An Information Security Model for an IoT-enabled Smart Grid

Abeer Akkad[1,2][a], Gary Wills[1][b] and Abdolbaghi Rezazadeh[1][c]
[1] *Electronic and Computer Science Dept., University of Southampton, University Road, Southampton, U.K.*
[2]*Information Systems Dept., Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, K.S.A*

Keywords: IoT, Internet of Things, IoT-enabled Smart Grid, IoT & Security, Cybersecurity, Threats Modelling.

Abstract: 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. One of these is protecting energy information exchange proactively, before an incident occurs. It is argued that Smart Grid systems were designed without any regard for security, which is considered a serious omission, especially for data security, energy information exchange, and the privacy of both the consumers and utility companies. This research is motivated by the gap identified in the requirements and controls for maintaining cybersecurity in the bi-directional data flow within the IoT-enabled Smart Grid. The initial stages of the research define and explore the challenges and security requirements, through the literature and industrial standards. The Threat Modelling identified nine internet-based threats. The analysis proposes a security model which includes 45 relevant security controls and 7 security requirements.

1 INTRODUCTION

The Smart Grid (SG) can be regarded as an extensive Cyber-Physical System (CPS) (Dagle, 2012). It is considered to be a critical infrastructure in all communities worldwide. Globally, the energy market is believed to be the most important asset that allows a country to expand its economy (Bedi *et al.*, 2018). Moreover, as cities want to assure sustainable green energy as a step towards their transformation into smart cities, implementing a SG is considered the best way to achieve this goal. Thus, the SG is one of the largest applications of IoT (Reka and Dragicevic, 2018; Al-Turjman and Abujubbeh, 2019). The McKinsey Global Institute predicted that the IoT will have a significant economic contribution from $3.9 to $11.1 trillion per year by 2025 (Manyika *et al.*, 2015). This influence will be felt in many areas and applications, including homes, factories, retail environments, offices, worksites, human health, outside environments, cities, and vehicles (Dalipi and Yayilgan, 2016).

The conventional power grid uses an analogue and electromechanical infrastructure in which electricity is transmitted from a centralised utility or power plant to the consumer through long-distance and high-voltage lines. The power is delivered to the neighbourhood by a distribution system consisting of transformers, distribution substations, and power lines. In this unidirectional model, there is no feedback from the consumer (Al Khuffash, 2018), so utility companies depend on meter readings by engineers to ensure that the balance of supply and demand is met in an effective manner. Meter readings provide insufficient information on the grid's condition and consumption, with no real-time energy information (Al Khuffash, 2018). Consequently, consumers are faced with being consumption-conscious. Besides real-time challenges, there are significant issues of exponential growth and changes of demand, an outdated grid architecture, latency, variations in load, many power outages, and increased carbon emissions (Al Khuffash, 2018). New infrastructure is needed that may overcome these

[a] https://orcid.org/0000-0002-7710-6378
[b] https://orcid.org/0000-0001-5771-4088
[c] https://orcid.org/0000-0002-0029-469X

Akkad, A., Wills, G. and Rezazadeh, A.
An Information Security Model for an IoT-enabled Smart Grid.
DOI: 10.5220/0011042200003194
In *Proceedings of the 7th International Conference on Internet of Things, Big Data and Security (IoTBDS 2022)*, pages 157-165
ISBN: 978-989-758-564-7; ISSN: 2184-4976

challenges, and the evolution of a SG could handle these drawbacks associated with the conventional grid.

The electric utility sector is currently developing an IoT-enabled SG. This is viewed as the largest-ever installation of an IoT, with thousands of smart objects and things such as smart meters, smart appliances, and other sensors (Reka and Dragicevic, 2018). This huge number of connected devices, besides the increasing demand for electric energy, results in significant challenges for a SG. Although the SG can address the drawbacks of the traditional power system, it involves issues of security, Big Data processing, cost, centralisation, scalability, interoperability, heterogeneity, and latency.

This research discusses the present challenges of an IoT-enabled electricity Smart Grid, focusing on securing the information flow that is essential for better automation, sensing, controlling, communicating, and timely decision-making (U.S. Department of energy, 2018). The current research proposes a comprehensive model for securing IoT-enabled SG.

This paper is organised as follows: Section 2 defines the IoT-enabled SG and components highlighting the security and the link between IoT and SG. In section 3 the security requirements are investigated. Section 4 looks at the threats modelling and identifies the security threats and controls. Then, the security model is proposed in section 5. Also, the potential future work is briefly discussed.

2 BACKGROUND

This section of the paper offers an overview of IoT-enabled SG, components, Then, the role of IoT in the SG is explained highlighting the security of IoT-enabled SG.

2.1 Definition of IoT-enabled Smart Grid

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. (IEEE, 2018; U.S. Department of energy, 2018; EPRI, 2005).

2.1.1 What Makes the Grid Smart?

It is argued that digital technology is what makes the grid smart (U.S. Department of energy, 2018). In order to achieve this, information technology systems have to be deployed to supply the data required for better sensing, precise control, wider information communication and sharing, powerful computing, and better decision-making (U.S. Department of energy, 2018).

2.2 Smart Grid Conceptual Model

The conceptual reference model by NIST (US National Institute of Standards and Technology) is commonly referred to in the sector (NIST, 2014). However, the NIST model encounters a lack of detail in terms of cybersecurity and information flow, especially in the IoT infrastructure. The NIST model contributes to the concept of the SG architecture only, while this research fills in the gaps in the NIST model to develop a case study that is useful for the related sectors. NIST case studies and scenarios are limited to privacy and some domains of SG without linking security requirements, threats, and controls for each access point in the system. Indeed, NIST IR and NERC CIP measure the compliance of any organisation with the policies.

2.3 IoT and Smart Grid

In this section, the role of IoT in the SG is explained. 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. These devices require tracking for monitoring purposes, connectivity, and automation (Al-Ali and Aburukba, 2015; Saleem *et al.*, 2019). The IoT is an enabling technology that brings internet connectivity to the SG (Al-Ali and Aburukba, 2015; Saleem *et al.*, 2019). From the cyber-physical systems point of view, SG is considered as one of the biggest applications of IoT (Al-Turjman & Abujubbeh, 2019; Reka & Dragicevic, 2018).

In SG, in the context of IoT each device is connected to the internet. To facilitate communication of information and receiving control commands via the internet protocols, each must have a unique IP address (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 plant, distribution, storage, and finally consumption to achieve efficiency management, demand management, renewable energy needed measurement, and CO_2 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. 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.

2.4 Smart Grid and Security

SG affords many opportunities, but it also presents security challenges. To get the most out of SG, it is essential to develop a highly secure information system. it is argued that automation systems such as SCADA were designed without any regard for security (Aloul, 2012). Moreover, Modbus, which exchanges SCADA information to control industrial processes, was not intended for critical security environments such as SG (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 that one of the main concerns in SG implementation worldwide is security. Security challenges of IoT-enabled SG can arise for many reasons. First, the entities in SG communicate using the IP-based communication network, exchanging sensitive and private data between both consumers and utility companies. Such networks are susceptible to many types of security threat, such as man-in-the-middle, denial of service, eavesdropping, and replay attacks, as shown in section 3. Secondly, SG consists of various components that communicate with one another, which requires interaction among these technologies. Accordingly, this communication introduces access points in SG that are vulnerable to security attacks (Mahmood *et al.*, 2016). Thirdly, SG uses wireless sensor networks to connect smart meters, for example. It has been argued that wireless networks are insecure (He *et al.*, 2013). Fourthly, by allowing unauthorised access to SG, the bi-directional information flow may expose SG to many threats. Fifthly, utilising IoT in SG may cause it to inherit IoT's security issues. For monitoring and control purposes with IoT devices, SG should use the internet (Ghasempour, 2019).

There are several security concerns over IoT technologies stemming from their exposure to the internet. The exposure can allow an attacker to tamper with the data. Besides, the ever-increasing number of IoT devices used in SG makes it more vulnerable to attack (Kimani *et al.*, 2019).

3 RELATED WORK

Security modelling has been carried out for the Smart Grid but these studies either focused on a part of the SG or they only partly covered the security controls. Some topics in the cybersecurity design stage, such as session mismanagement, have not been well investigated. Many challenges relating to security are still open. It is vitally important to develop an appropriate model to address all the information security challenges for the whole IoT-enabled SG. Although the studies discussed the optimisation of cost and performance, this research focuses on identifying the main potential access points that are vulnerable to internet-based threats in the SG, and all relevant security controls that could mitigate the internet-based threats and are applicable to each access point, in a comprehensive modelling approach that fills in the missing details in the NIST conceptual model without considering their cost of implementation.

4 PROPOSED MODEL

This section is focused on identifying the security requirements, Threats, and controls that contribute to the security of the SG information system.

4.1 Method for Model Development

This section charts the research roadmap to develop a security model for IoT-enabled SG that fills in the lack of details on the NIST model. Figure 1 presents the steps the research has undertaken for the development process. In Step 1, the security requirements were reviewed from international industrial standards and from academic publications. Then, both sets were combined and compared to generate the Security Requirements. In Step 2, threat modelling was carried out, based on the NIST conceptual model to identify the access points. Then, common internet-based threats were explored. Next, security threats and requirements were both identified using STRIDE analysis and classification. Step 3 assigned the identified threats to the access points, according to functions and the information system processed at each access point. In Step 4, the security controls were grouped by the security requirements. Finally, at Step 5 the security controls were mapped to the access points by assessing threats effects to find out the desired security requirements.

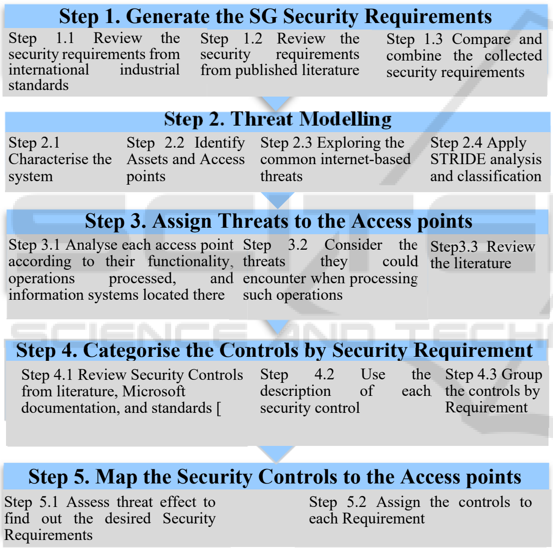
Step 1. Generate the SG Security Requirements
Step 1.1 Review the security requirements from international industrial standards
Step 1.2 Review the security requirements from published literature
Step 1.3 Compare and combine the collected security requirements
Step 2. Threat Modelling
Step 2.1 Characterise the system
Step 2.2 Identify Assets and Access points
Step 2.3 Exploring the common internet-based threats
Step 2.4 Apply STRIDE analysis and classification
Step 3. Assign Threats to the Access points
Step 3.1 Analyse each access point according to their functionality, operations processed, and information systems located there
Step 3.2 Consider the threats they could encounter when processing such operations
Step3.3 Review the literature
Step 4. Categorise the Controls by Security Requirement
Step 4.1 Review Security Controls from literature, Microsoft documentation, and standards [
Step 4.2 Use the description of each security control
Step 4.3 Group the controls by Requirement
Step 5. Map the Security Controls to the Access points
Step 5.1 Assess threat effect to find out the desired Security Requirements
Step 5.2 Assign the controls to each Requirement

Figure 1: Development of the Security Model.

4.2 Security Requirements

The security requirements gleaned from literature and industrial standards and authorities are reviewed and analysed as the following (Mrabet *et al.*, 2018; Benmalek *et al.*, 2019; Das and Zeadally, 2019; Tufail *et al.*, 2021):

1. Confidentiality: Ensuring that access to transmitted data is restricted to authorised people. It prevents the unauthorised disclosure of information. In Smart Grid, the transmitted data could be sensitive, such as personal information about a consumer's activities and billing data.

2. Integrity: Guarding the information and the source of the information against any tampering or unauthorised manipulation. Information could be power measurements or price signals. A loss of integrity may lead to false decision-making about energy management.

3. Availability: Guarantee timely and reliable access to the information (NISTIR 7628, 2014). The power system needs to be available whenever required by authorised entities. A loss of availability may cause power cuts. Availability is about the uptime and downtime of the SG system.

4. Authentication: Validating the identity of any communicated entities (devices/users) in the SG. For example, smart meters need to be authenticated so that the utility company can bill the correct consumer. Data authentication plays a significant role in proving that the transmitted data are genuine, using verification features such as digital signatures.

5. Authorisation: Granting the required rights to an authenticated device/user to access SG resources. The access control is that which guarantees that SG resources are accessed by the correctly identified entities.

6. Privacy: Guaranteeing that any private data belonging to the consumer cannot be obtained without permission and are used for pre-approved purposes only. An attacker can extract information on private data from the smart meter such as consumption readings.

7. Non-repudiation: Assuring that the accountability of any data transaction has been undertaken between entities without any denial of responsibility. It means assuring the traceability of the system by recording each transaction by node, device, consumer, and utility (Mrabet *et al.*, 2018).

4.3 Internet-based Threats

Below are the common types of internet-based cybersecurity threats found in the literature and analysed using the STRIDE modelling technique as described in the next section(Cisco, 2017; Marinos and Lourenço, 2018; Mrabet *et al.*, 2018; Otuoze *et al.*, 2018; Tonyali *et al.*, 2018; Benmalek *et al.*, 2019; Das and Zeadally, 2019; Ganguly *et al.*, 2019; Kimani *et al.*, 2019; Gunduz and Das, 2020; Tufail *et al.*, 2021):

1. Spoofing/Impersonation: This is an active attack that aims to communicate on behalf of a legal entity through unauthorised access, by stealing its identity. An attacker may impersonate another's smart meter identity in order to pay lower electric charges – or let the other pay.

2. Eavesdropping/Traffic analysis/Man-In-The-Middle (MITM): These are passive attack capturing the transmitted data by intercepting the communication between two entities in the SG. In Traffic analysis, the attacker intercepts the communication, analyses the network traffic, and then extracts information from patterns to locate key entities such as substations or disclose sensitive information such as future price information.

3. Replay attack: A replay attack is an active attack that intercepts the communication between two entities by recording, observing, copying the transmitted data, and then replaying a selected part of the copied data back in an attack. It manipulates the data before sending it back.

4. Data tampering: This strikes when an attacker manipulates the exchanged data, such as dynamic prices that are announced before peak times, making them cheaper. Consequently, it can increase consumer consumption instead of reducing it. This, in turn, overloads the power network and causes power outages.

5. Denial of Service (DOS)/Jamming channel: This is an active attack that floods the entire system, resources, or bandwidth, with a high number of fake requests to overload the system, slow it, or corrupt data transmission, thus making the SG unavailable. This congested traffic prevents authorised entities from accessing the system. A jamming channel attack is a type of DOS threat. A distributed DOS (DDOS) threat involves system servers or resources being flooded by multiple attackers.

6. Malware injection: This is the execution of malicious software on the SG, such as viruses, spyware, rootkits, adware, malvertising, ransomware, Trojan horses, or worms. It aims to damage, steal, delete, modify, or disable, the main functions in smart meters, or utility servers.

7. Phishing: Phishing that is included in this research's scope is internet-based Phishing such as email Phishing and search engine/websites Phishing that tricks users into believing that a message is from a trustworthy organisation, asking them to click a malicious link to obtain sensitive information. When users respond, the attacker can use this information to access the system (CISA, 2009).

8. SQL injections: A Structured Query Language (SQL) injection executes a harmful SQL query statement on the server that uses SQL, aiming to force the server to disclose information, modify, or delete the database contents. According to Cisco, this SQL query is entered by the attacker using a website search box on the client-side interface of the application and is used to target database applications.

9. False data injection: This type of attack sends fake information into the network, such as false meter readings or wrong prices. It causes false state estimation for the SCADA system and may cause a power system failure. Thus, it influences the electricity market financially by tampering with market price information.

4.4 Threat Modelling

This research used the STRIDE technique for threat modelling. 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, as shown in Figure 2. Threats are mapped to STRIDE categories using STRIDE definitions and the threats definitions of this research provided at section 4.3. Each identified threat is mapped to STRIDE categories based on the main effect of that threat at the first instance. Then, threats are mapped to security requirements based on STRIDE mapping as well as the literature (Mrabet *et al.*, 2018; Stellios *et al.*, 2018; Gunduz and Das, 2020; Tufail *et al.*, 2021).

Security controls are countermeasures to mitigate, delay or prevent threats in order to strengthen the information system against threats. The controls are approaches that ensure security requirements. The security controls are taken from the literature and Microsoft documentation (2009). Security controls are then categorised by security requirements using the description of each security control, as shown Table 1 at appendix A. In addition, all the standards, including NIST IR, NERC CIPS (1-9), NIST IR7628, and NIST SP 800-53, are reviewed as well as the publications (Mrabet *et al.*, 2018; Das and Zeadally, 2019; Ganguly *et al.*, 2019; Kimani *et al.*, 2019) to map the security controls to the security requirements.

4.5 Identifying Access Points

This step articulates the main access points that are vulnerable to internet-based threats in the IoT-enabled SG by reviewing publications, and the vulnerability analysis compiled by the U.S. electric sector issued by Idaho National Laboratory (Glenn

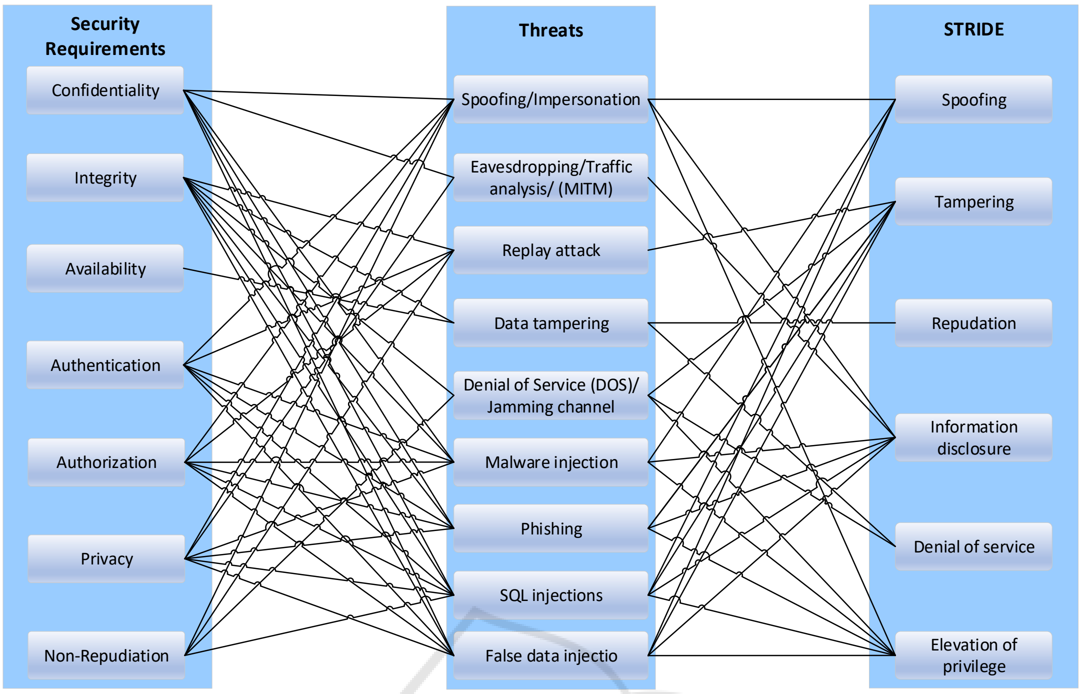

Figure 2: SG Threat modelling.

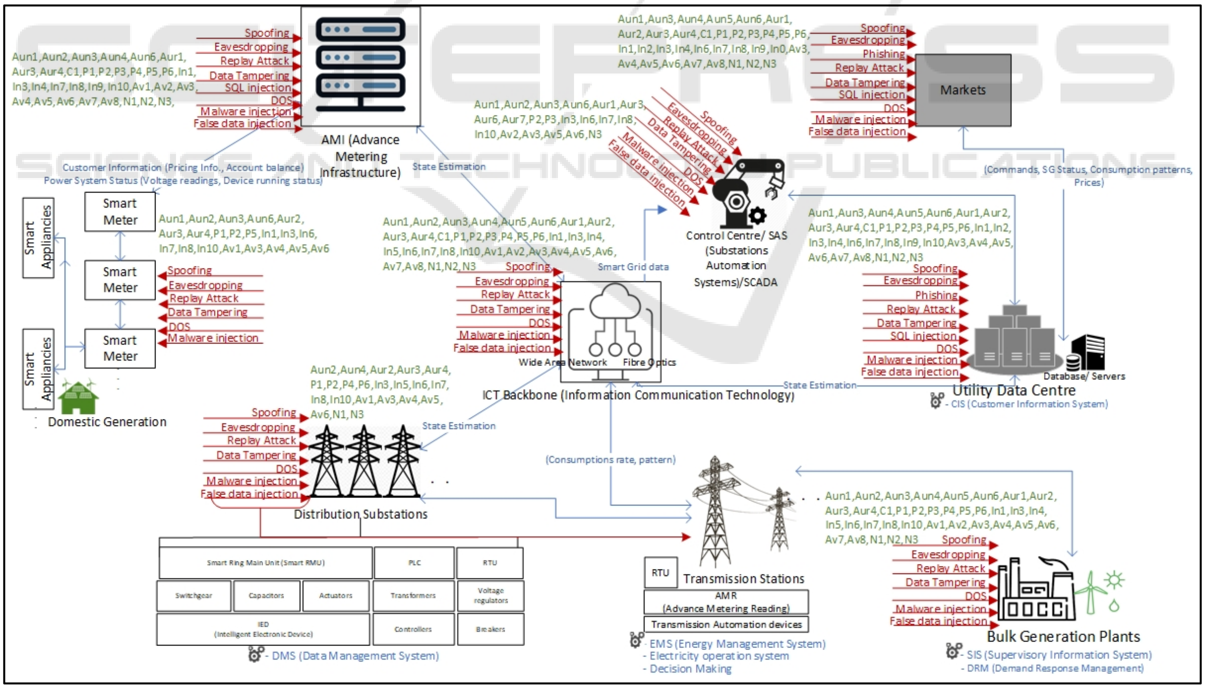
Aun1,Aun2,Aun3,Aun4,Aun6,Aur1, Aur3,Aur4,C1,P1,P2,P3,P4,P5,P6,In1, In3,In4,In7,In8,In9,In10,Av1,Av2,Av3, Av4,Av5,Av6,Av7,Av8,N1,N2,N3,
Spoofing
Eavesdropping
Replay Attack
Data Tampering
SQL injection
DOS
Malware injection
False data injection
AMI (Advance Metering Infrastructure)
Customer Information (Pricing Info., Account balance)
Power System Status (Voltage readings, Device running status)
State Estimation
Aun1,Aun3,Aun4,Aun5,Aun6,Aur1, Aur2,Aur3,Aur4,C1,P1,P2,P3,P4,P5,P6, In1,In2,In3,In4,In6,In7,In8, In9,In0,Av3, Av4,Av5,Av6,Av7,Av8,N1,N2,N3
Spoofing
Eavesdropping
Phishing
Replay Attack
Data Tampering
SQL injection
DOS
Malware injection
False data injection
Markets
(Commands, SG Status, Consumption patterns, Prices)
Aun1,Aun2,Aun3,Aun6,Aur1,Aur3, Aur6,Aur7,P2,P3,In3,In6,In7,In8, In10,Av2,Av3,Av5,Av6,N3
Spoofing
Eavesdropping
Replay Attack
Data Tampering
DOS
Malware injection
False data injection
Control Centre/ SAS (Substations Automation Systems)/SCADA
Smart Appliancies
Smart Meter
Smart Meter
Smart Meter
Smart Appliancies
Aun1,Aun2,Aun3,Aun6,Aur2, Aur3,Aur4,P1,P2,P5,In1,In3,In6, In7,In8,In10,Av1,Av3,Av4,Av5,Av6
Spoofing
Eavesdropping
Replay Attack
Data Tampering
DOS
Malware injection
Domestic Generation
Aun1,Aun2,Aun3,Aun4,Aun5,Aun6,Aur1,Aur2, Aur3,Aur4,C1,P1,P2,P3,P4,P5,P6,In1,In3,In4, In5,In6,In7,In8,In10,Av1,Av2,Av3,Av4,Av5,Av6, Av7,Av8,N1,N2,N3
Spoofing
Eavesdropping
Replay Attack
Data Tampering
DOS
Malware injection
False data injection
Smart Grid data
Wide Area Network
Fibre Optics
ICT Backbone (Information Communication Technology)
State Estimation
Aun1,Aun3,Aun4,Aun5,Aun6,Aur1,Aur2, Aur3,Aur4,C1,P1,P2,P3,P4,P5,P6,In1,In2, In3,In4,In6,In7,In8,In9, In10,Av3,Av4,Av5, Av6,Av7,Av8,N1,N2,N3
Spoofing
Eavesdropping
Phishing
Replay Attack
Data Tampering
SQL injection
DOS
Malware injection
False data injection
Database/ Servers
Utility Data Centre
- CIS (Customer Information System)
Aun2,Aun4,Aur2,Aur3,Aur4, P1,P2,P4,P6,In3,In5,In6,In7, In8,In10,Av1,Av3,Av4,Av5, Av6,N1,N3
Spoofing
Eavesdropping
Replay Attack
Data Tampering
DOS
Malware injection
False data injection
State Estimation
Distribution Substations
(Consumptions rate, pattern)
Smart Ring Main Unit (Smart RMU)
PLC
RTU
Switchgear
Capacitors
Actuators
Transformers
Voltage regulators
IED (Intelligent Electronic Device)
Controllers
Breakers
- DMS (Data Management System)
RTU
Transmission Stations
AMR (Advance Metering Reading)
Transmission Automation devices
- EMS (Energy Management System)
- Electricity operation system
- Decision Making
Aun1,Aun2,Aun3,Aun4,Aun5,Aun6,Aur1,Aur2, Aur3,Aur4,C1,P1,P2,P3,P4,P5,P6,In1,In3,In4, In5,In6,In7,In8,In10,Av1,Av2,Av3,Av4,Av5,Av6, Av7,Av8,N1,N2,N3
Spoofing
Eavesdropping
Replay Attack
Data Tampering
DOS
Malware injection
False data injection
Bulk Generation Plants
- SIS (Supervisory Information System)
- DRM (Demand Response Management)

Figure 3: The proposed Security Model.

et al., 2017). Figure 3 Shows seven access points that are most likely to be exploited to execute cyber-attacks: (1) Smart Meters and Smart Appliances; (2) Transmission Stations, Distribution Substations, and Smart automation devices for transmission and distribution (Switches, Sensors, Actuators, Transformers, Voltage regulator, Capacitors); (3) Generation Plant and Information Communication

Technology (ICT) Systems; (4) Advanced Metering Infrastructure (AMI); (5) SCADA (Supervisory Control and Data Acquisition)/SAS (Substations Automation Systems)/ Control Centre; (6) Utility data centre; (7) Market.

5 CONCLUSIONS

In conclusion, the proposed security model shown in Figure 3 consists of seven security requirements, nine threats, seven access points, and thirty-eight security controls.

The model addresses the limitation found in the NIST model as NIST is a very high-level conceptual model lacking details that make the proposed model more practical and useful for the related sectors to use.

This research will be beneficial to system designers, information security practitioners, and stakeholders to consider the key requirements and challenges, identify the security threats and vulnerabilities, and maintain the required mechanisms through the initial stages of the development of a SG system design.

For the future work, the next phase of this research is to have the model validated by experts in the industry including threats, access points, requirements, and controls. The initial reviews confirmed this model and the importance of it to support the energy sector towards securing automated Smart Grids. Then, the model will be verified by formal modelling.

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.

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

Aloul, F.A. (2012) ‘The Need for Effective Information Security Awareness’, Journal of Advances in Information Technology, 3(3), pp. 176–183.

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.

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

Benmalek, M., Challal, Y. and Derhab, A. (2019) ‘Authentication for Smart Grid AMI Systems: Threat Models, Solutions, and Challenges’, Proceedings - 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2019, pp. 208–213.

CISA (2009) ‘Understanding Digital Signatures | CISA’.

Cisco (2017) What Is a Cyberattack? - Most Common Types - Cisco. Available at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (Accessed: 21 February 2020).

Dagle, J.E. (2012) ‘Cyber-physical system security of smart grids’, 2012 IEEE PES Innovative Smart Grid Technologies, ISGT 2012, pp. 1–2.

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.

Das, A.K. and Zeadally, S. (2019) Data Security in the Smart Grid Environment, Pathways to a Smarter Power System. Elsevier Ltd. doi:10.1016/B978-0-08-102592-5.00013-2.

EPRI Electric Power Research Institute (2005) EPRI Smart Grid Resource Center. Available at: https://smartgrid.epri.com/.

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.

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

Glenn, C., Sterbentz, D. and Wright, A. (2017) Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Inl (Idaho National Laboratory).

Gunduz, M.Z. and Das, R. (2020) ‘Cyber-security on smart grid: Threats and potential solutions’, Computer Networks, 169, p. 107094.

He, D., Kumar, N., Chen, J., Lee, C.C., Chilamkurti, N. and Yeo, S.S. (2013) ‘Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks’, Multimedia Systems, 21(1), pp. 49–60.

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

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..

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.

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.

Marinos, L. and Lourenço, M. (2018) ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends, European Union Agency For Network and Information Security. doi:10.2824/622757.

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.

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.

NISTIR 7628 (2014) NISTIR 7628 Guidelines for Smart Grid Cyber Security, Revision 1, NIST.

Otuoze, A.O., Mustafa, M.W. and Larik, R.M. (2018) 'Smart grids security challenges: Classification by sources of threats', Journal of Electrical Systems and Information Technology, 5(3), pp. 468–483.

Reka, S.S. and Dragicevic, T. (2018) 'Future effectual 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.

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.

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C. and Lopez, J. (2018) 'A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services', IEEE Communications Surveys and Tutorials, 20(4), pp. 3453–3495.

Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A.S. and Nojoumian, M. (2018) 'Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems', Future Generation Computer Systems, 78, pp. 547–557.

Tufail, S., Parvez, I., Batool, S. and Sarwat, A. (2021) 'A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid', Energies, 14(18), pp. 1–22.

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

APPENDIX A

Table 1: Mapping security controls to security requirements.

Security requirement	Security controls	Code
Authentication (Aun)	1. Keyed cryptographic hash functions (HMAC), digital signatures, and Random numbers generators	Aun1
	2. Physically Unclonable Functions (PUF)	Aun2
	3. MAC-attached, and HORS-signed messages	Aun3
	4. Secure Sockets layer Certificates (SSL Certificates) and Transport Layer Security (TLS)	Aun4
	5. Multi-factor authentication mechanism	Aun5
	6. Automatic lockouts	Aun6
Authorisation (Aur)	7. Attribute-Based Encryption	Aur1
	8. Attribute Certificates	Aur2
	9. Attribute-Based Access Control System based on XACML (Extensible Access Control Markup Language)	Aur3
	10. Role-Based Access Control and allow/block listing	Aur4
Confidentiality (C)	11. Symmetric and asymmetric algorithms and Public Key Infrastructure certificate (PKI)	C1
Privacy (P)	12. Anonymisation	P1
	13. Trusted aggregators	P2
	14. Homomorphic encryption	P3
	15. Perturbation models	P4
	16. Verifiable computation models, and zero-knowledge proof systems	P5
	17. Data obfuscation techniques	P6

Table 1: Mapping security controls to security requirements (cont.).

Security requirement	Security controls	Code
Integrity (In)	18. Cryptographic hashing functions and session keys	In1
	19. Digital watermarking	In2
	20. Automated patch management for flaw remediation	In3
	21. Adaptive cumulative sum algorithm	In4
	22. Secure Phasor Measurement Units (PMUs) installation	In5
	23. Load profiling algorithms	In6
	24. Timestamps	In7
	25. Sequence numbers	In8
	26. Query sanitisation	In9
	27. Nonces	In10
Availability (Av)	28. Use multiple alternate frequency channels according to a hardcoded sequence	Av1
	29. Frequency quorum rendezvous between connected nodes	Av2
	30. Anomaly Intrusion Detection Systems (IDS)	Av3
	31. Specification-based IDS	Av4
	32. Intrusion Prevention Systems (IPS)	Av5
	33. Quality of Services (QoS)	Av6
	34. Load balancing	Av7
	35. Operating system-independent Applications	Av8
Non-repudiation (N)	36. Mutual Inspection technique	N1
	37. Unique keys and digital signatures	N2
	38. Transaction log	N3