On Security And Privacy In Smart Metering Systems

David Bačnar *, Lolita Leytner †, Rene Prenc **, Veljko Jardas ‡, Jonatan Lerga *
* University of Rijeka, Faculty of Engineering/Department of Computer Engineering, Rijeka, Croatia
** University of Rijeka, Faculty of Engineering/Department of Electric Power Systems, Rijeka, Croatia
† University of Angers, Polytech Angers/Automation and Computer Engineering Department, Angers, France
‡ Jatro d.o.o., Owner and CEO, Rijeka, Croatia
dbacnar@riteh.hr; leytnerlolita@gmail.com; rprenc@riteh.hr; veljko.jardas@jatro.hr; jlerga@riteh.hr

***Abstract*—Smart meters are modernizing the electrical energy systems, solving numerous problems of the classical systems, and introducing new functionalities to the grid. This paper aims to give an insight into these systems in terms of their security and privacy aspects. Special attention is paid to the energy theft problem (meter tampering, physical anti-tampering measures, and theft detection methods). We, next, address other security issues present in remote metering (attack types, risks, and threats to the system). Also, necessary security requirements and signature-based, anomaly-based, and specification-based Intrusion Detection Systems (IDS) are defined. We conclude by listing privacy concerns arising due to the remote meters and advanced metering infrastructures (AMI) being installed more and more.**

***Index Terms*—smart metering; energy theft; theft of service; advanced metering infrastructure (AMI); security; privacy**

I. Introduction

One of the major concerns for the Advanced Metering Infrastructure (AMI) and smart metering is security, opening various new security challenges when compared to the classical system with electromechanical meters [1]. Securing smart meters is a challenging task due to the fact that they are located at customer premises, thus making them easily accessible physically [1]. By gaining access to a smart meter, it is possible to alter its system (both hardware and software) and change the meter's readings [2]. This can lead to incorrect billing, resulting in financial gains for the fraudulent customer. There are many existing threats for the smart meters and AMI, with new ones constantly appearing, some of which can have serious consequences and be utilized for large-scale attacks. With the addition of new and more complex features and functionalities installed into the AMI, the cyber-security concerns for the AMI is also growing and needs to be taken into careful consideration [3]. Furthermore, some AMI security issues are related to customer privacy, while others are associated with cyber-security due to the possibility of unauthorized access to the smart meters and other devices. So it is a top priority to secure the smart meters and the AMI against these kinds of attacks.

A. Attacker profiles and misuse of smart metering data

To better understand the general security risks for the AMI and smart meters, an attacker profile needs to be established. This is done by determining which type of persons want the smart metering data and for what purpose. With that information, it is possible to determine the security requirements necessary to protect the AMI and remote meters. Also, there are third parties that want to use the smart metering data for more legal purposes, which still might infringe on the privacy of the customers [4]. The attackers and other parties that use smart metering data can be generally divided into a few groups depending on use case of the data, as follows [5]:

- *Utility companies:* To determine bills, monitor the electricity usage, and execute demand management.
- *Law enforcement:* To identify suspicious or illegal activities at the customer premises.
- *Marketers and data management agencies:* To collect private information for marketing or economic purposes.
- *Curious eavesdroppers:* To snoop on the activities of their neighbors.
- *Passive attackers:* To show off their hacking abilities and knowledge of penetration techniques.
- *Customers:* To steal electricity, paying less bills, thus achieving monetary gains.
- *Utility insiders:* Workers with direct access and knowledge of the system that, for some personal reason, want to sabotage the system or a certain customer.
- *Malicious eavesdroppers:* To identify wealthy households and estimate the best time for burglary.
- *Active attackers:* To launch large-scale terrorist attacks on the power system or the utility.

Sensitive data in the AMI can be classified into several groups, as follows [4]. System data that shouldn't be accessible to unauthorized parties, like meter health reports, firmware integrity, clock synchronization. Control commands that need to be received and executed correctly, and their logs. Network data such as collision rates, packet loss, traffic time, response times. Authorized AMI protocols and policies, devices, traffic patterns, routes, and firmware updates. Billing information that contains the price of electricity and bills paid that shouldn't be manipulated by unauthorized parties. Customer's personal information consisting of the customer's daily electricity use profile, credit card information, and other personal information

that unauthorized parties shouldn't access.
This paper provides an insight into the field of smart metering security and privacy, giving a good summary as a starting point for readers wanting to enter the field of smart metering. Thus, this paper addresses the topics of energy theft, meter tampering, anti tampering and theft detection methods. Further, it addresses security concerns by describing attack types, risks and general threats, as well as elaborates on security requirements and Intrusion Detection Systems. Finally, the privacy concerns and goals are showcased and discussed. The rest of the paper is structured as follows. Section II addresses electrical energy theft, followed by the theft detection methods described in Section III. Physical security meters implemented in smart meters are given in Section IV. Other security issues and requirements are defined in Section V, with privacy concerns being elaborated in Section VI. The paper closes with concluding remarks in Section VII.

II. Energy theft

Energy theft is one of the most common threats for AMI and smart metering systems. Also called theft of service, it occurs when a customer manipulates the metering device physically or, in the case of smart meters, manipulates the Power Consumption Data (PCD) sent to the utility [6]. Energy theft leads to great financial losses for utility companies worldwide, especially in developing countries, where sometimes up to 50% of electrical energy can be lost via theft of service, however it can occur in developed countries as well [4]. Energy theft in the legacy pre-AMI energy systems was committed by physical manipulation of the analog meters. In the AMI, it is committed by tampering with the data while being recorded, stored in the smart meter, or while being transmitted to the utility company [7].
Furthermore, the software-based attacks are more widespread due to criminal organizations that professionally develop such solutions for further commercial distribution, making them require less expertise, and hence being easier to run by the customer [7]. In general, there are three different types of electricity losses:

- Transmission and Distribution Losses (T&DL)
- Technical Losses (TLs)
- Non-Technical Losses (NTLs)

T&DLs are the total energy losses - they can be calculated as the difference between the energy supplied and the energy consumed. TLs are the internal losses of the system that are a result of energy dissipation in the system's various components [8]. NTLs are constituted of losses due to flaws in the supply, errors in billing, defective meters, and malicious activities by the consumer, such as meter tampering, that results in energy theft [9]. NTLs are determined simply by subtracting the calculated TLs from the T&DLs as follows:

$$NTL = T\&DL - TL \tag{1}$$

$$T\&DL = Energy\ Supplied - Bills\ Paid \tag{2}$$

$$NTL = Energy\ Supplied - Bills\ Paid - TL \tag{3}$$

Next, we list methods for meter tampering, voltage tampering, current tampering, and hacking/altering of meter's memory.

A. Meter tampering methods

There are several types of meter tampering methods that can be divided in the following categories [2], [9]:

1) Mechanical tampering: Mechanical tampering methods include some of the following. Putting magnets on the meter to interfere with the metering equipment, used mostly for analog meters. Opening the meter and manipulating the meter's insides, for instance, the current transformer or stopping the rotor on an analog meter. Jamming or blocking the wireless communication capabilities of the meter and making it unable to communicate with the utility, thus not sending billing information or acting upon commands. Exposing the meter to High-voltage and high-frequency discharge far larger than its nominal limitations, thus damaging the internal components.

2) Voltage tampering: Voltage tampering methods include some of the following. Interchanging the phase and neutral wires, reversing the energy flow through the meter, making it count backward, and thus affecting billing. The voltage inputs of the meter or its Potential Transformer (PT) are disconnected from the lines, making the total recorded power zero due to the missing potential difference. Manipulating the voltage on the meter's voltage inputs, by decreasing it, thus decreasing the energy billed. Disturbing the neutral wire of the meter load side is connected to the ground directly or through passive components like diodes, variable resistors, or capacitors, instead of the load neutral that is connected to the ground. Disconnecting the neutral, also known as single wire operation, where both the meter and load neutral wires are disconnected, and the load neutral is connected to the ground. Thus making the meter measure zero voltage, hence reading zero energy being consumed.

3) Current tampering: Current tampering methods include some of the following. Bypassing the current transformer (CT) terminals, reducing the current going through the meter and thus reducing the reading as well. Saturating the CT with direct current, limiting its performance for alternating current. Switching both the load and input terminals of the meter, making a reverse connection, thus reversing the energy flow through the meter. If an external CT is used, in case of high loads, its outputs can be disconnected from the meter, making the current reading zero. Double feeding or bypassing the meter, by connecting some loads directly to the supply, circumventing the meter, or bypassing the meter altogether for all loads by using bypass feeders, bypassing just the phase or both the phase and neutral. Disconnecting the neutral wire for three-phased systems reduces the meter readings by 30%.

4) Hacking or altering memory: New smart meter specific attacks are data-oriented and can be deployed in distinct ways, as follows [1]. Preventing the smart meter from being able to record the energy as it's being consumed. Modifying the already stored and recorded data that is in the memory of the smart meter before it is sent to the utility. Modifying data while being transmitted, where false data is injected, or the

data is intercepted and modified in the communication network while being sent from the smart meter to the utility. Resetting the maximum demand register that saves the maximum power that was consumed in the established billing interval [8]. If a customer surpasses a certain threshold, they are billed a penalty, so the penalty will be avoided by resetting it. Changing the tariff registers that store the energy prices and reducing them. Changing the calibrated stored ratios of the measurement transformer ratios used for the calculations, reducing them so that it seems like less energy was consumed. Changing the internal real-time clock of the meter so that the lower tariff is applied, for instance, to charge less during peak hours.
Next, we present different theft detection methods.

III. Theft detection

There are several classical theft detection techniques that originate from the era of analog meters and can still be used today. However, the smart meters have made it possible also to use the historical already recorded energy consumption data of the customer or the two-way communication with the meters in conjunction with computer software algorithms to generate a list of suspect customers that might be committing energy theft [10]. Some legacy theft detection techniques are the following [2]. Comparison of the meter's readings with a control balance meter, installed for a number of customers. Installing an additional control meter at the customer's premises as a way of proving that energy theft is occurring. By placing a roaming balance meter in the substation; if the readings of all the customers' metes do not balance with the roaming meter, then an additional meter is placed closer to the customers, and this process is repeated. In this way, it is possible to find the location of the energy theft, with 15-minute cycle meter reading periods.
Using the PCD from the smart meters, it is possible to determine the energy consumption load profile of a customer or group of customers over a period of time [4]. This is achieved by using data mining, data analytics, or artificial intelligence techniques. The purpose of this is to distinguish the suspicious energy usage patterns from all the other patterns using a threshold value. The types of these computer-aided techniques can be grouped as follows [4]:

- *State-based:* Uses devices in the field, like Radio-Frequency Identification (RFID) tags and wireless sensors. Physical monitoring, mutual smart meter inspection, or state estimation could be used as well. Its limitation is the extra investments required due to the specific hardware used for detection.
- *Classification-based:* Trains a classifier (nowadays usually artificial intelligence based) using malicious and non-malicious data samples. Machine learning techniques are used, such as support vector machine, convolutional neural networks, as well as fuzzy logic, and peer-to-peer computing for the data classification.
- *Game-theory-based:* Simulates a game between the utility and the electricity thieves, where the goal of the utility is to find the thieves, and the goal of the energy thieves is to steal energy unnoticed. This approach is low cost due to not requiring any extra field hardware. However, it is difficult to formulate the functions between the utility and the thieves.

It is also important to state that the recorded data resolution, or rather the period at which the used energy is recorded, greatly influences the theft detection rate; the greater the data resolution, the better the insight into the energy consumed (improved detection rate). However, this directly contradicts the privacy aspects because the larger data resolution means, on the other hand, increased privacy risks [4].

IV. Smart meter physical security measures

Smart meters have, besides software-based, several built-in physical protection mechanisms that are designed to deter and detect tampering of the meter; some of those are [2]:

a) Housing integrity: The housing of the meter is usually welded or held together by easily deformable screws or clips, or have tamper-indicating seals that break easily, which indicate tampering attempts.

b) Lack of physical switches: Most models of meters have no switches or knobs accessible, only some advanced models make use of those switch and knob capabilities. This is due to the fact that those can be used to allow for write access or other manufacturer functions.

c) Motherboard construction: The design of the motherboard is such that it is hard to access the microprocessor or communication circuits, often those being placed between other circuit boards. Also, some components or circuit boards may have omitted markings, thus making it harder to identify certain components and reverse engineer the smart meter.

d) Magnetic field detector and anti-tamper switches: These are used to record a tampering attempt, either by sensing a magnet being placed close to the meter with a magnetic reed switch or detecting the meter housing being removed by normally closed switches that are held in place by the housing.

e) Firmware and authorization: Each smart meter model needs to have proprietary firmware designed for only that model and a matching hardware-against-software-piracy key. Also, the meter is often designed so that it needs a password to do firmware modification, generated when the firmware is flashed in the factory (only known to the manufacturer).

f) Communication encryption: The usual encryption used is the advanced encryption standard using 128-bit length keys (AES-128). So even if attackers use the same technology and have access to the communication, they still can't access the data without the encryption-decryption key. Protection measures against replay attacks, besides encryption, include adding timestamps, sequences of numbers, session key signatures, using one number only once, to messages making them unique and not easily replayed or easily detectable as a replay attack by the system [10], [11]. In case the physical-protection mechanisms are triggered, the event is logged, alarming the utility company. The customer is then at least flagged as suspicious, or an inspection team is sent to investigate the tampering attempt [8].

V. Other security issues and requirements

The next big issue with smart metering is other kinds of attacks that aren't aimed at energy theft but may have more serious consequences, such as causing system failures or exposing the customers' privacy. The AMI and smart meters are adding new functionalities to the electric energy system; however, they are also adding new challenges and security risks, some of which are addressed in the sequel.

A. Attacks and risks

The smart meter consists of several components, each susceptible to different possible attack types, and when one smart meter is compromised, as a result, all the other smart meters become vulnerable, as well as the entire AMI. The list of smart meter components and corresponding distinctive attacks are given next [3]:

a) Control unit: Possible modification of the circuit board, giving the attacker remote control possibilities.

b) Metrology system: Possible hardware and firmware reverse engineering, enabling an attacker to steal information or to escalate privileges, thus having control over the metering.

c) Smart meter data collector: Possible interception of data, resulting in data theft or denial of data communication for multiple customers.

d) Home Area Network (HAN): Possible data theft and denial of data communication for one customer.

e) Optical interface: Possible port snooping to discover passwords or install modified firmware.

B. General threats

The threats to the AMI and smart meters can be grouped into the following categories [11]:

1) System-level threats: Where the goal of the attacker is shutting down parts or the entire power grid through the AMI, those threats include the following. Network subversion or takeover where the attacker takes control of a smart meter and through it targets other smart meters on the network also trying to take control over them, usually done with modified smart meter firmware on the wireless HAN. Network intrusion where the attacker joins the network to send unauthorized traffic, prevent the smart meters from communicating properly or intercept relay traffic with the possibility of modifying it. Most likely to happen with wireless communications. Denial-of-Service (DoS) where the attacker tries to make the network performance unusable. These kinds of attacks include techniques such as signal jamming that blocks the signal, routing attacks where traffic is redirected to a dead-end (also called a "black hole"), jabbering where a number of nodes are forced to send data overloading the network causing network flooding, stack smashing that overloads the smart meter's memory and crashes the operating system or application, dropping packets selectively allowing only certain data to go through the network, and resource exhaustion such as CPU or memory being kept constantly fully occupied. Credential compromise where the attacker tries to gain access to the entire system through authentication holes (the attacker tries to gain significant system control). Office backend compromise where attackers try to gain access to the AMI management database that stores confidential data such as credentials for system control, or they could access the billing, thus committing theft of service or gaining private customer information.

2) Theft of service threats: Where the goal is to steal electricity, or in case of organized attacks, destabilize the grid or the electrical energy price system, causing losses for the utility company, those being the following. Meter substitution/cloning where the meter is cloned and substituted with a duplicate that reports zero or reduced usage, or as a mean to impersonate other meters. Meter migration/swapping where the meter, or its communication module, is swapped from a location with high energy use to a location with low energy use, thus billing less energy consumption. Meter module interface intrusion, where the communication module can be disconnected from the main circuit board so that the meter stops reporting consumption data to the utility. It is also possible for the attacker to access the communication module and replay previous consumption data messages, also known as a replay attack.

3) Privacy/confidentiality threats: Where the goal is to access information that can expose customers private details, those threats include. Message interception/eavesdropping, where the attacker passively monitors the network to capture packets, usually on a wireless network. Forwarding point compromise where a node is compromised so that it forwards data to the attacker, usually a data concentrator or a gateway device. Backhaul Internet Protocol (IP) network interception can be intercepted as it is transmitted through the utility company backhaul network that is used for data aggregation and control commands.

C. Security requirements

Some security requirements for the AMI are covered by the Information Communication Technology network security standards by default. However, there are some AMI specific security requirements that also have to be addressed, the main of those being [7], [11]:

a) Confidentiality and privacy: The access to the data should only be allowed to authorized parties and should otherwise be kept confidential.

b) Integrity: The data needs to be authentic, complete and without modifications, exactly matching the source data.

c) Availability: The data needs to be accessible to authorized parties whenever needed under approved conditions.

d) Non-repudiation or accountability: All the parties that exchange the data, whether they received it or sent it, can't subsequently deny execution, or acknowledge it without it actually being executed. This is ensured through audit logs with time-synchronized records of the data exchanges.

e) Authentication or identification: There should be an authentication mechanism built-in that discards unauthorized parties from accessing the AMI.

f) Access control: All the parties that have access to the data need to enforce adequate authorization and authentication requirements.

D. Intrusion detection system (IDS)

One of the methods of verifying the smart metering data is to analyze the network traffic for anomalies in real-time using an Intrusion Detection System (IDS). The IDS can reduce the risk of energy theft and DoS or Distributed-Denial-of-Service (DDoS) attacks, among other possible attacks. An IDS can be embedded into several elements of the AMI and used for multiple parts of the AMI [12], or it can be used only for a specific part of the AMI [10]. There are three different approaches for IDS [10]:

- *Signature-based detection:* Searches for patterns of malicious behavior by searching a database of predefined attack patterns.
- *Anomaly-based detection:* Uses a predefined normal behavior profile obtained from statistical analysis and identifies deviations from the norm.
- *Specification-based detection:* Uses a predefined correct behavior profile obtained from logical specifications and identifies deviations from the correct behavior.

The signature-based IDS uses a black-list approach, while the anomaly-based and specification-based IDS techniques use a white-list approach. The black-list approach utilizes a knowledge base of known attacks and malicious activity; thus, it's not possible to detect unknown attacks, and it needs to be updated frequently [10]. As opposed to the black-list approach, the white-list approach requires training the system with normal and correct behavior; thus, it is more computationally expensive to train while providing little information on what kind of attack was detected. The IDS usually has a 20% threshold to eliminate false positive triggered events. However, there is a high possibility of detecting a false positive, by of up to 95% [1].

Several possible IDS deployment architectures can be used, as follows [1]. A centralized IDS is where a single sensor is used to monitor all traffic through the AMI. It can detect attacks on the network and insider attacks by monitoring logs. However, it isn't able to detect eavesdropping in the Neighborhood Area Networks (NANs) and meter firmware tampering. With an embedded sensing infrastructure it is possible to use a number of meters as sensors by having several specially outfitted meters, monitoring meter-specific information like memory, health reports, and firmware. Furthermore, in a mesh network, those sensor meters can also monitor traffic. However, the hardware power of these meters should be sufficient due to the more intensive processing (if compromised, severe harm would occur). There is also a possibility to have dedicated sensing infrastructure deployed in the field. Specialized sensors with high processing power are often deployed in a relatively small number. The sensors are able to monitor the network and have a smaller chance of being attacked due to their smaller number. However, these sensors cannot monitor the smart meter health status and firmware tampering or detect HAN attacks. Hybrid sensing infrastructure is the combination of central sensors together with sensors embedded in the smart meters, where meter sensors would cover attacks that target smart meters, malicious packet network attacks, and HAN attacks. Dedicated sensors could be used instead of embedded or in conjunction with them.

E. Communication standards

The security and privacy are essentially greatly dependent on the communication technology being used, being that wired communication (Power Line Communication - PLC, Public Switched Telephone Network - PSTN, Digital Subscriber Line - DSL) or wireless communication (Radio Frequency - RF, Zigbee, Bluetooth, WLAN, mobile communications, etc.), which we showcase in more detail in our latest paper that gives insight into communication technologies utilized in smart metering systems [13].

Likewise, the communication standards or protocols being used mostly depend on the technology selected, however they have a greater impact on privacy and safety. Some of the protocols that can be used are the following, PoweR-line Intelligent Metering Evolution (PRIME), G3-PLC, IEEE P1901 / Broadband over Power Lines (BPL), M-Bus, IEC 62056 / Device Language Message Specification (DLMS) / Companion Specification for Energy Metering (COSEM), among others. Where PRIME is an open and global standard used for multivendor equipment compatibility in the lower system layers. G3-PLC provides interoperability, robustness and security using Orthogonal Frequency Division Multiplexing (OFDM). M-Bus provides the prerequisites for remote reading multivendor smart meters. IEC 62056 / DLMS / COSEM has an object-oriented structure that allows for application data reading from multivendor smart meters, and supports most types of common communication technologies.

VI. Privacy concerns

Despite the privacy measures already implemented in smart meters and the AMI, privacy concerns are still raised due to the concept of smart metering itself. This is due to the fact that smart meters can send detailed PCD readings in near real-time [10], thus making it possible to extract much more information from that data than just the amount of energy being consumed. There are tools that have been developed for the purpose of profiling customers' electricity usage to determine which appliances are being used in the household [10]. Third parties or even criminals could use this information; thus, it represents a privacy concern. Research has shown that it is possible to analyze the smart meter data and extract personal information about the occupants of the household. The non-intrusive load monitoring shows spikes in consumption that can be correlated to specific appliances [14]. So by taking into account the magnitude and duration of the appliance use, it is possible to deduce information about the occupant's daily routine. For instance, some examples are: how many occupants are in the household, when do they wake up, when they go to bed, and when they are absent from the household [15]. There is an ongoing debate on who exactly owns the smart metering data [8], with the utility companies often arguing that they are the ones owning it because they own the smart meter itself.

However, that means that the utility company, or whoever they decide to provide the data to, can entirely trace the customers' behavior [7]. There is no complete solution for this issue yet, and the security measures put in place to combat energy thefts and cyber-attacks are raising these privacy concerns even more. The bare minimum that should be done about the privacy issues is for the utility company to guarantee the confidentiality of such information [7].

A. Privacy goals

There are several privacy goals set for the smart meters and AMI, some of which are listed in the following [11]:

a) Anonymity: It is possible to achieve this by using consumer-to-utility anonymity where the utility has only anonymous identifiers for the smart meters, thus making it impossible for an unauthorized third party to know the identity of the customer.

b) Unlinkability: It should be impossible to link two parties in the system using the captured data, since it isn't sufficiently descriptive on these two parties. This is implemented on the HAN or NAN side.

c) Undetectability: The network devices or the data that could be of interest to a third party could be used to detect information about the customer. Hence, the data should be undetectable to third parties.

d) Observability: A third party shouldn't be able to tell if the communication is occurring or not; it shouldn't be able to distinguish if the smart meter executed any actions according to sent commands.

e) Pseudonymity: The smart meter needs to have several identifiers, one for each of the authorized party that is accessing it and at least one anonymous identifier.

In concluding, the provided study gives an insight into security and privacy issues in smart metering systems, which will become even more critical with more frequent use of intelligent, remote metering devices. As shown, smart metering opens numerous beneficial potentials for customers and opens various questions that have to be properly addressed.

VII. Conclusion

This paper provides an insight into smart metering with a focus on security and privacy issues. We addressed the energy theft problem, detailing meter tampering methods, physical anti-tampering measures, and theft detection methods. Next, security concerns of smart metering were described, listing attack types, risks, and general threats to the system. We also elaborate on security requirements and the advantages of utilizing the IDS. Finally, the privacy concerns were discussed, with some privacy goals being listed. It can be concluded that the smart meters are modernizing the electrical energy system, solving many problems of the legacy system, and introducing new functionalities to the grid. However, they are also opening new security and privacy questions that need to be assessed and solved carefully, since, in some cases, their consequences could be severe. The two requirements set for the modern smart meters and the AMI, those being security and privacy, seemingly contradict each other, so a balance between them has to be established through careful studying all benefits and challenges for a particular technical solution.

Acknowledgement

This work was supported by the IRI2 project "ABsistemDCiCloud" (KK.01.2.1.02.0179), and University of Rijeka projects uniri-tehnic-18-17 and uniri-tehnic-18-15.

References

[1] Stephen McLaughlin, Brett Holbert, Ahmed Fawaz, Robin Berthier, and Saman Zonouz. A multi-sensor energy theft detection framework for advanced metering infrastructures. *IEEE Journal on Selected Areas in Communications*, 31(7):1319–1330, July 2013.

[2] Robert Czechowski and Anna Magdalena Kosek. The most frequent energy theft techniques and hazards in present power energy consumption. In *2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG)*, pages 1–7. IEEE, April 2016.

[3] Asad Masood Khattak, Salam Ismail Khanji, and Wajahat Ali Khan. Smart meter security: Vulnerabilities, threat impacts, and countermeasures. In Sukhan Lee, Roslan Ismail, and Hyunseung Choo, editors, *Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM) 2019*, pages 554–562, Cham, 2019. Springer International Publishing.

[4] Rong Jiang, Rongxing Lu, Ye Wang, Jun Luo, Changxiang Shen, and Xuemin Shen. Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, 19(2):105–120, April 2014.

[5] Enrique Reyes Archundia Juan Carlos Olivares Rojas. Smart metering system, 2018.

[6] Gueltoum Bendiab, Konstantinos-Panagiotis Grammatikakis, Ioannis Koufos, Nicholas Kolokotronis, and Stavros Shiaeles. Advanced metering infrastructures: Security risks and mitigation. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES '20, New York, NY, USA, jul 2020. Association for Computing Machinery.

[7] Ramyar Rashed Mohassel, Alan Fung, Farah Mohammadi, and Kaamran Raahemifar. A survey on advanced metering infrastructure. *International Journal of Electrical Power & Energy Systems*, 63:473–484, dec 2014.

[8] Fabio Toledo. *Smart metering handbook*. PennWell, Tulsa, Oklahoma, 2013.

[9] Arjun Choudhary and Lehri Divam. *A Survey of Energy Theft Detection Approaches in Smart Meters*, pages 9–24. Springer, 12 2020.

[10] Nikos Komninos, Eleni Philippou, and Andreas Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys Tutorials*, 16(4):1933–1954, Fourthquarter 2014.

[11] Pardeep Kumar, Yun Lin, Guangdong Bai, Andrew Paverd, Jin Song Dong, and Andrew Martin. Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Communications Surveys Tutorials*, 21(3):2886–2927, thirdquarter 2019.

[12] Panagiotis I. Radoglou-Grammatikis and Panagiotis G. Sarigiannidis. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access*, 7:46595–46620, 2019.

[13] David Bačnar, Lolita Leytner, Nino Stojković, and Jonatan Lerga. (in press). An Insight Into Communication Technologies Utilized in Smart Metering Systems. In *2022 45th International Convention on Information, Communication and Electronic Technology (MIPRO)*, May 2022.

[14] Timo Jakobi, Sameer Patil, Dave Randall, Gunnar Stevens, and Volker Wulf. It is about what they could do with the data: A user perspective on privacy in smart metering. *ACM Trans. Comput.-Hum. Interact.*, 26(1):1–44, jan 2019.

[15] Giulio Giaconi, Deniz Gündüz, and H. Vincent Poor. Smart meter data privacy. Preprint, 09 2020.