Security and Privacy issues in IoT based Smart Grids: A case study in a digital substation

Doney Abraham[1], Sule Yildirim Yayilgan[1], Mohamed Abomhara[1], Alemayehu Gebremedhin[2], and Fisnik Dalipi[3]

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway
{doney.abraham, sule.yildirim, mohamed.abomhara}@ntnu.no
[2] Department of Manufacturing and Civil Engineering, Norwegian University of Science and Technology, Norway
alemayehu.gebremedhin@ntnu.no
[3] Department of Informatics, Linnaeus University, Sweden
fisnik.dalipi@lnu.se

Abstract. Smart Grid is one of the increasingly used critical infrastructure that is essential for the functioning of a country. This coupled with Internet of Things (IoT) has huge potentials in several areas such as remote monitoring and managing of electricity distribution, traffic signs, traffic congestion, parking spaces, road warnings and even early detection of power influxes as a result of natural disasters, safety failures, equipment failures or carelessness. Despite the advantages of Smart Grids, there are security threats, privacy concerns and several open challenges related to Smart Grids. This chapter seeks to provide a review of the security and privacy perspectives inherent in IoT enabled Smart Grids. Firstly, the chapter explores the functionalities of Smart Grids as opposed to a traditional grid. Next the chapter provides an overview of Smart Grid architectures followed by positioning IoT concept into Smart Grid with a focus on architectures. Then, the proposed approach for identifying threats and attacks in IoT enabled Smart Grid, namely the security pyramid is presented. Lastly, we work on identifying the possible threats and attacks in the digital substation use case.

Keywords: Smart Grid; IoT; Security; Privacy; Attacks; Threats; Cyber-Physical systems

1 Introduction

The world is increasingly moving towards an Internet of Things (IoT) age and the importance of Cyber-Physical systems are ever rising [56]. IoT support numerous applications in different domains such as power grids, transportation systems, health care, water supply, oil and gas distribution and telecommunications that are crucial for the operation of society [44]. Since the critical infrastructure of a country such as energy, food, transport, telecommunications, healthcare, banking and finance depends on the previous mentioned domains, its security and privacy

are of utmost importance. Smart Grids based on IoT and data technologies have revolutionized the way power grids are built as opposed to traditional grids by providing features such as self-healing, bi-directional communication, feedback and disaster recovery plans [45]. Introduction of IoT to Smart Grids has made the power grids even more reliable and can be used to monitor electricity generation, protection of transmission line, ability by consumers to monitor usage by smart meters to name a few [3,13]. Globally, IoT is estimated to have a total economic impact of around USD 11 trillion by 2025 [23, 31]. Since IoT is a collection of different types of smart devices, it is also vulnerable to different types of security and privacy threats [9]. Some research works already focus on security and privacy challenges in IoT integrated Smart Grids [7,19,28,46,47,51]. In this chapter, we provide a review of these challenges.

The remaining parts of the chapter are structured as follows: Section 2 explains the overall architecture of a Smart Grid and shows the National Institute of Standards and Technology (NIST) conceptual model. An overview of IoT and its integration in Smart Grids with some proposed architectures are shown in Section 3. Further in Section 4, the security pyramid for analyzing use cases is proposed. Section 5 focus on applying and explaining the use of security pyramid on a digital substation use case. Conclusions are drawn in Section 6.

2 Overview of Smart Grid: Architecture

This section focuses on the overview of Smart Grid and its building blocks. It describes the architecture and shows the differences between traditional power grids and the advantages of Smart Grids.

A traditional power grid is one of the most complex critical infrastructures that has been ever build [34]. It consists of different parts like operations center, power generation plants, transmission towers and power distribution centers which are physically connected by cables and wires [41]. The main functions of a power grid are electricity generation, transmission and its distribution. Electricity is mostly generated utilizing central power plants using different energy sources and then transmitted to different load customers through high voltage lines. This in turn is distributed to consumers using distribution centers at a lower voltage [4]. Transmission and distribution of electricity are owned by power companies which make profit from the consumers. The electricity and information flow in a traditional power grid are uni-directional [41] which results in lack of flexibility, lack of information sharing to customers and control mechanisms that respond slowly in the event of power failures or attacks to the power grid. Traditional grids also lack self-healing and self-restoring capability in case of a down time [14]. Additionally, due to the high usage of electronic devices, traditional power grids have a large amount of wastage of resources due to inefficient distribution of electricity, lack of monitoring and communication and inadequate methods to store energy. All these coupled together has led to the introduction of Smart Grids.

Smart Grids enable the integration of both cyber and physical systems in the sense that Information and Communications Technology (ICT) is integrated with power networks to enable generation, transmission and distribution of electricity in a more efficient manner [55]. Following are some of key features and characteristics of a Smart Grid [22, 36]:

1. Information and electricity flow are bidirectional.
2. Robust and uninterrupted power supply as Smart Grid has self-healing capabilities that enable real time state monitoring to analyze faults and respond to them.
3. Integrates modern advanced sensor technology, measurement technology, communication technology, information technology, computing technology, and control technology.
4. Optimizes asset utilization and operates efficiently by reducing the cost of operations and investments. This is done by aptly managing power loss and improving power efficiency.
5. Operates resiliently against attacks and natural disasters
6. Interoperable as it enables logical grouping of standards among diverse components of the Smart Grid.
7. Enables active participation by customers, new products, services, and markets.

2.1 The NIST Conceptual model of Smart Grid

The main domains in NIST conceptual model as described by [11] are as follows:

1. **Power Generation**: This is domain where energy is generated in large quantities from different sources like wind, hydro, solar, biomass etc. and converted to electricity. These are normally linked straight to transmission systems that in turn offer applications smart in nature.
2. **Transmission**: Electricity is transmitted from the sites of bulk generation to long distances to the substations of areas where electricity demand is higher.
3. **Distribution**: This is the domain where electricity is distributed to customers.
4. **Consumer**: This is the domain where the electricity is consumed, managed and generated in some cases (e.g., Smart houses with solar panels). Consumer domain is sub-categorized into individual houses, commercial/building and industrial complexes with varying energy needs for each of these categories.
5. **Service Provider**: This provides services to business processes of power system producers, customers and distributors. These are utility services such as electricity billing, managing customer accounts, management of energy use in homes etc.
6. **Operations**: Operations domain ensure continuous functioning of the power system. The typical applications of operations domain are network operation monitoring including breaker and switch states, fault management

(identification of faults, informing customers, coordination), maintenance and construction (inspection, cleaning and adjustment of equipment), customer support for purchase, provision and troubleshooting of power system services etc.

7. **Markets**: This is the domain where power grid assets are traded. The supply/demand and prices are exchanged in this domain.

The following section focuses on the integration of IoT in Smart Grids.

3 IoT in Smart Grid

IoT in broad terms are all devices that are interconnected and communicate over internet [17]. IoT devices are broadly scattered with low storage capability, processing capabilities that can improve performance, security and reliability. Some examples of IoT devices are smart mobile phones, smart fridge, smart meters to measure power consumption, automobiles, smart buildings to name a few [1, 17]. Figure 1 shows a high level overview of IoT features [53]. It shows a communication dimension that can be maintained by anyone irrespective of the location of the person.

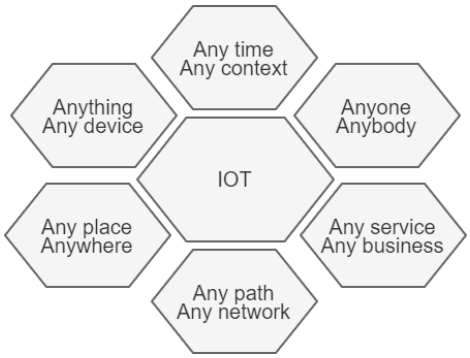

Fig. 1: IoT features

IoT technology has an important role in building Smart Grid infrastructure. Some of its usages are as follows [15]:

1. Monitoring electricity generation in power plants that operate with coal, wind, solar, biomass. It can help calculate the energy demands of customers and store energy accordingly. This facilitates efficient use of energy at a later stage when demand is higher.
2. Monitoring and protecting power transmission lines, controlling the devices (e.g., temperature, current, voltage sensors) used for transmission and assessing the power consumption.

3. From a consumer point, IoT have various uses like smart meters to monitor power usage, control charging of electric vehicles, scheduling the energy use among IoT devices in a household and to ensure the continuous connectivity across networks.

Table 1 shows some of the IoT architectures utilized in Smart Grids which vary in layers they are built of. The proposed architectures are either three or four layered. Architecture 1 has three layers namely perception, network and application layer [15,30,33]. Perception layer collects data using various sensors, tags, readers. Network layer maps data gathered by perception layer to different communication protocols using wired or industry standard wireless networks. The industry standards include 3G, 4G, 5G, broadband, Zigbee or Wi-Fi and these further transmit data to application layer that can monitor the IoT devices in real time. Application layer contains an application structure that can compute and process information and enable interfacing and integration.

Table 1: IoT architectures in Smart Grid proposals [15]

Layers/ Architectures	Architecture 1	Architecture 2	Architecture 3	Architecture 4
Layer 4		Application	Social	Master station system
Layer 3	Application	Cloud management	Application	Remote communication
Layer 2	Network	Network	Network	Field network
Layer 1	Perception	Perception	Perception	Terminal

Architecture 2 has four layers namely perception, network, cloud management and application layer [15,50]. Here the perception layer consists of two additional layers that include a thing layer that comprises of different IoT sensors, tags, readers to sense, control, collect data and a gateway layer that comprises of microcontrollers and displays that controls elements connecting to the thing layer. As in previous case, the network layer transmits data from perception to application layer which in-turn can provide services to consumers like manage energy pricing. Cloud management layer stores and analyses data and also manages users.

Architecture 3 in Table 1 has four layers as perception, network, application layer and a social layer [15]. The social layer integrates and regulates various IoT applications in terms of laws and regulations relevant for IoT devices, government and public management. Architecture 4 in Table 1 has a terminal, field network, remote communication and master station system layer [15]. The terminal layer consists of remote units, smart devices and smart meters; different communication channels like optic fiber, Wi-Fi, Zigbee etc. for field network layer; 3G, 4G, 5G or wired communication from the remote communication layer; control systems for Smart Grids for master station layer.

Even though IoT technologies are being adopted in Smart Grids, there are security and privacy challenges which need to be addressed. Communication in IoT enabled Smart Grids is conducted over the open Internet which is already vulnerable to cyber attacks [5]. Various approaches, measures and recommendations are proposed in the literature to tackle these challenges [12, 35, 40]. Besides, the diversity of devices and applications in Smart Grids adds upto the complexity of handling these challenges. In order to leverage the full capability of IoT integration, there is a need to clearly understand and locate these challenges in IoT enabled Smart Grid. Based on the literature and in cooperation with partners of digital substation (DS) projects, we have identified several challenges [2, 6, 8, 10, 12, 16, 20, 24, 25, 29, 32, 37–39, 42, 48, 49, 52, 54, 57].

4 The Proposed Approach for Use Case Analysis: The Security Pyramid

In this chapter, we propose the Security Pyramid (Figure 2) as an approach for identifying and analyzing threats and attacks in case studies of IoT enabled Smart Grid. First and foremost, such an identification and analysis require setting the security objectives that stakeholders of an IoT enabled Smart Grid e.g., digital substation prioritize to comply with (Peak of the pyramid). Next, in the middle layer of the pyramid, threats and attacks categories which particularly fall under the set objectives are identified. As the last step, in the bottom layer of the pyramid, actual threats and attacks which are identified for each attack and threat category are defined for the case study in hand.

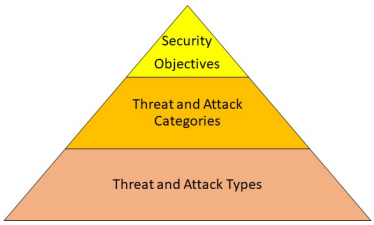

Fig. 2: The Proposed Security Pyramid

4.1 Security Objectives

In a power grid, the effective security objects and their descriptions are provided in this section.We assume the same security objectives hold for the IoT enabled Smart Grid. NIST has defined certain criteria to maintain the security and privacy of Smart Grids. These are Confidentiality, Integrity and Availability (CIA) principles [18]. Confidentiality is information protection from access without a

proper authorization. Integrity is the assurance of information not being modified without authorization. Availability guarantees that data, applications and resources are available to authorized users whenever they need them.

4.2 Threat and Attack Categories in IoT enabled Smart grids

In the previous sections, we have referred to the importance of ensuring security and privacy of Smart Grids. Besides, IoT devices are particularly vulnerable to security and privacy threats. In this section, we provide a summary of the threats and attacks that are likely to occur in Smart Grids, in IoT integrated Smart Grid architectures and in standalone IoT architectures and the IoT devices in them.

4.2.1 Data Manipulation: These are the types of data integrity threats where unauthorized users aim to mislead the Smart Grids towards making wrong actions. For example, an adversary can illegally manipulate a smart meter in order to modify energy consumption to decrease cost during the peak demands [8]. Another example is when an attacker accesses an unprotected substation and uses his/her own device to influence the communication among substation assets. This way, attacker is able to inject false data into the communication channels.

Solution: In the examples given above, data integrity is affected [24, 48]. We need to ensure that the communication channels, whether in a substation, or in an IoT infrastructure or in IoT devices (such as smart meters) are not manipulated or compromised by unauthorized parties. One method of ensuring integrity of Smart Grids is implementing different kinds of intrusion detection algorithms in order to prevent data manipulation attacks [10, 52]. Machine learning based models and other false data filtering schemes should be researched, developed and applied to detect such attacks in Smart Grids. This in turn will help to achieve sufficient data integrity levels [2, 20, 32].

4.2.2 Unauthorized Access of Data: It is important that data is available only to authorized users throughout the entire communication process in Smart Grids. It is very critical that data collected via IoT sensors will not be used to uncover information to anyone except for the Smart Grid operators. Otherwise, the confidentiality of data is lost.

Solution: For the purpose of achieving confidentiality of data, data acquisition frameworks which are confidentiality assured, secure key management, access control and trust management mechanisms are proposed [57]. Providing integrity and encryption of the data from IoT devices used by consumers ensures Confidentiality [49].

4.2.3 Attacks due to Unauthorized Access of Users or Devices

1. **Attacks due to unauthorized access of devices to IoT enabled Smart Grid:** It is important that only authorized devices and applications can be connected to IoT. For example, all the laptops located in a digital substation should be authorized to connect to digital substation whereas any other laptops which are in the digital substation accidentally or on malicious intentions should not connect to the digital substation. The process of authentication ensures that information distributed in the Smart Grid network is legitimate.

   Solution: Authenticity of devices is an integrity problem. The identity of any IoT device being used in context should be timely authenticated in order to escape any potential manipulation of the system. Nevertheless, in the time sensitive and traffic intensive nature of IoT based Smart Grid communications, authentication of data and object (e.g., smart meter) is an intricate mission and more research is needed in this direction [38,42]. Still, if the authenticity of the devices is guaranteed but the user accesses more than what he/she is authorized for, then the confidentiality is compromised (elevation of privilege). Elevation of privilege is a big threat of "insider users".

2. **Attacks due to unauthorized access of users to devices:** Data and network objects, such as smart meters, transformers and cables are available only for authorized users and services upon request. Authorized access can occur due to many facts such as failure of a device, user gets access because of elevation of privilege, errors in the access control mechanisms and policies, loss of device or use of fake device in the system etc.

   Solution: Authorization and access control is a solution here. Granting access privileges to Smart Grid devices and functionalities can significantly reduce the probability of unauthorized and malicious access to network devices. As indicated in the literature, restricting access to objects through for example Role Based Access Control (RBAC) [43] or/and attribute-based access control (ABAC) [21] can enhance the system reliability by eliminating potential cyber threats [12]. Since the controlling of IoT enabled Smart Grid is performed remotely over the open Internet, access control mechanisms are instrumental in order to prevent and restrain users or devices access in the network.

   In a complex and interaction intensive IoT enabled Smart Grids, it is vital to enforce security and privacy objectives among different types of objects, layers and applications [6]. Trust is an assured reliance on a claimed identity and assured reliance comes in the form of authentication/authorization. Authentication/Authorization can in turn be used to prevent unauthorized access. Providing trust management to millions of IoT devices and ensuring trusted governance of IoT device ownership remain as one of the open issues for future research to be addressed.

4.2.4 Threats on the Privacy of Customers: Smart Grid network resources contain private information of millions of users, including energy consumption and consumption patterns of users. Such information not only can be used for marketing purposes but also could provide clear indications to intruders about whereabouts of the consumers.

Solution: To ensure privacy and protection of personal information from unauthorized access or misuse, secure access to data for IoT enabled Smart Grids should be enforced by constantly adapting encryption mechanisms and privacy preservation schemes.

4.3 Attack and Threat Types

Depending on the use case, the actual attacks and threats are identified and they are linked to the attack and threat categories in the middle layer. Particularly, a close cooperation is required with the stake holders of the case study in order to be able to identify the assets and the attacks and threats that can occur along these assets.

5 A case study: Digital Substation

In this section, we examine digital substation as a case study for identifying possible threats and attacks in this particular critical infrastructure. A digital substation is both a physical and soft infrastructure. Below are the three steps followed in the case study.

5.1 Step 1

All the three security objectives, Confidentiality, Integrity and Availability are recognized and acknowledged by the stakeholder of a digital substation. Even though, a digital substation composes of a generic infrastructure, we particularly focus on the digital substations in Norway within the scope of the ECoDiS (Engineering and Condition monitoring in Digital Substations) project[4]. There are three pilot sites in the project from Norway: Furuset substation owned by Statnett SF - Statelig Foretak, Hafslund, and Skagerak substations.

5.2 Step 2

All the attack categories from the previous section are valid for examination for digital substation, particularly for our pilots, namely:
1) Data manipulation
2) Unauthorized access of data
3) Attacks due to unauthorized access of users or devices
4) Attacks on the Privacy of customers

[4] `https://www.sintef.no/en/projects/2019/ecodis/`

5.3 Step 3

In our previous work [27] [26], we have identified some attacks and developed a generic map of these attacks in digital substation pilots as shown in Figure 3. The identified assets in this digital substation pilots are SCADA (Supervisory Control And Data Acquisition), Gateway, IED (Intelligent Electronic Device), HMI (Human Machine Interface), Communication Network, MU (Merging Unit), Switch and NCIT - CT&VT (Non Conventional Instrument Transformers - Current and Voltage Transformer).

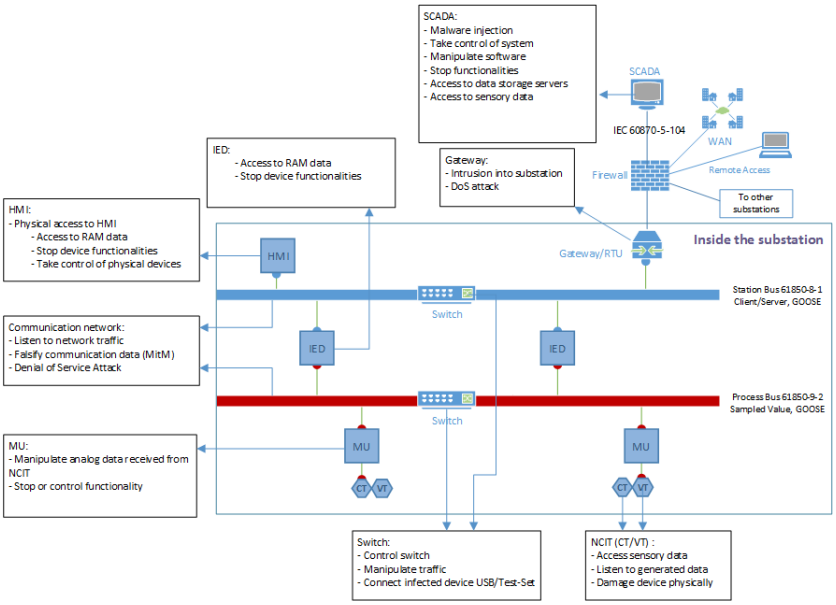

Fig. 3: Revised version of the map of possible attacks in digital substation from [27]

Now we will link each of the identified attacks in the map into categories in the middle layer of the security pyramid, by listing each asset and clarifying how each asset is identified under one or more of the attack and threat categories of the middle layer. These are elaborated in the following section.

5.3.1 Smart Grid Threat and Attack Categories vs. Attacks on DS

1. **SCADA:** Malware software can be designed to steal/copy data from devices and it does not only manipulate the data. In this case, if a Malware managed to access to data for unauthorized access, then the privacy of users is violated. If users gain an unauthorized access to a device, then they might

take a control of the system e.g., taking control of SCADA system. Manipulated software will produce manipulated data. Changing control data can stop functionality in the system, Access to data storage can lead to data manipulation. For example, if you manage to access to data in servers, you can change anything there. The type of sensory data is in a SCADA system can be temperature values from transformers, humidity of the devices etc.

2. **Gateway:** Attackers can use DoS attack on gateways to make system resource and system functionalities unavailable. We relate this to unauthorized access of users to devices.

3. **IED:** One of the ways an attacker can gain unauthorized access to IEDs is using brute force attack. An attacker can then access the data in RAM of the IED and depending on type of data in the RAM privacy may be influenced. The attacker can also stop the device functionalities by manipulating different data parameters.For example, modifying the messages from IEDs can mislead the operators about the actual state of DS.

4. **HMI:** By gaining access to HMI, an attacker can take control of the physical devices, stop the device functionalities and also gain access to RAM data. Depending on the type of data in RAM, it can also influence privacy.

5. **Communication Network:** Depending on the type of data listened to in the network traffic, data privacy may be influenced. This can be caused by Man-in-the-Middle (MitM) attack. A DoS attack here can make system resource and system functionalities unavailable. We relate this to unauthorized access of users to devices.

6. **MU:** By gaining access to MU, an attacker can control different functionalities in the MU. Data received from NCIT can also be manipulated with this attack.

7. **Switch:** The switches on the station bus and/or process buss can be controlled with this attack. If the attacker manages to manipulate the traffic in these switches, the might gain unauthorized access to data. Attacker can then for example redirect traffic to the server.

8. **NCIT - CT&VT:** Attacker here can gain access to different data from the sensors like current or voltage measurements and can physically damage the devices. Once the access is gained, then different values in the sensors can be manipulated causing disruptions to services and sending incorrect values further to other devices in the substation.

The results of the above categorization is shown in Table 2. The classification on the table will be used to identify the risk of these attack goals. Based on this identified risks and in co-ordination with the project partners, we plan to mitigate the risks based on their priorities.

Table 2: Classification of Attack and Threat Types from Digital Substation into Attack and Threat Categories

Smart grid threat and attack categories			Data manipulat-ion attacks	Unauthorized access of data	Unauthorized access of devices or users		Attacks on the privacy	Disruption attacks
DS Assets	Asset Access Type	Attack/Threat Types			Unauthorized access of devices to smart grid	Unauthor-ized access of users to devices		
SCADA	Gaining access to SCADA	Malware injection	X	X	X	X	X	
		Take control of system			X	X		X
		Manipulate software	X	X		X		
		Stop functionality	X			X		X
		Access to data storage servers	X	X			X	
		Access to sensory data		X				
Gateway	Access to Gateway	Intrusion into Substation		X		X		
		Denial of Service Attack						X
IED	Access to IED	Access to RAM data	X	X		X	X	
		Stop device functionalities	X			X		X
HMI	Physical access to HMI	Access to RAM data		X		X		
		Stop device functionalities	X		X	X		X
		Take control of physical devices	X	X		X	X	X
Communication Network	Access to Commun-ication Network	Listen to Network traffic		X			X	
		Falsify Communication data (MiMt)	X	X				
		Denial of Service Attack						X
MU	Access to MU	Manipulate analog data received from NCIT	X	X		X		
		Stop or control functionality	X			X		X
Switch	Access to Switch	Control the Switch				X		
		Manipulate Traffic	X	X	X		X	X
		Connect infected device (e.g. USB)	X	X		X	X	
NCIT (CT\VT)	Access to NCIT (CT/VT)	Access to sensory data		X				
		Listen to generated data		X			X	
		Damage device physically				X		

6 Conclusions

In this chapter, firstly we have given an overview of Smart Grid architectures. Next we discussed how IoT is integrated into Smart Grid with a focus on layered IoT architectures. Understanding and locating such attacks in a digital substation as a case study are essential in protecting Smart Grids. Consequently through such understanding, and analysis, confidentiality, integrity and availability of data in Smart Grids can be maintained. For that reason, we introduce the security pyramid as a proposal for examining and analyzing attacks and threats in IoT enabled Smart Grid use cases. For a given use case, pilot digital substations of the ECoDiS project in Norway, we have outlined attack and threat types that are likely to occur in IoT enabled Smart Grids using the security pyramid. Further works will involve (but not limited to) generating normal data based on the DS architecture as in Figure 3 and then simulating various DS attacks listed in Table 1. As part of future work, there will also be studies conducted on the different methods to detect these attacks.

The following abbreviations are used in this manuscript:

CIA	Confidentiality, Integrity and Availability
CT	Current Transformer
DMS	Distribution Management Systems
DoS	Denial of Service
DS	Digital Substation
ECoDiS	Engineering and Condition monitoring in Digital Substations
EMS	Energy Management Systems
HMI	Human Machine Interface
ICT	Information and Communications Technology
IED	Intelligent electronic device
IoT	Internet of Things
MAC	Mandatory Access Control
MitM	Man-in-the-Middle
MU	Merging Unit
NCIT	Non Conventional Instrument Transformers
NIST	National Institute of Standards and Technology
RAM	Random Access Memory
RBAC	Role Based Access Control
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
VT	Voltage Transformer

ACKNOWLEDGEMENTS

This work is partly carried out in the Engineering and Condition monitoring in Digital Substation (ECoDiS) which is a project funded by Research Council of Norway (NFR), Innovation Project for the Industrial Sector - ENERGIX

program, project number 296550, coordinated by Statnett RD group. Statnett is the system operator of the Norwegian power system. The project aims in exploiting the full potential of a digital station to increase security of supply, observability and reduce costs in a changing energy system.

References

1. Abdul-Qawy, A.S., Pramod, P., Magesh, E., Srinivasulu, T.: The internet of things (iot): An overview. International Journal of engineering Research and Applications **1**(5), 71–82 (2015)
2. Ahmed, S., Lee, Y., Hyun, S., Koo, I.: Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. IEEE Transactions on Information Forensics and Security **14**(10), 2765–2777 (2019)
3. Al-Turjman, F., Abujubbeh, M.: Iot-enabled smart grid via sm: An overview. Future Generation Computer Systems **96**, 579–590 (2019)
4. Ali, A.S.: Smart grids: opportunities, developments, and trends. Springer Science & Business Media (2013)
5. Aloul, F., Al-Ali, A., Al-Dalky, R., Al-Mardini, M., El-Hajj, W.: Smart grid security: Threats, vulnerabilities and solutions. International Journal of Smart Grid and Clean Energy **1**(1), 1–6 (2012)
6. Andrea, I., Chrysostomou, C., Hadjichristofi, G.: Internet of things: Security vulnerabilities and challenges. In: 2015 IEEE Symposium on Computers and Communication (ISCC). pp. 180–187. IEEE (2015)
7. Asghar, M.R., Dán, G., Miorandi, D., Chlamtac, I.: Smart meter data privacy: A survey. IEEE Communications Surveys & Tutorials **19**(4), 2820–2835 (2017)
8. Bekara, C.: Security issues and challenges for the iot-based smart grid. In: FNC/MobiSPC. pp. 532–537 (2014)
9. Boroojeni, K.G., Amini, M.H., Iyengar, S.: Overview of the security and privacy issues in smart grids. In: Smart grids: security and privacy issues, pp. 1–16. Springer (2017)
10. CHEN, D.d., LI, Z.q., Tian, L., TENG, M.x., Feng, X.: Big data based intrusion detection of smart meters. DEStech Transactions on Computer Science and Engineering (cnsce) (2017)
11. Cunjiang, Y., Huaxun, Z., Lei, Z.: Architecture design for smart grid. Energy Procedia **17**, 1524–1528 (12 2012). https://doi.org/10.1016/j.egypro.2012.02.276
12. Dalipi, F., Yayilgan, S.Y.: Security and privacy considerations for iot application on smart grids: Survey and research challenges. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). pp. 63–68. IEEE (2016)
13. Fadlullah, Z.M., Pathan, A.S.K., Singh, K.: Smart grid internet of things. Mobile Networks and Applications **23**(4), 879–880 (2018)
14. Fang, X., Misra, S., Xue, G., Yang, D.: Smart grid—the new and improved power grid: A survey. IEEE communications surveys & tutorials **14**(4), 944–980 (2011)
15. Ghasempour, A.: Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. Inventions **4**(1), 22 (2019)
16. Gunduz, M.Z., Das, R.: Cyber-security on smart grid: Threats and potential solutions. Computer Networks **169**, 107094 (2020)

17. Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., Henry, J.: IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things. Cisco Press (2017)
18. Harvey, M., Long, D., Reinhard, K.: Visualizing nistir 7628, guidelines for smart grid cyber security. In: 2014 Power and Energy Conference at Illinois (PECI). pp. 1–8. IEEE (2014)
19. He, H., Yan, J.: Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Physical Systems: Theory & Applications **1**(1), 13–27 (2016)
20. He, Y., Mendis, G.J., Wei, J.: Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. IEEE Transactions on Smart Grid **8**(5), 2505–2516 (2017)
21. Hu, V.C., Ferraiolo, D., Kuhn, R., Friedman, A.R., Lang, A.J., Cogdell, M.M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K., et al.: Guide to attribute based access control (abac) definition and considerations (draft). NIST special publication **800**(162) (2013)
22. Jain, A.: Changes and challenges in smart grid towards smarter grid (12 2016). https://doi.org/10.1109/ICEPES.2016.7915907
23. Jha, R.S., Sahoo, P.R.: Internet of things (iot)–enabler for connecting world. In: ICT for Competitive Strategies: Proceedings of 4th International Conference on Information and Communication Technology for Competitive Strategies (ICTCS 2019), December 13th-14th, 2019, Udaipur, India. p. 1. CRC Press (2020)
24. Karimipour, H., Dinavahi, V.: On false data injection attack against dynamic state estimation on smart power grids. In: 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE). pp. 388–393. IEEE (2017)
25. Khan, M.A., Salah, K.: Iot security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems **82**, 395–411 (2018)
26. Khodabakhsh, A., Yayilgan, S.Y., Abomhara, M., Istad, M., Hurzuk, N.: Cyber-Risk Identification for a Digital Substation. ACM (2020). https://doi.org/https://doi.org/10.1145/3407023.3409227
27. Khodabakhsh, A., Yildirim Yayilgan, S., Houmb, S.H., Hurzuk, N., Foros, J., Istad, M.K.: Cyber-Security Gaps in a Digital Substation: From Sensors to SCADA (2020). https://doi.org/10.1109/MECO49872.2020.9134350
28. Komninos, N., Philippou, E., Pitsillides, A.: Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials **16**(4), 1933–1954 (2014)
29. Li, S., Song, H., Iqbal, M.: Privacy and security for resource-constrained iot devices and networks: research challenges and opportunities (2019)
30. Mauri, J.L., Tomás, J., Canovas, A., Parra, L.: An integrated iot architecture for smart metering. IEEE Communications Magazine **54**, 50–57 (2016)
31. Ménard, A.: How can we recognize the real power of the internet of things? — mckinsey. `https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-can-we-recognize-the-real-power-of-the-internet-of-things#` (November 2017), (Accessed on 10/18/2020)
32. Ni, J., Zhang, K., Alharbi, K., Lin, X., Zhang, N., Shen, X.S.: Differentially private smart metering with fault tolerance and range-based filtering. IEEE Transactions on Smart Grid **8**(5), 2483–2493 (2017)
33. Ou, Q., Zhen, Y., Li, X., Zhang, Y., Zeng, L.: Application of internet of things in smart grid power transmission. pp. 96–100 (06 2012). https://doi.org/10.1109/MUSIC.2012.24

34. Pagani, G.A., Aiello, M.: The power grid as a complex network: a survey. Physica A: Statistical Mechanics and its Applications **392**(11), 2688–2700 (2013)
35. Parra, G.D.L.T., Rad, P., Choo, K.K.R.: Implementation of deep packet inspection in smart grids and industrial internet of things: Challenges and opportunities. Journal of Network and Computer Applications **135**, 32–46 (2019)
36. Paul, S., Rabbani, M.S., Kundu, R.K., Zaman, S.M.R.: A review of smart technology (smart grid) and its features. In: 2014 1st International Conference on Non Conventional Energy (ICONCE 2014). pp. 200–203. IEEE (2014)
37. Qureshi, K.N., Hussain, R., Jeon, G.: A distributed software defined networking model to improve the scalability and quality of services for flexible green energy internet for smart grid systems. Computers & Electrical Engineering **84**, 106634 (2020)
38. Rice, E.B., AlMajali, A.: Mitigating the risk of cyber attack on smart grid systems. In: CSER. pp. 575–582 (2014)
39. Rodriguez-Calvo, A., Cossent, R., Frías, P.: Scalability and replicability analysis of large-scale smart grid implementations: Approaches and proposals in europe. Renewable and Sustainable Energy Reviews **93**, 1–15 (2018)
40. Sadiku, M.N., Tembely, M., Musa, S.M.: Home area networks: A primer. International Journal **7**(5) (2017)
41. Saleem, Y., Crespi, N., Rehmani, M.H., Copeland, R.: Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. IEEE Access **7**, 62962–63003 (2019)
42. Salpekar, M.: Protecting smart grid and advanced metering infrastructure. In: 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on. pp. 22–26. IEEE (2018)
43. Sandhu, R.S.: Role-based access control. In: Advances in computers, vol. 46, pp. 237–286. Elsevier (1998)
44. Sanislav, T., Miclea, L.: Cyber-physical systems-concept, challenges and research areas. Journal of Control Engineering and Applied Informatics **14**(2), 28–33 (2012)
45. Shabanzadeh, M., Moghaddam, M.: What is the smart grid? definitions, perspectives, and ultimate goals (11 2013). https://doi.org/10.13140/2.1.2826.7525
46. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J.: A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials **20**(4), 3453–3495 (2018)
47. Tan, S., De, D., Song, W.Z., Yang, J., Das, S.K.: Survey of security advances in smart grid: A data driven approach. IEEE Communications Surveys & Tutorials **19**(1), 397–422 (2017)
48. Tian, J., Wang, B., Li, X.: Data-driven and low-sparsity false data injection attacks in smart grid. Security and Communication Networks **2018** (2018)
49. Valea, E., Da Silva, M., Flottes, M.L., Di Natale, G., Dupuis, S., Rouzeyre, B.: Providing confidentiality and integrity in ultra low power iot devices. In: 2019 14th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS). pp. 1–6. IEEE (2019)
50. Viswanath, S.K., Yuen, C., Tushar, W., Li, W.T., Wen, C.K., Hu, K., Chen, C., Liu, X.: System design of internet-of-things for residential smart grid (2016)
51. Wang, W., Lu, Z.: Cyber security in the smart grid: Survey and challenges. Computer networks **57**(5), 1344–1371 (2013)
52. Whitman, M.E., Mattord, H.J.: Principles of information security. Cengage Learning (2011)

53. Xia, F., Yang, L.T., Wang, L., Vinel, A.: Internet of things. International Journal of Communication Systems **25**(9), 1101–1102 (2012). https://doi.org/10.1002/dac.2417, https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.2417
54. Yamada, T., Suzuki, K., Ninagawa, C.: Scalability analysis on the smart grid fast automated demand response aggregation web services for widely distributed building facilities. Electrical Engineering in Japan **205**(1), 17–25 (2018)
55. Yu, X., Xue, Y.: Smart grids: A cyber–physical systems perspective. Proceedings of the IEEE **104**(5), 1058–1070 (2016)
56. Zanero, S.: Cyber-physical systems. Computer **50**(4), 14–16 (April 2017). https://doi.org/10.1109/MC.2017.105
57. Zhang, Y., He, Q., Chen, G., Zhang, X., Xiang, Y.: A low-overhead, confidentiality-assured, and authenticated data acquisition framework for iot. IEEE Transactions on Industrial Informatics (2019)