U.S. Department of energy, 2018), according to their location (Wang *et al.*, 2019):

* On the generation side, such as Supervisory Information System (SIS) and Demand Response Management (DRM).
* On the transmission side, such as Energy Management System (EMS), Electricity Operation System, and Decision-Making System.
* On the distribution side, such as Data Management System (DMS).
* On the Utility side, such as Customer Information System (CIS).
* On the SCADA side, such as Substations Automation System (SAS).

# Challenges in the IoT- enabled Smart Grid

As such, before implementing IoT-enabled Smart Grid, it is vital to research potential challenges and risks that could be faced. Many researchers have considered Smart Grids as the largest part of an IoT framework with billions of smart objects and entities. . Therefore, this section is giving a subset of challenges that filter the challenges of IoT infrastructure with the ones that apply to SG. The challenges that are inherent in the use of IoT.

As a result of the growth in the number of objects connected in the SG, **Big Data processing** becomes an issue (Sagiroglu *et al.*, 2017). AMI in the SG produces Big Data that needs to be handled, stored, and analysed efficiently (Shakerighadi *et al.*, 2018). Smart metering and ICT deployment lead to generating big energy data in terms of volume, velocity, and variety (Hu and Vasilakos, 2016). These data can be exploited to obtain insight, make decisions, predict future consumption patterns, and the required distribution of power supplies (Shakerighadi *et al.*, 2018; Ghasempour, 2019). With sophisticated data analytics, superior monitoring and control can be achieved by the SG. In this context, Big Data could consume huge amounts of energy and other resources when information is collected, transferred, and handled by IoT devices. The SG should thus be designed to deal with the collection of Big Data (Ghasempour, 2019).

The internet is used in SGs for monitoring and control purposes, exposing to attack the information from sensors, smart meters, and other smart devices. Any tampering with the data collected in and from smart meters may cause serious financial loss. Thus, the SG’s exposure to the internet could make it vulnerable, rendering its **security** another challenge (Bekara, 2014; Arasteh *et al.*, 2016; Risteska Stojkoska and Trivodaliev, 2017; Ghasempour, 2019).

Ghasempour (2019) and Mahmood et al. (2016) held the view that the implementation of SG should consider the **constrained nature of IoT devices** in computation power and storage capabilities. This, in turn, requires proper security algorithms to meet the limited ability of the IoT devices, so that they are capable of running them (Ghasempour, 2019).



The SG is considered one of the biggest applications of IoT, thus **security** is the greatest challenge that it faces, inherent in the use of IoT devices, as there are many security concerns around IoT technologies. As a cyber-physical system, it is argued that security represents a serious challenge for IoT-enabled SG. All studies are similarly concerned about the SG’s security (Arasteh *et al.*, 2016; Risteska Stojkoska and Trivodaliev, 2017; Bedi *et al.*, 2018; Reka and Dragicevic, 2018; Shakerighadi *et al.*, 2018; Ganguly *et al.*, 2019; Kimani *et al.*, 2019). As argued by Ghasempour (2019), an attacker could extract private information about prosumers and their consumption. Data values in smart meters could be manipulated. **Trust** **management and social factors** between parties such as consumers, substations, and utility companies could be violated through IoT devices, so the SG’s conﬁdentiality, integrity, and reliability could be affected negatively. As a consequence, the CIA triad of security may be compromised. The mobile nature of IoT devices in SG, such as electric vehicles, and connection stability, are major issues in SG security (Bekara, 2014; Shakerighadi *et al.*, 2018; Mugunthan and Vijayakumar, 2019). Specifically, this involves the identification of IoT devices over the internet, which allows identity spoofing attacks to hack the SG.

Shakerighadi et al. (2018) suggest that supplying sensors with energy may pose a challenge in terms of **cost**. The situation is complicated by the bi-directional flow of data, capacity and bandwidth limitations, smart meter constraints, and the long-distance transmission of data. Costs can be assigned to smart devices, software, staff training, regulations, and managing customer acceptance of smart meters (Bekara, 2014; Shakerighadi *et al.*, 2018; Connor and Fitch-Roy, 2019). From a performance point of view, the SG collects Big Data on a real-time basis from a variety of devices, presenting a significant challenge, since real-time analysis is computationally expensive, and this needs to be

taken into consideration, as discussed by Shakerighadi et al. (2018) and Bekara (2014). One explanation is that electricity varies in current, voltage, and frequency; consequently, power fluctuations may cause a power overload or shortage. Similarly, the **centralised** architecture of the SG is a challenge to performance, causing a single point of failure in a power system (Atlam and Wills, 2019). If the node processing the information is attacked and thus unavailable, the whole power system becomes unavailable; however, a decentralised architecture may support power distribution and enhance the system’s bandwidth (Al Khuffash, 2018).

An increase in connected smart devices, with their constrained nature, leads to another challenge, that is **scalability,** which causes a bottleneck in SG. Multiple requests may not be processed synchronously, thus increased communication latency could occur and a noticeable delay in serving consumers could be experienced (Mahmood *et al.*, 2016). Since the SG is used to connect many cities in a country, there is a need for a scalable system (Bekara, 2014). Scalability is the adaptability of the SG to expand incrementally, aiming to meet the prospective future rapid growth in electricity demand and to assure clustering and load balancing techniques (Bekara, 2014; Al-Turjman and Abujubbeh, 2019). Al-Turjman and Abujubbeh (2019) considered that scalability plays an essential role in enhancing the power grid’s reliability and quality since it affects the availability of this vital asset. Thus, scalability affects security. Furthermore, SG consists of devices from various vendors, applications, services, protocols, and communication stacks, introducing **heterogeneity and complexity** challenges (Bekara, 2014; Arasteh *et al.*, 2016; Bedi *et al.*, 2018). The SG comprises subsystems of power systems, control systems, and communication systems. Furthermore, integrating these subsystems involves issues of information management that need to be considered, since the SG system is a system of systems (Shakerighadi *et al.*, 2018).

From a communication point of view, the challenge of **interoperability** relates to heterogeneity. SG exchanges information among many IoT devices and gateways of varying specifications. By combining the views of Bekara (2014), Risteska Stojkoska and Trivodaliev (2017), Shakerighadi et al. (2018), and Ghasempour (2019), it can be seen that interoperability may be attributed to the heterogeneity of protocols and communication stack, as discussed above. There are many separate standards for IoT devices with no unified standardisation efforts in the SG, causing interoperability issues for IoT devices (Ghasempour, 2019). For example, legacy systems cannot communicate with IP-based systems in the SG due to the lack of support for some protocols, such as TCP/IP (Bekara, 2014; Risteska Stojkoska and Trivodaliev, 2017; Shakerighadi *et al.*, 2018).

From the above, it can be concluded that the security of the SG system is affected by issues of heterogeneity, complexity, interoperability, and constrained devices. Furthermore, it is argued that centralisation may affect the availability of the system. Therefore, it is significant to remember each of these challenges alongside the others in SG implementation: for example, to maintain security it is important to consider correlated aspects.

# Future Directions

According to the challenges of Smart Grid that are identified in the last section, a list of Smart Grid requirements could be listed. As described above, it is argued that automation systems such as SCADA were designed without any regard for security (F. A. Aloul, 2012). Moreover, Modbus, which exchanges SCADA information to control industrial processes, was not intended for critical security environments such as SG (F. A. Aloul, 2012). Thus, securing the information system in SG must be assigned the highest priority, since power assets represent critical national infrastructure that may attract terrorists and state actors. Any damage, such as security attacks on the power grid, could cause chaos across whole cities. Electric Power Research Institute (ERPI) reported security is the main concern in IoT-enabled SG worldwide. Compromising the security of smart meters will mislead estimations, and an incorrect consumption estimation would lead to large financial losses (Mahmood, Ashraf Chaudhry, Naqvi, Shon, & Farooq Ahmad, 2016). Security is also important to protect the privacy of consumers and the utility.

Threat modelling is the process of analysis that allows security experts to discover the potential vulnerabilities to be addressed (Swiderski & Snyder, 2004). Threat modelling for an IoT-enabled SG during system design identifies the necessary controls and countermeasures (Khan et al., 2017): potential attacks need to be identified at the system design stage by the security designer, not the attacker (Myagmar et al., 2005).

In developing a threat model, security designers are concerned with defining threats (Myagmar et al., 2005). Security requirements can be mapped to threats to show the effect of each threat and the required security criteria of the system. It is argued that security requirements for the system can be defined clearly once the threats are identified.

# Conclusion

In this paper, the link between IoT modules and the Smart Grid is highlighted. Firstly, a comprehensive overview is given of IoT-enabled Smart Grid. Then, the challenges of the IoT- enabled Smart Grid are discussed which will help in directing future research. Finally, further threat analysis will be undertaken in future work to identify the controls required to build a secure information system for the IoT -enabled Smart Grid. This research could serve and direct the research objectives in the future.

# Acknowledgements

I sincerely acknowledge the awards of the King Abdulaziz University scholarship and the Saudi Arabian Cultural Bureau in London (SACB) for allowing the research to be funded and undertaken.

##### References

Al-Ali, A.R. and Aburukba, R. (2015) ‘Advanced role of internet of things in the smart grid technology’, Journal of Computer and Communications, pp. 229–233. doi:http://dx.doi.org/10.4236/jcc.2015.35029 Role.

Al-Omar, B., Al-Ali, A.R., Ahmed, R. and Landolsi, T. (2012) ‘The Role of Information and Communication Technologies in’, Journal of Emerging Trends in Computing and Information Sciences, 3(5), pp. 707–716.

Al-Turjman, F. and Abujubbeh, M. (2019) ‘IoT-enabled smart grid via SM: An overview’, Future Generation Computer Systems, 96, pp. 579–590. doi:10.1016/j.future.2019.02.012.

Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-Khah, M. and Siano, P. (2016) ‘Iot-based smart cities: A survey’, EEEIC 2016 - International Conference on Environment and Electrical Engineering, pp. 1–6. doi:10.1109/EEEIC.2016.7555867.

Atlam, H.F. and Wills, G.B. (2019) Technical aspects of blockchain and IoT. 1st edn, Advances in Computers. 1st edn. Elsevier Inc. doi:10.1016/bs.adcom.2018.10.006.

Banerjee, M., Lee, J. and Choo, K.K.R. (2018) ‘A blockchain future for internet of things security: a position paper’, Digital Communications and Networks, 4(3), pp. 149–160. doi:10.1016/j.dcan.2017.10.006.

Bedi, G., Venayagamoorthy, G.K., Singh, R., Brooks, R.R. and Wang, K.C. (2018) ‘Review of Internet of Things (IoT) in Electric Power and Energy Systems’, IEEE Internet of Things Journal, 5(2), pp. 847–870. doi:10.1109/JIOT.2018.2802704.

Bekara, C. (2014) ‘Security issues and challenges for the IoT-based smart grid’, Procedia Computer Science, 34, pp. 532–537. doi:10.1016/j.procs.2014.07.064.

Cisco (2013) The Internet of Everything Global Public Sector Economic Analysis. Available at: https://www.cisco.com/c/dam/en\_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf (Accessed: 26 January 2020).

Colak, I. (2016) ‘Introduction to smart grid’, 2016 International Smart Grid Workshop and Certificate Program, ISGWCP 2016, pp. 1–5. doi:10.1109/ISGWCP.2016.7548265.

Connor, P. and Fitch-Roy, O. (2019) The Socio-Economic Challenges of Smart Grids, Pathways to a Smarter Power System. Elsevier Ltd. doi:10.1016/B978-0-08-102592-5.00014-4.

Dalipi, F. and Yayilgan, S.Y. (2016) ‘Security and privacy considerations for IoT application on smart grids: Survey and research challenges’, Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016, pp. 63–68. doi:10.1109/W-FiCloud.2016.28.

DeBlasio, R. and Tom, C. (2008) ‘Standards for the smart grid’, 2008 IEEE Energy 2030 Conference, ENERGY 2008, (November), pp. 1–7. doi:10.1109/ENERGY.2008.4780988.

EPRI (2005) EPRI | SmartGrid Resource Center. Available at: https://smartgrid.epri.com/ (Accessed: 7 January 2020).

ETP (2006) Smart Grids European Technology Platform-EARPA. Available at: https://www.earpa.eu/earpa/39/etp\_smartgrids.html.

Flick, T. and Morehouse, J. (2011) ‘Threats and Impacts: Consumers’, pp. 19–33. doi:10.1016/B978-1-59749-570-7.00002-9.

Ganguly, P., Nasipuri, M. and Dutta, S. (2019) ‘Challenges of the Existing Security Measures Deployed in the Smart Grid Framework’, Proceedings of 2019 the 7th International Conference on Smart Energy Grid Engineering, SEGE 2019, pp. 1–5. doi:10.1109/SEGE.2019.8859917.

Ghasempour, A. (2016) ‘Optimized Advanced Metering Infrastructure Architecture of Smart Grid based on Total Cost , Energy , and Delay’, 2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–6. doi:10.1109/ISGT.2016.7781250.

Ghasempour, A. (2019) ‘Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges’, Inventions, 4(1). doi:10.3390/inventions4010022.

Gungor, V.C., Lu, B., Member, S., Hancke, G.P. and Member, S. (2010) ‘Opportunities and Challenges of Wireless Sensor Networks in Smart Grid’, 57(10), pp. 3557–3564.

Hu, J. and Vasilakos, A. V. (2016) ‘Energy Big Data Analytics and Security: Challenges and Opportunities’, IEEE Transactions on Smart Grid, 7(5), pp. 2423–2436. doi:10.1109/TSG.2016.2563461.

IEEE (2018) About - IEEE Smart Grid. Available at: https://smartgrid.ieee.org/about-ieee-smart-grid (Accessed: 4 December 2019).

IET (2013) What is a Smart Grid?

IoTSF (2020) Best Practice Guidelines 2 – IoT Security Foundation. Available at: https://www.iotsecurityfoundation.org/best-practice-guidelines/ (Accessed: 23 July 2020).

Jenkins, N., Long, C. and Wu, J. (2015) ‘Smart Grid — Review An Overview of the Smart Grid in Great Britain’, Engineering, 1(4), pp. 413–421. doi:10.15302/J-ENG-2015112.

Kaur, M. and Kalra, S. (2016) ‘A Review on IOT Based Smart Grid’, International Journal of Energy, Information and Communications, 7(3), pp. 11–22. doi:10.14257/ijeic.2016.7.3.02.

Khan, R., Mclaughlin, K., Laverty, D. and Sezer, S. (2017) ‘STRIDE-based Threat Modeling for Cyber-Physical Systems’, pp. 0–5.

Al Khuffash, K. (2018) Smart grids—Overview and background information, Application of Smart Grid Technologies. Elsevier Inc. doi:10.1016/b978-0-12-803128-5.00001-5.

Kimani, K., Oduol, V. and Langat, K. (2019) ‘Cyber security challenges for IoT-based smart grid networks’, International Journal of Critical Infrastructure Protection, 25, pp. 36–49. doi:10.1016/j.ijcip.2019.01.001.

Mahmood, K., Ashraf Chaudhry, S., Naqvi, H., Shon, T. and Farooq Ahmad, H. (2016) ‘A lightweight message authentication scheme for Smart Grid communications in power sector’, Computers and Electrical Engineering, 52, pp. 114–124. doi:10.1016/j.compeleceng.2016.02.017.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. and Aharon, D. (2015) Unlocking the potential of the Internet of Things | McKinsey &amp; Company, McKinsey.

Martins, J.F., Pronto, A.G., Delgado-Gomes, V. and Sanduleac, M. (2019) ‘Smart Meters and Advanced Metering Infrastructure’, in Pathways to a Smarter Power System, pp. 89–114. doi:10.1016/b978-0-08-102592-5.00004-1.

Mohassel, R.R., Fung, A., Mohammadi, F. and Raahemifar, K. (2014) ‘A survey on Advanced Metering Infrastructure’, International Journal of Electrical Power and Energy Systems, 63, pp. 473–484. doi:10.1016/j.ijepes.2014.06.025.

Mollah, M.B., Zhao, J., Niyato, D., Lam, K.-Y., Zhang, X., Ghias, A.M.Y.M., Koh, L.H. and Yang, L. (2020) ‘Blockchain for Future Smart Grid: A Comprehensive Survey’, IEEE Internet of Things Journal, X(vi), pp. 1–1. doi:10.1109/jiot.2020.2993601.

Mrabet, Z. El, Kaabouch, N., Ghazi, Hassan El and Ghazi, Hamid El (2018) ‘Cyber-security in smart grid: Survey and challenges’, Computers and Electrical Engineering, 67, pp. 469–482. doi:10.1016/j.compeleceng.2018.01.015.

Mugunthan, S.R. and Vijayakumar, D.T. (2019) ‘REVIEW ON IOT BASED SMART GRID ARCHITECTURE IMPLEMENTATIONS’, 01(01), pp. 12–20.

NIST (2014) NIST Special Publication 1108R3 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, NIST Special Publication. doi:10.6028/NIST.SP.1108r3.

Pour, M.M., Anzalchi, A. and Sarwat, A. (2017) ‘A review on cyber security issues and mitigation methods in smart grid systems’, Conference Proceedings - IEEE SOUTHEASTCON, pp. 17–20. doi:10.1109/SECON.2017.7925278.

PTI (2011) Smart Grid 101 for Local Governments.

Rahman, S. (2009) ‘Smart grid expectations: What will make it a reality’, IEEE Power and Energy Magazine, 7(5). doi:10.1109/MPE.2009.933415.

Reka, S.S. and Dragicevic, T. (2018) ‘Future e ff ectual role of energy delivery : A comprehensive review of Internet of Things and smart grid’, Renewable and Sustainable Energy Reviews, 91(April), pp. 90–108. doi:10.1016/j.rser.2018.03.089.

Risteska Stojkoska, B.L. and Trivodaliev, K. V. (2017) ‘A review of Internet of Things for smart home: Challenges and solutions’, Journal of Cleaner Production, 140, pp. 1454–1464. doi:10.1016/j.jclepro.2016.10.006.

Sagiroglu, S., Terzi, R., Canbay, Y. and Colak, I. (2017) ‘Big data issues in smart grid systems’, 2016 IEEE International Conference on Renewable Energy Research and Applications, ICRERA 2016, 5, pp. 1007–1012. doi:10.1109/ICRERA.2016.7884486.

Sajid, A., Abbas, H. and Saleem, K. (2016) ‘Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges’, IEEE Access, 4, pp. 1375–1384. doi:10.1109/ACCESS.2016.2549047.

Saleem, Y., Crespi, N., Rehmani, M.H. and Copeland, R. (2019) ‘Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions’, IEEE Access, 7, pp. 62962–63003. doi:10.1109/ACCESS.2019.2913984.

Shakerighadi, B., Anvari-Moghaddam, A., Vasquez, J.C. and Guerrero, J.M. (2018) ‘Internet of things for modern energy systems: State-of-the-art, challenges, and open issues’, Energies, 11(5). doi:10.3390/en11051252.

Singer, J. (2009) Enabling Tomorrow’s Electricity System: Report of the Ontario Smart Grid Forum.

Sortomme, E., Hindi, M.M., MacPherson, S.D.J. and Venkata, S.S. (2011) ‘Coordinated charging of plug-in hybrid electric vehicles to minimize distribution system losses’, IEEE Transactions on Smart Grid, 2(1), pp. 186–193. doi:10.1109/TSG.2010.2090913.

U.S. Department of energy (2018) Smart Grid System Report: 2018 Report to Congress.

US Public Law (2007) Energy independence and security act of 2007, US Government Printing Office.

Wang, Q., Tai, W., Tang, Y. and Ni, M. (2019) ‘Review of the false data injection attack against the cyber-physical power system’, IET Cyber-Physical Systems: Theory and Applications, 4(2), pp. 101–107. doi:10.1049/iet-cps.2018.5022.

Yang, Q. (2019) ‘Internet of things application in smart grid: A brief overview of challenges, opportunities, and future trends’, in Smart Power Distribution Systems. doi:10.1016/b978-0-12-812154-2.00013-4.