IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 9 December 2023, accepted 25 December 2023, date of publication 1 January 2024,
date of current version 9 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3349091

RESEARCH ARTICLE

A Secure and Resilient Smart Energy Meter

HUSSAM A. HSEIKI[1], AHMAD M. EL-HAJJ[2], (Member, IEEE), YOUSSEF O. AJRA[1], FATHELALEM A. HIJA[3], (Member, IEEE), AND ALI M. HAIDAR[1]

[1]Department of Electrical and Computer Engineering, Beirut Arab University (BAU), Beirut 1107 2809, Lebanon
[2]Olayan School of Business, American University of Beirut, Beirut 1107 2020, Lebanon
[3]Cyber Security Graduate Program, Joaan Bin Jassim Academy for Defence Studies, Al Khor, Qatar

Corresponding author: Hussam A. Hseiki (hah350@student.bau.edu.lb)

ABSTRACT The expansion of the Internet of Things (IoT), Smart Grids (SG), and renewable energy sources has created a greater need for effective cybersecurity measures. These systems need to be protected from all threats in order to maintain continuity and functionality. Smart grids are made up of integrated modules that rely on essential data communication. Each module is exposed to different cybersecurity issues that, if compromised, will affect the entire system. This study addressed the security and data integrity issues in smart energy meters (SEMs), which are critical components in smart grid networks. After a comprehensive review of existing products and their features, a security-focused design for the SEM was proposed. The proposed solution provides a multi-level design to ensure the hardware, communication, and data security of the SEM. The solution mitigates Distributed Denial of Service (DDoS) attacks, data integrity issues, data privacy and energy theft. The security of a smart meter depends on securing two-way data communication, data processing and data integrity. To achieve this goal, the authors leveraged LoRaWAN technology in smart grid communications and unidirectional data transmission to ensure network security and resilience.

INDEX TERMS Artificial intelligence, cybersecurity, data diode, Internet of Things (IoT), LoRaWAN, smart grid, smart meter, sustainable energy.

I. INTRODUCTION

Energy production, distribution, control, and management systems must be integrated to solve issues arising from increased energy demand, environmental concerns surrounding fossil fuels, various green energy sources, variable energy tariffs, smart meters, and smart homes [1].

As a result, sustainable energy systems have become more complicated, leading to additional vulnerabilities that cybercriminals can exploit, as well as an increase in the likelihood of catastrophic failures and wide-ranging effects.

Because the energy infrastructure is so vital and depends so heavily on technology, it is crucial to address cyber risks in sustainable energy systems. The environment, economy, and society may all be significantly affected by any disruption or collapse of sustainable energy systems. Cyber assaults on sustainable energy systems can have several negative effects, including equipment damage, data breaches, power outages, and financial losses [2]. Many entities, including nation-states, criminal gangs, and single hackers, can launch these attacks [3].

In order to protect the energy infrastructure from the previously stated risks, it is imperative to identify the cyber-attack surfaces with respect to hardware and network configurations, protocols, and software [4], as the proverb says: ''A chain is only as strong as its weakest link''.

This paper presents a study on the evolution of energy meters from conventional induction and incremental counting type meters to Automatic Meter Reading (AMR), and Remote Meter Reading (RMR), and finally smart energy meters. A detailed comparison of the different types of meters in terms of functionalities and security vulnerabilities is presented in section II.

Section III introduces the Smart Energy Meter (SEM) functionalities and the cyber-attack surface including the physical, data and communication layers.

Section IV discusses the use of LoRaWAN technology in smart grids in terms of security, power consumption, strengths, and weaknesses.

The associate editor coordinating the review of this manuscript and approving it for publication was Arash Asrari.

Section V presents the novel design of smart energy meter that preserves the network from distributed denial of service attacks (DDOS) along with data feasibility and protection. A practical description of the proposed SEM is presented in section VI. The seventh section of this paper discusses the implementation of the proposed SEM showing some results and data communication in addition to presenting a client-side application for home appliances control.

Section VIII presents a security evaluation of the proposed design versus other SEM design and a commercial SEM using an ethical hacking methodology in lab environment.

The paper concludes by giving an insight for future research in this sector.

II. BACKGROUND

The invention of energy meters was essential after the commercialization of electricity, with the main goal of measuring the energy usage in (kilowatt-hours). This goal was the base of all the evolution of energy meters which can be categorized into three different groups: conventional, AMR/RMR, and smart energy meters [5].

The conventional power networks utilize the conventional meters that measure and display the total consumption of consumer load [6]. There is no data communication between the meter and the utility company which requires manual reading of the consumption and prevents dynamic pricing, load shifting, automatic billing and other limitations.

The second evolution in energy metering was the AMR and RMR, which depended on an electronic reader with one-way communication to send the consumption value to the utility company [7]. This type of meters provides the utility with time-based reading which is crucial for dynamic pricing, network monitoring, load shifting, etc.. However, this information is not provided to the consumer limiting the energy management and monitoring in an interactive way.

The third group and most recent type is the SEM that fills up the gaps in the AMRs data communication, by allowing a bi-directional communication between the smart meter and the utility company as well as data interchange between the smart meter and the consumer's home area network [8]. It consists of a computing unit attached to multiple sensors, power supply, timing module, control, and a communication infrastructure (wired such as Power Line Communication (PLC) or wireless). This huge development exposed the meter and its data to multiple cyber-attacks and cyber threats resulting in smart meter shutdowns and service interruptions.

Another comparison between the meters' types in terms of data security and integrity, according to [5], [9], [10], and [11], is shown in Table 1. It reveals the advantage of AMR over the SEM in protecting data integrity and preventing denial of service attacks.

Based on [12], [13], [14], and [15], a comparison between the different types of meters in terms of functionality is shown in Table 2, which highlights the huge advantage of the smart energy meters have over the other types. The SEM has the lowest operational cost and best power grid stability.

TABLE 1. Security and data issues in conventional, AMR/ RMR and SEM.

Meter type / Security issues	Conventional	AMR/RMR	SEM
Human error	True	False	False
Malicious code	N/A	False	True
Buffer overflow	N/A	False	True
SQL injection	N/A	False	True
DOS / DDOS	N/A	False	True
Data integrity issue	N/A	False	True

TABLE 2. Functionality comparison between conventional, AMR/ RMR and SEM.

Meter type / Functionality	Conventional	AMR/RMR	SEM
Energy use measurement	Ture	True	True
Display	True	True	True
Energy theft detection	False	Partial	Mostly
Remote reading	False	True	True
Automatic billing	False	True	True
Data communication	N/A	One way	Bi-direct.
Home device control	False	False	True
Dynamic pricing	False	True	True
Load shifting	False	Partial	True
Peak clipping	False	Partial	True
Firmware update	N/A	False	True

A comparison of conventional, AMR/RMR, and SEM electricity meters demonstrates that SEMs have different advantages. Because they rely on manual readings, traditional meters lack data security safeguards, making them vulnerable to human mistake and data tampering. AMR/RMR meters provide automation benefits by minimizing manual errors and permitting remote readings; however, they still have data security constraints. SEMs, on the other hand, reduce human errors, provide exact energy measurements, and improve data integrity through enhanced automation. SEMs, on the other hand, are more vulnerable to malicious code and attacks, demanding robust security measures. SEMs provide real-time remote reading, comprehensive home device control, dynamic pricing flexibility, and sophisticated load-management features. They also support firmware updates for continued improvement. Although AMR/RMR meters provide automation benefits, SEMs are the leading option, providing a comprehensive and advanced framework for effective energy management in the growing digital ecosystem, with a particular emphasis on data security

TABLE 3. Comparison between existing smart meter designs in terms of computing units, features, and the security of WiFi connection.

Authors Features & issues		Muralidhara et al. [16]	Purnama et al. [17]	Munoz et al. [18]	Pawar et al. [19]	Spanò et al. [20]	US
Properties	Number of processors	1	2	1	1	2	2
	Communication b/w processors	-	Two-way	-	-	Two-way	One-way
	Control home equipment	Yes	No	Yes	Yes	Yes	Yes
	Duplicate data storing	No	Yes	No	No	No	Yes
	Separate communication (meter→ HAN & meter→ DC)	No	Yes	No	Yes	Yes	Yes
Security Breaches (WiFi 2.4 GHz)	Buffer Overflow	Yes	Both computing units	Yes	Yes	Both computing units	CUB only affected
	DOS - HAN	Yes	Yes	Yes	Yes	Yes	Maybe
	DOS – meter	Yes	Yes	Yes	Yes	Yes	No
	DOS – Utility Network	Yes	Yes	Yes	Yes	Yes	No
	Data Integrity	Yes	Yes	Yes	Yes	Yes	No
	SQL injection	Yes	Yes	Yes	Yes	Yes	No

concerns. The proposed meter integrates the beneficial security and data integrity aspects of AMR/RMR with the advanced functionality of smart energy meters. The proposed SEM addresses key security issues as well as improved load management, dynamic pricing, and home appliance control. It improves system stability and resilience by mitigating the risks of SQL injection, DOS attacks and data integrity issues, protecting against potential vulnerabilities in the energy management infrastructure.

III. SMART ENERGY METER (SEM) CYBER ATTACK SURFACE

SEM is a key component of the AMI which in turn is a component of the SG architecture. SEM has two communication paths: one connects to the Home Area Network (HAN) and the other links to the utility network via the Data Concentrator (DC) [21].

According to the "Benchmarking smart metering deployment in the EU-28" [22], SEM is expected to provide ten key functionalities:

a) Direct readings directly to the consumer and/or any third party.

b) Regularly updated readings to support energy saving schemes.

c) Remote reading by the operator.

d) 2-way communication for maintenance and control

e) Sufficient of frequent readings for network planning

f) Support for advanced tariff systems

g) Remote ON/OFF control of the supply AND/OR flow or power limitation

h) Secure data communications

i) Fraud prevention and detection

j) Import/export and reactive metering

SEMs face a spectrum of security challenges, spanning the physical, data, and communication layers, making them susceptible to diverse types of attacks. Given their deployment at customer sites, outside the direct control of utility companies, SEMs are particularly vulnerable to hardware-based attacks. These vulnerabilities manifest in attacks targeting the physical components of the SEM, posing a direct threat to its integrity and functionality. These security vulnerabilities include bidirectional communications between SEM and Utility Center (UC) through DC [23], [24], lack of resources in SEM [25], customer interference [26], and direct access via web application. These weaknesses may be exploited by impersonation [27], overflow, SQL injection [28], [29], DoS, or DDoS [30] attacks, which have a critical impact on the system such as SEM instability or complete shutdown.

The exposures in data layer can be stated as direct customer access to the SEM [31], remote firmware update, and lack of security configuration in the UC, leading to exploitation by firmware manipulation [32], injection of false data [33], [34], and DoS attacks. These hazards have a main influence on all smart grid functionalities such as data loss [35], integrity, theft, and denial of transfer [36].

The communication layer plays a crucial role in SEM as it connects the UC to the HAN. This layer is susceptible to multiple threats including wireless communication technology [37], [38], transmission media [39], and wireless technology security [40], [41]. These vulnerabilities lead to session hijacking [42], data loss, and bandwidth loss, resulting in data theft, data manipulation, and denial of service.

Table 3 compares the features of various smart meter designs and evaluates their resilience to different types of attacks. Among the designs considered, the proposed SEM design exhibits the least susceptibility to security breaches in the WiFi 2.4 GHz spectrum.

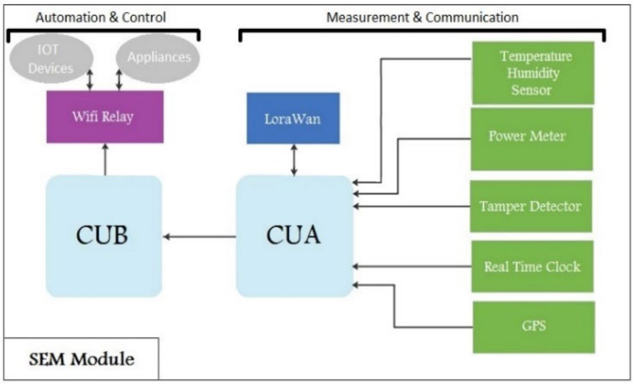


FIGURE 1. Block level SEM design.

IV. LORAWAN USAGE IN SMART GRIDS

The incorporation of the LoRaWAN technology into the design of a smart grid network offers several major benefits. First, LoRaWAN's capacity to communicate over great distances (up to 10 km) makes it particularly appropriate for smart-grid applications [43]. This increased range is critical for linking SEMs in diverse locations [44], [45].

Furthermore, the low power consumption of LoRaWAN is advantageous, particularly in battery-powered SEMs [46], [47]. This function significantly increases the lifespan of SEM batteries, lowers maintenance costs and improves the overall smart-grid efficiency.

Security is critical in smart grid systems, and LoRaWAN addresses this issue by using AES encryption [48]. This encryption ensures secure communication by protecting data from illegal access and breach.

The adaptability of LoRaWAN can be seen in its usefulness in both local and large-scale applications [49]. This scalability enables simple deployment with few infrastructure requirements, resulting in a cost-effective solution [50]. The usage of unlicensed frequency ranges, as well as the relatively low cost of network deployment [51], contributes to the cost-effectiveness of LoRaWAN. However, it is crucial to remember that this benefit may have negative side effects in the form of network congestion [4]. Effective network planning [52], use of Adaptive Data Rate (ADR), and efficient channel utilization tactics are recommended to address this issue

Although there are some general drawbacks to LoRaWAN [53], such as low bandwidth, line-of-sight constraints, and limited device compatibility, these limitations are not important in the current architecture. The use of small message sizes, a preplanned network architecture, and the inclusion of the LoRaWAN connection in both SEM and DC ensure that these limitations have no negative impact on the performance of the smart grid system. Overall, the use of LoRaWAN technology improves the architecture of smart grids by offering a strong, secure, and cost-effective communication infrastructure [54].

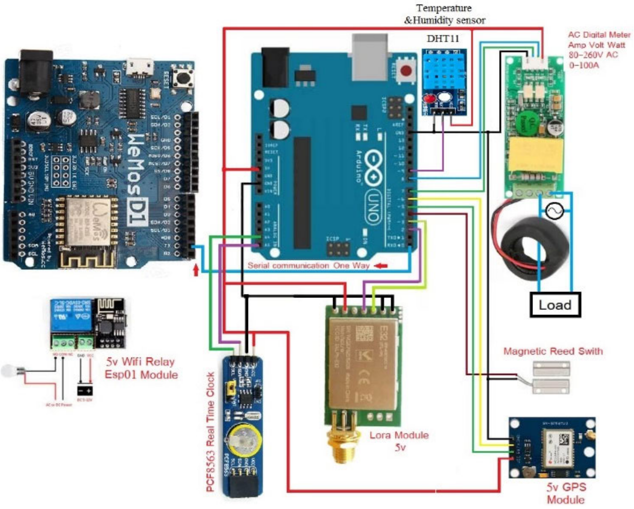


FIGURE 2. Real SEM circuit design.

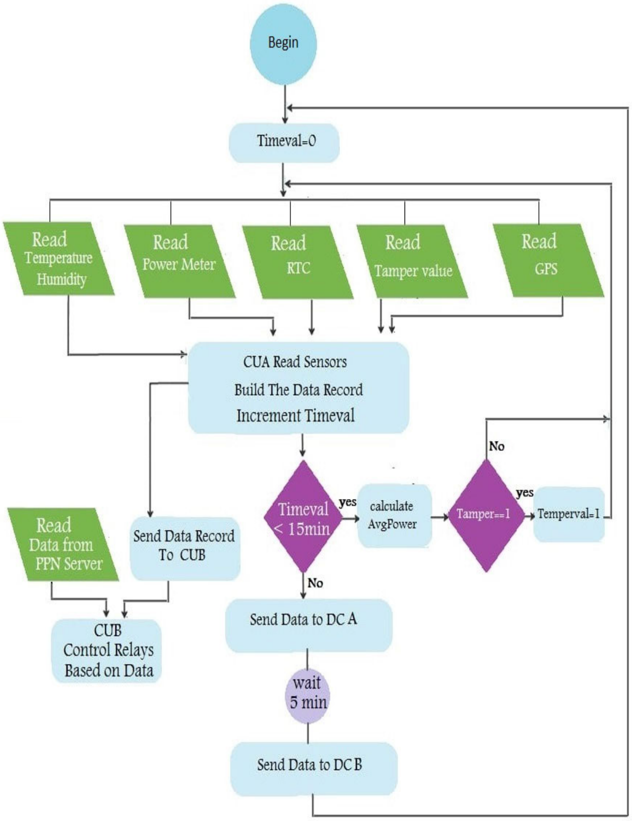


FIGURE 3. SEM data communication flowchart.

LoRaWAN is a communication technology that is vulnerable to the effects of meteorological variables [55] such as sun radiation, humidity, and temperature [17]. These weather conditions influence the Received Signal Strength Indicator (RSSI), which is a metric measured by the receiving device. The RSSI values shift in response to weather changes, thereby providing a dynamic aspect into the communication environment [56], [57].

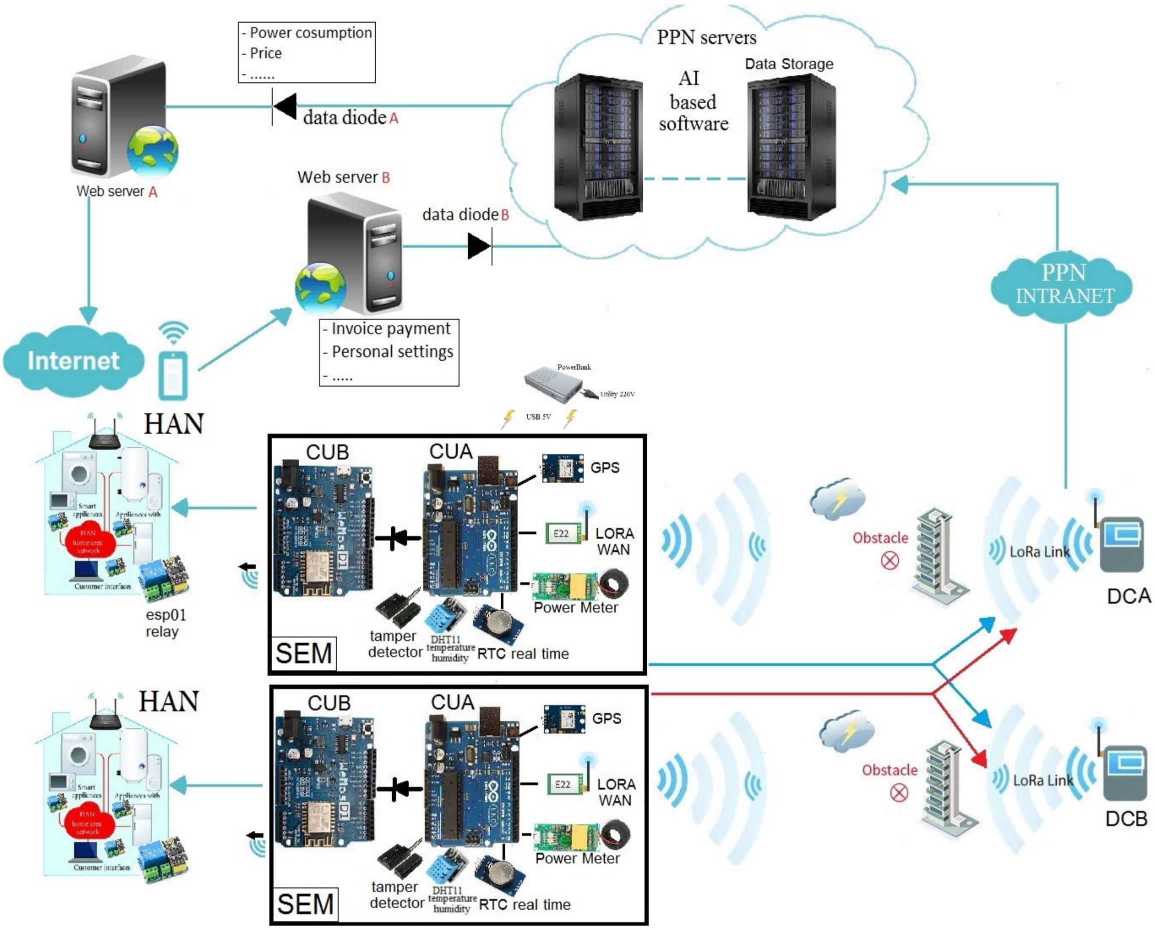


FIGURE 4. Proposed smart grid security design.

To overcome the difficulty of weather-related changes in the RSSI [58], [59], one solution involves storing acceptable RSSI ranges. These preconfigured ranges serve as reference points for comparing real-time RSSI values. An increase in the number of out-of-range connection trials is read as a warning, indicating a possible DoS assault. This strategy allows the system to detect anomalous communication patterns that indicate malicious attempts to disrupt or compromise the network.

Weather conditions have been identified as a potential risk in LoRaWAN, particularly in terms of RSSI changes. However, the use of preset RSSI ranges and redundant DCs contributes to a more robust system, allowing for the identification of potential denial-of-service attacks and improving overall network stability.

V. PROPOSED SMART ENERGY METER (SEM)

The proposed smart energy meter (SEM) design aims to provide a novel solution for energy measurement that incorporates multiple components, ensuring secure, robust, and resilient functionality. The design, as illustrated in Fig.1 and Fig.2 addresses the aforementioned threats and vulnerabilities. According to the design, every SEM is composed of two computing units: A (Arduino-UNO), B (Arduino-WeMos D1), tamper detection sensor, GPS module, real-time clock, LoRaWAN module, temperature sensor, humidity sensor, and digital multipurpose meter.

This design prevents attacks on the UC network from SEM by isolating the customer network from the utility network. This isolation takes into consideration the requirement of feeding the HAN with information and control signals from the SEM or UC. Computing unit A performs all functionalities of the ordinary computing unit in an SEM, except for the ability to connect to the customer's network or the HAN. However, it transmits the required data in a one-way direction to computing unit B, which has the resources to connect to the customer's network and control IoT devices.

A. MAIN COMPUTING UNIT (CUA)

As shown in Fig.3, CUA is responsible for data gathering of power related readings (power, voltage, current, etc.), GPS, real-time clock, and tamper detection. These data are partially processed in CUA then encrypted through the LoRaWAN connection to the Data Concentrators (DCA, DCB) redundantly to ensure reception and integrity for every preset time interval that does not exceed 15 min. The data sent to the DCs were also sent to the secondary computing unit CUB through a one-way serial connection. To keep the consumer connected directly and frequently updated on the consumption, extra data is generated and sent to the CUB with time intervals not exceeding 30 seconds.

B. SECONDARY COMPUTING UNIT (CUB)

The CUB receives the required information through an input serial port in a minimum data sampling of 2 records per minute. This information is stored for a certain number of records in a First Come First Served (FCFS) queue technique. It processes this information and controls the IoT devices in the HAN according to the preset control rules, or when the customer makes a policy change.

C. CUSTOMER'S APPLICATION

Web and mobile applications are developed that allow the customer's device to connect to the CUB in addition to the utility's public server, as shown in Figure 4. Records saved in the CUB are limited by the small memory, but they are used for comparison with those saved at the utility server to ensure data integrity and provide the consumer with data at a higher frequency rate (two records per minute instead of one record every 15 minutes).

D. CONNECTION TO THE DCs

Every SEM has two predefined LoRaWAN connections to Data Concentrator A (DCA) and Data Concentrator B (DCB), which receives connections according to certain GPS value ranges and the stored Received Signal Strength Indicator (RSSI) interval ($RSSI_{min}$, $RSSI_{max}$) per connection. LoRaWAN offers several advantages for transmitting small amounts of information including low power consumption, long range communication, frequency range, and AES encryption [46], [48], [60]. A DC has two primary goals: relaying data from SEMs to the UN, and transmitting commands to SEMs from the UN. To ensure that data are received, with no single point of failure due to hardware faults or cyberattacks, the design specifies a redundant DC connection for every SEM.

Reliance on redundant DC is a crucial element in this scenario. The RSSI values of SEM connections can vary based on the DC employed, whether DCA or DCB. Taking use of this redundancy increases the resilience to the system. By comparing RSSI values across redundant DCs, the network receives more insight into the dependability and consistency of the SEM-to-DC connections, assisting in filtering out aberrant fluctuations caused by weather conditions.

VI. PRACTICAL DESCRIPTION OF THE PROPOSED SMART ENERGY METER (SEM)

This section presents a complete explanation of the design with respect to the physical, data, and communication layers and how it diminishes the effect of various types of attacks on each layer.

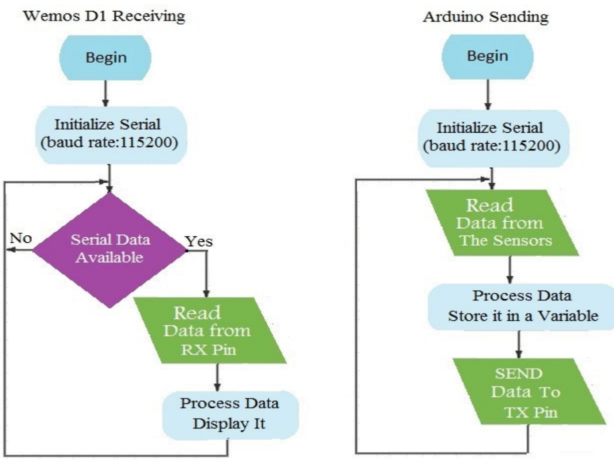

Wemos D1 Receiving
Begin
Initialize Serial (baud rate:115200)
No
Serial Data Available
Yes
Read Data from RX Pin
Process Data Display It
Arduino Sending
Begin
Initialize Serial (baud rate:115200)
Read Data from The Sensors
Process Data Store it in a Variable
SEND Data To TX Pin

FIGURE 5. Arduino-UNO & Arduino-WeMos D1 data transfer flowchart.

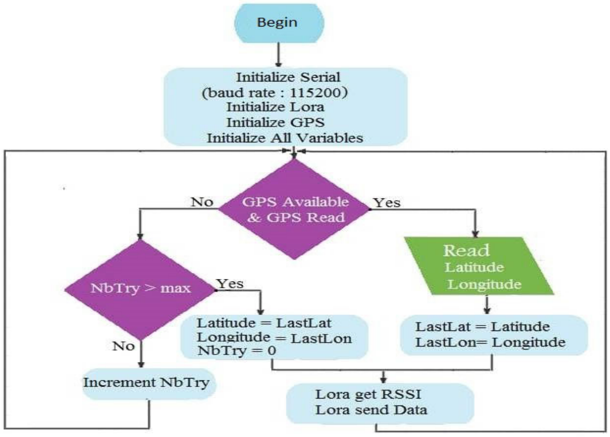

Begin
Initialize Serial (baud rate : 115200) Initialize Lora Initialize GPS Initialize All Variables
No
GPS Available & GPS Read
Yes
NbTry > max
Yes
No
Read Latitude Longitude
Latitude = LastLat Longitude = LastLon NbTry = 0
LastLat = Latitude LastLon= Longitude
Increment NbTry
Lora get RSSI Lora send Data

FIGURE 6. GPS and RSSI values read & sent to data concentrators flowchart.

Numerous attacks at the physical level of SEM have the ability to shut down the SEM to the widespread denial of service and total blackout. The attacker executes a buffer overflow attack, sends malicious code to affect the firmware of the SEM or the data stored in the SEM, or performs an SQL injection, DoS, or DDoS attack. All the aforementioned attacks can be achieved in a unique processor design by direct access to the user. However, in the proposed design, the attacker cannot access the main computing unit (CUA). The main computing unit (CUA) sends the required information to the client through the secondary computing unit (CUB) in a one-way link ensured by the hardware. The main computing unit CUA ensures that the hardware is not manipulated by checking tamper detection sensor readings. If any unauthorized access to hardware is detected, this initiates a predefined action by disabling the SEM and triggering anti-theft measures. The Global Positioning System (GPS) module is read by the CUA and its information is sent to the utility network through the data concentrators. This information was checked by the data concentrator before forwarding the message to the UC. Any invalid matching of the SEM ID and the GPS value will cause the message to be disregarded, and an alert is raised if a certain number of mismatches or thresholds are exceeded.

Denial of data transfer and data loss or modification are the most influential results of attacks at the data layer. In the proposed meter design, the data cannot be modified because of the separation of the data-gathering processor CUA from the direct access of the client. Regarding the data loss or denial of data transfer risk, every SEM has a predefined redundant connection to two data concentrators with different parameters. These parameters include the GPS location and signal power range in which authorized data messages are received with a very high accuracy.

The communication layer plays an essential role in the smart grid infrastructure and is a target for multiple attacks such as man-in-the-middle, session hijacking and bandwidth loss. In the SEM design, the main computing unit CUA communicates internally with the secondary computing unit CUB in a one-way direction link. In addition, CUA connects with two data concentrators (DC) through LoRaWAN connectivity that uses symmetric encryption technology to protect end-to-end communication. The third communication channel connects the CUB to the home area network (HAN) via a WiFi connection. The client can access an informative page directly to obtain the live values of power consumption. In addition, the CUB controls the devices in the HAN according to the user configuration. To ensure data integrity and transparency, the client may connect through an application to the UC data web server and compare the saved records at the utility-side server with those on the SEM.

Fig. 5 shows the algorithm flowchart for sending data from the main computing unit CUA to the secondary computing unit CUB such that the data are stored in CUA and sent through a one-directional serial port. Subsequently, it is received through a serial input port in the CUB. The rate of data communication was set to be the same on both computing units.

Every SEM communicates with two DCs to ensure data reception and generate link-specific attribute values, namely, GPS and RSSI. Fig. 6 shows a pseudocode sample for reading the GPS and RSSI values that are encapsulated in the AES encrypted message and sent through the LoRa module to the DCA. The operation is repeated to send data to the DCB after encapsulating the link attributes.

VII. RESULTS AND ANALYSIS

The proposed smart energy meter was built and tested along with the related applications. The SEM is used in its full functionality; the readings for the voltage and current with variable granularity provide the best-precision measurement. In addition, the test contains the message transmission to the utility network through the LoRaWAN module connected to the data concentrators containing the timestamp, SEM ID, power consumption, GPS, RSSI, humidity, and temperature. A client-side application is applied to control home devices and monitor power consumption through different dynamic criteria.

The following equation is a sample of used equations in calculating power consumption:

$$P = \sum_{j=0}^{N-1} \frac{v_j . i_j}{N} \tag{1}$$

The active power P is calculated in equation (1) where v_j and i_j are the voltage and current in the j^{th} measurement, respectively, and N is the number of samples.

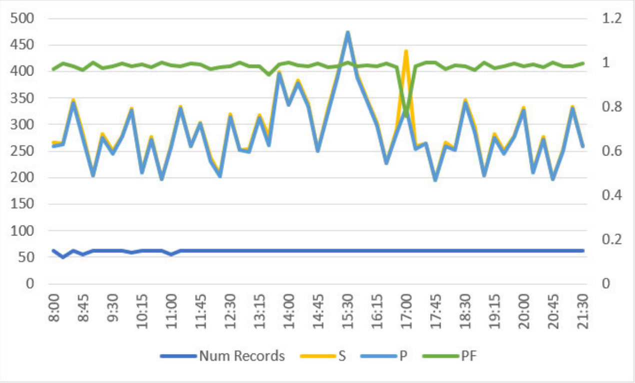
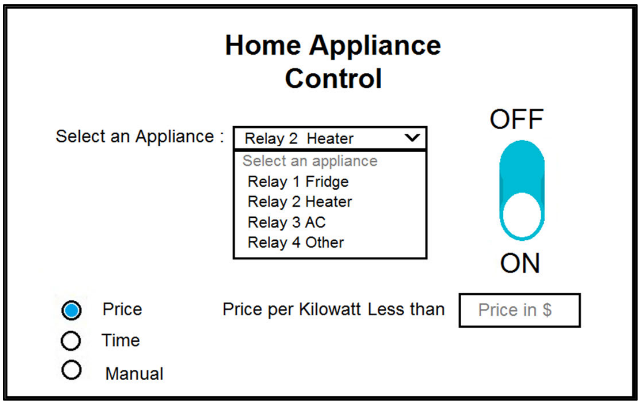


FIGURE 7. Sample data for apparent power, active power, power factor and number of readings.


Home Appliance Control

Select an Appliance : Relay 2 Heater

● Price
○ Time
○ Manual

Price per Kilowatt Less than [Price in $]

FIGURE 8. Client-side appliance control.

Fig. 7 shows the output data for the SEM readings with the number of samples(granularity) between every two readings.

Fig. 8 displays a sample interface of the client-side application to control the appliances according to different criteria, such as the price of the kilowatt-hour, time intervals, or set the command to be changed manually.

This control is enforced by the Arduino-WeMos by sending orders through the home network to the relays of every controlled load.

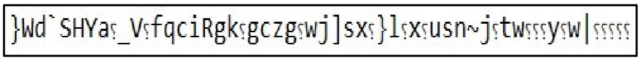

```
}Wd`SHYaʕ_VʕfqciRgkʕgczgʕwj]sxʕ}1ʕxʕusn~jʕtwʕʕʕyʕw|ʕʕʕʕʕ
```

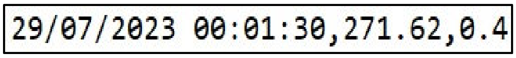
FIGURE 9. Sample of the encrypted data sent to DC.

The test of the proposed SEM focused on the message generated by the Arduino-UNO and transmitted to the utility network via the LoRaWAN module. The data concentrators

TABLE 4. Sample data fields of transmitted messages from SEM to DCA and DCB.

SEM_id	Date & Time	# of Rec	Power	X_Coord	Y_Coord	Temp	Humidity	RSSI_A	RSSI_B	Tamper
1	29-07-23 0:45	83	259.5988774	xxxx	yyyy	26.5	47	-87	-77	0
1	29-07-23 1:00	103	262.614392	xxxx	yyyy	26.6	47	-86	-76	0
1	29-07-23 1:15	93	340.3643613	xxxx	yyyy	26.7	47	-86	-76	0
1	29-07-23 1:30	103	274.69795	xxxx	yyyy	26.8	47	-89	-79	0
1	29-07-23 1:45	103	204.0534581	xxxx	yyyy	26.8	46	-88	-78	0
1	29-07-23 2:00	103	275.4425806	xxxx	yyyy	26.8	46	-87	-77	0
1	29-07-23 2:15	103	245.5692387	xxxx	yyyy	26.8	46	-86	-76	0
1	29-07-23 2:30	97	277.4545935	xxxx	yyyy	26.8	46	-86	-76	0
1	29-07-23 2:45	103	325.9633172	xxxx	yyyy	26.9	46	-87	-77	0
1	29-07-23 3:00	103	209.5990903	xxxx	yyyy	26.9	46	-87	-77	0

receive sent messages containing the timestamp, SEM ID, power consumption, GPS, RSSI, humidity, and temperature. Table 4 shows the sample records of the message data field sent from the SEM to the data concentrators (DCA and DCB). These data are sent as an encrypted message, as shown in Fig 9. The size of the message is 57 bytes with a baud rate of 115200 bits/sec and a transmission delay of 3.958 ms, knowing that a SEM sends data to DCs every 15 min.



```
29/07/2023 00:01:30,271.62,0.4
```

FIGURE 10. Sample of the data sent to WeMos.

The data sent from CUA (Arduino-UNO) to CUB (Arduino-WeMos) is shown in Fig. 10, which is internally sent every 30 s through a one-way serial port with a size of 30 bytes and contains the timestamp, power consumption, and the updated fee for every kilowatt hour as received from the utility.

Fig. 7 - 10 show the operation of a smart meter with full functionality. The SEM power consumption reading was performed with high accuracy, owing to the number of samplings between the two output records. The client-side application shown before offers the consumer a dynamic interface to control the home appliances power on and off. This feature represents an intersection of interest between the consumer and utility company, such that the former may control his energy bill, whereas the latter may perform load shifting and peak clipping. The client application features a dual connectivity capability, which allows the power consumption values to be read from two sources: SEM directly (CUB) and the utility server (Web Server A). This two-fold connectivity trait maintains data integrity by comparing synced records from diverse sources. The proposed SEM-transmitted information contains humidity and temperature sensor output in addition to GPS coordinates and the value of RSSI, such that this information is fed to an AI module at the utility side to detect any malicious connection. The proposed SEM design focuses not only on the security of the network and data integrity but also on the privacy of the client by encrypting the transmitted messages. The hardware of the proposed SEM is protected from misuse or theft by using a tamper detector sensor.

TABLE 5. Proposed SEM specification.

Grid Voltage Range	80 – 260 V
Max. Current	100A
Max. Power	26 KW
Grid Frequency Range	45- 65 HZ
Distance (open air)	10 KM
Oper. Temperature Range	-20 – 60 °C
Power Consumption	1.275 W
Voltage	5 – 12 V (DC)
Transmission Frequency	868 MHZ

The security and functionality issues discussed previously and shown in Table 1 and 2 are solved through the proposed SEM. The implementation of the proposed SEM proved that it can completely perform the functionalities of a smart meter by solving all the local security and data integrity issues of SEM. In the proposed SEM design, the use of dual computing units with unidirectional data transfer protects the primary computing unit from any unauthorized access or manipulation of the obtained data and utility network. In the event of a successful attack and takeover, the attacker would only manipulate and access the secondary compute unit, affecting the service of the targeted SEM for this client, and cannot be used as a foundation for a DDOS attack on the network.

Table 5 shows the proposed SEM specifications in terms of the operating environment, measured power, and power dissipation. The proposed SEM is a single-phase meter that can be upgraded to a three-phase meter to increase the measured power.

VIII. SECURITY EVALUATION TEST

A critical step in evaluating the security effectiveness of the proposed SEM design in comparison with existing SEM designs is to put them to a carefully organized attack scenario. This scenario is designed to carefully examine the security landscape connected with the use of WiFi 2.4 GHz—a critical communication channel for the SEM, allowing interactions with both household devices and the utility network.

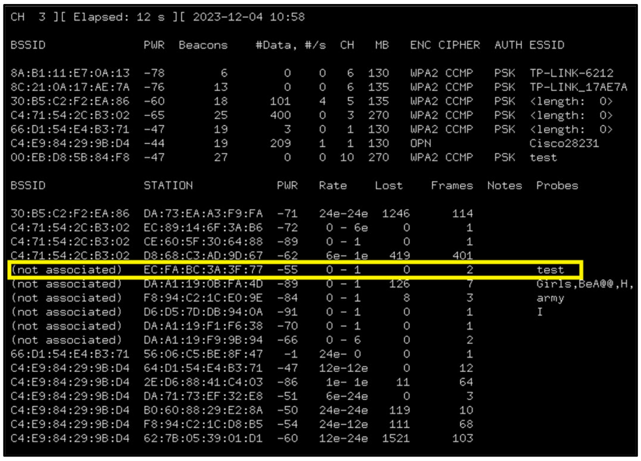
The analysis focuses on the security concerns associated with the use of WiFi 2.4 GHz, acknowledging its critical role in facilitating data transfers within the smart metering ecosystem. The goal is to shed light on potential weaknesses in this communication medium and their potential impact on the reliability and privacy of smart metering data by digging into the operating principles of WiFi 2.4 GHz and its popular usage in smart metering.

The test, which was carried out in a controlled lab environment using an ethical hacking methodology, emphasizes the importance of responsible testing to uncover vulnerabilities without causing harm. The three smart meters under examination are SEM-A (Matismart MT61GP), SEM-B (SEM design proposed in [18]) and SEM-C (SEM design proposed in this paper).

WiFi 2.4 GHz, a focal point of vulnerability, presents exploitable issues such as default credentials on smart meters, Evil Twin attacks, and Key Reinstallation attacks.

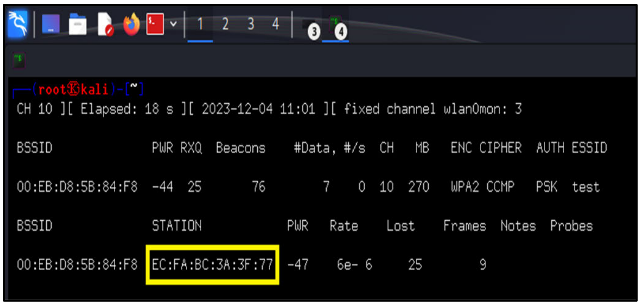
The lab contains the following items:

- A laptop running the Kali Linux OS and an Aircrack-ng suite installed.



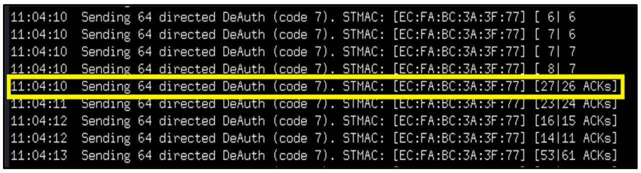
```
CH  3 ][ Elapsed: 12 s ][ 2023-12-04 10:58

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

8A:B1:11:E7:0A:13  -78        6        0    0   6  130   WPA2 CCMP   PSK  TP-LINK-6212
8C:21:0A:17:AE:7A  -76       13        0    0   6  135   WPA2 CCMP   PSK  TP-LINK_17AE7A
30:B5:C2:F2:EA:86  -60       18      101    4   5  135   WPA2 CCMP   PSK  <length:  0>
C4:71:54:2C:B3:02  -65       25      400    0   3  270   WPA2 CCMP   PSK  <length:  0>
66:D1:54:E4:B3:71  -47       19        3    0   1  130   WPA2 CCMP   PSK  <length:  0>
C4:E9:84:29:9B:D4  -44       19      209    1   1  130   OPN              Cisco28231
00:EB:D8:5B:84:F8  -47       27        0    0  10  270   WPA2 CCMP   PSK  test

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

30:B5:C2:F2:EA:86  DA:73:EA:A3:F9:FA  -71   24e-24e  1246      114
C4:71:54:2C:B3:02  EC:89:14:6F:3A:B6  -72    0 - 6e     0        1
C4:71:54:2C:B3:02  CE:60:5F:30:64:88  -89    0 - 1      0        1
C4:71:54:2C:B3:02  D8:68:C3:AD:9D:67  -62    6e- 1e   419      401
(not associated)   EC:FA:BC:3A:3F:77  -55    0 - 1      0        2         test
(not associated)   DA:A1:19:0B:FA:4D  -89    0 - 1    126        7         Girls,BeA@@,H,
(not associated)   F8:94:C2:1C:E0:9E  -84    0 - 1      8        3         army
(not associated)   D6:D5:7D:DB:94:0A  -91    0 - 1      0        1         I
(not associated)   DA:A1:19:F1:F6:38  -70    0 - 1      0        1
(not associated)   DA:A1:19:F9:9B:94  -66    0 - 6      0        2
66:D1:54:E4:B3:71  56:06:C5:BE:8F:47   -1   24e- 0      0        1
C4:E9:84:29:9B:D4  64:D1:54:E4:B3:71  -47   12e-12e     0       12
C4:E9:84:29:9B:D4  2E:D6:88:41:C4:03  -86    1e- 1e    11       64
C4:E9:84:29:9B:D4  DA:71:73:EF:32:E8  -51    6e-24e     0        3
C4:E9:84:29:9B:D4  B0:60:88:29:E2:8A  -50   24e-24e   119       10
C4:E9:84:29:9B:D4  F8:94:C2:1C:D8:B5  -54   24e-12e   111       68
C4:E9:84:29:9B:D4  62:7B:05:39:01:D1  -60   12e-24e  1521      103
```

FIGURE 11. Identifying the BSSID.



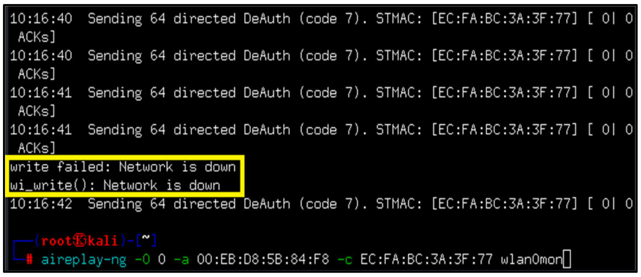
```
┌──(root㉿kali)-[~]
CH 10 ][ Elapsed: 18 s ][ 2023-12-04 11:01 ][ fixed channel wlan0mon: 3

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:EB:D8:5B:84:F8  -44  25       76        7    0  10  270   WPA2 CCMP   PSK  test

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:EB:D8:5B:84:F8  EC:FA:BC:3A:3F:77  -47    6e- 6    25        9
```

FIGURE 12. BSSID identified.



```
11:04:10  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [ 6| 6
11:04:10  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [ 7| 6
11:04:10  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [ 7| 7
11:04:10  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [ 8| 7
11:04:10  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [27|26 ACKs]
11:04:11  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [23|24 ACKs]
11:04:12  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [16|15 ACKs]
11:04:12  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [14|11 ACKs]
11:04:13  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [53|61 ACKs]
```

FIGURE 13. De-authentication process.



```
10:16:40  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [ 0| 0
 ACKs]
10:16:40  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [ 0| 0
 ACKs]
10:16:41  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [ 0| 0
 ACKs]
10:16:41  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [ 0| 0
 ACKs]
write failed: Network is down
wi_write(): Network is down
10:16:42  Sending 64 directed DeAuth (code 7). STMAC: [EC:FA:BC:3A:3F:77] [ 0| 0

┌──(root㉿kali)-[~]
└─# aireplay-ng -0 0 -a 00:EB:D8:5B:84:F8 -c EC:FA:BC:3A:3F:77 wlan0mon
```

FIGURE 14. Network failure.

- Internet router using WiFi 2.4 GHz
- SEM-A
- SEM-B
- SEM-C

This procedure is performed on SEMs A, B, and C. The steps are as follows:

- **Identification of the Smart Meter (BSSID)**: The adversary, armed with sophisticated tools such as a KALI laptop running the aircrack app, initiates the attack by stealthily identifying the Basic Service Set Identifier (BSSID) of the smart meter as shown in Fig. 11 and Fig. 12. This clandestine maneuver is crucial for singling a specific device within the network.
- **Flood Attack Against the Router**: Having pinpointed the smart meter, the attacker launches a calculated flood attack against the WiFi router responsible for providing internet connectivity to the smart meter. Employing the command: *aireplay-ng -0 100000 -a [The BSSID found in step 1] [Name of SEM]*, an overwhelming volume of traffic is directed at the router to exhaust its resources and disrupt normal communication, as shown in Fig. 13.
- **Blocking Communication to the Server**: The flood attack is strategically orchestrated to interfere with the transmission of packets from the smart meter to the utility's server as shown in Fig. 14.

After performing the attack:

- **SEM-A & SEM-B**: the attacker was able to block the communication between both smart meters and the utility server. The data generated by the load connected to SEM-A and SEM-B, indicating energy consumption, failed to reach the server in a timely manner.
- **SEM-C**: the attacker was not able to block the communication between SEM-C and the utility server, and the computing unit responsible for reading the consumption values and communicating with the utility server through the data concentrators was not affected because it is protected with unidirectional communication with the computing unit connected to the WiFi module.

The following are the effects of the attack:

Possible consequences on SEM-A and SEM-B:

A- Electricity Supply Cut-off: The utility, deprived of the data indicating smart meter energy consumption due to the attack, interprets this anomaly as a potential breach. In response, the utility system triggers an automatic cutoff of the electricity supply to the residence as a precautionary measure.

B- Financial Loss for the Utility: Alternatively, if the attack successfully disrupts the communication between the smart meter and the utility server without triggering a cutoff, the utility faces financial repercussions. The lack of accurate and timely data compromises the utility's ability to accurately bill the client for energy usage. This discrepancy could result in financial losses because the utility underestimates the actual consumption, leading to revenue shortfalls.

C- Loss in device control: Programmed relays for devices controlled by SEM-A and SEM-B were disconnected from the smart meter. This may affect their functionality, either totally or partially, according to the default program reaction to this interference.

Possible consequences on SEM-C:

The attacker was not able to affect the communication between the SEM-C and the utility server, and for this, the attack did not leave any consequence on the energy consumption values recorded.

The attack blocked communication between the SEM-C and the programmed relays for devices, but the effect was minimized because the relay's reaction to this situation was to stick to the last order received from the smart meter.

Observations of the executed procedure on both smart meters revealed distinctive outcomes. SEM-A and SEM-B, with their data-gathering components attached to the same microcontroller connected to the WiFi module, experienced a complete functional breakdown. This resulted in interrupted data gathering, cessation of home-controlled devices, and a total power shutdown.

In contrast, the SEM-C demonstrated higher resilience to attacks. The WiFi module in SEM-C is connected to a secondary processing unit (CUB) that receives data in one-way communication from the main processing unit (CUA). As a result, the attack failed to induce a total power shutdown or compromise data integrity. The only affected service was the directly controlled devices in the home area network.

In conclusion, the comparative analysis highlights the superior security measures in the proposed SEM design. The ability of SEM-C to withstand an attack underscores the significance of robust security frameworks in the evolving landscape of smart metering systems. This comprehensive evaluation provides valuable insights into enhancing the security and reliability of smart energy meters in an ever-expanding digital ecosystem.

IX. CONCLUSION

This study addressed the security and data integrity issues in smart energy meters (SEM), which are critical components in smart grid networks. Following a comprehensive survey of existing products and their features, a security-focused design for the SEM was proposed. The proposed solution offers a multilevel design to ensure the hardware, communication, and data security of the SEM. It also presents a client-side application that allows the user to control home appliances according to dynamic criteria and monitor power consumption in real time. The additional information gathered, generated, and sent to the utility network through a redundant data concentrator design will enable a more accurate control system for the smart grid.

Future work will be devoted to the development of the complete data cycle from the gathering at the client side to the power production network and back to the client side, maintaining data integrity, availability, and security in all phases. The work is underway on an AI-enabled control module to improve the quality of service in smart grids depending on the information offered by the proposed SEM and data gathered from the production systems and data concentrators.

ACKNOWLEDGMENT

The authors would like to thank George A. Farah for his help with data collection. They like to extend their gratitude to Eng. Wassim Abbas for sharing his experience with the LoRaWAN Technology. They also like to thank Eng. Imane Haidar for her invaluable remarks. Finally, they thank Eng. Rida El-Helou for his assistance in the security evaluation test execution.

REFERENCES

[1] H. Hseiki, H. Bazzi, R. Kassem, A. El-Hajj, and A. Haidar, "AI to preserve energy and environment," in *Proc. Int. Conf. Smart Syst. Power Manag. (ICSPM)*, Nov. 2022, pp. 29–34, doi: 10.1109/IC2SPM56638.2022.9988899.

[2] H. T. Reda, A. Anwar, and A. Mahmood, "Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts," *Renew. Sustain. Energy Rev.*, vol. 163, Jul. 2022, Art. no. 112423, doi: 10.1016/j.rser.2022.112423.

[3] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Protection*, vol. 25, pp. 36–49, Jun. 2019.

[4] J. Chris Foreman and D. Gurugubelli, "Identifying the cyber attack surface of the advanced metering infrastructure," *Electr. J.*, vol. 28, no. 1, pp. 94–103, Jan. 2015, doi: 10.1016/j.tej.2014.12.007.

[5] D. B. Avancini, J. J. P. C. Rodrigues, S. G. B. Martins, R. A. L. Rabelo, J. Al-Muhtadi, and P. Solic, "Energy meters evolution in smart grids: A review," *J. Cleaner Prod.*, vol. 217, pp. 702–715, Apr. 2019.

[6] A. Hambley, *Electrical Engineering: Principles and Applications*. London, U.K.: Pearson, 2017.

[7] C. Müller, H. Georg, and C. Wietfeld, "A modularized and distributed simulation environment for scalability analysis of smart grid ICT infrastructures," in *Proc. 5th Int. Conf. Simul. Tools Techn.*, 2012, pp. 327–330.

[8] D. M. Murray, L. Stankovic, V. Stankovic, and N. D. Espinoza-Orias, "Appliance electrical consumption modelling at scale using smart meter data," *J. Cleaner Prod.*, vol. 187, pp. 237–249, Jun. 2018.

[9] X. He, Q. Ai, R. C. Qiu, W. Huang, L. Piao, and H. Liu, "A big data architecture design for smart grids based on random matrix theory," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 674–686, Mar. 2017, doi: 10.1109/TSG.2015.2445828.

[10] X. Xu, X. He, Q. Ai, and R. C. Qiu, "A correlation analysis method for power systems based on random matrix theory," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1811–1820, Jul. 2017, doi: 10.1109/TSG.2015.2508506.

[11] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision," *Future Gener. Comput. Syst.*, vol. 136, pp. 358–377, Nov. 2022, doi: 10.1016/j.future.2022.06.013.

[12] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011, doi: 10.1109/TII.2011.2166794.

[13] Q. Sun, H. Li, Z. Ma, C. Wang, J. Campillo, Q. Zhang, F. Wallin, and J. Guo, "A comprehensive review of smart energy meters in intelligent energy networks," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 464–479, Aug. 2016, doi: 10.1109/JIOT.2015.2512325.

[14] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1963–1976, Dec. 2012, doi: 10.1109/TSG.2012.2197425.

[15] J. N. Bharothu, M. Sridhar, and R. S. Rao, "A literature survey report on smart grid technologies," in *Proc. Int. Conf. Smart Electric Grid (ISEG)*, Guntur, India, Sep. 2014, pp. 1–8, doi: 10.1109/ISEG.2014.7005601.

[16] S. Muralidhara, N. Hegde, and P. M. Rekha, "An Internet of Things-based smart energy meter for monitoring device-level consumption of energy," *Comput. Electr. Eng.*, vol. 87, Oct. 2020, Art. no. 106772, doi: 10.1016/j.compeleceng.2020.106772.

[17] A. A. Faradila Purnama and M. Imam Nashiruddin, "Designing LoRaWAN Internet of Things network for advanced metering infrastructure (AMI) in Surabaya and its surrounding cities," in *Proc. Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI)*, Dec. 2019, pp. 194–199, doi: 10.1109/ISRITI48646.2019.9034571.

[18] O. Munoz, A. Ruelas, P. Rosales, A. Acuña, A. Suastegui, and F. Lara, "Design and development of an IoT smart meter with load control for home energy management systems," *Sensors*, vol. 22, no. 19, p. 7536, Oct. 2022, doi: 10.3390/s22197536.

[19] P. Pawar and P. Vittal K, "Design and development of advanced smart energy management system integrated with IoT framework in smart grid environment," *J. Energy Storage*, vol. 25, Oct. 2019, Art. no. 100846, doi: 10.1016/j.est.2019.100846.

[20] E. Spanò, L. Niccolini, S. D. Pascoli, and G. Iannacconeluca, "Last-meter smart grid embedded in an Internet-of-Things platform," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 468–476, Jan. 2015, doi: 10.1109/TSG.2014.2342796.

[21] Y. M. Rind, M. H. Raza, M. Zubair, M. Q. Mehmood, and Y. Massoud, "Smart energy meters for smart grids, an Internet of Things perspective," *Energies*, vol. 16, no. 4, p. 1974, Feb. 2023.

[22] C. Alaton, and F. Tounquet. (2020). *Benchmarking Smart Metering Deployment in the EU-28*. European Commission, Directorate-General for Energy. [Online]. Available: https://data.europa.eu/doi/10.2833/492070

[23] S.-H. Seo, X. Ding, and E. Bertino, "Encryption key management for secure communication in smart advanced metering infrastructures," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2013, pp. 498–503, doi: 10.1109/SMARTGRIDCOMM.2013.6688007.

[24] C. Lee, H. Yang, B. Lee, and D. Won, "A novel privacy-enhanced AMI system using searchable and homomorphic encryption techniques," in *Proc. Int. Conf. Hybrid Inf. Technol.* Cham, Switzerland: Springer, 2012, pp. 608–617, 2012, doi: 10.1007/978-3-642-32645-5_76.

[25] Y. Lee, E. Hwang, and J. Choi, "A unified approach for compression and authentication of smart meter reading in AMI," *IEEE Access*, vol. 7, pp. 34383–34394, 2019, doi: 10.1109/ACCESS.2019.2903574.

[26] M. I. Ibrahem, M. M. Badr, M. M. Fouda, M. Mahmoud, W. Alasmary, and Z. Md. Fadlullah, "PMBFE: Efficient and privacy-preserving monitoring and billing using functional encryption for AMI networks," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–7, doi: 10.1109/ISNCC49221.2020.9297246.

[27] N. Saxena, B. J. Choi, and S. Grijalva, "Secure and privacy-preserving concentration of metering data in AMI networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7, doi: 10.1109/ICC.2017.7996874.

[28] I. Parvez, A. Sarwat, L. Wei, and A. Sundararajan, "Securing metering infrastructure of smart grid: A machine learning and localization based key management approach," *Energies*, vol. 9, no. 9, p. 691, Aug. 2016, doi: 10.3390/en9090691.

[29] T. Robles, B. Bordel, R. Alcarria, and D. S.-D. Rivera, "Blockchain technologies for private data management in AMI environments," in *Proc. MDPI*, 2018, vol. 2, no. 19, p. 1230, doi: 10.3390/proceedings2191230.

[30] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Fog-based distributed intrusion detection system against false metering attacks in smart grid," in *Proc. ICC - IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6, doi: 10.1109/ICC.2019.8761752.

[31] A. H. M. Jakaria, M. A. Rahman, and M. G. Moula Mehedi Hasan, "Safety analysis of AMI networks through smart fraud detection," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–7, doi: 10.1109/CNS.2019.8802845.

[32] S. Tonyali, K. Akkaya, N. Saputro, and X. Cheng, "An attribute & network coding-based secure multicast protocol for firmware updates in smart grid AMI networks," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–9, doi: 10.1109/ICCCN.2017.8038415.

[33] L. Na, X. Xiaohui, M. Xiaoqin, M. Xiangfu, and Y. Peisen, "Fake data injection attack detection in AMI system using a hybrid method," in *Proc. IEEE Sustain. Power Energy Conf. (iSPEC)*, Dec. 2021, pp. 2371–2376, doi: 10.1109/iSPEC53008.2021.9735875.

[34] L. Blakely, M. J. Reno, and K. Ashok, "AMI data quality and collection method considerations for improving the accuracy of distribution models," in *Proc. IEEE 46th Photovoltaic Specialists Conf. (PVSC)*, Jun. 2019, pp. 2045–2052, doi: 10.1109/PVSC40753.2019.8981211.

[35] J. Wang, D. Shi, Y. Li, J. Chen, H. Ding, and X. Duan, "Distributed framework for detecting PMU data manipulation attacks with deep autoencoders," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4401–4410, Jul. 2019, doi: 10.1109/TSG.2018.2859339.

[36] S. K. Singh, R. Bose, and A. Joshi, "Entropy-based electricity theft detection in AMI network," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 3, no. 2, pp. 99–105, Jun. 2018, doi: 10.1049/iet-cps.2017.0063.

[37] S. Kulkarni, R. Rahul, R. Shreyas, S. Nagasundari, and P. B. Honnavalli, "MITM intrusion analysis for advanced metering infrastructure communication in a smart grid environment," in *Proc. Int. Conf. Comput. Intell., Security Internet Things*. Cham, Switzerland: Springer, 2020, pp. 256–267, doi: 10.1007/978-3-030-66763-4_22.

[38] W. Jiang, Z. Yang, Z. Zhou, and J. Chen, "Lightweight data security protection method for AMI in power Internet of Things," *Math. Problems Eng.*, vol. 2020, pp. 1–9, Nov. 2020, doi: 10.1155/2020/8896783.

[39] A. Sahu, H. N. R. K. Tippanaboyana, L. Hefton, and A. Goulart, "Detection of rogue nodes in AMI networks," in *Proc. 19th Int. Conf. Intell. Syst. Appl. Power Syst. (ISAP)*, Sep. 2017, pp. 1–6, doi: 10.1109/ISAP.2017.8071424.

[40] M. H. Haider, S. B. Saleem, J. Rafaqat, and N. Sabahat, "Threat modeling of wireless attacks on advanced metering infrastructure," in *Proc. 13th Int. Conf. Math., Actuarial Sci., Comput. Sci. Statist. (MACS)*, Dec. 2019, pp. 1–6, doi: 10.1109/MACS48846.2019.9024779.

[41] E. S. Parizy, H. R. Bahrami, and S. Choi, "A low complexity and secure demand response technique for peak load reduction," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3259–3268, May 2019, doi: 10.1109/TSG.2018.2822729.

[42] S. M. Alfassa, S. Nagasundari, and P. B. Honnavalli, "Invasion analysis of smart meter in AMI system," in *Proc. IEEE Mysore Sub Sect. Int. Conf. (MysuruCon)*, Oct. 2021, pp. 831–836, doi: 10.1109/MysuruCon52639.2021.9641595.

[43] Y. Bagariang, M. I. Nashiruddin, and N. Mufti Adriansyah, "LoRa-based IoT network planning for advanced metering infrastructure in urban, suburban and rural scenario," in *Proc. Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI)*, Dec. 2019, pp. 1–6.

[44] J. L. Gallardo, M. A. Ahmed, and N. Jara, "LoRa IoT-based architecture for advanced metering infrastructure in residential smart grid," *IEEE Access*, vol. 9, pp. 124295–124312, 2021.

[45] F. Y. Aznaveh and M. Mansub Bassiri, "Evaluation of using LoRaWAN to implement AMI in big city of Tehran," in *Proc. 3rd Int. Conf. Internet Things Appl. (IoT)*, Apr. 2019, pp. 1–4, doi: 10.1109/IICITA.2019.8808835.

[46] P. Kanakaraja, S. Upadhyay, S. K. Kotamraju, G. V. S. Suneela, and R. Neelesh, "Design and implementation of smart energy meter using LoRa-WAN and IoT applications," *J. Phys., Conf.*, vol. 1804, no. 1, Feb. 2021, Art. no. 012207, doi: 10.1088/1742-6596/1804/1/012207.

[47] F. Sánchez-Sutil, A. Cano-Ortega, and J. C. Hernández, "Design and implementation of a smart energy meter using a LoRa network in real time," *Electronics*, vol. 10, no. 24, p. 3152, Dec. 2021, doi: 10.3390/electronics10243152.

[48] Z. Xia, H. Zhou, K. Gu, B. Yin, Y. Zeng, and M. Xu, "Secure session key management scheme for meter-reading system based on LoRa technology," *IEEE Access*, vol. 6, pp. 75015–75024, 2018, doi: 10.1109/ACCESS.2018.2883657.

[49] F. Al-Turjman and M. Abujubbeh, "IoT-enabled smart grid via SM: An overview," *Future Gener. Comput. Syst.*, vol. 96, pp. 579–590, Jul. 2019, doi: 10.1016/j.future.2019.02.012.

[50] S. M. A. A. Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-enabled smart energy grid: Applications and challenges," *IEEE Access*, vol. 9, pp. 50961–50981, 2021, doi: 10.1109/ACCESS.2021.3067331.

[51] A. Meffe, M. Prieto, F. Romero, A. Gracez, A. Jesus, and J. J. Teodoro, "A low-cost LoRaWAN wireless IoT solution for remote management and analysis of consumers' measurement data," in *Proc. CIRED*, 2019, pp. 1–5.

[52] B. Al Homssi, K. Dakic, S. Maselli, H. Wolf, S. Kandeepan, and A. Al-Hourani, "IoT network design using open-source LoRa coverage emulator," *IEEE Access*, vol. 9, pp. 53636–53646, 2021.

[53] G. Helou, M. Ibrahim, R. Tawil, and Y. Mohanna, "Are existing analytical models for LoRa networks accurate?" in *Proc. 4th IEEE Middle East North Afr. Commun. Conf. (MENACOMM)*, Amman, Jordan, Dec. 2022, pp. 24–31, doi: 10.1109/MENACOMM57252.2022.9998193.

[54] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 4th Quart., 2018, doi: 10.1109/COMST.2018.2855563.

[55] O. Elijah, S. K. A. Rahim, V. Sittakul, A. M. Al-Samman, M. Cheffena, J. B. Din, and A. R. Tharek, "Effect of weather condition on LoRa IoT communication technology in a tropical region: Malaysia," *IEEE Access*, vol. 9, pp. 72835–72843, 2021, doi: 10.1109/ACCESS.2021.3080317.

[56] Y. A. Al-Gumaei, N. Aslam, M. Aljaidi, A. Al-Saman, A. Alsarhan, and A. Y. Ashyap, "A novel approach to improve the adaptive-data-rate scheme for IoT LoRaWAN," *Electronics*, vol. 11, no. 21, p. 3521, Oct. 2022, doi: 10.3390/electronics11213521.

[57] S. A. Bhat, N. F. Huang, I. Hussain, and U. Sajjad, "Correlating the ambient conditions and performance indicators of the LoRaWAN via surrogate Gaussian process based bidirectional LSTM stacked autoencoder showkat," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 3, pp. 3413–3427, Sep. 2023, doi: 10.1109/TNSM.2023.3238013.

[58] K. Mikhaylov, P. Masek, T. Hanninen, M. Stusek, and J. Hosek, "Improving LoRaWAN performance by randomizing network access for data and on-air activation," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 4432–4437, doi: 10.1109/ICC45855.2022.9838306.

[59] O. Elijah, S. K. A. Rahim, M. J. Musa, Y. O. Salihu, M. J. Bello, and M.-Y. Sani, "Development of LoRa-Sigfox IoT device for long distance applications," in *Proc. IEEE Nigeria 4th Int. Conf. Disruptive Technol. Sustain. Develop. (NIGERCON)*, Lagos, Nigeria, Apr. 2022, pp. 1–5, doi: 10.1109/NIGERCON54645.2022.9803173.

[60] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 907–921, May 2016, doi: 10.1109/TIFS.2015.2512525.

HUSSAM A. HSEIKI was born in Baissour, Aley, Mount Lebanon, Lebanon, in 1980. He received the B.E. degree in computer engineering from Beirut Arab University, in 2003, and the M.E. degree in computer and communication engineering from the American University of Beirut, in 2007. He is currently pursuing the Ph.D. degree in computer engineering with Beirut Arab University.

Since 2006, he has been a government employee and involved in computer communication, cyber security, system automation, and application development. He is the author of a book titled "*An Adaptive Hierarchical Data Structure Searching Data Archives*," in 2009.

Mr. Hseiki has been a member of the Order of Engineers and Architects, Beirut, since 2003. He was a recipient of the Military Appreciation Medal in 2017 and the Lebanese Order of Merit in 2023.

AHMAD M. EL-HAJJ (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in electrical and computer engineering from the American University of Beirut, in 2007, 2009, and 2014, respectively.

He is currently a Lecturer with the American University of Beirut and Phoenicia University. His research interests include wireless network optimization, game theory, neuro-engineering, biomimetics, artificial intelligence, and natural language processing. He serves as a member for the Executive Committee of the Lebanon Chapter of the IEEE Communications Society (IEEE ComSoc).

YOUSSEF O. AJRA received the B.S. degree in electrical power and machines engineering (EPME) from Beirut Arab University, Dibbiyeh, Lebanon, in 2016, and the M.S. degree in renewable energy from Lebanese University and Université Saint-Joseph, Beirut, Lebanon, in 2020. He is currently pursuing the Ph.D. degree in electrical engineering with the ESIGELEC Laboratory, Université de Rouen Normandie, Rouen, France.

From 2017 to 2021, he was an Assistant Specialist with BAU, Lebanon, where he has been a Lecturer, since 2022. Within his Ph.D. research, he focuses on the fault diagnosis and detection (FDD) of power electronic components and sensors and employing model-based techniques as part of his FDD approaches.

FATHELALEM A. HIJA (Member, IEEE) received the B.Sc., M.E., and Dr.-Eng. degrees, and the Ph.D. degree in information engineering with a specialization in complex intelligent systems engineering from the University of the Ryukyus, Japan.

With more than two decades of experience in higher education, he was a Professor of information engineering and computer science with Meio University, Japan. He is currently associated with the Joaan Bin Jassim Academy for Defence Studies, Qatar. He is also a Joint Researcher with the Research Institute, Meio University. He holds a position as a Full Professor of cybersecurity graduate program with the Joaan Bin Jassim Academy for Defence Studies, while collaborating with international institutions mainly in Japan, Malaysia, Europe, and the Middle East. His professional expertise and research interests span several domains, including computational intelligence, information and cyber security, information warfare, and information operations in hybrid warfare. His recent focus has been on exploring advanced technologies, such as AI, blockchain, and the IoT technologies and their impact on information domain and cyber security.

ALI M. HAIDAR received the B.E. degree in electrical engineering (electronics and telecommunications) from Beirut Arab University, in 1986, the M.E. degree in computer and information engineering from the Faculty of Engineering, University of the Ryukyus, Japan, in 1992, and the Ph.D. degree in computer engineering from the Department of Computer and Information Engineering, Faculty of Engineering, Saitama University, Japan, in 1995. He joined Hiroshima City University, Japan, in April 1995. Then, he joined Beirut Arab University, in October 1997, where he is currently a Professor with the Department of Electrical and Computer Engineering. His research interests include digital theories, modeling and applications, neural networks, AI, machine learning, deep learning, Petri nets, cloud computing, digital communication, advanced computer architectures, security systems, and smart grids.