Central Power Research Institute

Vol. 20(1)/27-33, June 2024
ISSN (Print) : 0973-0338
DOI : 10.33686/pwj.v20i1.1164

Power Research

System Architecture and Threat Modelling of Advanced Metering Infrastructure

Anurag Chevendra*, Parul V. Sindhwad, Rigved Kulkarni, Mahita Samant, Sharal Deegoju and Faruk Kazi

Electrical Engineering Department, VJTI, Mumbai - 400019, Maharashtra, India; amchevendrab19@ee.vjti.ac.in

Abstract

Advanced Metering Infrastructure (AMI) is a collection of smart meters, communications networks, and data management systems that have been specifically designed to facilitate the effective integration of energy resources. As AMI continues to become more complex and integrated with advanced functionalities, additional questions about cyber security must be considered. The security of an AMI is of critical importance. The implementation of secure protocols and the enforcement of strict security requirements may be able to stop vulnerabilities from being exploited. This research analyses AMI from a security standpoint. It also discusses potential flaws related to various smart meter attack surfaces, as well as the security and threat implications of these flaws. Threat modelling is an engineering undertaking that helps identify security threats, potential vulnerabilities, and their criticality and prioritize corrective or countermeasures. The results show how threat models, specifically STRIDE and LINDDUN, can be used in the case of an AMI and demonstrate the dangers connected to this AMI configuration.

Keywords: AMI, CyberSecurity, LINDUNN, STRIDE, Threat Modelling, Vulnerabilities

1. Introduction

The development of the "smart" meter led to the creation of AMI -an integrated system of smart meters, communications networks, and data management systems built on two-way communication between utilities and customers[1]. Within the context of the smart grid, the Advanced Metering Infrastructure (AMI) plays an essential part in the process of gathering data from Phasor Measuring Units (PMUs), smart meters, and sensors. AMI networks enable utilities and the metering devices located on the customer's side to communicate with one another in both directions[2]. The utility company can collect information on real-time consumption and output from individual homes, which it then relays to its clientele in the form of real-time prices. This is one of the benefits of the smart network. In addition, for purposes of load management, the utility company can exercise remote control over a customer's home appliances. It provides benefits to consumers as switching and moving are easily facilitated, power outages are reduced, bills are based on actual consumption, the necessity of bill estimation is reduced and there is an increased knowledge of the quality of delivery along with detailed feedback on energy use[3]. It gives utilities the ability to build models to detect power theft, information to reduce peak demands, reduce power outages, enable dynamic pricing, optimize income, and give automated and remote meter readings[4]. As utilities work to upgrade the electric grid, one of their most crucial undertakings is the deployment of AMI on a global scale. India's policymakers are encouraging the adoption of variable renewable energy. Smart metering is considered crucial for achieving the primary goals of the National Smart Grid Mission. With the demand and use of smart meters rising in the country and on a global scale, there is an ever-growing need to provide cyber security and privacy to these devices. With the advancement of computation and communications, cybersecurity has become a major concern for AMI networks, which require privacy and integrity.

We have chosen to utilize the STRIDE threat model for AMI due to its ability to provide better coverage of potential

*Author for correspondence

threats that are relevant to these devices. It encompasses a wide range of security checks, including spoofing, repudiation, tampering, information disclosure, DoS, and elevation of privilege. These align closely with the security concerns commonly faced by smart meters[5]. Additionally, STRIDE was originally developed to address threats in software systems, making it highly suitable for analysing the security of software components and communication protocols in the context of smart meters. Furthermore, for privacy considerations, the LINDDUN threat model can be used alongside STRIDE to ensure the security of smart meters. In this study, we have combined both threat models, which allows for a more comprehensive analysis of potential threats, encompassing both security and privacy dimensions[6]. By leveraging this combination, organizations can address the full range of security and privacy concerns associated with smart meters. The structure of the paper is organized as follows: Section 2 provides a background with literature study and motivation along with a concise summary of the components and the security standards set. Section 3 presents STRIDE and LINDDUN threat modelling of the AMI architecture and observations. Finally, concluding remarks are presented in Section 4.

2. Background

An adversary can impersonate a meter[7] to modify the bill or take down the grid. The proposed security approaches use mutual authentication techniques and isolation of the logical network segments. However, they focused on the attacks from smart meters to devices located in a substation. Several scholars have also undertaken studies focusing on enhancing hardware security measures for safeguarding private keys against unauthorized access and malicious software within smart grid networks[8]. Studies have addressed eavesdropping attacks, integrity breaches, and potential DoS attacks targeting elements of the AMI network[9,10]. They propose a resolution employing a combination of symmetric key management and public key infrastructure. Moreover, they highlight the persistent challenge of managing keys for the AMI network due to its imperative for cost-effectiveness and timely operations.

2.1 AMI Components and Security Requirements

This section describes an AMI network and security needs and requirements for it. Figure 1 presents the AMI network, which comprises of Head End System (HES), Data aggregator, Smart meter, and several networks WAN, NAN, and HAN.

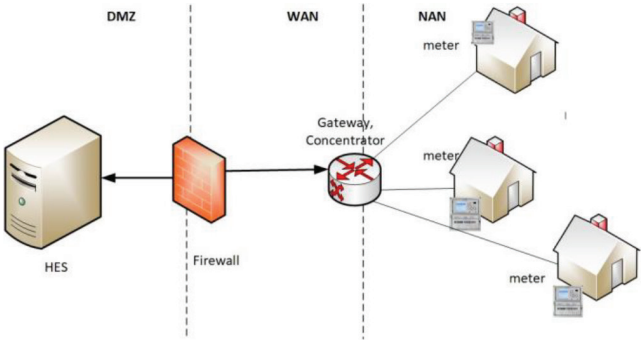

Figure 1. AMI Network.

HES is situated within the facilities of the Distribution System Operator (DSO). The servers establish direct communication with the meters and are situated within a Demilitarized Zone (DMZ). The data that has been gathered is effectively managed using a Metering Data Management System (MDMS), which facilitates the association of data with the corresponding consumer. Security measures are required in AMI, as Smart meters are attractive targets for hackers and the vulnerabilities can be easily monetized. The smart meter is composed of five main elements: the control room, smart meter collector, HAN, metering system, and optical interface. Each of these components represents a specific target for potential attacks, thereby affecting the overall security of the targeted AMI system[11].

Exploiting such vulnerabilities allows attackers to gain unauthorized access to sensitive data and elevate their privileges through stealthy side-channel attacks[12]. An alternative type of assault includes substituting the control panel board with a malicious board that holds parasitic devices. This puts their data in jeopardy of being stolen or misused. Moreover, this grants the attacker authority over the smart meter, potentially leading to disruption of service for lawful users. Denial of Service (DoS) attacks are commonly employed against smart meters, aiming to disrupt communication and compromise system integrity and confidentiality. Various types of attacks can be carried out on Smart Meters, including the direct hacking of meters by gaining unauthorized access to onboard memory and exploiting diagnostic ports and network interfaces. Hackers employ a range of tools, such as commercially available hardware or open-source software tools, to facilitate these attacks[13].

Man-in-the-Middle (MITM) attacks are executed by adversaries who position themselves between

communicating devices, intercepting and analysing the traffic exchanged between them. These attacks combine elements of eavesdropping, injection, and spoofing techniques mentioned earlier. By acting as an intermediary, the attacker establishes connections between the devices while discreetly observing the transmitted data[14]. Sophisticated MITM attacks can undermine encryption by substituting genuine encryption keys with counterfeit ones.

3. Threat Modelling

In the context of defending something of value, threat modelling seeks to detect, convey, and comprehend threats and provide mitigation[15]. A threat model is an organised representation of all the data that influences an application's security. It essentially involves looking at the program and its surroundings via a security lens[16].

3.1 System Architecture

The system architecture serves as the foundation for any threat model, enabling the definition of boundaries and data flow between different elements. A simplified AMI has been developed (refer to the figure below) and consists of the following components:

- **MDMS:** The MDMS is a software solution utilized for data collection, validation, estimation, and storage. It serves as a centralized hub for collecting and conducting data quality checks. It incorporates predefined algorithms and analytics to estimate missing data values. Additionally, it maintains a historical record of meter readings and consumption patterns.
- **Customer Data Management System (CDMS):** The CDMS works in conjunction with the MDMS and provides comprehensive customer information and management capabilities. It offers tools for accurate billing, customer engagement, and self-service functionalities.
- **HES:** The head-end system manages and coordinates the data flow between the utility's backend system and various field devices within the AMI. It assumes responsibility for overall system security and data management within the AMI.
- **Gateway:** It plays a critical role in connecting the utility's communication network with the meters and other devices in the field. It supports multiple communication protocols, such as DLMS/COSEM, to establish connectivity with the devices it serves.

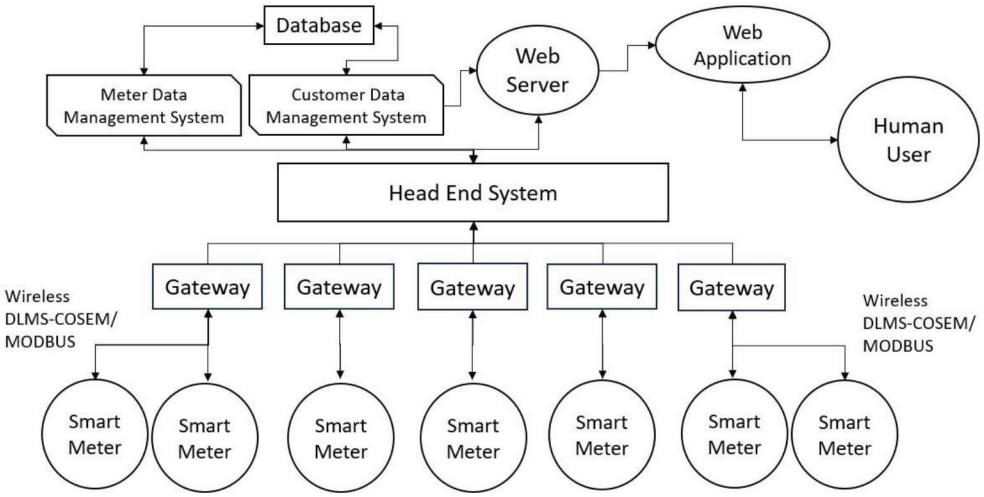

Figure 2. System architecture. Smart meters: are typically deployed by utility companies as part of their efforts to modernize the energy grid and enhance efficiency. Equipped with digital displays, smart meters provide energy usage information.

3.2 STRIDE

Decompose system into components: The proposed system can be broadly grouped into 5 components namely the utility centre consisting of A, B, C, and D. Head End System (HES), E, Data concentrator (G) and Smart meters(F).

Note: Threat analysis does not consider physical components that are not vulnerable to cyberattacks, such as load, electrical wire connections or utility supplies[17].

Plot DFD into system components*:* Instead of creating separate Data Flow Diagrams (DFDs) for individual system

components, a consolidated DFD is utilized to illustrate the entire system[2], as depicted in Figure 3. In this system architecture, effective communication is established between the smart meter and the gateway, employing two protocols, specifically DLMS/COSEM and MODBUS.

Analyse threats in the DFD:

Spoofing: An attacker could potentially falsify meter data management, resulting in the delivery of inaccurate data to the web server. Similarly, the web server itself might be targeted for spoofing by an attacker, potentially resulting in unauthorized access to the web application. Additionally, there is a risk of an attacker spoofing the web application, which could potentially lead to the disclosure of information by the web server[18].

Tampering with data: When an attacker tampers with the data being transmitted, potentially resulting in various forms of attacks. These could range from a DoS attack against the webserver to an elevation of privilege attack or even information disclosure by the web server itself.

Repudiation threats: The instance involves the meter data management system asserting that it has not recorded data received from an entity situated on the opposing side of the trust boundary.

Information disclosure: Instances of information disclosure encompass scenarios where data in transit could be intercepted by an attacker. The severity of the data exposed depends on the specific type of information being targeted by the attacker.

DoS: DoS attacks hinder legitimate users from accessing their rightful resources. For instance, external actors disrupt the flow of data across trust boundaries in either direction.

Elevation of privileges: By elevating privileges, a user within the system, whether authorized or not, can attain access to information beyond their authorized scope.

3.3 LINDDUN

The LINDDUN approach is founded on a model-based strategy, utilizing a Data Flow Diagram (DFD) as a visual representation of the system under analysis[19]. This DFD forms the foundation of the analysis process, with every constituent systematically scrutinized to uncover potential privacy vulnerabilities. A crucial aspect of this methodology is its knowledge-driven nature. It furnishes an inclusive outline of prevalent attack routes linked to the array of privacy threat categories encapsulated within the LINDDUN acronym (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Noncompliance). To provide a clearer view, Table 2 presents a comprehensive breakdown of all threats, mapped alongside their corresponding LINDDUN types.

3.3.1 Analyse Threats in the DFD

Likability: An AMI system adeptly gathers intricate energy consumption data from intelligent meters and skilfully integrates it with the personal information of individual customers. By analysing discernible energy usage patterns, this sophisticated system establishes meaningful connections with Specific individuals, thereby unveiling valuable insights into their activities and lifestyle preferences.

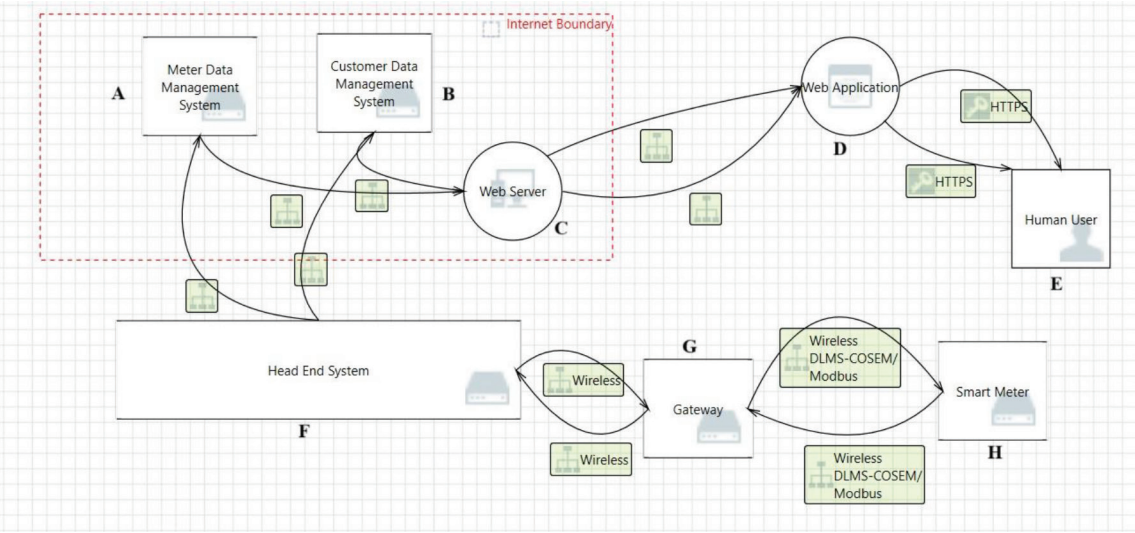

Figure 3. Data flow diagram.

Table 1. Stride threat-modelling table

Threats	Stride types						
	Dialog	S	T	R	I	D	E
Source data store meter data management	A, B, C	X					
Web application	C, D	X	X	X		X	
Web applications may be subject to elevation of privilege using remote code execution.	C, D						X
Elevation by changing the execution flow in web application	C, D						X
Elevation using impersonation	C, D						X
Source data store customer data management	B, C	X					
Weak access control for a resource	A, B, C				X		
Destination data store meter data management	A, B, C, F	X					
Data store denies meter data management potentially writing data	A, B, C, F		X				
Source data store head end system	A, B, C, F, G	X					
Destination data store customer data management	A, B, C, F	X					
Data store denies customer data management potentially writing data	A, B, C, F			X			
Data store inaccessible	A, B, C, F					X	
Data flow sniffing	C, D				X		
Data flow is potentially interrupted	A, B, C, D, F					X	
Web servers may be subject to elevation of privilege using remote code execution	C, D						X
Elevation by changing the execution flow in the web server	C, D						X
Human user external entity	D, E	X					
Elevation using impersonation	A, B, C, D, E						X
Source data store head end system	A, B, C, F, G	X					
Destination data store gateway	F, G, H	X					
Source data store gateway	F, G, H	X					
Destination data store head end system	F, G	X					
Destination data store smart meter	G, H	X					
Source data store smart meter	G, H	X					

Identifiability: An AMI system inadvertently exposes customer energy consumption data through insecure interfaces or public channels, which creates an avenue for unauthorized individuals to identify and track specific customers. This vulnerability enables potential attackers to exploit the exposed data, compromising individuals' privacy and potentially engaging in malicious activities.

Non-repudiation: The present condition of an AMI system highlights a lack of viable measures to guarantee the integrity and non-repudiation of energy consumption data. As a result, customers can deny their actual energy usage or manipulate meter readings without detection.

Detectability: This system also demonstrates a deficiency in its ability to detect anomalies or unauthorized activities in energy consumption patterns, such as meter tampering or abnormal usage. This limitation exposes a vulnerability, enabling malicious individuals to manipulate energy consumption or bypass metering mechanisms.

Disclosure of information: This system encounters a critical breach in its security infrastructure, allowing unauthorized individuals to gain illicit access to customer energy consumption data. Exploiting this breach, malicious actors can exploit the compromised information for malicious purposes, leading to significant privacy violations and potential harm to the affected individuals.

Table 2. LINDDUN

DFD Elements	LINDDUN TYPES							
	Threat targets	L	I	N	D	D	U	N
Web application	Cookies	X				X		
	Communication	X		X		X	X	
Web server	MDM	X						
	CDM		X		X			
	Storage	X			X		X	
HES	Data flow		X			X	X	
Gateway	Communication		X		X	X		
Smart meter	Communication			X				

Unawareness: The system shares energy consumption data with third-party entities or services without implementing proper anonymization techniques. This practice allows these entities to link the data to specific customers, enabling them to aggregate and analyse it. Consequently, this compromises individuals' privacy by revealing intimate insights into their energy usage habits.

Non-compliance: The system fails to comply with essential data protection and privacy regulations, including the General Data Protection Regulation (GDPR) and pertinent local legislation.

4. Conclusion

The security of AMI is of utmost importance, especially considering its extensive deployment in modern utility systems and because it is a foundational component of the smart grid. This paper introduces a sophisticated threat modelling framework for AMI using STRIDE and LINDDUN models. The primary contribution of this study is the development of a systematic methodology that effectively characterizes system-specific threats using the STRIDE and LINDDUN approaches. To validate the framework, a real laboratory-based smart meter setup is used as a case study for threat modelling.

The study brings to light the concerning revelation that attackers can achieve targeted malicious objectives by exploiting vulnerabilities at different locations within the system. The STRIDE and LINDDUN approach provides meaningful and easily understandable results, enabling system designers to develop appropriate security solutions. Furthermore, the outputs produced by this framework have practical implications in the domain of risk analysis, facilitating the recognition of pivotal threats and the development of suitable strategies for mitigation. Through the utilization of the STRIDE and LINDDUN approach, the framework adeptly addresses system vulnerabilities, leading to an enhanced level of security within the AMI.

5. References

1. Mohassel RR, Fung AS, Mohammadi F, Raahemifar K. A survey on advanced metering infrastructure and its application in smart grids. In: 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE); 2014. p. 1-8. https://doi.org/10.1109/CCECE.2014.6901102
2. Potter B. Microsoft sdl threat modelling tool. Network Security. 2009; 2009(1):15-8. https://www.sciencedirect.com/science/article/pii/S135348580970008. https://doi.org/10.1016/S1353-4858(09)70008-X
3. MS, VD, KBR, PK, Gupta P. Smart metering system. In: 2021 Innovations in Power and Advanced Computing Technologies (i-PACT). 2021.
4. Yan Y, Hu R, Das S, Sharif H, Qian Y. A security protocol for advanced metering infrastructure in smart grid. IEEE Network. 2013; 27:64-71. https://doi.org/10.1109/MNET.2013.6574667
5. Khan R, McLaughlin K, Laverty D, Sezer S. Stride-based threat modelling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE; 2017. p. 1-6. https://doi.org/10.1109/ISGTEurope.2017.8260283
6. Sion L, Wuyts K, Yskout K, Van Landuyt D, Joosen W. Interaction-based privacy threat elicitation. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroSandPW). IEEE; 2018. p. 79-86. https://doi.org/10.1109/EuroSPW.2018.00017
7. Metke R, Ekl RL. Security technology for smart grid networks. IEEE Trans Smart Grid. 2010; 1:99-107. https://doi.org/10.1109/TSG.2010.2046347
8. Paverd J, Martin AP. Hardware security for device authentication in the smart grid. In: Cuellar J, editor. Smart Grid Security. Berlin, Heidelberg: Springer Berlin Heidelberg; 2013. p. 72-84. https://doi.org/10.1007/978-3-642-38030-3_5
9. Wang W, Lu Z. Cyber security in the smart grid: Survey and challenges. Comput Netw. 2013; 57:1344-71. https://doi.org/10.1016/j.comnet.2012.12.017
10. Fan Z, Kulkarni P, Gormus S, Efthymiou C, Kalogridis G, Sooriyabandara M, Zhu Z, Lambotharan S, Chin WH. Smart grid communications: Overview of research challenges, solutions, and standardization activities. IEEE Commun Surv Tutor. 2013; 15(1):21-38. https://doi.org/10.1109/SURV.2011.122211.00021

11. Anzalchi, Sarwat A. A survey on security assessment of metering infrastructure in smart grid systems. In: SoutheastCon; 2015. p. 1-4. https://doi.org/10.1109/SECON.2015.7132989
12. Gupta H, Mondal S, Majumdar R, Ghosh NS, Suvra Khan S, Kwanyu NE, Mishra VP. Impact of side channel attack in information security. In: 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). 2019; 291-5. https://doi.org/10.1109/ICCIKE47802.2019.9004435
13. Huseinovic, Mrdovic S, Bicakci K, Uludag S. A taxonomy of the emerging denial-of-service attacks in the smart grid and countermeasures. In: 2018 26th Telecommunications Forum (TELFOR); 2018. p. 1-4. https://doi.org/10.1109/TELFOR.2018.8611847
14. Patni P, Iyer K, Sarode R, Mali A, Nimkar A. Man-in-the-middle attack in http/2. In: 2017 International Conference on Intelligent Computing and Control (I2C2); 2017. p. 1-6. https://doi.org/10.1109/I2C2.2017.8321787
15. Marback, Do H, He K, Kondamarri S, Xu D. A threat model-based approach to security testing. Softw Pract Exp. 2013; 43(2):241-58. https://doi.org/10.1002/spe.2111
16. Hussain S, Kamal A, Ahmad S, Rasool G, Iqbal S. Threat modelling methodologies: a survey. Sci Int (Lahore). 2014; 26(4):1607-9.
17. Khan S. A stride model-based threat modelling using unified and or fuzzy operator for computer network security. Int J Comput Netw Technol. 2017; 5:13-20. https://doi.org/10.12785/ijcnt/050103
18. Hussain S, Kamal A, Ahmad S, Rasool G, Iqbal S. Threat modelling methodologies: A survey. Sci Int (Lahore). 2014; 26(4):1607-9.
19. Wuyts K, Joosen W. Linddun privacy threat modelling: A tutorial. CW Reports; 2015.