Advanced Metering Infrastructure (AMI) System Security

Bala Krishna Yadav Kunati(40292128), Jaykit Kukadiya(40261905), Raghu Pavan Annam(40303699),
Virenkumar Virani(40279337), Vishal Vishal(40294677)
CIISE, Concordia University, Montreal, QC, Canada

I. Abstract

The term Advanced Metering Infrastructure or AMI used in this paper is definitely a game changer in implementing two way communication between the utilities and their consumers in most energy management systems. This paper reviews all aspects of AMI including its designs, its physical architectures, its deployment in terms of communication technologies, its oriented security concerns and the relation of AMI in conjunction with the Home Area Network (HAN). Components related such as smart meters, DCUs, MDMs include them, we discuss such devices in relation to the usage in data gathering, billing and device control systems, remotely. The research provides a comparative analysis of the different communication types including networks such as WiMAX, Zigbee, Wireless Mesh Networks and cellular networks on their benchmarks criteria that will include their suitability for AMI technology in terms such as efficiency, coverage and the cost. Security risks like DDoS, data loss, replay when are attacked already in place also incorporated and there is the presentation of recommendations including creating unity between IDS and PKI. The paper also examines these and other issues like interoperability, risk assessment and other security risks associated with data privacy issues related to HAN. Importance of continuous risk assessment and strong security controls has also been highlighted in order to make sure that AMI is efficient and robust in smart grid scenarios.

Keywords: Advanced Metering Infrastructure (AMI), Smart Meters, Wireless Communication, Security Challenges, Intrusion Detection System (IDS), Public Key Infrastructure (PKI), Home Area Networks (HAN), Smart Grid.

II. Introduction and Background

The electric power industry is currently witnessing a paradigm shift owing to recent advancements in technology, increasing usage of renewable energy, and a growing focus on sustaining and improving efficiency. Traditionally, the electric power sector interfaced with customers through a vertically integrated system wherein distinct electric power was produced for consumption by customers through large-scale power plants connected via grids. However, this holistic view faces challenges due to inefficiencies, energy loss, susceptibility to shocks, and low integration of renewable resources.

As a result, modern society needs to evolve into *smart grids*, where distributed generation units within the grid networked by advanced communication, control, monitoring, and computing technologies work together efficiently. Smart grids support two-way communication, enabling remote sensing and optimization of electricity generation, aiming for an eco-friendly and robust energy network.

The Electric Power Industry's Shift: A Quick Overview

The transition from conventional to smart grids involves several key components:

Decentralized Generation: Unlike conventional systems generating energy from large-scale facilities, modern grids use dispersed sources like solar panels, wind turbines, and micro-grids. This increases grid resilience and reduces dependency on federal systems.

Renewable Sources of Energy: Smart grids facilitate the integration of variable renewable sources like wind, solar, and hydroelectric power through predictive and adaptive controls to balance supply and demand efficiently.

Two-Way Communication: Smart grids enable real-time communication between utilities and consumers. This allows consumers to monitor usage and participate in demand-response programs while utilities manage load distribution effectively.

Digitalization and Automation: IoT, AI, and ML technologies enable automated grid operations, predictive maintenance, and anomaly detection, enhancing overall efficiency and uptime.

Introduction to Advanced Metering Infrastructure (AMI) and Its Role in Smart Grids

Advanced Metering Infrastructure (AMI) is a foundational component of smart grids, comprising smart meters, communication networks, and data management systems. It facilitates bidirectional communication between consumers and utility providers, offering numerous advantages:

- **Real-Time Monitoring and Data Collection:** AMI records energy consumption patterns, aiding in optimization and accurate billing.
- **Demand Response and Load Shedding:** Utilities can implement demand-response programs, reducing or increasing electricity usage during peak periods to balance loads and reduce grid pressure.
- **Dynamic Pricing and Consumer Engagement:** AMI enables variable pricing based on demand and supply, allowing consumers to adjust usage and costs accordingly.

- **Support for Renewable Integration:** Continuous power and consumption data from AMI help manage variable outputs from renewable sources, supporting their integration into the grid.

Objectives, Scope, and Importance of the Study

Objectives:

- Examine AMI's impact on smart grid performance in terms of reliability, efficiency, and sustainability.
- Evaluate technical, economic, and regulatory challenges and opportunities in AMI deployment.
- Investigate emerging trends and innovations in AMI technology.

Scope:

- Covers technical, economic, and social aspects of AMI in smart grids.
- Includes case studies on successful AMI deployments.
- Addresses challenges like data security, privacy, and system interoperability.

Importance:

- Optimizes energy efficiency and minimizes waste.
- Enhances grid resilience with automated self-healing capabilities.
- Facilitates renewable energy integration.
- Empowers consumers through cost savings and real-time interaction.
- Provides data for developing effective energy policies and regulations.

III. AMI Architecture, Technologies, and Security Challenges

A. AMI Architecture

Advanced metering infrastructure enables bidirectional communication across the utility provider and the customer. it helps to fulfil better electricity demand response. to achieve these various benafits, AMI architecture estabilished various components, networks, and communication technologies at various different stages. the entire network is devided in 4 different domains such as operation, transmission, distribution, and customer as it showed in fig2. every domain has it's different technologies in terms of components and communication technologies.

1) ***Customer Domain:*** *:* it is the essential part of AMI networks where it holds the smart meters at customer's home. the smart meter plays vital role in AMI network responsible for data transmission back and forth to the utility provider about the usage of electricity, estimated surge in usage, quality of electricity, fault in meters, electricity theft etc. it is connected to different devices in the house via zigbee, powerline communication(PLC), bluetooth or wifi networks as it is sutable for the range limit and data transfer limit such as energy controller, smart sensors, and smart sockets where it monitors the usage patterns and display the related information on the energy controller dashboard. fig1 shows the map how smart meter is connected to other devices in the house.

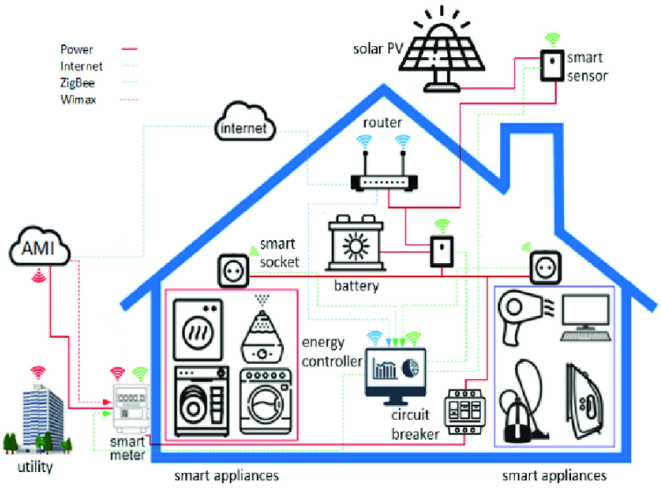

Fig. 1. AMI in Home

2) ***Distribution Domain:*** this part of ami network is responsible for collectin of local data from smart meters and send it to the main relay server or data collector access point through neighbourhood area network. this domain of the AMI incorporates various data collectors at various level and connected to each other through mash network that assures the robustness of the network. all the smart meters are the the leaf of the tree structure while the level 1 data collector gather and communicates with the those smart meters, the laven 2 data collectors communicates with level 1 data collectors and so on till the root data aggrigation accesspoint. the communication technologies mostly includes wifi, cellular, and PLC.

3) ***Transmission Domain:*** This domain ensured the connectivity the data aggrigation accesspoint which is actually works like a gateway to the AMI head end located in operation domain having long distance around hundreads of kilometers using wide area network. the component of this domains mainly have the Wimax, cellular networks, satelite communication, optical fibers to communicate and transfer the information as these modes of communication provides long range to transmit the data over the wireless networks around 100KM with data rate of 10Mbps to 1Gbps.

4) ***Operation Domain:*** this is the most important domain of AMI networks where the everything is recorded, calculated and managed. it holds several components includes mainly the AMI headend, meter data management system and utility center. AMI headend can communicate with the smartmetere and the meter data management system(MDMS). it can communicate with smart meters bi-directionally to get the data and execute the commands, update the firmware, and other configuration, control and dignostics commands on meters. The meter data management system(MDMS)'s main job is to make data available to other smartgrid components. it is responsible for aggrigation, validation, estimation, and other permission of editing meter data including energy usage, generation and meter logs. it stores the data lor limited period of time before is goes to archive. while utility center on other

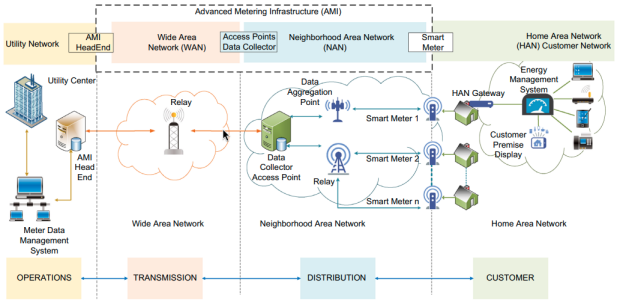

Fig. 2. AMI in Home

hand responsible for billing operations.

B. *Security Challenges*

Physical Attack: Smart meters are equipped with strong tamper-proof mechanisms to ensure robust physical security. If the meter case is opened without authorization, physical alterations may be made, and logs can be tampered with. This scenario aligns with the billing fraud incidents in Puerto Rico, where such unauthorized alterations are typically involved.

Protocol weakness Smart meters can be vulnerable due to reliance on 3G, 4G, or older 2G networks, with many utilities not implementing encryption, allowing attackers to exploit shared credentials across meters. also wireless communication standards like ZigBee suffer from poor encryption and weak implementations that put major threat on AMI security.

Legacy Infrastructure: Outdated and old designed infrastructure components that was made without taking security under consideration may have high probability of exploitation as it is not up to date with current security standards.

Data Privacy & Integrity: As AMI transmits large amounts of sensitive data, it becomes vulnerable to unauthorized access. A breach could harm the utility's reputation, expose customers to risks like identity theft, and lead to data manipulation, negatively affecting both the operator and customers, resulting in financial losses and eroded trust.

IV. Proposed Security Framework

A. *Framework Overview*

The proposed Advanced Metering Infrastructure (AMI) security framework is centered on safeguarding the system's vital elements, such as centralized servers, communication networks, data aggregation systems, and smart meters. The framework uses a number of encryption approaches to provide secure communication between components, intrusion detection systems (IDS) for real-time threat detection, and PKI-based authentication to secure access to AMI devices. By guarding against illegal access, tampering, and data breaches, these security procedures are intended to preserve the AMI system's availability, confidentiality, and integrity.

*1) **PKI-based Authentication with Digital Certificates**:* In order to secure connections between smart meters and central management systems, PKI authentication is essential. A reliable Certificate Authority (CA) should issue a distinct digital certificate for every meter and system component in the AMI network. This method guarantees that data transferred between devices is encrypted and impenetrable by unauthorized parties, and that only authorized devices are able to engage in communication.

Digital Certificates: By verifying the identification of central servers and smart meters, digital certificates stop unwanted devices from joining the network. This is essential for stopping assaults like man-in-the-middle (MitM) attacks, in which hackers intercept and perhaps change device-to-device connections.

Public and Private Keys: Each device (such as a smart meter) employs a different public/private key pair as part of the system's asymmetric encryption. To make sure that only the designated receiver can read the data, the public key is used for encryption and the private key is used for decryption.

Revocation and Renewal of Certificates: To make sure that compromised devices are swiftly taken off the network, compromised or expired certificates are tracked using a Certificate Revocation List (CRL).

*2) **Intrusion Detection Systems (IDS) for Insider and Outsider Threat Detection**:* Since AMI systems are distributed, it is necessary to address both external (like hackers or cybercriminals) and internal (like rogue employees or contractors) threats. IDS systems are essential for identifying network attacks or questionable activity. These systems keep an eye on communication between central servers, communication gateways, and smart meters in order to spot irregularities or known attack signatures.

Network-based intrusion detection systems (NIDS) : Keeps an eye on network traffic, searching for odd patterns like traffic flooding or illegal access to communication channels that can point to an attack.

Host-based IDS (HIDS): Keeps an eye out for indications of compromise, like configuration changes or the execution of illegal commands, on individual smart meters or other devices.

To identify zero-day assaults or advanced tactics that don't fit established attack signatures, intrusion detection systems (IDS) should be integrated with machine learning (ML) and behavioral analytics. In AMI systems, where attackers might attempt to alter readings or interfere with service without setting off conventional IDS warnings, this is very crucial.

B. *Mechanisms and Strategies*

Secure Communication Channels and Encryption Methods Both wide-area (such as between meters and central servers) and local (such as between meters and local gateways) communication are commonly used in AMI systems. To stop hackers from altering data or listening in on conversations, it is crucial

to make sure that all communications are encrypted from beginning to end.

Symmetric Encryption (AES): Large amounts of data sent between smart meters and aggregation sites are encrypted using symmetric encryption, or AES. Fast encryption with robust security is offered by AES.

Asymmetric encryption (RSA, ECC): Used to safely exchange keys and use digital certificates to confirm the identity of devices (like gateways or smart meters). When it comes to safeguarding the communication channel between central servers and smart meters, RSA and ECC work very well.

Transport Layer Security (TLS): It is a crucial protocol for protecting communication channels. It makes sure that information transported across a network is encrypted and safe against man-in-the-middle assaults. All communications between central management systems and smart meters should use TLS.

Countermeasures for Common Attacks in AMI Systems

*1) **Denial of Service (DoS) & Distributed Denial of Service (DDoS) Attacks**:* DoS/DDoS attacks have the potential to overload central servers or communication channels in AMI systems, making them unusable. The goals of these attacks could be to produce erroneous readings, delay data reporting, or interfere with power distribution. Countermeasures consist of:

Traffic Filtering and Rate limitation: Network gateways should use rate limitation and traffic filtering to avoid request flooding. Traffic from IPs displaying questionable patterns may be blocked as a result.

DDoS Mitigation Services: By absorbing harmful traffic, services such as Content Delivery Networks (CDNs) or specialized DDoS mitigation solutions can lessen the impact on vital systems.

Intrusion Prevention Systems (IPS):By detecting and stopping attack traffic in real time, intrusion prevention systems (IPS) can lessen the impact of DDoS attacks before they affect vital infrastructure.

*2) **Spoofing and Device Impersonation**:* AMI systems are particularly vulnerable to spoofing attacks, in which criminals pose as trustworthy smart meters or network equipment in order to obtain illegal access or introduce erroneous data into the system. One way to lessen this is by:

Digital Certificates for Mutual Authentication: Digital certificates should be used by every device and communication gateway to authenticate itself to the network. This guarantees that only authorized devices can engage in data exchanges and stops unauthorized devices from connecting to the network.

Device Whitelisting: A device's identity and certificate must be pre-registered and validated before it is permitted to communicate on the network. By doing this, rogue devices are kept out of the network.

Physical Security: Make sure that gadgets are shielded from unauthorized replacement or modification.

*3) **Man-in-the-Middle (MitM) Attacks**:* MitM attacks include a hacker intercepting and perhaps changing the communication between a central system and a smart meter. The attacker might be able to add erroneous readings or alter data as a result. In AMI systems, MitM attacks can be avoided by:

End-to-End Encryption (TLS): All information sent between meters and central servers is kept confidential and safe from manipulation by employing TLS to encrypt communication routes.

Digital Signatures: By adding digital signatures to communication packets, you may make sure that any data sent is authentic and unaltered.

Key management: Using public key infrastructure (PKI) and rotating keys on a regular basis prevents the system from being compromised even if one key is compromised.

V. Risk Assessment and Application

A. Risk Assessment Framework

*1) **Vulnerabilities in AMI**:* AMI Systems are a critical component of Smart Grids Infrastructure. Since all these devices are connected through air, they are obviously vulnerable to cybersecurity threats and has a huge attack surface. These include sniffing the data packets during transmission, unauthorized device access, device spoofing attacks, denial-of-service (DOS/DDOS) attacks and man-in-the-middle (MITM) attacks like manipulation of smart meter readings.

Layer	Vulnerabilities	Attacks	Impacts
Hardware (SM, Data Concentrator, Utility Center)	Remote Disconnect, Lack of Resources, Web Access	Denial of Power, Buffer Overflow, SQL Injection, DoS, DDoS	Data Theft, Firmware Modification, Denial of Power
Data (SM & DC to UC)	Data Manipulation, Firmware Manipulation, IP-Based Data Transfer	Data Manipulation, IP Spoofing, Teardrop Attacks, DoS	Confidentiality, Integrity, Availability
Communication (Wireless, Wired and Communication Channels)	Wireless Communication, Communication Line Failure	MITM, Session Hijacking, Communication Channel Failure	Data Leakage, Data Fraud, Service Availability

Fig. 3. Threats and Vulnerabilities in AMI

*2) **Mitigation Strategies**:* Mitigation Strategies for AMI Systems involves implementing strong encryption protocols like AES for symmetric encryption and ECC for asymmetric encryption to secure both local and wide-area networks. Implementing strategies like intrusion detection systems (IDS) for anomaly detection and using public key infrastructure (PKI) for robust device authentication can reduce the susceptibility to attacks. Additionally, regular security assessments and updates can go a long way in reducing the risks of DOS/DDOS attacks.

*3) **Challenges**:* There are a lot of challenges faced by utilities. This is often due to the lack of expertise in information security, difficulty in estimating the probability of new threats and insufficient past incidents data. Moreover, AMI's reliance on emerging technologies and complex systems adds even more uncertainity by increasing the attack surface and making it harder to identify potential risks.

B. AMI in Home Area Networks (HAN)

*1) **Communication Models: Controlled vs. Uncontrolled**:* In controlled models, AMI centrally dictates the operational schedule of appliances based on system constraints and energy pricing, thereby improving the overall grid efficiency. On the other hand, uncontrolled models allow appliances to operate independently, with minimal communication primarily for monitoring purposes. Controlled models require robust two-way communication protocols to handle real-time scheduling, whereas uncontrolled models focus on simplicity and consuming less bandwidth.

*2) **Use Cases**:* Smart Appliances like smart refrigerators, washing machines, etc., can interact with AMI to adjust their operation based on dynamic pricing signals, ensuring cost-effective energy usage. For example, high-load appliances like air conditioners can delay their activities to off-peak hours. This reduces the consumption from the grid during peak hours, while providing cost benefits to the consumers.

*3) **Addressing Challenges**:* One key issue with AMI systems is maintaining consumer privacy. It's important to ensure that only aggregate usage data is shared, avoiding any exposure of specific appliance-level information. Techniques like encryption and anonymization plays a crucial role in preserving the privacy in AMI Systems. Moreover, integrating these systems with a variety of appliances pose a complex set of challenges. For example, it's crucial to make sure different appliances can work seamlessly with AMI, all while minimizing disruptions to the actual usage of the devices in people's day to day lives.

VI. Evaluation, Future Work And Conclusion

A. Evaluation

*1) **Security Evaluation:**:* Defenses Against Spoofing: Below is a proposed framework that uses PKI-based authentication using the digital certificate to ensure a unique identification and verification system for every device in the AMI network. This will nullify the spoofing attack when the attacker is posing to be legitimate devices. It will contain a digital certificate and mutual authentication so that only the authorized devices can communicate through this network to reduce spoofing.

Resistance to Sybil Attacks: The Sybil attack is an attack in which an attacker creates multiple identities to overcome the network. Herein, the main contribution of the PKI-based authentication mechanism is that each device is configured with its own certificate, which creates difficulty for an attacker to create and manage multiple identities. Continuous monitoring by the IDS at the trusted authentication in the framework enhances the resistance against Sybil attacks.

Resistance to Denial of Service (DoS) attacks: It deploys various countermeasures against DoS attacks. Traffic filtering and rate limitation at network gateways avoid the flooding of requests. It also uses DDoS mitigation services and intrusion prevention systems to absorb and block malicious traffic. The simulation results done on NS3 evidence that under DoS attacks, there is still stability in the performance of the network with just a few packet drops and still tolerable end-to-end delay.

*2) **Efficiency Evaluation:**:* Latency: The implementation of effective communication protocols such as Zigbee and Wireless Mesh Networks (WMN) within the framework facilitates a reduction in latency associated with data transmission. Results from simulations demonstrate that the average end-to-end delay remains low, even in the presence of attack scenarios. Additionally, the channel switching algorithm diminishes the effects of jamming attacks, thereby preserving the promptness of communication.

Reliability: Overall redundancy from the mesh network paths and its reconfigurable routing are used to make the proposed framework fault-tolerant. Continuously monitoring the network by using the IDS and IPS systems will ensure that it is highly available and reliable. It can be observed from the simulation results that even under severe conditions, the packet delivery ratio of the proposed network is high.

Selection Criteria: The performance of the framework can be measured based on the packet delivery ratio, end-to-end delay, and packet drop ratio. Simulation results by NS3 indicate that the framework functions well, with high packet delivery ratios and negligible delays. Moreover, encryption and authentication mechanisms ensure secure and highly efficient communication.

B. Future Work

The proposed framework presents a strong solution toward ensuring the security in the AMI system, though there exist manifold areas of future research and development:

1. AI-Powered Threat Detection: This would be possible with the integration of AI and machine learning algorithms that are capable of strengthening threat detection frameworks. Thus, AI-driven systems can learn from attack history, adapt themselves according to new attack patterns, and provide proactive and precise threat detection.

2. Integration with IoT and EV: The integration of IoT devices and EVs in the AMI network has thus created new vulnerabilities linked with security. Further research needs to be directed toward the development of safe communication protocols along with all relevant authentication schemes suitable for the integration of IoT and EV-related technologies toward overall security and efficiency in the smart grid.

3. Advanced Cryptographic Techniques: Exploring advanced encryption mechanisms, such as homomorphic encryption, can further enhance the confidentiality and integrity of data in transit. Future research should focus on developing and implementing these advanced encryption techniques in AMI systems.

4. Secure Routing Protocols: A scheme would ensure safe and efficient data transmission, developing secure routing protocols in AMI networks. Future works in the design of attack-resilient routing protocols that are able to adapt dynamically to network conditions include works.

Addressing these aspects, future research will manage to enhance security and efficiency in the AMI system for the purpose of ensuring robustness and reliability in the smart grid environments.

C. *Conclusion*

The proposed security framework for the AMI system addressed critical security concerns of the smart grid. It also includes PKI-based authentication support with IDS, hence it is able to resist spoofing, Sybil attack, and hence DoS attacks. Simulation results are presented that validate the efficacy of the proposed framework in offering high security and operational performance.

Key findings of the present review underline the need for proper continuous risk assessment and stringent security controls that may be applied to provide reliable and resilient AMI systems. The proposed framework undertakes an overall solution for securing the AMI system, considering specific constraints and requirements of smart grid environments. It forms a very solid base for further research in the field of smart grid security and opens new ways toward more secure, efficient, and resilient energy management.

VII. **References**

[1] Patel, A. R., & Gupta, S. K. (2021). Security Challenges in Smart Grid AMI Networks. Cybersecurity in Smart Grids, 7(4), 204-219.

[2] O'Connor, E., & Chao, L. (2021). Home Area Networks and AMI: Future Directions. Residential Energy Journal, 9(2), 77-85.

[3] Kapoor, V., & Singh, P. (2020). Risk Assessment Methods in AMI: A Comparative Study. Risk Management in Energy Systems, 6(1), 45-59.

[4] Greene, A., & Baxter, J. (2019). Integration of AMI with Home Area Networks: Prospects and Challenges. Journal of Sustainable Energy, 11(4), 234-248.

[5] Martinez, R., & Rodriguez, F. (2018). Wireless AMI Application and Security for Controlled Home Area Networks. Journal of Network Security, 10(2), 112-127.

[6] T. Baumeister, "Adapting PKI for the Smart Grid," Cyber and Physical Security and Privacy (IEEE SmartGridComm), 2011.

[7] V. Dehalwar, R. K. Baghel, M. Kolhe, "Multi-Agent based Public Key Infrastructure for Smart Grid," The 7th International Conference on Computer Science & Education (ICCSE 2012), July 2012.

[8] A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks," IEEE Transactions on Smart Grid, vol 1, No.1, June 2010.

[9] K. Mitkovic, S. Dietrich, D. Dittrich, and P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms, 1st ed. Prentice Hall, 2005.

[10] A. A. Crdenas, R. Berthier, R. B. Bobba, J. H. Hub, D. G. Jorjeta G. Jetcheva, and W. H. Sanders, "A framework for evaluating intrusion detection architectures in advanced metering infrastructures," IEEE Trans. Smart Grid, vol. 5, no. 2, pp. 906 - 915, March 2014.

[11] IEEE802.13.4, IEEE Standard 802. part 13.4: Wireless Medium Access Control (MAC) and PHY Specifications for Low Rate Wireless Personal Area Networks (WPANs), 2003.

[12] A. Shamir, "On the Generation of Cryptographically Strong Pseudorandom Sequences," ACM Trans. Comput. Syst., vol. 1, 1983.

[13] F. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure (AMI)," in Power and Energy Society General Meeting Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, 20-24 2008.

[14] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in 33rd Annual Conference of the IEEE Industrial Electronics Society, 2007, November 2007, pp. 46-51.

[15] F. M. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure (AMI)," in Power and Energy Society General Meeting Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, 20-24 2008.

[16] Inger Anne Tondel, Maria B. Line and Gorm Johansen, "Assessing Information Security Risks of AMI," in IEEE International conference on Information Systems Security and Privacy, 2015.

[17] P. Jokar, H. Nicanfar, and V. Leung, "Specification-based intrusion detection for home area networks in smart grids," in IEEE International Conference on Smart Grid Communications (SmartGridComm), Oct. 2011, pp. 208-213.

[18] R. Berthier and W. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in IEEE Pacific Rim International Symposium on Dependable Computing, 2011, pp. 184-193.

[19] Desai, S., Alhadad, R., Chilamkurti, N. et al. A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure. Cluster Comput 22, 43–69 (2019). https://doi.org/10.1007/s10586-018-2820-9

[20]Desai, S., Alhadad, R., Chilamkurti, N. et al. A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure. Cluster Comput 22, 43–69 (2019). https://doi.org/10.1007/s10586-018-2820-9

[21]Intelligent Scheduling of Smart Home Appliances Based on Demand Response Considering the Cost and Peak-to-Average Ratio in Residential Homes - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Basic-architecture-of-the-HEMS-with-a-wireless-home-area-network_fig1_357177534

[22]Hart, D. (2008) Using AMI to Realize the Smart Grid. Available at: https://pdfs.semanticscholar.org/8c3b/c76854093b104421f70f49570b8a979da130.pdf.

[23]Tonyali, Samet. "Security and Privacy Concerns in Smart Metering: The Cyber-Physical Aspect - IEEE Smart Grid." Smartgrid.ieee.org, July 2018, smartgrid.ieee.org/bulletins/july-2018/security-and-privacy-concerns-in-smart-metering-the-cyber-physical-aspect.

[24]MANOHAR, ANIL. "The Deployment of Advanced Metering Infrastructure (AMI) Has

Revolutionized." Linkedin.com, 17 June 2023, www.linkedin.com/pulse/cybersecurity-challenges-solutions-advanced-metering-anil-manohar/. Accessed 1 Dec. 2024.