Computers and Electrical Engineering 105 (2023) 108491

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

An information security model for an IoT-enabled Smart Grid in the Saudi energy sector

Abeer Akkad [a,b,*], Gary Wills [b], Abdolbaghi Rezazadeh [a]

[a] Electronic and Computer Science Dept., University of Southampton, UK
[b] Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, K.S.A

ARTICLE INFO

This paper is for regular issues of CAEE. Reviews were processed by Associate Editor Dr. Xiaokang Zhou and recommended for publication

Keywords:
Internet of Things
IoT-enabled Smart Grid
IoT and security
Cybersecurity
Threat modelling
Security model

ABSTRACT

Data supply and transmission in the Smart Grid achieve better sensing, control, information communication and sharing, and more rational decision-making. An Internet of Things-enabled Smart Grid affords better automation, monitoring, and control of electricity consumption. However, rapid growth in connected entities, accompanied by electricity demand, brings about challenges such as securing energy information exchange before an incident occurs. It is argued that Smart Grid systems were designed with no regard for security, which is a serious omission for data, energy information exchange, and consumers' and utilities' privacy.

This study is motivated by the gap identified between the requirements and controls for cybersecurity in the IoT-enabled Smart Grid's bidirectional data flow. It develops and confirms a model with seven security requirements and 45 security controls. In future, this model is to be verified and validated.

This research focuses solely on the information flow's cybersecurity through using technical security controls to counter internet-based threats in IoT-enabled Smart Grids.

1. Introduction

The conventional power grid uses an analogue and electromechanical infrastructure to transmit electricity from a centralised power plant to neighbourhoods over long-distance, high-voltage lines. Power is delivered to consumers by a distribution system consisting of transformers, distribution substations, and power lines. In this traditional unidirectional model there is no feedback from consumers [1], so utility companies must rely on meter readings taken 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 [1]. Consequently, consumers must be consumption-conscious. Besides the real-time challenges are the significant issues of exponential growth in KSA and changes in demand, an outdated grid architecture, latency, variations in load, frequent power outages, and increased carbon emissions [1]. New infrastructure is needed to overcome these challenges, and the evolution of an Internet-of-Things (IoT)-enabled Smart Grid (SG), with its bidirectional information flow, could answer the challenges associated with the conventional grid's unidirectional information flow.

The electricity sector is currently developing an IoT-enabled SG. The McKinsey Global Institute predicts that by 2025 the IoT will make a significant annual economic contribution of $3.9 to $11.1 trillion [2]. This influence will be felt in many areas and applications,

* Corresponding author.
E-mail addresses: asaa1n1@soton.ac.uk (A. Akkad), gbw@ecs.soton.ac.uk (G. Wills), ra3@ecs.soton.ac.uk (A. Rezazadeh).

https://doi.org/10.1016/j.compeleceng.2022.108491
Received 28 March 2022; Received in revised form 9 November 2022; Accepted 15 November 2022
Available online 23 November 2022

Table 1
Summary of 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. [8]
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 characterise a Smart Grid. [5]
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. [9]
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 prosumers to supply sustainable, and secure power energy. [13]
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 minimise environmental impact, enhance markets, improve reliability and service, and reduce costs and improve efficiency. [12]

including homes, factories, retail environments, offices, worksites, human health, outside environments, cities, and vehicles [3]. Globally, the energy market is believed to be the key asset that allows a country to expand its economy. The IoT-enabled SG is considered to be a critical infrastructure in all communities worldwide. Moreover, cities want to assure sustainable green energy as a step toward their transformation into smart cities, and implementing an IoT-enabled SG is the best way to achieve this goal.

The concept of an IoT-enabled SG involves employing ICT to enable communicating, monitoring, and controlling facilities for a bidirectional information flow around the SG. An SG is viewed as the largest-ever installation of an IoT, with thousands of 'smart' objects and items such as smart meters, smart appliances, and other sensors [4]. This huge number of connected devices, besides increasing demand for electricity, raises issues of security, Big Data processing, cost, centralisation, scalability, interoperability, heterogeneity, and latency.

Thus the IoT-enabled SG is seen as essential for better automation, sensing, controlling, communication, and timely decision-making [5], and this study focuses on the security of its bidirectional information flow. It proposes a comprehensive model for securing IoT-enabled SG. As a cyber-physical system, it is argued that it has an inherent serious security challenge due to its use of IoT devices, as there are many security concerns around such technologies. Previous studies are similarly concerned about the SG's security [4,6,7]. Attackers could extract private information about an individual's power consumption, manipulating the data on their smart meter.

A detailed literature review was conducted on both industrial standards and academic publications to identify the main access points of an IoT-enabled SG. Threat analysis was undertaken on the information flow around an IoT-enabled SG. A gap analysis revealed that few studies had comprehensively addressed the security controls to counter internet-based threats to the information flow around the IoT-enabled SG, either internationally or specifically in KSA's electricity sector.

Next, a security model was developed for the information flow around an IoT-enabled SG. To supply the detail missing from the US National Institute of Standards and Technology (NIST) conceptual model, by taking a comprehensive, structured approach this model identifies the controls required to mitigate internet-based threats. The model developed represents a high-level concept, lacking only detailed cybersecurity considerations, in contrast to the NIST case studies and scenarios that are limited to privacy and certain other domains of SG, without linking access points to their security requirements, threats, or controls. Indeed, NIST IR and NERC CIP merely measure organisations' compliance with policies. The model was confirmed by interviewing experts in Saudi Arabia on IoT-enabled SG.

This article is organised as follows: section 2 defines the IoT-enabled SG and components, highlighting security and the links between IoT and SG. Section 3 presents related works. In section 4 the model's method of development is explained, including threat modelling. Next, the research methodology is presented in section 5. Section 6 discusses the expert findings. The study concludes in section 7, where potential future work is briefly discussed.

2. Background

This section offers an overview of the IoT-enabled SG and its components. The role of IoT in the SG is explained, highlighting the security issues presented by an IoT-enabled SG.

2.1. Definition of the IoT-enabled Smart Grid

Definitions of SG differ between organisations and studies, as shown in Table 1, and there is no consensus; however, the common concept is that SG revolves around an information communication infrastructure. For instance, the largest standardisation authority, IEEE, describes the SG as a new age of electricity featuring the use of ICT in the generation, delivery, and consumption of electricity and the electric system [8]. Likewise, in the view of Ontario's Independent Electricity System Operator (IESO), the leader in SG, it involves using ICT to optimise all power system operations for the benefit of both consumers and the environment [9].

Both these definitions focus on the SG component, which is specifically a communication infrastructure, whereas others dwell on the SG's benefits. For instance, the first official definition, from the 2007 Energy Independence and Security Act (EISA) of 2007 [1,10]

in a report to US Congress, defines an SG as:

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 characterise a Smart Grid. [5,10]

By contrast, in the IEEE and EISA definitions, it is the SG domain that is prominent, including electricity generation, transmission, distribution, and consumption [8,10].

Other definitions focus on how information could be transferred through the SG in the context of information technologies. The bidirectional flow has given rise to the term "prosumers" [3], meaning customers who generate energy for the grid, as stressed by the European Union and the UK Institution of Engineering and Technology (IET) [11], also shown in Table 1. The IET's definition is based on that of the European Technology Platform (ETP) [11]. Other definitions have an environmental perspective [9] and [12], citing green energy and benefits to the environment as the SG's most important advantages by virtue of reducing CO2 output.

From the above, the SG can be seen as the integration of ICT into the existing electricity network, consisting of renewable sources and involving multiple domains (generation, transmission, distribution, and consumption) in the efficient automation and real-time demand management of reliable, sustainable, bidirectional, and economical green electricity.

2.1.1. What makes the grid smart?

It is argued that digital technology is what makes the grid smart [5]. Information technology systems must be deployed to supply the data necessary for better sensing, precise control, wider information communication and sharing, powerful computing, and more rational decision-making [5].

2.2. Smart Grid conceptual model

The conceptual reference model by NIST is commonly referred to in the electricity sector [14]; however, it has few details on cybersecurity and information flow, especially regarding IoT infrastructure. It contributes only to the concept of the SG architecture, and its case studies and scenarios are limited to privacy and certain domains of SG, without linking these to security requirements, threats, and controls for each access point in the system. This current study responds to the lack of detail in the NIST model to develop a case study that has utility for the related sectors.

2.3. IoT and Smart Grid

This section explains the role of IoT in the SG. [15] suggests that all objects in a SG can be represented as IoT devices distributed throughout our residential networks, substations, and utilities. These devices require tracking for the purposes of monitoring, connectivity, and automation [15]. The IoT is an enabling technology that gives the SG its internet connectivity [15]. From the cyber-physical systems point of view, SG is considered to be IoT's key application [4].

In SG, each IoT device is connected to the internet. To facilitate the communication of information and receipt of control commands via internet protocols, each has a unique IP address. Under the IP addressing schemas, IoT can offer monitoring and control capabilities for SG. This monitoring aspect covers generation, distribution, storage, and finally consumption to achieve efficiency management, demand management, measurement of the renewable energy needed, and administration of CO2 emissions. Therefore, IoT devices contribute to accurate estimation of required energy and a reduction in wasted energy.

Further, those devices exchange data in bidirectional flow via the SG communication layer. IoT standardises communication, reducing the protocols relating to SG components [15]. There is an emphasis on the fact that IoT technologies enable SGs to communicate across the many subsystems of generation, transmission, distribution, and consumption [15], since each device exchanges data and commands among control centres and utilities [15].

2.4. Smart Grid and security

SG affords opportunities, yet it also presents many 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 with no regard for security [16]; neither was Modbus, which exchanges SCADA information to control industrial processes, ever intended for the SG's critical security environment [16]. Since power assets are critical national infrastructure that may attract terrorists, the highest priority must be assigned to securing the SG information system: damage from security attacks on the power grid could cause chaos across entire cities. The Electric Power Research Institute (ERPI) confirms that, worldwide, one of the main concerns over SG implementation is indeed its security.

Security challenges arise with IoT-enabled SG for many reasons. Several stem from their exposure to the internet, allowing an attacker to tamper with data. Moreover, the ever-increasing number of IoT devices used in SG makes it more vulnerable to attack [6].

First, the entities in SG communicate using the IP-based communication network, exchanging sensitive and private data among consumers and utility companies. Such networks are susceptible to many types of security threats, such as man-in-the-middle, denial of service, eavesdropping, and replay attacks, as in section 3. Second, SG consists of various components that communicate with one another, which requires interaction among these technologies. Accordingly, there are access points in SG that are vulnerable to security attacks. Third, to connect smart meters, for example, SG uses wireless sensor networks. It has been argued that they are insecure. Fourth, by allowing unauthorised access to SG, the bidirectional information flow itself may expose SG to many threats. Fifth, using the IoT in an SG may cause the SG to inherit its security issues: for monitoring and controlling IoT devices, SG should use the internet.

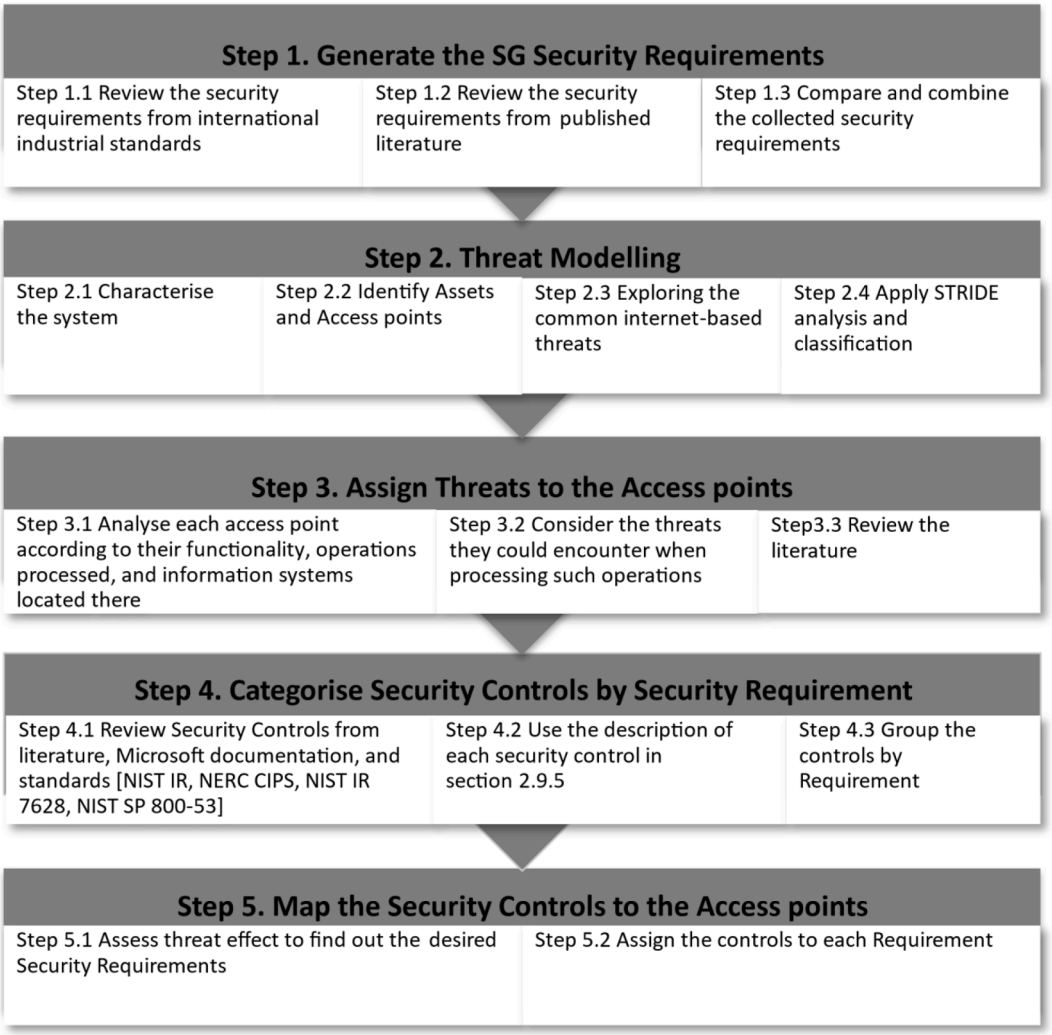

Fig. 1. Development of the security model

3. Related work

Security modelling for the SG has been undertaken previously, but the studies either focus on only a part of the SG or cover the security controls only partially. This section describes the reported security modelling results, demonstrating that many challenges that relate to security are ongoing. It is vitally important to develop an appropriate model to address all the information security challenges across the entire IoT-enabled SG. While past studies discuss optimizing cost and performance, this current study focuses on identifying the main potential access points that are vulnerable to internet-based threats in an IoT-enabled SG. It looks at all the relevant security controls to mitigate the internet-based threats applicable to each access point, taking a comprehensive modelling approach that, without regarding the implementation cost, supplies the details missing from the NIST conceptual model.

Studies have investigated key encryption [17], developing a security management scheme that depended on key distribution. This scheme focused on integrity, privacy, and authentication in the HAN, yet it was vulnerable to Man-In-The-Middle (MITM) attacks and had a scalability issue [18]. Next developed was a mutual authentication scheme in Advance Metering Infrastructure (AMI) that prevented impersonation, MITM, data tampering, and replay attacks [19], yet focused on non-repudiation and privacy and did not consider computational overheads or efficiency [18]. A lightweight authentication scheme that relied on the Diffie-Hellman protocol was then presented [20], but its security requirement was limited to integrity. Similar was a lightweight authentication scheme against impersonation, replay, and MITM attacks [21]. That scheme increased the computation load [18]. Another used a Fully Homomorphic Encryption (FHE) and Multiparty Computation (MPC) system to enable multiple operations to be performed on concealed data [22], yet it resolved only the privacy issue.

Regarding frameworks, a framework was proposed using fuzzy logic [23], and it included a unique one-way cryptographic function. It detected data tampering in AMI smart meters using a modular algorithm, the Meter Data Tampering Algorithm (MDTA).

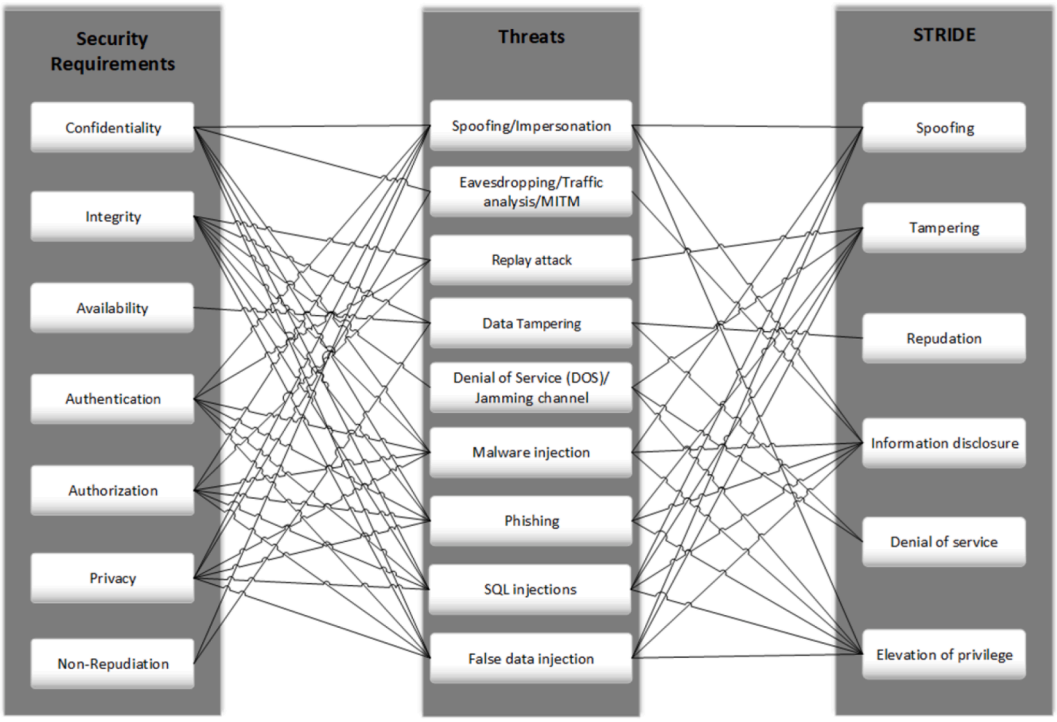

Fig. 2. Threat modelling of the IoT-enabled Smart Grid

On threat modelling, a study took the STRIDE per-element approach and used a data flow diagram for the system components [24]. The next modelled a threat vector for use against IoT devices [25], discussing IoT-enabled cyberattacks in critical infrastructures including SGs. The Dolev-Yao threat model was adopted by a further study [26]. These threat models discuss security attacks, using controls without privacy as their security requirement, yet do not cover common cyber-attack by false data injection. A taxonomy of cyber-attacks in SG surveying security requirements and countermeasures was devised [27], yet this classification is limited to Confidentiality, Integrity, and Availability (CIA) as security requirements.

4. Method for model development

This section charts the study's roadmap in developing a security model for IoT-enabled SG that supplies the details missing from the NIST model. Fig. 1 presents the steps that undertaken during the development process.

Step 1 reviewed security requirements, using both international industrial standards and academic publications. The two sets were combined and compared to generate the study's security requirements. Step 2 carried out threat modelling to identify the access points, based on the NIST conceptual model. Next, common internet-based threats were explored. Security threats and requirements were identified using STRIDE analysis and classification. Step 3 assigned each identified threat to the access points on the basis of the functions and the information system processed at each. In Step 4, the security controls were grouped by their security requirements. Finally, at Step 5 each security control was mapped to the access points by assessing the threats' effects, thus establishing the desired security requirements.

4.1. Step 1. Security requirements

The security requirements for an IoT-enabled SG comprise what an SG needs to deliver enhanced security. Those gleaned from literature and industrial standards and authorities (such as DOE, NIST 7628, EPRI, ENISA, IEC62351, and IoTSF) were reviewed and analysed, together with numerous studies [16,18,26,28–30]:

1 **Confidentiality:** Ensures that access to transmitted data is restricted to the authorised people. It prevents unauthorised disclosure of information. In SG, the transmitted data could be sensitive, such as personal information about a consumer's activities and bills.
2 **Integrity:** Guards the information and the source of the information against any tampering or unauthorised manipulation. The information could be power measurements or price signals. A loss of integrity may lead to poor decision-making about energy management.

Table 2
Threat classification with STRIDE threat modelling

Identified Threat	STRIDE Threat Modelling					
	Spoofing Identity	Tampering with Data	Repud- iation	Information Disclosure	Denial of Service	Elevation of Privilege
1. Spoofing/Impersonation	✓					
2. Eavesdropping/Traffic analysis/MITM				✓		
3. Replay attack		✓		✓		
4. Data tampering		✓				
5. Denial of Service (DOS)/ Jamming channel					✓	
6. Malware injection		✓				
7. Phishing				✓		
8. SQL injections		✓				
9. False data injection		✓	✓			

Table 3
Threat classification with security requirements

Identified Threat	Security Requirement						
	Confidentiality	Integrity	Availability	Authentication	Authorisation	Privacy	Non-repudiation
1. Spoofing/Impersonation				✓	✓		
2. Eavesdropping/Traffic analysis/MITM	✓						
3. Replay attack		✓					
4. Data tampering		✓					
5. Denial of Service (DOS)/ Jamming channel			✓				
6. Malware injection		✓	✓				
7. Phishing	✓						
8. SQL injections		✓					
9. False data injection		✓					✓

3 **Availability:** Guarantees timely and reliable access to information. The power system needs to be available whenever required by authorised entities, as a loss of availability may result in power cuts. Availability is about the uptime and downtime of the SG system.
4 **Authentication:** Validates the identity of any communicated entities (devices/users) in the SG. For example, smart meters need to be authenticated so that the utility company bills 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:** Grants the required rights to an authenticated device/user to access SG resources. Access control guarantees that SG resources are accessed by correctly identified entities.
6 **Privacy:** Guarantees that no private data belonging to the consumer can be obtained without permission and that they are used for approved purposes only. An attacker can extract from the smart meter private data, such as consumption readings.
7 **Non-repudiation:** Assures 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.

4.2. Step 2. Threats modelling

This research used the STRIDE technique for threat modelling. Security requirements can be mapped to threats to show the effect of each and the security criteria for the system. It is argued that the system's security requirements can be defined clearly once its threats are identified, as shown in Fig. 2 and Tables 2 and 3.

4.2.1. Characterising the system and identifying access points

This step articulates the main access points in the IoT-enabled SG that are vulnerable to internet-based threats, reviewing publications and the vulnerability analysis compiled by the U.S. electricity sector as issued by Idaho National Laboratory. Fig. 4 shows the seven access points most likely to be exploited in 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) Supervisory Control and Data Acquisition (SCADA)/Substations Automation Systems (SAS)/control centre; (6) the utility data centre; and (7) the market.

Table 4
Security controls and corresponding security requirements

Security Requirement	Security Control	Code
Authentication	1. Keyed Cryptographic Hash Functions (HMAC), digital signatures, and random number generators	Aun1
	2. Physically Unclonable Functions (PUF)	Aun2
	3. MAC-attached and HORS-signed messages	Aun3
	4. Secure Sockets Layer (SSL) certificates and Transport Layer Security (TLS)	Aun4
	5. Multi-factor authentication mechanism	Aun5
	6. Automatic lockouts	Aun6
	7. Secure session management	Aun7
	8. Anti-spoofing algorithm	Aun8
Authorisation	9. Attribute-based encryption	Aur1
	10. Attribute certificates	Aur2
	11. Attribute-based access control system based on XACML (Extensible Access Control Markup Language)	Aur3
	12. Role-based access control	Aur4
	13. Allow/block listing	Aur5
	14. Privileged Access Management (PAM)	Aur6
	15. Principle of Least Privilege (POLP)	Aur7
Confidentiality	16. Symmetric and asymmetric algorithms and Public Key Infrastructure (PKI) certificate	C1
Privacy	17. Anonymisation	P1
	18. Trusted aggregators	P2
	19. Encryption	P3
Integrity	20. Cryptographic hashing functions and session keys	In1
	21. Digital watermarking	In2
	22. Adaptive cumulative sum algorithm	In3
	23. Secure Phasor Measurement Units (PMUs) installation	In4
	24. Load profiling algorithms	In5
	25. Timestamps	In6
	26. Sequence numbers	In7
	27. Query sanitisation	In8
	28. Nonces	In9
Availability	29. Use multiple alternate frequency channels according to a hardcoded sequence	Av1
	30. Anomaly Intrusion Detection Systems (IDS)	Av2
	31. Specification-based IDS	Av3
	32. Intrusion Prevention Systems (IPS)	Av4
	33. Quality of Services (QoS)	Av5
	34. Load balancing	Av6
	35. Operating system-independent applications	Av7
	36. Redundancy	Av8
	37. Web Application Firewall (WAF)	Av9
	38. Anti-DDOS algorithm	Av10
	39. Segregation, segmentation, data diode isolation, DMZ, and air gap	Av11
Non-repudiation	40. Mutual inspection technique	N1
	41. Unique keys and digital signatures	N2
	42. Transaction log	N3
Common Controls across all the above requirements	43. Patch management for flaw remediation	Common1
	44. Firewalls	Common2
	45. Endpoint for Detection and Response (EDR)	Common3

Table 5
Sample matrix for the Transmission and Distribution stations access point

Access Point	Internet-based Security Threats from the STRIDE analysis	Security Requirement	Security Control
2. Transmission, Distribution stations	Spoofing	Authentication	Aun2: Physically Unclonable Functions (PUF) Aun4: Secure Sockets Layer (SSL) certificates and Transport Layer Security (TLS) Aur2: Attribute Certificates
		Authorisation	Aur3: Attribute-Based Access Control System based on XACML Aur4: Role-Based Access Control and allow listing

4.2.2. Identifying internet-based threats

Below are the usual types of internet-based cybersecurity threats reported in the literature. They are analysed and grouped on the basis of their STRIDE classification, threat behaviour, and type – whether active or passive [6,7,18,22–24,27,29,30]:

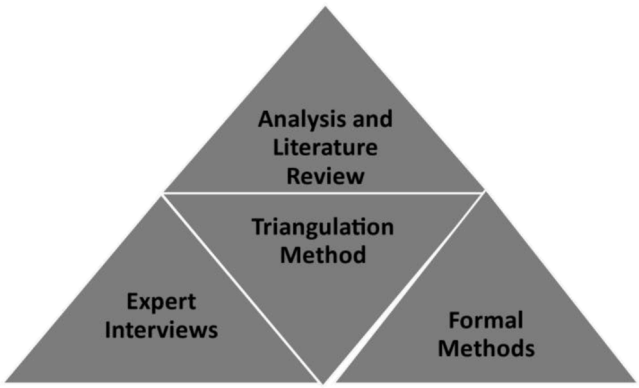

Fig. 3. Research method

Table 6
Summary of interviewees

Expert	Job Description	Domain	Years of Experience
1	Electrical Engineering Associate Professor	Electrical Engineering	12
2	Electrical & Computer Engineering Assistant Professor	Electrical Engineering	14
3	IT Security Engineer at the electricity company, with risk management experience	IT security in electricity systems	22
4	Cybersecurity engineer in the distribution department of the electricity company	Cybersecurity, Distribution	6
5	Cybersecurity Engineer and Risk management expert in Governance Risk Compliance (GRC) sector at the electricity company. Certified by GICSP global industrial cybersecurity professional.	Cybersecurity, Generation, Transmission, and Distribution	7
6	Cybersecurity analyst at the electricity company	Cybersecurity, Distribution	7
7	Cybersecurity engineer in server management	IT Security	15
8	Cybersecurity engineer at the oil company, previously US Smart Grid Engineer, cyber security algorithms developer, and cyber security mentor for 40 trainees	Cybersecurity in Electricity Systems	30
9	Electrical Engineer in contractor company for smart meters project	Electricity Contractor	10
10	Smart Meters Developer, designer and developer SW/HW firmware, experience in security standards	Smart Meter Manufacturing	8
11	Electrical Engineer in an oil company, advanced smart meters project manager, committee secretary of a renewable energy association, a member of standards, metrology and quality organisation	Electrical Engineering	8
12	Telecommunication devices engineer in the transmission department of the electricity company	Transmission (National Grid), Communication	7
13	Electrical engineer at French electricity company, experience in smart meters project in KSA, experience in renewable energy	Electrical Engineering, Energy value chain including Generation, Transmission, Distribution	10
14	Cybersecurity consultant at the electricity company	Cybersecurity, Distribution	12

1 **Spoofing/Impersonation:** An active attack that aims to communicate on behalf of a legal entity through unauthorised access, by stealing its identity. An attacker may impersonate the identity of another's smart meter to pay lower electricity charges – or to get the other person to pay.
2 **Eavesdropping/Traffic analysis/Man-In-The-Middle (MITM):** Passive attacks, capturing transmitted data by intercepting communications between two entities in the SG. In Traffic analysis, the attacker intercepts the communication, analyses the network traffic, then extracts information from the patterns found. This locates key entities such as substations or discloses sensitive information (such as future price information, routeing structure, or the SG's control structure.
3 **Replay attack**: An active attack that intercepts communications between two entities by recording, observing, copying the transmitted data, then replaying a selected part of the copied data back: it manipulates the data before sending back.
4 **Data tampering:** This strikes when an attacker manipulates exchanged data such as dynamic prices ahead of an announcement, making them cheaper. Consequently, it may increase consumer consumption instead of reducing it. This can overload the power network and cause power cuts.
5 **Denial of Service (DOS)/Jamming channel**: An active attack that floods the entire system, resources, or bandwidth with 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.

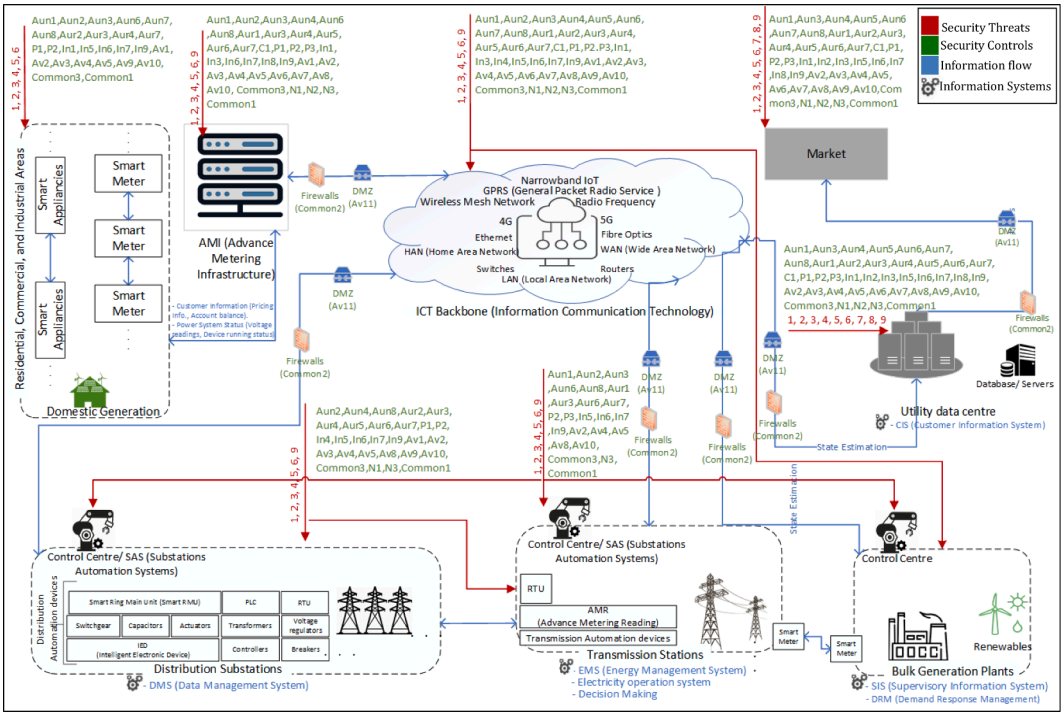

Fig. 4. Security model for an IoT-enabled Smart Grid

6 **Malware injection**: 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 of smart meters or utility servers.

7 **Phishing:** The type within this study's scope is internet-based, such as email phishing and search engine/websites phishing. It tricks users into believing that a message is from a trustworthy organisation, asking them to click a link. This link is malicious, and aims to obtain sensitive information. If a user responds, the attacker can use the information to access the system.

8 **SQL injections:** Structured Query Language (SQL) injections execute a harmful SQL query statement on a server that uses SQL, aiming to force the server to disclose information or modify or delete the database contents. According to Cisco, the query is entered by the attacker using a website search box on the app's client-side interface, and it is used to target databases.

9 **False data injection:** This attack sends fake information into the network, such as false meter readings or wrong prices, and could be carried out against energy distribution and grid state estimation. It causes false state estimation for the SCADA system and may cause power system failure. It has a financial effect on the electricity market by tampering with market price information.

4.2.3. Applying STRIDE

Table 2 shows how threats are mapped to STRIDE categories using the STRIDE and threat definitions used in this study, as provided in Section 4.2.2. In the first instance, each identified threat is mapped to a STRIDE category on the basis of its main effect, thus a spoofing/impersonation threat is mapped to Spoofing in STRIDE. Since eavesdropping, traffic analysis, and MITM threats are passive attacks that observe and capture transmitted data, these threats are mapped to Information disclosure in STRIDE. By contrast, a replay attack is active, in which the attacker observes data then manipulates them, sending them back to the SG. Therefore, this threat is mapped to Information disclosure and Tampering. Data tampering is mapped to Tampering: they have the same meaning. Also, the Denial of Service (DOS)/jamming channel threat is mapped to Denial of service. Malware is mapped to Tampering, as it includes execution of malicious software on the SG. Phishing aims to trick users into believing that a message is from a trustworthy source, trying to obtain sensitive information that could be used to access the system. Thus, as its main effect, phishing is mapped to Information disclosure. Both SQL injection and false data injection are mapped to Tampering, as both involve changing transmitted data and thus targeting a database. False data injection is mapped also to Repudiation, as it could change audit logs and transaction records, leading to denial of responsibility.

Table 3 shows how, in this study, each threat was mapped to security requirements on the basis of the STRIDE mapping and previous studies [25,27,29,30]. Each was assessed to find the key security requirement that had been compromised. In spoofing, as mentioned in the STRIDE mapping, it is Authentication that is affected. In addition spoofing was mapped to Authorisation, because the identity of an authorised user is impersonated. In eavesdropping, in the first instance it is Confidentiality that is affected. Both replay and data tampering attacks were mapped to Integrity, being the security requirement that is most affected. Looking at the desired property column in STRIDE mapping, the Denial of Service (DOS)/jamming channel was mapped to Availability. Malware executes malicious software, thus may Degrade the availability of the system as well as changing the data, threatening also its Integrity.

Table A1
Smart meters and smart appliances matrix

A	B	Common controls	C	D
Access Point	Internet-Based Security Threats from the STRIDE Analysis		Security Requirement	Security Control
1. Smart Meters and Smart Appliances	Spoofing	Common1: Patch management for flaw remediation.	Authentication Authorisation	Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun2: Physically Unclonable Functions (PUF) Aun3: MAC-attached, and HORS-signed messages Aun6: Automatic lockouts Aun7: Secure Session Management Aun8: Anti-Spoofing algorithm Aur2: Attribute Certificates Aur3: Attribute-Based Access Control System based on XACML Aur4: Role-Based Access Control and block listing Aur7: Principle of Least Privilege (POLP)
	Eavesdropping/ Traffic Analysis/ Man-In-The-Middle (MITM)		Confidentiality	Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun2: Physically Unclonable Functions (PUF) Aun3: MAC-attached, and HORS-signed messages Aun7: Secure Session Management Aun8: Anti-Spoofing algorithm Aun6: Automatic lockouts P1: Anonymisation P2: Trusted aggregators
	Replay Attack		Integrity	In1: Cryptographic hashing functions and Session keys In5: Load profiling algorithms In6: Timestamps In7: Sequence numbers
	Data Tampering		Integrity	In9: Nonces
	Denial Of Service		Availability	Av1: Use multiple alternate frequency channels according to a hardcoded sequence Av2: Anomaly Intrusion Detection Systems (IDS) Av3: Specification-based IDS Av4: Intrusion Prevention Systems (IPS) Av5: Quality of Services (QoS) Av9: Web Application Firewall (WAF)
	Malware injection		Availability Integrity	Av10: Anti-DDOS algorithm Av11: Segregation, segmentation, data diode isolation, DMZ, and air gap Common3: Endpoint for Detection and Response (EDR)

Phishing was mapped to Confidentiality as it discloses information. Both SQL injection and false data injection were mapped to Integrity, because they tamper with the data. In addition to Integrity, False data injection was mapped to Non-repudiation due to denial of responsibility, as explained earlier.

4.3. Step 3. Assign threats to the access points

In order to assign the threats identified to an access point, each access point was analysed according to its functionality, operations processed, and information systems located there, as discussed in step 4.2.2. The threats that could be encountered in processing such operations were then considered, and a literature review undertaken, better to map threats to access points [7,30]. The STRIDE model was applied by considering how each threat in the model affects each access point, component, and interconnection [31]. Essentially, each access point was examined to determine whether there were any threats within the S, T, R, I, D, or E categories [31].

Smart meters and smart appliances are devices that send readings yet cannot receive data, so false data injection does not apply. None of the access points, including smart meters, distribution, transmission, generation, ICT, AMI, and SCADA, have a client-side interface, thus neither does phishing apply. Moreover, because they have no database, smart meters, distribution, transmission, generation, ICT, or SCADA are not attacked by SQL injection. Fig. 4 shows the threats at each access point. Details of the matrix for each access point are in Appendix A.

Table A2
Transmission stations, distribution substations, smart automation devices for transmission and distribution matrix

A	B	Common Controls	C	D
Access Point	Internet-Based Security Threats from the STRIDE Analysis		Security Requirement	Security Control
2. Transmission stations, distribution substations, and smart automation devices for transmission and distribution (Switches, Sensors, Actuators, Transformers, Voltage regulator, Capacitors)	Spoofing	Common1: Patch management for flaw remediation	Authentication Authorisation	Aun2: Physically Unclonable Functions (PUF) Aun4: Secure Sockets Layer (SSL) certificates and Transport Layer Security (TLS) Aun8: Anti-Spoofing algorithm Aur2: Attribute Certificates Aur3: Attribute-Based Access Control System based on XACML Aur4: Role-Based Access Control Aur5: allow listing Aur6: Secure Session Management Aur7: Anti-Spoofing algorithm
	Eavesdropping/ Traffic Analysis/ Man-In-The-Middle (MITM)		Confidentiality	Aun2: Physically Unclonable Functions (PUF) Aun4: Secure Sockets Layer Certificates (SSL Certificates) P1: Anonymisation P2: Trusted aggregators
	Replay Attack		Integrity	In4: Secure Phasor Measurement Units (PMUs) installation In5: Load profiling algorithms In6: Timestamps In7: Sequence numbers
	Data Tampering		Integrity	In9: Nonces
	Denial Of Service		Availability	Av1: Use multiple alternate frequency channels according to a hardcoded sequence Av2: Anomaly Intrusion Detection Systems (IDS) Av3: Specification-Based IDS Av4: Intrusion Prevention Systems (IPS) Av5: Quality of Services (QoS) Av8: Redundancy Av9: Web Application Firewall (WAF) Av10: Anti-DDOS algorithm
	Malware injection		Availability Integrity	Av11: Segregation, segmentation, data diode isolation, DMZ, and air gap Common3: Endpoint for Detection and Response (EDR)
	False data injection		Integrity Non-Repudiation	N1: Mutual inspection technique N3: transaction log

4.4. Step 4. Categorise security controls by security requirements

Security controls are countermeasures to mitigate, delay, or prevent threats, thus strengthening the information system. They are the approaches that meet the security requirements. The study's security controls were taken from the literature and Microsoft documentation (2009), and each was categorised by its description, as in Table 4. To map the security controls to the security requirements, the study reviewed all the standards, including NIST IR, NERC CIPS (1-9), NIST IR7628, and NIST SP 800-53. Publications also were reviewed for the purposes of mapping [6,7,26,30]. Table 4 shows the categories of security control across the security requirements.

Table A3
Generation plant and Information Communication Technology (ICT) systems matrix

A	B		C	D
Access Point	**Internet-Based Security Threats from the STRIDE Analysis**	**Common Controls**	**Security Requirement**	**Security Control**
3. Generation Plant and Information Communication Technology (ICT) Systems	Spoofing	Common1: Patch management for flaw remediation	Authentication Authorisation	Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun2: Physically Unclonable Functions (PUF) Aun3: MAC-attached, and HORS-signed messages Aun4: Secure Sockets Layer (SSL) certificates and Transport Layer Security (TLS) Aun5: Multi-factor authentication mechanism Aun6: Automatic lockouts Aun7: Secure Session Management Aun8: Anti-Spoofing algorithm Aur1: Attribute-Based Encryption Aur2: Attribute Certificates Aur3: Attribute-Based Access Control System based on XACML Aur4: Role-Based Access Control Aur5: allow listing Aur6: Privileged Access Management (PAM) Aur7: Principle of Least Privilege (POLP)
	Eavesdropping/ Traffic Analysis/ Man-In-The-Middle (MITM)		Confidentiality	C1: Symmetric and asymmetric algorithms and Public Key Infrastructure certificate (PKI) Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun2: Physically Unclonable Functions (PUF) Aun3: MAC-attached, and HORS-signed messages Aun4: Secure Sockets Layer (SSL) certificates and Transport Layer Security (TLS) Aun5: Multi-factor authentication mechanism Aun6: Automatic lockouts Aun7: Secure Session Management P1: Anonymisation P2: Trusted aggregators P3: Encryption
	Replay Attack		Integrity	In1: Cryptographic hashing functions and session keys
	Data Tampering		Integrity	In3: Adaptive cumulative sum algorithm In4: Secure Phasor Measurement Units (PMUs) installation In5: Load profiling algorithms In6: Timestamps In7: Sequence numbers In9: Nonces
	Denial Of Service		Availability	Av1: Use multiple alternate frequency channels according to a hardcoded sequence Av2: Anomaly Intrusion Detection Systems (IDS) Av3: Specification-based IDS Av4: Intrusion Prevention Systems (IPS) Av5: Quality of Services (QoS) Av6: Load balancing Av7: Operating system-independent Applications Av8: Redundancy

(*continued on next page*)

Table A3 (*continued*)

A	B	C	D
			Av9: Web Application Firewall (WAF)
			Av10: Anti-DDOS algorithm
	Malware injection	Availability Integrity	Av11: Segregation, segmentation, data diode isolation, DMZ, and air gap
			Common3: Endpoint for Detection and Response (EDR
	False data injection	Integrity	N1: Mutual inspection technique
		Non-Repudiation	N2: Unique keys and digital signatures
			N3: Transaction log

4.5. Step 5. Mapping the security controls to the access points

In step 5, each access point had an assigned set of security requirements that, after assessing threats' effects, could be countered by applying appropriate security controls. For every access point, each threat was mapped in the first instance to the security requirements that might be compromised by an attack, as in Table 3 Then, controls were allocated to the relevant security requirements as in Table 4. Only relevant controls that apply to the corresponding access point were assigned, based on the specifications and functionality of that access point. In Authentication, for example, cryptographic hash functions and MAC/HORS-signed messages were not applied to the Transmission and Distribution stations since, as machinery, they are not designed for this type of data processing. Therefore, the controls Aun1 and Aun3 were not assigned to the Transmission and Distribution stations, yet SSL/TLS Certification (Aun4) and Physically Unclonable Functions (PUF) (Aun2) were. In this case, the controls for the Transmission and Distribution stations were mapped as shown in the sample matrix in Table 5.

Authorisation is also compromised in the event of spoofing. Thus, the controls list for Authorisation, as in Table 5, was assessed to determine the relevant controls to be applied to the Transmission and Distribution stations. Attribute-Based Encryption (Aur1) was not assigned, since these stations are not designed to perform encryption, yet Aur2, Aur3, and Aur4 were.

The full mapping matrices for each access point are in Appendix A. The mapping process was validated by expert review, as in Sections 5 and 6.

5. Research methodology

Both quantitative and qualitative approaches were used, because this research is based on mixed methods [32]. A methodical triangulation research technique was adopted to create a comprehensive picture of the research topic and increase the possibility of validating the results [33]. The research technique comprises three methods: analysis and literature review, threat modelling, and expert interview, as shown in Fig. 3.

Using qualitative research techniques, the interviews reviewed 14 experts in the KSA in various electricity domains, including cybersecurity, distribution, transmission, generation, and Information Technology (IT), as in Table 6. Semi-structured interviews were adopted, characterised by open-ended questions. Before conducting any interviews ethical approval was achieved, reference number 62423.

Each interview had three parts. In order to confirm the access points, in Part A the experts were given a diagram of possible access points and invited to suggest changes. To confirm the security controls and requirements in a general context, in Part B the experts were given a table of the controls mapped to each security requirement. In Part C, the experts were asked to confirm the mapping of the controls for each access point to a specific set of potential threats.

6. Experts' review findings

All 14 experts stressed the importance of the security model and of securing such a critical electricity infrastructure across the country. They confirmed that the suggested model could contribute a useful model to support KSA's initiatives to secure automated SGs. The following statement is from **Expert 2:** "*This model is excellent and could have a strong contribution to the field.*" **Expert 3** commented: "*Cybersecurity is a major concern for all countries and critical in any country wishing to secure the electricity infrastructure.*" The findings were grouped into these three parts.

6.1. Part A: Access points

All experts agreed that the access points were all correct and represented IoT-enabled SGs. **Expert 3** said: "*All access points are correct and correspond to our practical datasheets.*" Two changes were proposed and adopted:

1 Adding smart meters between the domains of Generation plants and Transmission.
2 Having control centres within each SG domain, including Generation plants, Transmission, Transmission, Distribution, as shown in Fig. 4.

Table A4
Advanced Metering Infrastructure (AMI) matrix

A	B		C	D
Access Point	**Internet-Based Security Threats from the STRIDE Analysis**	**Common Controls**	**Security Requirement**	**Security Control**
4. Advanced Metering Infrastructure (AMI)	Spoofing	Common1: Patch management for flaw remediation.	Authentication Authorisation	Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun2: Physically Unclonable Functions (PUF) Aun3: MAC-attached, and HORS-signed messages Aun4: Secure Sockets Layer (SSL) Certificates and Transport Layer Security (TLS) Aun6: Automatic lockouts Aun8: Anti-Spoofing algorithm Aur1: Attribute-Based Encryption Aur3: Attribute-Based Access Control System based on XACML Aur4: Role-Based Access Control Aur5: allow listing Aur6: Privileged Access Management (PAM) Aur7: Principle of Least Privilege (POLP)
	Eavesdropping/ Traffic Analysis/ Man-In-The-Middle (MITM)		Confidentiality	C1: Symmetric and asymmetric algorithms and Public Key Infrastructure certificate (PKI) Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun2: Physically Unclonable Functions (PUF) Aun3: MAC-attached, and HORS-signed messages Aun4: Secure Sockets Layer (SSL) certificates) and Transport Layer Security (TLS) Aun6: Automatic lockouts P1: Anonymisation P2: Trusted aggregators P3: Encryption
	Replay Attack		Integrity	In1: Cryptographic hashing functions and session keys
	Data Tampering		Integrity	In3: Adaptive cumulative sum algorithm In6: Timestamps In7: Sequence numbers In8: Query sanitisation
	SQL injection		Integrity	In9: Nonces
	Denial Of Service		Availability	Av1: Use multiple alternate frequency channels according to a hardcoded sequence
	Malware injection		Availability Integrity	Av2: Anomaly Intrusion Detection Systems (IDS) Av3: Specification-based IDS Av4: Intrusion Prevention Systems (IPS) Av5: Quality of Services (QoS) Av6: Load balancing Av7: Operating system-independent Applications Av8: Redundancy Av10: Anti-DDOS algorithm Av11: Segregation, segmentation, data diode isolation, DMZ, and air gap Common3: Endpoint for Detection and Response (EDR)
	False data injection		Integrity Non-Repudiation	N1: Mutual Inspection technique N2: Unique keys and digital signatures N3: Transaction log

6.2. Part B: Security requirements and controls

The experts viewed the requirements and controls from their field of expertise. Accordingly, they acknowledged that the controls are significant, advanced, and comprehensive. **Expert 6** said that "*All the controls listed here are recommended and applicable*". **Expert 8** confirmed that "*the controls included in this research are compatible with the playbook of the company in terms of acting against threats*". **Expert 8** noted: "*The security controls mentioned in the research are beyond the standards in NIST IR and NERC CIP, which both measure the*

Table A5
SCADA Systems matrix

A	B		C	D
Access point	**Internet-based Security Threats from the STRIDE analysis**	**Common Controls**	**Security Requirement**	**Security Control**
5. SCADA/ SAS control centre	Spoofing	Common1: Patch management for flaw remediation.	Authentication Authorisation	Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun2: Physically Unclonable Functions (PUF) Aun3: MAC-attached, and HORS-signed messages Aun6: Automatic lockouts Aun8: Anti-Spoofing algorithm Aur1: Attribute-Based Encryption Aur3: Attribute-Based Access Control System based on XACML Aur6: Privileged Access Management (PAM) Aur7: Principle of Least Privilege (POLP)
	Eavesdropping/ Traffic Analysis/ Man-In-The-Middle (MITM)		Confidentiality	Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun2: Physically Unclonable Functions (PUF) Aun3: MAC-attached, and HORS-signed messages Aun6: Automatic lockouts P2: Trusted aggregators P3: Encryption
	Replay Attack		Integrity	In5: Load profiling algorithms
	Data Tampering		Integrity	In6: Timestamps In7: Sequence numbers In9: Nonces
	Denial Of Service		Availability	Av2: Anomaly Intrusion Detection Systems (IDS)
	Malware injection		Availability Integrity	Av4: Intrusion Prevention Systems (IPS) Av5: Quality of Services (QoS) Av8: Redundancy Av10: Anti-DDOS algorithm Av11: Segregation, segmentation, data diode isolation, DMZ, and air gap Common3: Endpoint for Detection and Response (EDR)
	False data injection		Integrity Non-Repudiation	N3: Transaction log

compliance of any organisation with the policies." The experts concluded that the controls had been correctly mapped to the requirements with the exception of Patch management, where they were of the view that it could serve many security requirements rather than solely Integrity.

All experts agreed that encryption is important for Privacy, yet questioned the use of advanced specific techniques of encryption to preserve privacy: Homomorphic encryption (P3), Perturbation models (P4), Verifiable computation models, and zero-knowledge proof systems (P5), and Data obfuscation techniques (P6). Although Privacy in IoT-enabled SG is important, identifiable data is not highly sensitive at a critical level, unlike medical data records. Therefore, basic encryption should be sufficient to preserve privacy. Consequently, controls P3, P4, P5, and P6 were replaced by basic encryption as a control (P3). Similarly, given the focus of this study, the experts saw the Frequency quorum rendezvous (Av2) as an unnecessary detail, thus Av2 was discarded.

Where the experts wanted to add more controls was in the area of the Availability requirement. These controls include Redundancy, Web Application Firewall (WAF), anti-DDOS, Segregation, Segmentation, Data Diode isolation, DMZ, and Air gap. They stated: "*WAF is a control used to protect the Smart Grid against Distributed Denial Of Service attack (DDOS). This control may be costly for the company. Subsequently, it was recommended that this control be used when the risk exists.*" For Authentication, the experts added two controls: Secure Session Management, and an anti-spoofing algorithm. For Authorisation, the experts added Privilege Access Management (PAM), and Principle of Least Privilege (POLP), saying: "*this principle is that users should only be granted the necessary privileges to complete their tasks*." Moreover, Role-based access control and allow/block listing was split into two controls: Aur4 and Aur5.

A common controls list was added to the model to serve more than one security requirement, which includes Patch management, Firewalls, and EDR.

All added controls and changes are shown in Table 4, giving both the confirmed modified controls list and the common list.

6.3. Part C: Threats and controls

All experts agreed on the list of attacks for each access point. **Expert 3** stated, "*all these attacks are potential threats in electricity systems*". The experts concluded that the controls are correctly mapped to the access points and threats. **Expert 2** reported: "*These*

Table A6
Utility data centre matrix

A	B		C	D
Access point	**Internet-based Security Threats from the STRIDE analysis**	**Common Controls**	**Security Requirement**	**Security Control**
6. Utility data centre	Spoofing	Common1: Patch management for flaw remediation.	Authentication Authorisation	Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun3: MAC-attached, and HORS-signed messages Aun4: Secure Sockets Layer (SSL) certificates and Transport Layer Security (TLS) Aun5: Multi-factor authentication mechanism Aun6: Automatic lockouts Aun7: Secure Session Management Aun8: Anti-Spoofing algorithm Aur1: Attribute-Based Encryption Aur2: Attribute Certificates Aur3: Attribute-Based Access Control System based on XACML (Extensible Access Control Markup Language) Aur4: Role-Based Access Control Aur5: Allow listing Aur6: Privileged Access Management (PAM) Aur7: Principle of Least Privilege (POLP)
	Eavesdropping/ Traffic Analysis/ Man-In-The-Middle (MITM)		Confidentiality	C1: Symmetric and asymmetric algorithms and Public Key Infrastructure certificate (PKI) Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun3: MAC-attached, and HORS-signed messages Aun4: Secure Sockets Layer (SSL) certificates and Transport Layer Security (TLS) Aun5: Multi-factor authentication mechanism Aun6: Automatic lockouts Aun7: Secure Session Management P1: Anonymisation P2: Trusted aggregators
	Phishing		Confidentiality	P3: Encryption
	Replay Attack		Integrity	In1: Cryptographic hashing functions and Session keys
	Data Tampering		Integrity	In2: Digital watermarking In3: Adaptive cumulative sum algorithm In5: Load profiling algorithms In6: Timestamps In7: Sequence numbers In8: Query sanitisation
	SQL injection		Integrity	In9: Nonces
	Denial Of Service		Availability	Av2: Anomaly Intrusion Detection Systems (IDS)
	Malware injection		Availability Integrity	Av3: Specification-based IDS Av4: Intrusion Prevention Systems (IPS) Av5: Quality of Services (QoS) Av6: Load balancing Av7: Operating system-independent Applications Av8: Redundancy Av9: Web Application Firewall (WAF) Av10: Anti-DDOS algorithm Av11: Segregation, segmentation, data diode isolation, DMZ, and air gap Common3: Endpoint for Detection and Response (EDR)
	False data injection		Integrity Non-Repudiation	N1: Mutual Inspection technique N2: Unique keys and digital signatures N3: Transaction log

security controls are deeply covered for each access point in this research." **Expert 8** stated: "*it is of importance to invest in the security controls presented in this research*."

Some experts did not comment on all the aspects and access points, as each team was responsible for just part of the SG. One control previously added in Part B was the Endpoint for Detection and Response (EDR), which was mapped against malware threats for all access points. Staff training was not added to the controls list since this is not an internet-based technical control: non-technical and human-based controls are beyond the scope of this research.

Since this study focuses on IoT-enabled SGs, it assumes the use of IP addresses, so legacy systems are not considered to be a potential physical threat but merely an internet-based threat. For the same reason, non-internet based social engineering is beyond the scope of

Table A7
Market matrix

A	B		C	D
Access point	**Internet-based Security Threats from the STRIDE analysis**	**Common Controls**	**Security Requirement**	**Security Control**
7. Market	Spoofing	Common1: Patch management for flaw remediation.	Authentication Authorisation	Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun3: MAC-attached, and HORS-signed messages Aun4: Secure Sockets Layer (SSL) certificates and Transport Layer Security (TLS) Aun5: Multi-factor authentication mechanism Aun6: Automatic lockouts Aun7: Secure Session Management Aun8: Anti-Spoofing algorithm Aur1: Attribute-Based Encryption Aur2: Attribute Certificates Aur3: Attribute-Based Access Control System based on XACML (Extensible Access Control Markup Language) Aur4: Role-Based Access Control Aur5: allow listing Aur6: Privileged Access Management (PAM) Aur7: Principle of Least Privilege (POLP)
	Eavesdropping/ Traffic Analysis/ Man-In-The-Middle (MITM)		Confidentiality	C1: Symmetric and asymmetric algorithms and Public Key Infrastructure certificate (PKI) Aun1: Keyed cryptographic hash functions (HMAC), digital signatures, and Random number generators Aun3: MAC-attached, and HORS-signed messages Aun4: Secure Sockets Layer (SSL) certificates and Transport Layer Security (TLS) Aun5: Multi-factor authentication mechanism Aun6: Automatic lockouts Aun7: Secure Session Management P1: Anonymisation P2: Trusted aggregators
	Phishing		Confidentiality	P3: Encryption
	Replay Attack		Integrity	In1: Cryptographic hashing functions and session keys
	Data Tampering		Integrity	In2: Digital watermarking In3: Adaptive cumulative sum algorithm In5: Load profiling algorithms In6: Timestamps
	SQL injection		Integrity	In7: Sequence numbers In8: Query sanitisation In9: Nonces
	Denial Of Service		Availability	Av2: Anomaly Intrusion Detection Systems (IDS)
	Malware injection		Availability Integrity	Av3: Specification-based IDS Av4: Intrusion Prevention Systems (IPS) Av5: Quality of Services (QoS) Av6: Load balancing Av7: Operating system-independent Applications Av8: Redundancy Av9: Web Application Firewall (WAF) Av10: Anti-DDOS algorithm Av11: Segregation, segmentation, data diode isolation, DMZ, and air gap Common3: Endpoint for Detection and Response (EDR)
	False data injection		Integrity Non-Repudiation	N1: Mutual inspection technique N2: Unique keys and digital signatures N3: Transaction log

this study. Internet-based phishing is considered, such as email phishing and search engine/websites phishing. Furthermore, this research focused on common types of internet-based security threats identified from the literature and STRIDE analysis. Therefore, the current study did not investigate sophisticated, multi-stage threats such as SolarWinds and APT.

Buffer overflow attack was not added to the threats list, as it is considered to be a common type of Denial Of Service attack (DOS) that is an effective method of performing DOS attacks. Buffer overflow attack is included under DOS. Similarly, DDOS was not added to the threats list because it is considered to be a type of DOS attack, in which multiple systems send fake requests to a single target.

7. Conclusion

In conclusion, five controls were discarded from the model initially proposed, while two were subdivided, nine were added, and one was re-assigned. This created a common control list. It was clear that the proposed security model is significant and useful, and this was confirmed. As shown in Fig. 4 it contains seven access points, seven security requirements, nine threats, and 45 controls. All elements have undergone threat analysis, literature review, and expert review.

The model addresses the limitation of the NIST model, namely that it is a high-level conceptual model that lacks detail. By contrast, the proposed model is more practical and useful for related sectors to employ. This research will be beneficial to system designers, information security practitioners, and other 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 system design for the IoT-enabled SG. This model could be applied in other countries, worldwide, but would require further research.

The next phase of this study is to have the model verified using Event-B formal methods with the Rodin platform and provers. A formal security model will be developed, using formal modelling to demonstrate that the developed model maintains appropriate controls to mitigate internet-based threats to the information flow around the IoT-enabled SG. A formal template will be developed to allow field experts and engineers to verify any changes that are made so that these do not compromise the security of this information flow.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No data was used for the research described in the article.

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.

Appendix A. The access points matrixes

This part shows the modified matrixes of each access points according to findings analysed from the expert review.
Table A1-A7

References

[1] Al-Ali AR, Aburukba Raafat. Advanced role of Internet of Things in the Smart Grid technology. J Comput Commun 2015:229–33. https://doi.org/10.4236/jcc.2015.35029. Role.
[2] Mohammadali Amin, Haghighi Mohammad Sayad, Tadayon Mohammad Hesam, Mohammadi-Nodooshan Alireza. A novel identity-based key establishment method for advanced metering infrastructure in Smart Grid. IEEE Trans Smart Grid 2018;9(4):2834–42. https://doi.org/10.1109/TSG.2016.2620939.
[3] Das Ashok Kumar, Zeadally Sherali. Data security in the Smart Grid environment. Elsevier; 2019. https://doi.org/10.1016/B978-0-08-102592-5.00013-2.
[4] Bekara C, Luckenbach T, Bekara K. A privacy preserving and secure authentication protocol for the advanced metering infrastructure with non-repudiation service. Proc ENERGY 2012;(c):60–8.
[5] Bekara Chakib. Security issues and challenges for the IoT-based Smart Grid. Procedia Comput Sci 2014;34:532–7. https://doi.org/10.1016/j.procs.2014.07.064.
[6] EPRI, "EPRI | SmartGrid Resource Center," 2005. https://smartgrid.epri.com/ (accessed Jan. 07, 2020).
[7] ETP, "Smart Grids European Technology Platform-EARPA," 2006. https://www.earpa.eu/earpa/39/etp_smartgrids.html.
[8] Aloul Fadi A. The need for effective information security awareness. J Adv Inf Technol 2012;3(3):176–83. https://doi.org/10.4304/jait.3.3.176-183.
[9] Dalipi Fisnik, Yayilgan Sule Yildirim. "Security and privacy considerations for IoT application on Smart Grids: survey and research challenges. In: Proc. - 2016 4th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2016; 2016. p. 63–8. https://doi.org/10.1109/W-FiCloud.2016.28.
[10] IEEE, "About - IEEE Smart Grid," 2018. https://smartgrid.ieee.org/about-ieee-smart-grid (accessed Dec. 04, 2019).
[11] IET, "What is a Smart Grid?," 2013. Accessed: Jan. 07, 2020. [Online]. Available: https://www.theiet.org/media/1251/smart-grids.pdf.
[12] Stellios Ioannis, Kotzanikolaou Panayiotis, Psarakis Mihalis, Alcaraz Cristina, Lopez Javier. A survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun Surv Tutorials 2018;20(4):3453–95. https://doi.org/10.1109/COMST.2018.2855563.
[13] Manyika James, Chui Michael, Bisson Peter, Woetzel Jonathan, Dobbs Richard, Bughin Jacques, Aharon Dan. Unlocking the Potential of the Internet of Things. McKinsey 2015 [Online]Available: //mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.
[14] Joel Singer, "Enabling Tomorrow's Electricity System: Report of the Ontario Smart Grid Forum," 2009. [Online]. Available: http://www.ieso.ca/en/Learn/Ontario-Power-System/etno/-/media/files/ieso/document-library/smart_grid/Smart_Grid_Forum-Report.pdf.
[15] Creswell John Ward, Creswell John David. Research Sesign: qualitative, quantitative, and mixed methods approaches. Sage 2017.
[16] Kamto Joseph, Qian Lijun, Fuller John, Attia John. Light-weight key distribution and management for advanced metering infrastructure. In: 2011 IEEE GLOBECOM Work. GC Wkshps 2011; 2011. p. 1216–20. https://doi.org/10.1109/GLOCOMW.2011.6162375.

[17] Khuffash Kamal Al. Smart grids—overview and background information. Elsevier; 2018. https://doi.org/10.1016/b978-0-12-803128-5.00001-5. vol. 2007, no. Eisa 2007.
[18] Kimani Kenneth, Oduol Vitalice, Langat Kibet. Cyber security challenges for IoT-based Smart Grid networks. Int J Crit Infrastruct Prot 2019;25:36–49. https://doi.org/10.1016/j.ijcip.2019.01.001.
[19] Mahmood Khalid, Chaudhry Shehzad Ashraf, Naqvi Husnain, Shon Taeshik, Ahmad Hafiz Farooq. A lightweight message authentication scheme for Smart Grid communications in power sector. Comput Electr Eng 2016;52:114–24. https://doi.org/10.1016/j.compeleceng.2016.02.017.
[20] Cohen Louis, Manion Lawrence, Morrison Keith. Research methods in education. 8th edition. Routledge; 2013. https://doi.org/10.4324/9781315456539.
[21] Microsoft, "The STRIDE Threat Model | Microsoft Docs," *Microsoft Docs*, 2009. https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN (accessed May 12, 2020).
[22] Benmalek Mourad, Challal Yacine, Derhab Abdelouahid. Authentication for Smart Grid AMI systems: threat models, solutions, and challenges. In: Proc. - 2019 IEEE 28th Int. Conf. Enabling Technol. Infrastruct. Collab. Enterp. WETICE 2019; 2019. p. 208–13. https://doi.org/10.1109/WETICE.2019.00052.
[23] Gunduz Muhammed Zekeriya, Das Resul. Cyber-security on Smart Grid: threats and potential solutions. Comput Networks 2020;169:107094. https://doi.org/10.1016/j.comnet.2019.107094.
[24] NIST, "NIST Special Publication 1108R3 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," 2014. doi: 10.6028/NIST.SP.1108r3.
[25] Ganguly Pallab, Nasipuri Mita, Dutta Sourav. A novel approach for detecting and mitigating the energy theft issues in the smart metering infrastructure. Technol Econ Smart Grids Sustain Energy 2018;3(1). https://doi.org/10.1007/s40866-018-0053-x.
[26] Ganguly Pallab, Nasipuri Mita, Dutta Sourav. Challenges of the existing security measures deployed in the Smart Grid framework. In: Proc. 2019 7th Int. Conf. Smart Energy Grid Eng. SEGE 2019; 2019. p. 1–5. https://doi.org/10.1109/SEGE.2019.8859917.
[27] Khan Rafiullah, Mclaughlin Kieran, Laverty David, Sezer Sakir. STRIDE-based threat modeling for cyber-physical systems. *Proc - IEEE PES Innovative Smart Grid Technologies* 2017:0–5.
[28] Sofana Reka S, Dragicevic Tomislav. Future effectual role of energy delivery : a comprehensive review of Internet of Things and Smart Grid. Renew Sustain Energy Rev 2018;91(April):90–108. https://doi.org/10.1016/j.rser.2018.03.089.
[29] Tonyali Samet, Akkaya Kemal, Saputro Nico, Selcuk Uluagac A, Nojoumian Mehrdad. Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems. Futur Gener Comput Syst 2018;78:547–57. https://doi.org/10.1016/j.future.2017.04.031.
[30] Shahid Tufail, Imtiaz Parvez, Shanzeh Batool, and Arif Sarwat, "A survey on cybersecurity challenges, detection, and mitigation techniques for the Smart Grid," *Energies*, vol. 14, no. 18, pp. 1–22, 2021, doi: 10.3390/en14185894.
[31] U.S. Department of Energy, "Smart Grid System Report 2018: Report to Congress," 2018. [Online]. Available: www.energy.gov/sites/prod/files/2019/02/f59/SmartGridSystemReportNovember 2018_1.pdf.
[32] US Public Law, "Energy Independence and Security Act of 2007," 2007. [Online]. Available: https://www.gpo.gov/fdsys/pkg/PLAW-110publ140/html/PLAW-110publ140.htm.
[33] Mrabet Zakaria El, Kaabouch Naima, Ghazi Hassan El, Ghazi Hamid El. Cyber-security in Smart Grid: survey and challenges. Comput Electr Eng 2018;67:469–82. https://doi.org/10.1016/j.compeleceng.2018.01.015.

Abeer Akkad is a lecturer in the Information System at the faculty of Computing and Information Technology at King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia. She is a PhD Candidate in the Computer Science at the University of Southampton, United Kingdom

Gary Wills is an associate professor in Computer Science at the University of Southampton. He graduated from the University with an Honours degree in Electro-mechanical Engineering, and then a PhD in Industrial Hypermedia Systems. He is a member of the Institute of Engineering Technology, The International Association of Privacy Professionals. His research focuses on Secure Systems Engineering and Applications.

Abdolbaghi Rezazadeh is a Senior Teaching Fellow in the Cyber-Physical Systems (CPS) Research Group of the Electronics and Computer Science Department at the University of Southampton, United Kingdom.