A Comprehensive Survey of Intrusion Detection in Advanced Metering Infrastructure: Toward Scalable Data-Driven Security in Smart Grids

Shampa Banik *

Posted Date: 16 April 2026

doi: 10.20944/preprints202604.1188.v1

Keywords: smart grid; AMI; cybersecurity; intrusion; multimodality; IoC; correlation; MIDS

 doi:10.20944/preprints202604.1188.v1

Article

A Comprehensive Survey of Intrusion Detection in Advanced Metering Infrastructure: Toward Scalable Data-Driven Security in Smart Grids

Shampa Banik

Department of Computer Science, Tennessee Technological University, Cookeville, TN 38505, USA; sbanik42@tntech.edu

Abstract

With the integration of the Internet of Things (IoT), the Advanced Metering Infrastructure (AMI) plays a key role in improving grid efficiency and consumer awareness, and has transformed the traditional grid into a new intelligent, efficient paradigm, the Smart Grid (SG). However, the increasing dependencies of Information and Communication Technology (ICT) for machine-to-machine communications expose the AMI system to a wide range of cyber-physical intrusions or threats, such as data tampering, denial-of-service attacks, and unauthorized access. Vulnerabilities in various AMI's cyber-physical systems (CPSs) components might compromise the integrity and confidentiality of the SG systems. In addition to other defensive mechanisms, the Intrusion Detection System (IDS) acts as a robust countermeasure to safeguard the AMI against cyber-attacks and threats. Though designing an effective IDS and deploying it in a highly distributed AMI network is greatly hindered by the growing number of heterogeneous, multi-sourced, and interconnected system components, as well as the evolving nature of various recent cyber-physical intrusions. This paper presents a comprehensive survey of IDSs in a structured way to address the key challenges of system scalability, heterogeneity, deployment constraints, and, most importantly, detection of various evolving attack patterns tailored for AMI in SG. Unlike current surveys, this study ushers a unified taxonomy of IDS applied in AMI across categories such as data sources, detection mechanisms, and deployment techniques and architectures. A comparative analysis of contemporary methods is provided to highlight their strengths, limitations, and applicability in real-world smart grid scenarios. This paper identifies critical gaps by analyzing contemporary methods used in the current IDSs to tackle various cyber-physical system security vulnerabilities. applicable to distributed system dynamics, AMI in SG. To address key challenges of existing IDSs, a multimodal intrusion detection system (MIDS) is proposed, featuring data-driven, adaptive security solutions for the next-generation AMI system. The technical insights for developing the experimental framework presented in this study aim to guide future research and development of data-driven, robust, scalable, and intelligent IDS solutions for securing AMI infrastructure in the SG system.

Keywords: smart grid; AMI; cybersecurity; intrusion; multimodality; IoC; correlation; MIDS

1. Introduction

Advanced Metering Infrastructure (AMI) plays a crucial role in the Smart Grid (SG), facilitating bidirectional communication between consumers and the utility provider for monitoring and evaluating energy consumption. The AMI, with its intelligent infrastructure and technology, enhances power systems' capabilities for controlling and optimizing the dynamic invoicing, load monitoring, and grid management. Through the widespread integration of smart meters (SMs) and IoT sensors, and by providing real-time, high-resolution data for timely and accurate monitoring, the AMI plays a pivotal role in the grid paradigm. The Information Technology (IT) and Operational Technology (OT) are architectural blocks of AMI architecture and are heterogeneous in nature. Both the IT and OT

 doi:10.20944/preprints202604.1188.v1

support efficient energy management, real-time monitoring, and enhanced security. While IT ensures all device-to-device communication in the AMI network, OT comprises the hardware and software that control and monitor physical devices and processes of the AMI infrastructure. In particular, the OT systems of AMI also include the Smart Meters (SMs), Data Concentrators, Meter Data Management Systems (MDMS), SCADA (Supervisory Control and Data Acquisition), Distribution Management Systems (DMS), and Head-End Systems (HES). The AMI, a distributed system, is depicted in Figure 1.

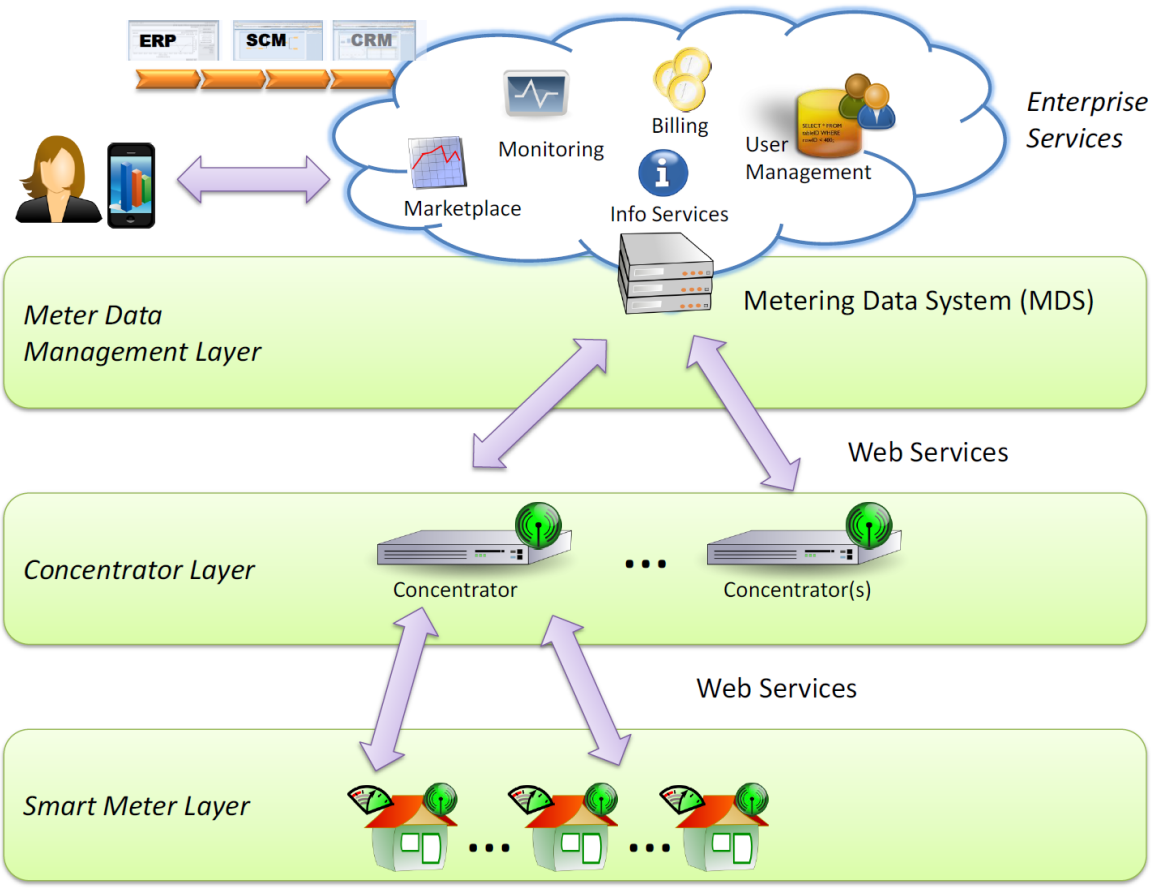

Figure 1. The overview of AMI in the smart grid system [1].

Although the AMI plays a key role in the grid system, it suffers from severe cyber-physical vulnerabilities stemming from the critical nature of its devices and network connections. In particular, the low-power devices such as SMs are typically installed on customer premises or in public locations, making them widely exposed to meter opening or casing breaches, bypassing current/voltage sensors, manipulating calibration components, or short-circuiting measurement circuits, as easy targets to energy theft, inaccurate billing, and falsified consumption data.

Moreover, the devices in the AMI are mostly network-connected, have limited computational power, and lack security features such as strong encryption. All these together make the AMI highly vulnerable to various cyberattacks or intrusions, including unauthorized access, data manipulation, and potential disruptions to the grid operations.

Since existing AMI components use legacy OT systems with limited processing power and outdated security protocols, these legacy components lack adequate security standards, sufficient computational resources for cryptographic methods, essential antivirus software for security compliance, and secure communication protocols. Hence, different components in AMI are vulnerable to many ever-growing attacks and threats that compromise the security and privacy of the AMI systems, such as false data injection, snooping on sensitive data, and data modification, which can disrupt AMI services or be used for personal gain. For instance, a malicious entity with the cryptographic

 doi:10.20944/preprints202604.1188.v1

key can lead to substantial financial repercussions for the electricity provider and potentially severe consequences for people's lives and safety, shutting down numerous smart meters remotely.

Breaches will occur in any distributed system, such as AMI, no matter how hardened, such as energy theft and smart meter compromise. A malevolent actor can disable a large number of smart meters, resulting in severe financial losses and security issues with the cryptographic key in hand. Such an incident could result in significant economic losses for the country [2]; estimates of electricity theft losses in the United States and India are 6 billion and 17 billion, respectively [3,4]. In addition, such exploitation of AMI can not only cause widespread disruptions but also put human life at risk of loss, which is one of the most disastrous effects [5,6]. Hence, securing AMI is essential for safeguarding national critical energy infrastructure, not only to protect people's lives and safety but also to preserve consumer privacy from a wide range of cyber intrusions.

Among other security measures, the IDS acts as a robust detection mechanism to identify anomalous behaviour in the AMI system by continuously monitoring data sources such as network traffic packets, log files,and smart meter data to detect irregular patterns, unauthorized access, data breaches, or suspicious activities[7].

To combat known and unknown cyber assaults targeting the AMI, the IDS generates an alert upon detecting an intrusion, enabling the utility to take action to mitigate the intrusion as soon as possible, ensuring the grid's stability, reliability, and efficiency. The IDS enhances AMI security by mitigating cyber intrusions, energy theft, and data manipulation by integrating both real-time alerts and automated responses [8].

A meticulously designed IDS is necessary to combat various cyberattacks and threats and to adequately address vulnerabilities, thereby safeguarding a critical system like AMI. In recent years, only a few can detect promptly and respond effectively to cyberattacks or threats, although various categories of IDSs have been implemented so far for the AMI. Because recent IDSs for the AMI system are not efficiently equipped with sophisticated monitoring and decision-support tools to collect and analyze real-time data from the entire power system to detect and deter intrusion,

Furthermore, most IDSs fail to address two issues that are paramount in any distributed system: erroneous alerts and scalability issues. Many of the IDSs generate erroneous alerts when no intrusion actually occurs. Another issue is related to the scaling of the IDSs across the distributed system. These issues are significantly contributing factors in AMI because it is a complex, distributed system with numerous devices and networks, where an attack can occur anywhere.

Therefore, to address AMI-related cybersecurity issues, developing sophisticated IDSs for AMI with extensive research and analysis is required. Most of the IDSs are now ML-based, where the training involves both the attack and non-attack data in detecting intrusion, where false positives and false negatives are not completely avoidable. However, a well-trained IDS will minimize the occurrence of such alerts. Besides, the regular IDSs performed over single modality data, multimodal data could be considered for increasing the accuracy and precision of an IDS of a system where different kinds of data are available and can give a good indication of various intrusions [9]. Such an IDS featuring multimodal data first needs to fuse data from various sources with differing modalities, e.g., sensor, network, and customer load data, which may improve IDS results. For a precision

A multimodal intrusion detection system (MIDS) involves methods for fusing and then training data with various modalities collected from different components of the AMI system. In addition, when addressing the scalability issues associated with MIDS, methods for determining which data should be transferred, as well as the optimal amount of data transfer into the detection system with reduced bandwidth and low latency, should also be considered to detect intrusions correctly [10]. Unfortunately, scalability becomes challenging for the IDS when dealing with data from multiple devices and networks. In particular, transferring multimodal datasets to the AMI system can incur network overhead, potentially causing delays and data loss. To minimize this delayed response or network overhead, high-end methods or mechanisms are required in the MIMDS.

 doi:10.20944/preprints202604.1188.v1

This paper aims to serve as a technical reference for researchers to understand the challenges in developing an efficient IDS. Hence, as significant contributions, the paper includes an overview of cyber-physical components of AMI and addresses crucial security issues associated with these components, as well as presents a tailored survey of the state-of-the-art research on IDS from recent literature. Following a thorough survey, a framework is presented that is currently a work-in-progress to investigate strategies for fusing heterogeneous data modalities to train the MIDS for AMI while addressing real-time intrusion detection with scalable performance.

1.1. The Scope of Our Survey and Contributions

The scope and significant contributions of this paper are as follows:

- This survey is organized in a comprehensive way to serve as a roadmap for academic researchers to obtain knowledge of integrating threat intelligence to develop advanced IDS.
- First, A taxonomy-based review is presented in a Figure 2, framing a comprehensive overview of AMI security challenges associated with the IDS development. The vulnerabilities of AMI components, which create the attack surfaces for a range of intrusions, along with their threat landscape, are overviewed in the survey that undermines AMI and SG security. Additionally, the paper examines the malicious objectives or goals of attackers or intruders underlying diverse security attacks and intrusive activities in detail.
- Second, a general background on IDS as robust countermeasures, addressing the security aspects of AMI in the SG, is provided. The IDS overview various categories of IDSs, including detection mechanisms, architectures, and related factors with conventional approaches and advanced architectural distinctions, and different diverse technologies for deployments across AMI and SG paradigm.
- Third, the survey compares various IDSs for AMI and SG systems to identify what several current and novel IDSs focusing on AMI are computationally lacking, in order to be more effective and robust at detecting actual attacks or assaults that threaten the AMI system.
- Then, A prospective defence-in-depth approach is proposed to address security gaps identified in recent literature, leading to the design of intelligent IDSs for AMI. Security-critical components are identified and integrated to enable comprehensive monitoring of intrusive activities targeting AMI.
- Finally, the design algorithm for developing the MIDS is introduced with guidelines for integrating essential components to build an effective MIDS for AMI. The proposed scalable architecture of MIDS and the related key research challenges requiring systematic investigation are highlighted.

The structure of our review's findings comprises five distinct sections. Section 2 provides an overview of the AMI architecture. Then, the article progressed according to the taxonomy of the study presented here. In Section 3, which provided a detailed overview of the security-related aspects of IDSs and their classification, with applications in the grid paradigm. Section 4 presents the current pertinent work and the summarized table of selected relevant research works. Next, section 5 discusses potential gaps in current research and proposes a solution model as a future research direction. Finally, Section 6 concludes the paper.

2. AMI Security Background

This section introduces a taxonomy to guide the discussion throughout the survey. This paper presents the conceptual taxonomy based on the IDS study in the AMI domain, as depicted in the Figure 2.

 doi:10.20944/preprints202604.1188.v1

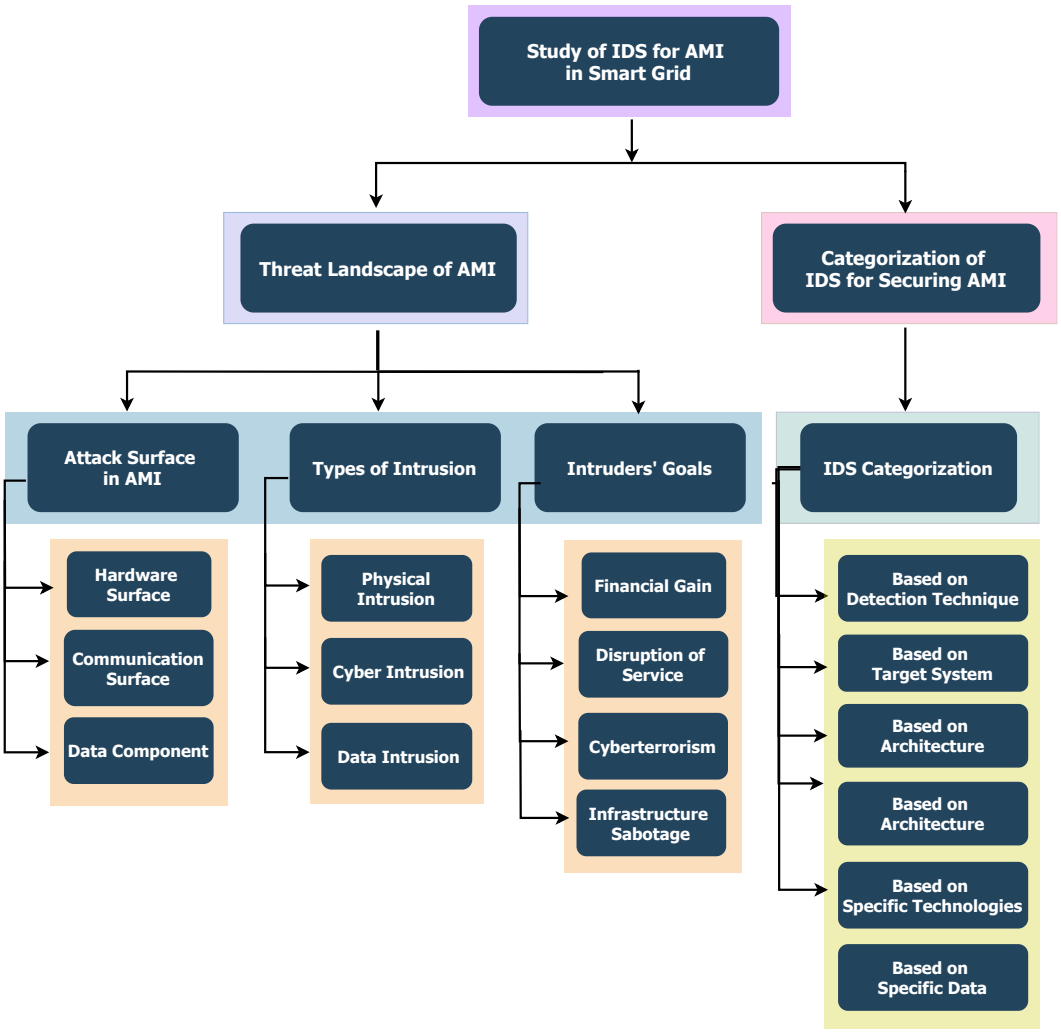

Figure 2. A taxonomy of mapping between the security aspect and study of IDSs targeting AMI.

2.1. Overview of AMI Architecture

In the first stage of the taxonomy, the AMI's typical architecture is discussed. This architecture relies on a three-layer, entirely IP-based, hierarchical service-oriented infrastructure, as depicted in the Figure 1. The distinguished components are as follows:

- **Meter Layer:** This is the layer where residential meters passively control and measure the energy consumption or production of the devices to which they are attached.
- **Concentrator Layer:** The meters communicate with this layer through various protocols, many of which are proprietary, to submit their measurements. The data reported is aggregated and submitted to the Metering Data System (MDS).
- **Metering Data Management Layer (MDMS):** Here, usage data and infrastructure-related events are collected for long-term storage, analysis, and management. To facilitate several managerial applications such as forecasting and invoicing, different enterprise services typically employ this [1].

2.2. Attack Surface: AMI Paradigm

This section provides a general overview of the target components for physical and communication systems in AMI paradigms. Then, from a security perspective, it discusses how the components of AMI have a broad attack surface and Security vulnerabilities for hackers.

(1) Vulnerabilities in the AMI Hardware Components: An AMI system comprises three basic end devices: smart meters (SMs), a data concentrator unit (DCU), and a headend. Smart meters

 doi:10.20944/preprints202604.1188.v1

aim to track the power usage of electrical appliances and other metrics [11]. The smart meter serves three distinct purposes. First, it measures the electricity used. It measures the customer's energy, a key component of smart metering. Therefore, it is fundamental that smart meters can detect energy consumption rates in real-time [12]. Second, it serves as an energy control centre and aggregator for data gathered by the Home Area Network (HAN). Lastly, it also serves as a gateway connecting both the external network and HAN.

Data collectors must preserve the information produced by numerous smart meters in a particular region. The utility company's central server is the AMI headend, which receives, stores, and maintains the data collected by the data collectors. On the basis of collected information from the AMI headend, the utility companies can make informed decisions regarding power generation, transmission, and distribution.

A smart meter has five primary components, as illustrated in the Figure 3. These compartments are as follows: (i) Central Processing Unit (CPU), (ii) Random Access Memory (RAM), (iii) Communication Module, (iv) Flash Memory (EEPROM), and (v) energy sensors.

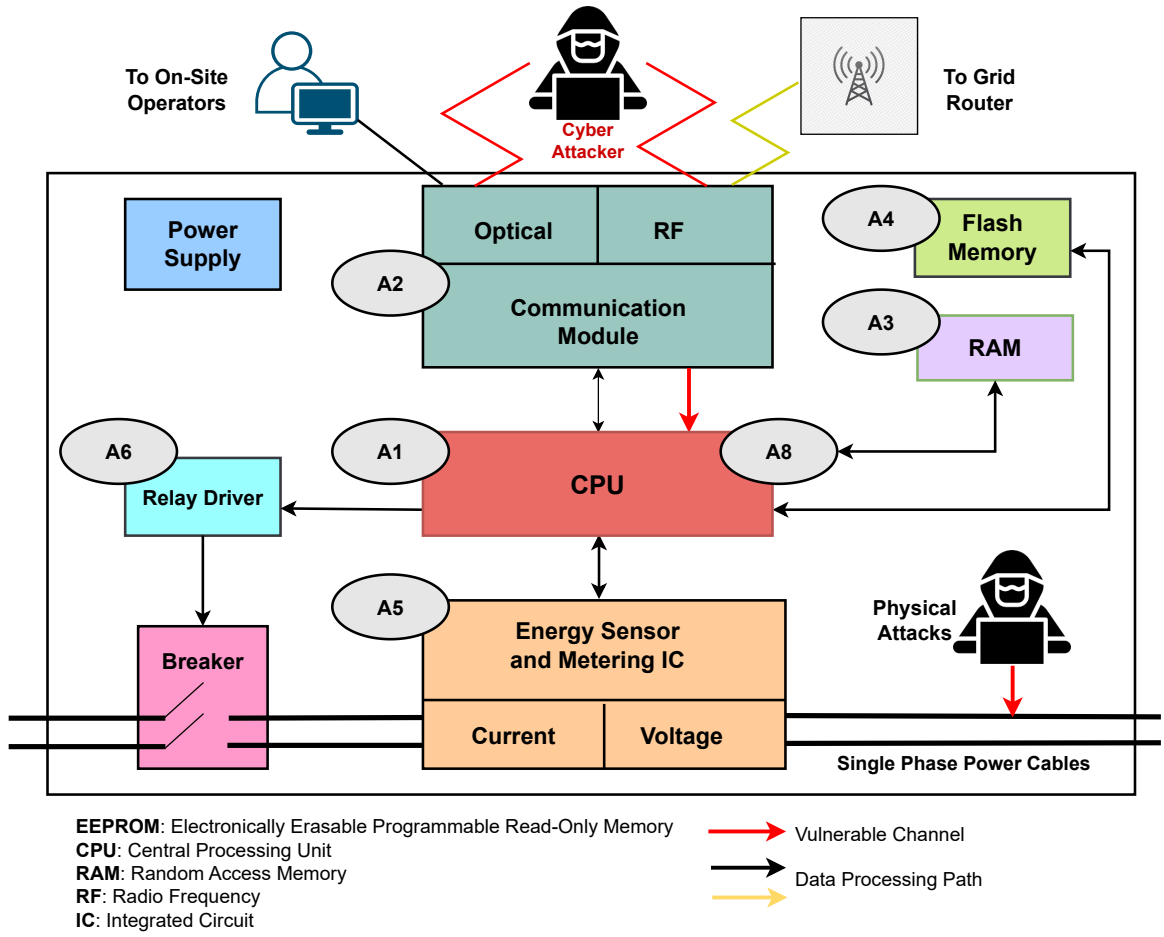

Figure 3. Attack surface in hardware components inside a smart meter [13].

These components are also targeted by various types of attacks as follows:

— **CPU (A1):** Malware installation that results in dummy operations exhausts the computational resources of the CPU.

— **Communication Module (A2):** The communication channels may be disabled or manipulated unintentionally. Furthermore, AMI devices communicate over frequency bands that are vulnerable to monitoring, jamming, or compromise.

 doi:10.20944/preprints202604.1188.v1

— **RAM (A3):** Metering and communication applications may also experience freezing or slowdown due to RAM exhaustion. To address these errors, the kernels of operating systems (OS) either terminate the application(s) that are currently running or reboot the system.
— **Flash Memory (A4):** Attackers can alter recorded consumption data, device calibration, and operation modes by modifying configuration registers.
— **Sensor (A5)/Actuator Compromise (A6):** The utility system can disconnect a customer by sending a tripping command.
— **Inter-Board Communications (A7):** The low-level communication protocols that are implemented by all components are depicted in Figure 3 can be analyzed and adjusted to accommodate the attacker's requirements. These attacks are typically isolated due to the physical access requirements.

Carpenter et al. in [14] have proposed a variety of attack methods against AMI, including EEPROM/microcontroller dumping, bus snooping, firmware disassembly, key extraction, and power- and clock-glitching. In [15], Gurugubelli et al. present the potential attack surface in AMI regarding hardware and network configurations, protocols, and software.

(2) Vulnerabilities in AMI Communication Network Components: AMI supports real-time two-way interaction, enabling advanced applications such as distributed energy management, customer information platforms, and demand response management. The AMI needs end-to-end communication to incorporate these features, which is achieved by combining various network architectures through integration of communication protocols and interfacing between the control center and field devices. AMI communication networks encompass several hierarchical structures, including LAN (local area network) for connecting diverse business systems at the utility level, WAN (wide area network) for connecting the AMI headend with data concentrators, NAN (neighborhood area network) for linking data concentrators to smart meters, and HAN (home area network) for interfacing smart meters with intelligent devices at the consumer level. In contrast to conventional TCP/IP networks in LANs, wide area networks (WANs), neighbourhood area networks (NANs), and local area networks (LANs) may utilize various wired and wireless communication media, along with various public and private protocols, complicating their security. Malicious attackers may execute cyberattacks against LAN (A1), WAN (A2), NAN (A4), and HAN (A6), where the field devices, such as smart meters and concentrators in power utilities, are mostly susceptible to physical attacks (A3 and A5) as shown in the Figure 4 because they are typically implemented on embedded systems and located in public areas, rendering them more vulnerable than the conventional IT infrastructure. Thus, the AMI network components are highly vulnerable to critical types of cyberattacks that primarily target the information and communication networks as they underpin malicious actions such as theft of sensitive data, energy theft, fraud, service interruption for any kind of terrorism, extortion, hacktivism, sabotage and other similar threats, which constitute significant risks [16]. Moreover, even a system integrating with various advanced IT security solutions, including commercial IDSs, firewalls, and malware prevention, can also get exposed to illegal operational functionality, which can result in significant repercussions for the system due to various potential cyberattacks within the LAN. In the first phase of this type of intrusion, the intruder gains access to the network of AMI through unauthorized means and then intends to perform malicious or illicit actions on the system by exploiting any kind of network vulnerability, such as a legacy protocol, low maintenance, a less secure channel, or a lack of robust security mechanisms like encryption. For instance, exploiting the trusted perimeter, such as the firewall, if poorly configured due to incorrect rules or a lack of standard methods, sometimes allows reckless intruders or attackers to gain access to communication networks and infiltrate the network by injecting malicious payloads into control systems and rapidly disrupt the entire process, leading to a catastrophic outcome. In another scenario of intrusion, a cyber attacker or intruder can compromise the trusted AMI control network by exploiting a VPN connection, for example, by waiting for a legitimate user to join, and then intercepting or hijacking the VPN session. The above-mentioned network-based attacks are highly risky because they allow an attacker outside the trusted control system to gain control and exploit the

 doi:10.20944/preprints202604.1188.v1

AMI system [17]. Alongside being an extensively distributed system, the AMI is particularly highly susceptible to distributed attacks or adversaries, for example, distributed denial of service (DDoS), which may concurrently target multiple machines to render bandwidth or resources inaccessible to legitimate users, thereby causing prolonged service disruptions [18,19]. Figure 4 illustrates the general overview of a Smart Metering Network (SMN) in the AMI system.

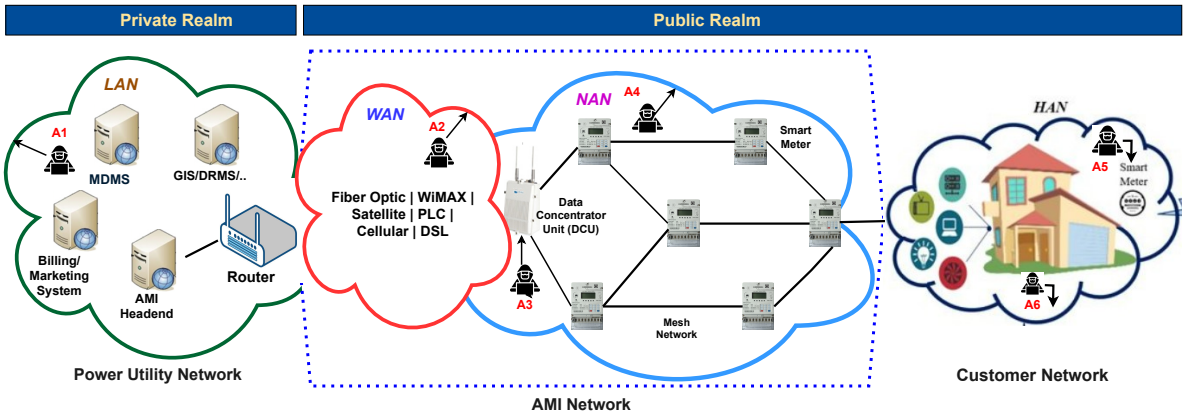

Figure 4. Attack Vector in AMI Network.

(3) Vulnerabilities in AMI Data Components: Collecting data from Smart Meters (SMs) is the primary role of the AMI, and then transmitting this information via Data Concentrators (DCs) to the Utility Center (UC), where it is received, stored, integrated, and analyzed. The data layer serves as the foundational component of an AMI system and is responsible for efficient data operation from data aggregation and ingestion, data storage and management by validating, analyzing, and disseminating smart meter data to utility applications. By bridging between field measurements and utility applications, these components play a pivotal role in AMI by enabling the information backbone for the grid utility service. These data components not only increase reliability by utilizing real-time data through reliable analytics and control but also enhance decision-making across the grid. For transmitting a substantial volume of data across the AMI, encompassing users' energy consumption, personal information, and the operational status of components within the AMI, including health assessments and logs, the data layer plays a key role [20]. By leveraging this component, the utility can improve customer service and make more informed decisions. Since the AMI data contain sensitive information about the consumers, the data layer is highly susceptible to a wide range of intrusions or threats. The predominant attack vectors target the data layer of an AMI by compromising the direct link between the consumer and utility, which is facilitated by the remote updating capability of an AMI system. These threats or intrusions stem from manipulating various components, for example, firmware manipulation; however, the data components, such as SMs, are highly targeted components in AMI fraudulent for alteration, manipulation, insertion, hijacking customers' energy consumption metrics for energy theft, and so on [21].

Besides these, various potential attacks can be executed within this tier of AMI. For instance, exploiting the vulnerability of the Internet Protocol (IP) for data transmission can lead to data theft. The interconnection among different AMI data components is maintained through the high reliance on IP-based systems, which is utterly targeted to cyberattacks, such as IP spoofing, teardrop attacks, and denial-of-service (DoS) attacks[22,23]. Moreover, various types of data manipulation in the WAN within the UC in the AMI system could be carried out by either an internal or an external attacker, which might manipulate the commands transmitted to SMs, leading to SG instability and potentially inducing a power denial [24].

2.3. Type of Intrusion on AMI

Intrusion refers to when an unauthorized user gains access to the system either physically or cyber and gets the ability to control the system with a malignant intention to breach the three main

 doi:10.20944/preprints202604.1188.v1

cybersecurity goals for the SG, which are the AIC triad *Availability*, *Integrity*, and *Confidentiality* (CIA) [25]. Various forms of cyber-attacks, physical threats, and anomalies are now considered "Intrusions" in AMI, alongside cyber and physical threats or attacks. Intrusions targeting the AMI can be categorized by attacker type, motivation, and attack methodology. This section examines each perspective by reviewing the literature.

(1) Cyber Intrusion on AMI: The AMI is an interconnected system within the distribution process of the power grid, which consists of physical components, transformers and circuit breakers, smart meters that are deployed across a metropolitan region, typically serving thousands to millions of consumers. Any type of attack targeting these components can attempt to hack into power plants or distribution network control systems, deceiving sensors and monitoring systems, or destabilizing communication networks that link different grid components. Disruption in AMI can induce instability in this physical process, potentially damaging equipment and causing physical injury to those using the electricity system. The consequences of various cyber intrusions targeting AMI may impact more services and urban areas, potentially influencing the entire nation [26]. Types of assaults against the power grid encompass the following:

- **Denial of Power (DoP):** Denial of power service to a consumer through intrusions on smart meters individually. This form of attack can cause substantial harm when targeted at critical users. A denial-of-service (DoS) is a potential attack on an AMI that results in service denial, that is, a power interruption, in which the attacker floods the AMI's communication network (e.g., wireless channels or control servers) with excessive, fake requests or traffic. A denial-of-service (DoS) attack in the AMI communication network, as defined by [18,24], is an attempt to overwhelm a targeted computer system or network with traffic or requests to disrupt routine operations and prevent authorized users from accessing it. This is what such an attack may entail. Alternatively, the intruder exploits the cyber vulnerabilities in the AMI's communication protocols to inundate the system. In particular, another potential cyber-attack, Man-in-the-Middle (MitM), can exploit the vulnerability of a legacy protocol, such as Modbus [27], to compromise the AMI system by intercepting the communication channel between two parties and can cause the denial of energy [28–30]. Two frequently utilized MitM attack strategies are ARP spoofing and DNS spoofing. In a replay attack, a hacker intercepts previously obtained data, maliciously retransmits it to impersonate the original sender, and gains unauthorized access to the system's network. One of the security threats that isolated SGs face is the replay attack, which involves the fraudulent delay of data transmission [31].
- **Theft of Power (ToP):** With an aim to steal power from the utility, individual smart meters are targeted by various attacks. Consumers or attackers may covertly reconnect to the electricity and intentionally disconnect from the power utility, or can manipulate the legacy protocols by cyber attacks to create discrepancies or break the agreement between physical consumption and recorded data. In addition, data stored in a smart meter may be altered to inaccurately represent power consumption across multiple smart meters. Smart meter manipulation is a common form of cyber intrusion or attack for energy theft [3,20,32–34].
- **Disruption of Grid (DoG):** A large number of smart meter compromises can lead to instability in the power grid, as these are able to be connected and disconnected rapidly in erratic sequences. The power grid may suffer partial failure and pervasive power loss if it cannot absorb this transient behaviour on a sufficiently large scale. For instance, the False Data Injection Attack (FDIA), which manipulates data collected by AMI sensors to mislead grid operational decisions, thereby disrupting grid service [35,36]. Coupled with the limited defence resources and the broad deployment of SMs, other potential cyber attacks, such as Distributed Denial of Service (DDoS), Authentication Attacks, Meter Spoofing and Energy Fraud Attacks, Data Confidentiality Attacks, etc., aim to compromise the AMI system [37,38].

 doi:10.20944/preprints202604.1188.v1

An occurrence of anomalous events that aligns with the predefined attack routes is classified as intrusive behaviour only if it is identified within a sequence. Otherwise, system failure can be considered by the identified anomalous events.

(2) Physical intrusions on AMI: Along with these examples of cyber-attacks, a wide range of physical intrusions can have detrimental effects, such as damaging equipment in AMI infrastructure, meter tampering, device theft, and hardware manipulation, which can even create power outages in the entire SG system. In instances of physical tampering, unauthorized users may manipulate their meters to report reduced consumption by reversing, disconnecting, or applying a strong magnet to the meters [3]. Such actions can result in inaccurate recording of electricity usage.

In instances of physical attacks such as meter tampering, unauthorized customers may manipulate their meters to report lower usage, such as by disconnecting or reversing the meters or applying a strong magnet [3], the meters may not accurately record usage. In this context, various attempts to launch energy theft have often become a grave security concern in the AMI system. To do so, customers may connect high-consuming appliances directly to an external feeder through wiring to bypass the meters. The SMs in AMI are more likely to be attacked physically due to their ease of access and prevalence. Active attackers may consider this an open opportunity and be motivated by financial gain or terrorist objectives to cause widespread disruption of the grid by remotely disconnecting a significant number of SMs or destabilizing distribution or transmission networks [39]. Anderson and Fuloria investigated [40], where an attacker might remotely turn off millions of smart meters simultaneously.

(3) Data Intrusion on AMI: Physical and cyber attacks can be launched to target metering values. In addition to the three potential False Data Injection Attack (FDIA) integrity and confidentiality, energy theft attacks are designed to compromise data integrity and privacy. By gaining unauthorized access, exploiting vulnerabilities, or using or spreading malware, attackers can intercept, manipulate, or exploit SM data to disrupt service or operations, steal information, or cause financial damage. Data tampering, injection and theft are common forms of data attacks in AMI.

In modern SG systems, the Distribution System Operators (DSOs) use real-time AMI data for monitoring and control. As a type of data attack, a potential False Data Injection Attack (FDIA) can mislead operational decisions and undermine Smart Grid stability. A significant class of cyber-attacks, FDIA, can impede the evaluation of the power system's state. This attack could potentially lead to unexpected problems for the power system if the state estimator provides the system operator with false data. This article examines FDI attacks and power system stability, identifying weaknesses in AMI nodes [41]. The Advanced Metering Infrastructure (AMI) in smart IDSs enhances intelligent information processing but introduces new vulnerabilities. Na et al. investigate how FDIA exploits new cyber vulnerabilities of AMI to compromise grid data integrity and disrupt operations [35].

The FDI attack was discovered in [35,36] following a series of attacks and the processing of an innocuous data set. Such injection attacks, whether targeting the smart meter or the command line, can produce seriously abnormal load patterns or power consumption in Singapore, as one example [42].

For instance, Aburomman and Reaz [43] presented a review of IDSs highlighting the hybrid and ensemble classifiers against coordinated attacks, such as distributed denial-of-service (DDoS) attacks. In contrast, Zhou et al. [44] provide an overview of collaborative IDSs. As Arshad et al. [45] point out, future IDS research should focus more on computing overhead, energy usage, and privacy consequences when comparing current IDSs. Berman et al. [46] presented a thorough analysis of deep learning strategies in the context of computer security.

While Tong et al. [47] presented an overview of IDSs for SG's AMI alone, the IDSs for SG's ecosystems and subsystems are covered in great detail by Grammatikis and Sarigiannidis [8]. Furthermore, Grammatikis et al. note that no IDSs have been proven in the literature to defend SG microgrids.

2.4. Intruders' Goals

The intruder or attackers' intentions can vary depending on their goals, but the common objectives include financial profit, political aims, or service disruption. Proactively safeguarding AMI systems is

 doi:10.20944/preprints202604.1188.v1

crucial to defending AMI from such threats. Typically, attackers seek to exploit vulnerabilities in AMI components for various malicious purposes when targeting AMI in a smart grid through different forms of cyberattacks. Among the following are the specific objectives of the intruders or attackers:

1. **Espionage and Intelligence Gathering:** Espionage targeting AMI in SG constitutes a complex danger necessitating aggressive and extensive cybersecurity strategies[48]. With an aim to monitor consumer profiles, the attackers gather intelligence on the smart grid's infrastructure, architecture, operations, and cyber–physical vulnerabilities, which can be used for subsequent reconnaissance assaults or state-sponsored attacks by interrupting the grid's activities as geopolitical objectives.
2. **Privacy Invasion and Data Theft:** As the AMI deals with different types of data, the power consumption data contains sensitive customer-level information. Any invasion of the data, including the data breaches, theft of sensitive consumer data, confidential information, billing data, or energy consumption patterns, can pose significant risks to both consumers and electricity companies [3,49]. When this data is leaked or sold on the black market, it can be misused for different malevolent purposes, either physical crime or cyber exploitation. Different type of organized crime groups including cybercriminals can get a dual-use of this data by planning large-scale residential intrusions (e.g., determining when a residence is vacant) or targeting infrastructure by exploiting Weak grid assets.
3. **Service Disruption:** Manipulating or turning off AMI physical components like breakers can disrupt the typical AMI operation, which may result in interrupting the grid service, such as power outages, grid system overloads, or undermining the reliability of energy distribution [3,49].
4. **Financial Profit:** The cyber criminals can manipulate billing information propagated from SMs to fraud, including energy theft by decreasing energy charges for specific clients or inflating bills to become financial gainers, which may incur substantial economic loss for utilities and result in a decline in consumer confidence[50].
5. **Unauthorized Control:** Gaining unauthorized access or control over any cyber-physical devices of AMI, such as smart meters or a security breach of the communication channel, can allow the attacker or hacker to manipulate energy flow, tamper with meter readings, disable devices, or engage in any malevolent activities [51].
6. **Sabotage and Infrastructure Damage:** The reliability of AMI depends on the integrity of thousands of field devices such as SMs and communication links, which are mostly distributed. Inflict physical damage on these components, i.e., physical sabotage of SMs, DCs, or communication links can severely hamper AMI by interrupting data flows from the field to the utility center or fault induction [15]. Such tangible damage to grid infrastructure can potentially cause disruption of the energy supply.

Our objective is to comprehend the potential manifestations of various attacks associated with attackers' goals within an AMI and to identify them as presented in Table 1.

 doi:10.20944/preprints202604.1188.v1

Table 1. Attacks on cyber-physical systems and how they violate CIA security constraints.

Type of Attacks	Target Surface in AMI	Attacker's Goals				Potential Threat Actor
		Espionage	Data Theft	Energy Theft	Disruption of Grid	
Advanced Persistent Threats (APT)	- Network Infrastructure - Physical Infrastructure - Data Concentrators and Gateways - Utility Backend Systems	✓	✓		✓	- Nation-State Actors - Hacktivists - Cybercriminals - Insiders - Competitors
Denial of Service (DoS)	- NAN Network - Smart Meters - Data Concentrator		✓	✓	✓	- Nation-State Actors - Cybercriminals
Packet Sniffing	- Network Infrastructure - Communication Channel		✓	✓	✓	- Nation-State Actors - Hacktivists - Cybercriminals - Insiders - Competitors
Nation-State Attacks	- Eavesdropping - Man-in-the-Middle (MitM) - Replay Attacks - Denial of Service (DoS) - Jamming		✓	✓	✓	- Nation-State Actors - Hacktivists - Cybercriminals
False Data Injection Attacks (FDIA)	- Manipulating Meter Data - Injecting False Consumption Data		✓	✓	✓	- Nation-State Actors - Hacktivists - Cybercriminals - Insiders - Competitors
Authentication and Authorization Attacks	- Credential Theft - Privilege Escalation - Unauthorized Remote Access		✓	✓	✓	- Nation-State Actors - Hacktivists - Cybercriminals - Insiders - Competitors
Malware and Exploits	- Malware Insertion - Exploiting Software Vulnerabilities - RAM Exhaustion - CPU Overloading		✓	✓	✓	- Nation-State Actors - Hacktivists - Cybercriminals - Insiders - Competitors
Physical Attacks	- Tampering with Smart Meters - Device Theft or Replacement	✓		✓	✓	- Hacktivists - Cybercriminals - Insiders - Competitors

 doi:10.20944/preprints202604.1188.v1

Table 1. *Cont.*

Type of Attacks	Target Surface in AMI	Attacker's Goals				Potential Threat Actor
		Espionage	Data Theft	Energy Theft	Disruption of Grid	
Rogue Devices Attacks	- Inserting Rogue Smart Meters - Malicious Data Concentrators		✓	✓	✓	- Nation-State Actors - Hacktivists - Cybercriminals - Insiders - Competitors
Time Synchronization Attacks	- Manipulating Timestamps - Disrupting Time Synchronization Protocols		✓	✓	✓	- Nation-State Actors - Hacktivists - Cybercriminals - Insiders - Competitors
Social Engineering Attacks	- Phishing - Spear Phishing - Pretexting - Baiting - Quid Pro Quo - Impersonation - Tailgating		✓	✓	✓	- Nation-State Actors - Hacktivists - Cybercriminals - Insiders - Competitors
Supply Chain Attacks	- Compromised Smart Meters - Malware in Software Updates				✓	- Nation-State Actors - Hacktivists - Cybercriminals - Insiders - Competitors

 doi:10.20944/preprints202604.1188.v1

3. Overview of Intrusion Detection Systems

To safeguard AMI from malicious intrusions, IDSs are a secondary security solution following the basic AMI security approaches, including encryption, authorization, and authentication [52]. IDSs are monitoring mechanisms to identify unauthorized entities within a designated system, such as an advanced metering infrastructure (AMI). Intrusion detection and prevention should be the primary goals of these measures, and they should also support mitigation techniques to enable rapid recovery of vital systems in the event of an attack. Therefore, developing robust countermeasures in the AMI system has become a grave concern due to technical, organizational, and regulatory issues, as well as ongoing research and development initiatives. In [47], the authors examined recent academic approaches to intrusion detection systems and techniques for AMI, and discussed threats that could affect this industry. To identify potential threats and unusual occurrences, the Intrusion Analysis Engine uses several methods. As in SG, AMI relies on various factors such as detection technique, placement, network architecture, deployment, technology and data. The current power system frequently uses three types of IDSs for AMI based on their detection mechanisms: anomaly-based, specification-based, and signature-based.

According to the original data source, intrusion detection systems for the smart grid have two major categories: host-based and network-based intrusion detection [53]. The former scrutinizes and evaluates application logs, file integrity, system calls, and other relevant data. The other component observes and evaluates the communication network's data packet and flow attributes.

3.1. Categorization of IDS Based on Detection Technique:

Based on the target systems, IDS falls into different categories and can be tailored to each environment's specific constraints, requirements, and vulnerabilities as a robust security solution. IDSs can be categorized based on their detection techniques to identify potential threats. Each method employs different strategies to detect malicious activity and can be tailored to specific applications or environments. Below are the main types of IDSs based on detection techniques:

(1) Signature-Based IDS:

A Signature-based Intrusion Detection System (IDS) is a security mechanism that employs a security tool known as an Analysis Engine to check the current activity against a list or database of known attack patterns called "signatures" to spot or detect potential threats and intrusions. An alert is generated when an observed activity is matched by comparing it with each signature. However, this method offers excellent reliability and a low false-positive rate, it cannot identify unknown intrusions or attacks that do not match any signature. Essentially, this mechanism requires a thorough understanding of the tested system's weaknesses or vulnerabilities to detect emerging threats effectively. Also, this type of IDS must periodically update its signature sets to include new attack types. Using MATLAB, the authors of [54] developed an AMI IDS that incorporates temporal and geographic detection approaches. The suggested system primarily focuses on black hole and time-delay attacks. However, time-delay attacks aim to make packet transmission sluggish.

(2) Anomaly-Based IDS:

Conversely, the effectiveness of the other technique (anomaly-based) relies on identifying abnormal or unusual actions that cause anomalous behaviour of the system as potential intrusions. Compared with the prior method, this approach could be more precise. Intrusion detection methods that identify anomalies in runtime behaviour are called "anomaly-based." The commonplace can be defined in two ways: regarding a set of training data (semi-supervised) or the past of the test signal (unsupervised). Unsupervised machine learning is illustrated through clustering. However, the second method's usefulness is predicated on labelling anomalous actions as malicious intrusions. Bayesian networks, neural networks, and Markov models are examples of machine learning techniques typically used in this approach to detect hostile or malevolent actions. This method's application is less precise than its predecessor. One benefit is that it can identify previously unseen forms of cyber-attack. Typically, this strategy uses statistical analytic procedures or machine learning techniques

 doi:10.20944/preprints202604.1188.v1

to identify malicious behaviour, including Bayesian networks, neural networks [55], and Markov models. However, it offers the benefit of identifying previously undetected cyberattacks.

Any unusual or suspicious activity that deviates from the allowed range or the system's whitelist of actions can be detected by the anomaly-based IDS as intrusive behaviour.

As an intrusion detection technique, the model is trained using a normalized baseline against which all activities are analyzed [56] IN an anomaly-based IDS. Besides the common ways, attackers are more likely to adopt novel approaches to undermine the intelligent grid system, and such attacks are more likely to be detected by anomaly-based intrusion detection systems.

Denning [57] established the first anomaly detection model as an adjunct to misuse-based detection techniques. The purpose of statistical models that describe typical behaviours is to detect outliers. An anomaly-based IDS operates under the assumption that routine activities can be statistically predicted and that outliers indicate malicious intent. Point, contextual, and collective anomalies are the three types of anomalies identified by [58]. Anomaly detection studies typically center on point anomalies and single data instances. Each data object carries contextual attributes and behaviour characteristics, making contextual anomalies conditional anomalies. Sequence, graph, or spatial data collectively exhibit an abnormality.

Yen et al. examine in [59] how smart meter data collection frequency affects short-duration attacks detection. An algorithm was developed to analyze smart meter voltage data at residential loads for anomalies. Multiple data-collection intervals were tested in MATLAB/Simulink on a smart-grid model under three operating conditions. More frequent data collection improves short-duration anomaly detection, showing smart meters' potential to improve grid reliability. This study [60] has suggested anomaly-based IDS as a state-of-the-art machine learning approach that can identify small but significant changes in the system through the analytical investigation of the set of parameters of the system. It focuses on one of the crucial components of AMI, which generates large volumes of consumption data daily. Here, the intrusion detection technique would detect any attack or adversary on AMI by incorporating the anomaly detection technique. Despite the sheer number of researchers investigating this area of SG, only a few detection methodologies have attempted to blend network and smart meter data to reveal the anomalous pattern for effective detection.

(3) Specification-Based IDS:

Finally, the third method (Specification-based) relies on predefined rules that characterize the typical operation of the system under test. Specifications refer to these guidelines or predefined rules. This approach can reveal previously unknown attacks by identifying potential irregularities. An alert is sent when an action's properties deviate from a requirement. It differs from the signature-based approach by assuming that the system's security policy cannot be breached if all specifications are met.

A specification-based intrusion detection framework for the grid paradigm has been built to categorize substation scenarios and detect cyber-attacks targeting various grid components. For instance, to maintain the reliability and stability of the grid's distribution infrastructure, a specification-based intrusion-detection-enabled sensor has been introduced to monitor Advanced Metering Infrastructure (AMI) [61]. In another study [62], the authors developed specification-based IDSs for Home Area Networks (HANs), which observe and detect intrusion based on scenarios or rules observing the data transfer among smart meters and household devices. Its design targets medium access control layers and ZigBee's physical components, defining its normal behaviour based on extracted specifications. Any change from usual behaviour may signal an attack. Figure 5. illustrates the frequently used IDS technique in the AMI system.

 doi:10.20944/preprints202604.1188.v1

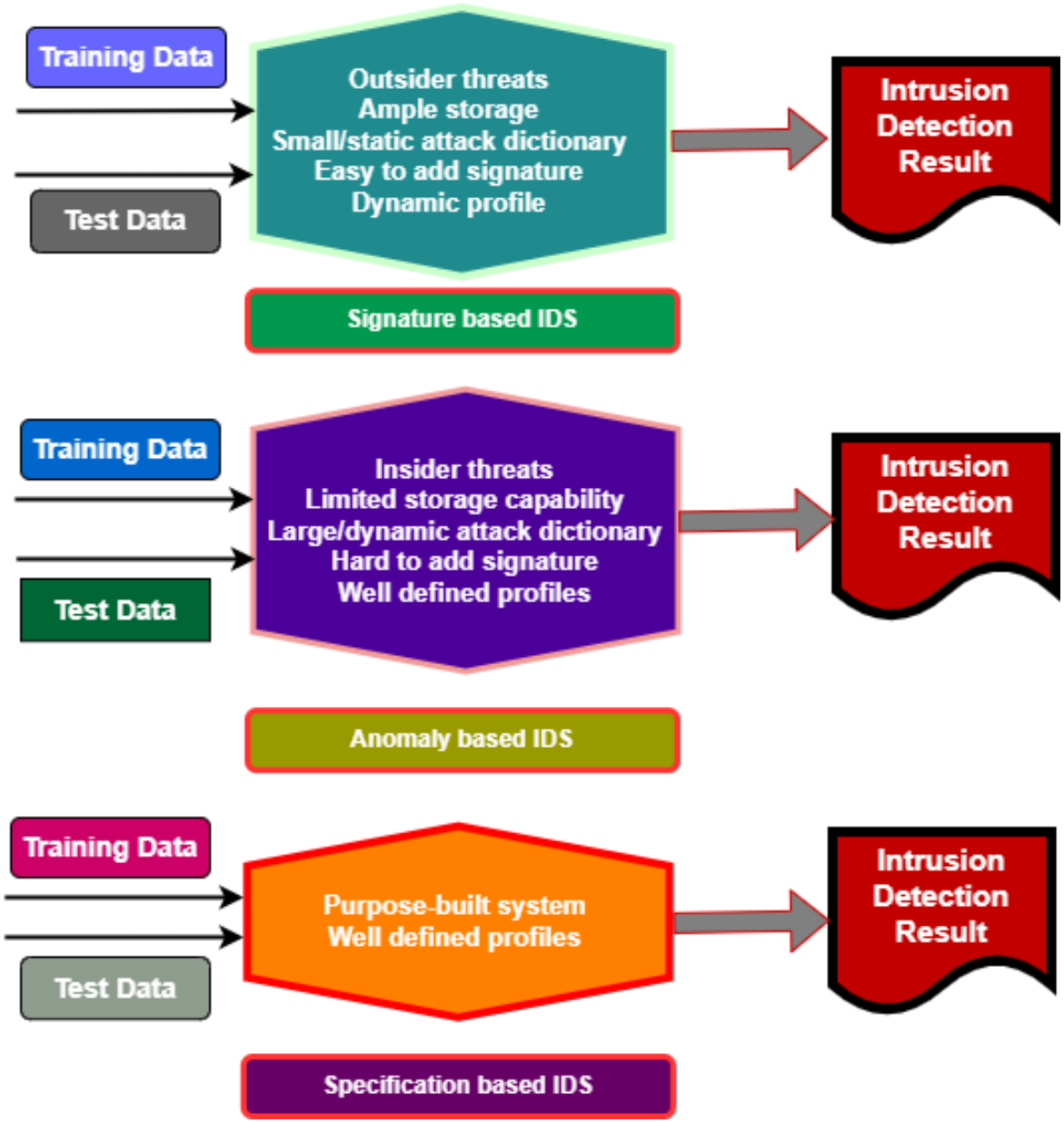

Figure 5. Frequently used Intrusion detection technique in AMI system.

(4) Hybrid Detection IDS:

Hybrid IDSs in the SG domain are one robust approach with specific applications, particularly for enhancing efficiency, security, and scalability in smart grIDSs to detect known and unknown cyber intrusions targeting AMI. Furthermore, IDSs must consider the hybrid nature of AMI, which integrates industrial and ICT components. In particular, the hybrid IDS must adopt some functionality to cope with the restricted processing capabilities of legacy industrial and IoT devices, such as RTUs and smart meters [8]. Moreover, the heterogeneous nature of SG components necessitates prompt responses upon detecting various cyberattacks and anomalies. Ruanand et al. [63] proposed the hybrid IDS framework, integrating both signature-based and specification-based approaches to address known and unknown attacks. In the AMI, the framework can also be deployed on devices with restricted resources. Khan et al. [64] developed a hybrid IDS integrating both specification-based and signature-based approaches for synchrophasor systems that employs the IEEE C37.118 protocol. The proposed system architecture, in particular, comprises distinct HIDS and NIDS agents and sensors. Sensors manage network traffic, while agents monitor PMUs or PDCs. The management server collects and merges information from individual agents or sensors. Furthermore, the database server monitors and archives any alerts or notifications. Six components comprise the agent and sensor system: a state manager, an events

 doi:10.20944/preprints202604.1188.v1

manager, an analyzer/detector, PCAP filters, and an IEEE C37.118 decoder. IEEE C37.118 packets are captured by PCAP filters developed in C/CCC. The IEEE C37.118 decoder extracts reinformation by examining previous sensor packets. The analyser/detector diagnoses anomalous behaviours using criteria. This collection includes four rule categories: signature-based, range-based, threshold-based, and stateful behaviour-based. The authors assert that their algorithms can detect various cyberattacks, including ARP poisoning, DoS attacks, replay attacks, port scanning, GPS spoofing, command injection, and physical attacks.

3.1.1. Categorization Based on Target System:

Based on the target system, the IDSs can be classified with their distinct design to monitor and protect the system. This classification focuses on the specific layer, system, or environment being safeguarded, such as networks, hosts, applications, or specialized environments. Below is an overview of the primary categories:

(1) Network-Based IDS (NIDS): The role of this type of IDS is to monitor network traffic across the smart grid infrastructure to detect threats affecting multiple devices or communications. NIDSs analyze the features and patterns of communication protocols to focus on the aggregate network traffic exchanged among network entities [8]. This is scalable for large networks. However, it has limitations in handling encrypted traffic. Detecting Distributed Denial of Service (DDoS) attacks targeting control centres or substations. IDSs can be installed at the network edge router, on a subset of hosts, or on each connected device to provide adequate intrusion detection. At the same time, the capacity of IDSs to query the network state can often increase communication overhead between LLN (Low-power Lossy Networks) nodes and the border router. In reality, Zarpelo et al. [65] outlined three primary methods for IDS implantation.

(2) Host-Based IDS (HIDS): A host-based IDS works as a software application installed on specific devices. It examines device activity and aims to identify intrusions, often by verifying audit trails or system logs generated by the host operating system. Host-based IDS is considered more effective for identifying attacks on a specific device [66].

(3) Hybrid IDS Combining HIDS and NIDS: It typically combines multiple HIDSs and NIDSs across a network. This type of hybrid IDS deals with numerous integrated, autonomous components across all subsystems of the SG system and facilitates interactions among them by monitoring and regulating both network traffic connections and system logs. Thus, as a safeguard, the hybrid IDS systems secure the SG and its components significantly from emerging threats and attacks.

3.1.2. Categorization Based on Architecture:

On the basis of architecture, IDS can also be categorized, which defines how the system is deployed and operates in a network or system. The primary architectural categories include Centralized IDS, Distributed IDS, and Hybrid IDS. Here's an overview of these architectures:

(1) Centralized IDS: SG is a complex heterogeneous system, so a wide range of data is crucial in IDSs. Data is collected and analyzed in centralized IDSs from all substations at a single central point or control centre. Centralized IDSs (C-IDSs) are typically used in a centralized infrastructure that is simple to manage and suitable for small to medium AMI networks. However, it has a slower response time due to its central processing and lower fault-tolerance capacity. As a result, the LLN can collect and transmit data across international borders. As a result, centralized IDSs may examine all data travelling between the LLN and the Internet. Since it is challenging to monitor each node during an ongoing attack [67], it is not sufficient to identify attacks affecting nodes within the LLN. The primary objective is to determine how to defend against a botnet attack. Kasinathan et al. developed a centralized placement that enables the mitigation of DDoS attacks, ensuring the uninterrupted transmission of IDS data even in the event of an attack. Kasinathan et al. developed a centralized placement that enables the mitigation of DDoS attacks, ensuring the uninterrupted transmission of IDS data even in the event of an attack [68]. Wallgren et al. [69] implemented a centralized method for detecting attacks on the

 doi:10.20944/preprints202604.1188.v1

physical domain in the border router. As per our findings, a centralized IDS implemented in the power utility network is essential yet inadequate within the framework of AMI [47,52].

(2) Distributed IDS: On the other hand, a highly recommended distributed IDS encompasses all field devices and the network edge. Both network and host IDSs are essential due to their complementary feand weaknesses. As an optimal solution for contemporary smart grids, a distributed IDS for AMI guarantees scalability and addresses the resource constraints by maintaining high detection accuracy. It has improved detection for real-time anomalies through processing data locally on smart meters, eliminating the need for centralized data sharing and enhancing user privacy. On the other hand, in the decentralized IDSs, each substation or region monitors threats or intrusion independently, and the detection occurs locally at multiple nodes or devices. However, conventional machine learning (ML) methodologies dealing with smart meters employ the exchange of local meter data with a central server, which increases concerns regarding breaching data security, user privacy, and issues such as high latency, bandwidth requirements, and centralized computing dependence. To resolve these concerns, a Federated Learning (FL)-based anomaly detection scheme is suggested in [70,71].

Faisal et al. [72] proposed a distributed IDS for AMI comprising three local IDSs in smart meters, data concentrators, and the headend. The IDSs utilize stream data mining to detect network attacks. This paper introduces IDSs for the neighbourhood area network (NAN), an AMI subsystem connecting smart meters to data concentrators. The IDSs utilize data mining to detect malicious activities resulting from black hole attacks in this area.

In [73], Zhang and colleagues introduced distributed IDSs for AMI and SCADA systems. The system utilizes anomaly-based HAN, NAN, WAN, and SCADA network sensors. IDS sensors come from communication streams. Two machine learning techniques (SVM and CLONALG/Airs2Parallel) are used to identify harmful behaviour in security-related data. Effective training is crucial for these algorithms to function optimally, but attack samples in AMI are scarce.

For instance, most AMI components are deployed in the public domain; therefore, deploying centralized IDS in a utility network will not provide the requisite coverage for AMI [47]. In the interim, AMI faces numerous constraints in deploying a sophisticated IDS solution. These constraints include the high cost of deploying complex IDS, the limited computing and processing resources in field devices, and the heterogeneity of communication networks and protocols. Consequently, many factors must be considered when developing and implementing IDS for AMI. Researchers have recently contributed to this field by proposing a range of solutions and methodologies.

(3) Hybrid IDS Combining Centralized and Distributed IDS: The word "hybrid" is now used to describe an IDS that combines two or more of the approaches mentioned above. H-IDSs utilize the advantages of both centralized and distributed deployments, thereby eliminating their respective limitations. The first method divides the network into clusters, with the cluster's primary node hosting an IDS instance and then being responsible for monitoring its neighbours. This means a hybrid IDS deployment can use more resources than a standard IDS deployment [74].

Le et al. [75] also successfully organized the network into smaller clusters, each with its cluster head, from the same number of initial nodes. Each cluster head might host an IDS instance, with nodes relaying information about themselves and their neighbours to the central node. The second method involves inserting IDS modules into the border router, various network nodes, and a centralized hub. Using data from the Routing Protocol for Low-power and Lossy Networks (RPL) network, Raza et al. [76] developed the IDSs they called SVELTE, in which the hosts of border routers are tasked with running processing-intensive IDS modules that detect intrusion attempts. According to Pongle et al., [77], network nodes are to blame for any observable shifts in their immediate vicinity. Additionally, network nodes communicated neighbourhood details to a centrally located module hosted by a border router, which is tasked with data storage and analysis. This facilitates the detection of intrusions and the early detection of attacks. Thanigaivelan et al. presented an IDS in [78] that divides tasks between individual nodes and the router's perimeter. The IDSs module can monitor its neighbouring nodes, looking for signs of intrusion, and alert its fellow IDS modules if it finds any. Chun et al. in [79]

 doi:10.20944/preprints202604.1188.v1

formulated an attack model (CONSUMER) that demonstrates how a compromised smart meter can enable an unauthorized customer to steal electricity by reducing their own energy use and increasing that of others in a neighbourhood distribution network. Unlike typical poor measurement detectors, the hybrid intrusion detection system mechanism depends on power information and sensor location to identify hostile actions such as consumer attacks. The study indicates that grid sensor placement can enhance detection rates, but their absence can also lower them.

3.1.3. Categorization Based on Specific Technologies:

IDS can be categorized based on the specific technologies they use, such as machine learning (ML) and other advanced techniques. A detailed categorization of IDSs is presented below on the basis of various technologies, their applications, advantages, and challenges.

(1) Machine Learning-Based IDS: A Machine Learning–based Intrusion Detection System (ML-IDS) is one of the robust security systems that differs from the conventional IDS by learning both normal and malicious behaviour or patterns from data rather than relying only on predefined attack signatures or static rules. For example, anomaly detection system, as a ML-IDS, is able to detects anomalies, subtle manipulations, and unseen attacks by dynamically acquiring patterns and behavior from significant amounts of data over time, learning various statistical and behavioral patterns from those data and then analyzing the anomaly score by the model computation based on the threshold or baseline values to and detect known and unknown threats. As a state-of-the-art, modern ML-IDSs are now capable of operating in noisy, evolving, high-stakes environments such as smart grids and cyber-physical systems. Instead of depending on simple anomaly scorers, recent ML-IDSs evolve with system behaviour and adopt the adaptive thresholding technique to enhance their efficacy in response to evolving network conditions or novel attack methods. Hence, the emerging ML-IDSs are far more proficient in detecting deviations from the typical behaviour of the system by enabling the model to identify potential hazards that do not conform to predetermined signatures [80]. Recent ML-IDSs are featured with real-time detection, which are designed for rapidly detecting and responding to threats. Which basically depends on high-dimensional data from complex components of real-time dynamic environments, such as network traffic records or smart meter data, smart utilities, or IoT networks, and making them well-suited for distributed structures such as the smart grid. Thus, modern ML-IDSs play a pivotal role as an adequate safeguard because of the scalability, automation, and reduced reliance on human intervention; ML-IDSs are against increasingly sophisticated cyber threats.

Tong et al. [47] exhaustively examined IDS techniques for Advanced Metering Infrastructure (AMI) threat analysis based on attack surfaces, methodologies, and effects. The latest ML-based IDS solutions, classifications, and critical principles for developing and deploying IDSs for AMI, as well as research problems, were reviewed. They survey metrics, attacks, and evaluation methodology sparingly. The smart meter communication network transmits real-time power usage data via bidirectional communication; however, direct customer-device interactions increase the risk of attacks. Atef et al. evaluate the effectiveness of federated learning (FL) combined with adversarial training (AT) in securing electricity theft detectors for smart grid advanced metering infrastructure (AMI) while preserving consumer privacy[81]. This paper addresses the challenges of detecting evasion attacks (EAs).

In another study, Sun et al. introduced a transformer-based intrusion detection model (Transformer-IDM) to enhance intrusion detection performance in advanced metering infrastructure (AMI), address privacy concerns, and reduce detection delays. By integrating 5G technology and a hierarchical federated learning intrusion detection system (HFed-IDS), the approach enables collaborative training of Transformer-IDM to protect and preserve consumer privacy in AMI networks [82].

Khraisat et al. presented the role of Federated Learning (FL), which enhances IDS by enabling collaborative model training on decentralized data sources while preserving data privacy[83]. Unlike traditional IDS, which faces scalability and privacy challenges, participants of FL can be trained on their individual machine learning models locally without sharing sensitive data. Moreover, this approach addresses computational constraints by ensuring data sovereignty. Thus, FL-based IDSs

 doi:10.20944/preprints202604.1188.v1

are considered the best fit for the industrial cyber-physical systems (CPSs) due to their aggregation strategies, privacy-preserving techniques, and effectiveness of collaborative threat detection. aLi et al. proposed the DeepFed: Federated Deep Learning (DeepFed)-based IDS for industrial CPS, using deep learning models, including convolutional neural networks and gated recurrent units, to improve the efficacy of IDS [84]. The experimental results demonstrate the effectiveness of DeepFed in detecting cyber threats, outperforming existing IDS approaches in industrial CPS environments.

Transformer-IDM enhances advanced metering infrastructure (AMI) intrusion detection, resolving privacy concerns and reducing detection times. AMI network user privacy is protected through collaborative Transformer-IDM training, leveraging 5G technology and a hierarchical system with feature selection and user detection. Testing shows that the recommended strategy outperforms existing methods in both detection and communication. Vijayanand et al. came up with a hierarchical, deep learning-based multi-layered attack detection system that analyzes smart meter traffic to improve accuracy [85]. The system is compared to simpler multi-layer deep learning algorithms and hierarchical SVM techniques, both with feature selection, using the CICIDS 2017 dataset [85].

Song et al. introduced IDSs, which are referred to as an Artificial Immune System (AIS), an AI-driven system for AMI's WAN, leveraging the Negative Selection Algorithm to detect anomalies and prevent cyber-attacks [86]. It employs a proof-of-concept design using synthetic data, aiming for scalability in real-time smart grid networks while enhancing resilience and proactive defence. Another well-suited distributed IDS architecture for AMI is an Extreme Learning Machine (ELM). ELM's quick training speed and robust model generalization ability are ideally suited for intrusion detection in the smart meter of the SG system. A genetic algorithm (GA)-based ELM intrusion detection model is proposed to address the limitations of ELM's random input weights and hidden-layer bias, which hinder optimal performance [53].

(2) Protocol-Based IDS (PIDS) A Protocol-based Intrusion Detection System (PIDS) is a type of IDS that deals with a specific protocol and monitors whether it behaves as it is supposed to behave, and raises a flag if any traffic violates that protocol's specification or expected state machine. Moreover, the PIDS leverages protocol analysis and employs validation tools to monitor and detect intrusions specifically within communication protocols used in AMI, such as Zigbee, LoRa, and DNP3. To ensure secure protocol implementation, these systems identify malformed packets, unauthorized access attempts, or protocol misuse that could compromise the smart grid's integrity.

For example, Zografopoulos et al. (2021) [39] demonstrated a novel intrusion detection and prevention system (PIDS) designed for ZigBee-based home area networks (HANs) applicable for SG. One of the popular PIDS is Host and Network-based Intrusion Detection and Prevention System (HANIDPS), not only to detect but also to defend against various attacks, which is a model-based intrusion detection mechanism with a machine learning-based intrusion prevention system. The HANIDPS analyzes network features to assess normal behaviour based on SEP 2.0 and IEEE 802.15.4 standards through its detection module. Whereas the prevention system adopts Q-learning to dynamically learn effective defence strategies against attacks. Without prior knowledge of attacks, a model-based approach for detection and dynamic learning for prevention ensures high performance. Through extensive analysis and experiments, the effectiveness of HANIDPS is validated.

A novel anomaly-based intrusion detection system (IDS), ARIES, reliably safeguards SG communications against intrusions [87]. ARIES comprises detection layers—(a) network flows, (b) Modbus/Transmission Control Protocol (TCP) packets, and © operational data—to identify potential cyberattacks and anomalies. The ARIES Generative Adversarial Network (ARIES GAN) was built utilizing cutting-edge error reduction techniques with a focus on the third layer (operational data-based detection) to detect anomalies in operational data (i.e., time series electricity measurements).

3.1.4. Categorization Based on Specific Data:

An IDS for AMI in a smart grid can provide comprehensive protection against a wide range of intrusions by incorporating diverse data types, ensuring the security and reliability of the infrastructure as follows:

 doi:10.20944/preprints202604.1188.v1

(1) Audit Log-Based IDS: Audit logs based on IDS work on historical records of system behaviour that provide critical insights into current and past system conditions. The majority of existing software likely has logging systems where the trails or logs from the record can be examined to identify events to reveal intrusions. Moreover, for tracking the origins of assaults, audit logs serve as notifications for the IDS. It can also serve as a data source for both host-based IDSs, which typically analyze system calls, and network-based IDSs. For instance,to identify assaults on network hosts, Pan et al. in [88] utilized event logs generated from network communication.

(2) Network Flow Based IDS: Network flow-based Intrusion Detection Systems (NIDS), referred to as connection-oriented IDSs, utilize data from the network and transport levels of the OSI model. This type of IDS is primarily suited for detecting network-level threats, including denial-of-service attacks and port scanning [87]. Packet data is applicable in both network-based and host-based intrusion detection systems. An example is a stack-based Intrusion Detection System (IDS), which operates directly on the TCP/IP stack and extracts packets from it before the host operating system processes them [66].

(3) Packet Payload Based IDS: Since packet payload typically refers to data at the application layer, instead of headers or traffic patterns, Packet Payload Based IDS inspects the actual content inside network packets (the payload) to detect malicious activity. The studies demonstrated how the application layer of heterogeneous system vulnerabilities is the primary target for attackers in the contemporary threat landscape[89,90], where many of these attacks occur typically when examining packet header attributes alone. However, they may markedly vary from valid traffic upon inspection of packet contents. Thus, packet payload-based intrusion detection systems are crucial for identifying attacks, while depending on exclusively network flow statistics may no longer be feasible.

(4) Sensor Data-Based IDS: In recent years, Wireless Sensor Networks (WSNs) have become prevalent in the grid paradigm, particularly by significantly impacting the functionality of the AMI system in SG. Since throughout the AMI network, smart meters and utility providers, including electricity consumption components largely designed with a wide range of sensors to gather and process various real-time data such as current, voltage, power, and numerous sensor data, WSN has become crucial, especially for utilities. Using WSN, the utilities are able to wirelessly communicate among different components, can remotely monitor and manage power outages, faults, and load conditions, and thus eliminate the need for physical inspections and reduce infrastructure and maintenance costs [91]. With the expansion of the grid, its scalability demands seamless device integration. Bidirectional connectivity is supposed for remote meter reading, which largely depends on the sensor network, WSN, not only enabling real-time consumption data, but also for more efficient operations such as predictive maintenance, firmware updates, and so on. Thus, to enhance sustainability, WSNs play a pivotal role by optimizing energy distribution and integrating renewable energy sources in energy management. However, as the sensors are interconnected through the internet, WSNs in the AMI system are also highly susceptible to a wide range of intrusions or cyberattacks, which need robust encryption and authentication to mitigate them [92].

As WSN provides a vital layer for the SG by leveraging the operational and environmental data collected from AMI components, the sensor data-based IDS systems for AMI are a promising security area for both research and practical applications. The sensor-based IDS operates on sensor-based data in designing an intelligent security system for AMI, which typically begins by collecting operational, device, environmental, voltage levels, current flow, and energy consumption data [93]. In particular, to optimize their potential use of sensors across the WSN inside the AMI in the smart grid, signal interference and energy efficiency of sensor nodes must be addressed. Further technical analysis of sensor-based IDSs encompasses the sensors' operations, their baseline profiling, real-time data analysis, anomaly detection, and, ultimately, a response mechanism.

Table 2 provides the comprehensive comparison of various Intrusion Detection Systems (IDSs) examined in contemporary scholarly studies.

 doi:10.20944/preprints202604.1188.v1

Table 2. Comparison of various IDSs for AMI.

Type of IDSs	Detection Accuracy	Scalability	Complexity	New Threat Detection
Signature-Based IDSs [94,95]	High for known threats	High	Low	No
Anomaly-Based IDSs [87,96,97]	Moderate	Moderate	Moderate	Yes
Hybrid IDSs [98–101]	High	Moderate	High	Yes
Network-Based IDSs (NIDSs) [73,102,103]	High	High	Moderate	Yes
Host-Based IDSs (HIDSs) [104–106]	High	Low	High	Yes
Distributed IDSs (DIDSs) [107–109]	High	High	High	Yes
ML-Based IDSs [80,110–112]	High	High	Very High	Yes

3.2. Performance Metrics of IDS:

As the operation of AMI in SG is multi-layered as well as multifunctional, the performance of IDSs designed for the AMI and smart grid environments should be assessed beyond the traditional machine learning (ML) measures but using a comprehensive, multi-layered metric framework. In IDS, researchers frequently use various metrics such as True Positive Rate (TPR), the inverse of the False Positive Rate (FPR), and the False Negative Rate (FNR) to assess performance [80]. An IDS produces a false negative when it erroneously identifies a malicious node as benign. Given that false positives (FPs) and false negatives (FNs) are paramount indicators of intrusion detection system (IDSs) efficacy, the authors in [113] investigated the reduction of FNs through a dual-tier intrusion detection approach that concurrently tackles anomaly and signature detection for wireless sensor networks (WSN) inside the smart grid (SG) framework. Therefore, relying only on ML-based metrics can not sufficiently measure the performance of modern IDS; the evaluation frameworks should also incorporate system-level performance metrics, including response time, detection latency, and the ability to detect diverse and zero-day intrusions. Collectively, to ensure reliable and timely protection of AMI-based smart grid infrastructures, a comprehensive set of performance metrics should be incorporated for the IDS assessment that integrates model-level statistical accuracy, temporal responsiveness, operational efficiency, and detection coverage.

(a) ML-Based Performance Metrics: For any ML-based IDS model, performance metrics measure the performance as follows:

(1) Accuracy: A model's accuracy is a performance metric that shows what percentage of its predictions were accurate. It is frequently used to gauge how often the model correctly recognizes each class in classification tasks.

In a binary classification setting, predictions are usually divided into four types:

- **True Positives (TP):** Correctly predicted positive cases.
- **True Negatives (TN):** Correctly predicted negative cases.
- **False Positives (FP):** Incorrectly predicted positive cases (actual negative).
- **False Negatives (FN):** Incorrectly predicted negative cases (actual positive).

Besides the accuracy metrics there are other metric to measure the model performance such as the Receiver Operating Characteristic (ROC), AUC (Area Under the Curve), Detection Rate (DR), Precision, Recall (Sensitivity), F1 Score, Confusion Matrix, Running time (in seconds), Model size (KB) and so on [114,115].

(b) System Performance Metrics:

Along with the ML model's performance, the following metrics are considered to evaluate the entire system's performance in the IDS paradigm.

(1) Timely intrusion detection: The phrase "timely" does not inherently suggest real-time detection, as this state presents significant operational and reaction challenges. Conversely, it is essential to detect an infiltration on time [8].

Timely intrusion detection can be calculated by the following means:

 doi:10.20944/preprints202604.1188.v1

(2) Detection Time (Latency): The interval between the initiation of an attack and its identification by the IDSs. This measure can assess the detection delay throughout the development and testing phases of modern IDSs.

$$\text{Attack Detection Latency} = T_{\text{detection\_started}} - T_{\text{attack\_started}}$$

This is critical because shorter latency = faster mitigation (blocking, alerting, response). Example:

- Attack packet injected at 12:00:05
- IDS raised an alert at 12:00:07
- Detection Latency = (12:00:07 - 12:00:05) = 2 seconds [116].

(3) Time to Respond (Response Time): It indicates the time duration that the IDSs take to commence a response, such as issuing an alert, obstructing traffic, or implementing countermeasures, when an intrusion is identified. For an efficient IDS, a prompt response is essential to thwart the escalation of the attack.

Formula: Response Time = Time of Response Action - Time of Detection

(4) Detecting a wide range of intrusions: It depends on the ability to detect not only known intrusions but also any malicious activity from external unauthorized users or malevolent insiders. To address zero-day attacks, contemporary IDS must incorporate such robust measures.

4. IDS Applied to AMI

This study concentrates on Intrusion Detection Systems (IDSs) for Advanced Metering Infrastructure (AMI), emphasizing diverse methodologies and considerations for building IDSs to safeguard the AMI throughout the examination. After looking at the most relevant recent literature, we noticed a lot of study gaps. Most IDSs for AMI systems look at either network traffic or energy use statistics. Both of these are very important for finding and figuring out new or unknown sorts of attacks. Because of the gap, we need to look into a new way to design IDSs for AMI. Our experimental framework merits examination owing to its multiple enhancements. These include several data-driven modes, automatic attack detection, and the ability to find specific layers or parts of AMI infrastructure that are damaged. This solves security problems that come up because of the unique features of AMI components. However, most IDSs for AMI systems will likely deal with either network traffic or energy consumption data, whereas our focus is on highlighting the importance of considering multiple data modes collected from multiple nodes of AMI to develop an intelligent IDS. This approach ensures that the IDS can identify any attacks or threats across the broad cybersecurity spectrum, regardless of other attack components that may emerge within the AMI system. Some researchers have recently explored this topic, offering several methods and insights. However, there is still much to learn about this area of study. Multimodal deep learning differs from unimodal models, which can process only one data type. It is also different from the combined unimodal models trained independently. Multimodal deep learning approaches are being rigorously implemented as a cybersecurity framework for detecting facial video forgery in intelligent solutions for cloud and IoT applications [117–119]. Unlike the typical machine learning approach, Multimodal deep learning is becoming an innovative method for detecting anomalies or intrusions in grid environments. Although multimodal image data in smart grids has drawn the attention of recent security researchers, many other cyber-physical data sources are still unexplored. Zhou et al. in [120] present a comprehensive evaluation of the utilization of deep learning (DL) methodologies for identifying anomalies in smart grids through multimodal image data. The report emphasizes that incorporating multimodal data, including infrared, optical, and electromagnetic imagery, enhances the identification of faults and anomalies in intricate smart grid settings. In [121], Ullah, Farhan, et al. proposed a framework that integrates multimodal big data representation, transfer learning, and game theory to improve as an innovative methodology to enhance network intrusion detection systems (NIDSs) within Internet of Things (IoT) environments, focusing on the detection and prevention of cyber-intrusions on IoT devices. The authors emphasize the importance of mitigating

 doi:10.20944/preprints202604.1188.v1

vulnerabilities to ensure grid stability, privacy, and security by adopting multimodal approaches in contemporary energy systems. Beyond conventional machine learning techniques, multimodal deep learning-based IDS is an emerging novel approach for detecting abnormalities or intrusions in grid systems. Zhou et al. examined the utilization of deep learning methodologies for identifying anomalies in SG using multimodal imaging data [120].

An innovative approach for detecting false data injection (FDI) attacks in smart grid systems is proposed by Zhang et al. in [122], where a semi-supervised deep learning framework is employed as multimodal learning by combining diverse data types, including sensor measurements, anomaly signals, and historical data, for analysis and detection.

In another study, Kiflay et al. in [123] introduce an innovative method by integrating multimodal features for improving network intrusion detection systems (NIDSs), where the authors acknowledge that relying on unidimensional data such as network traffic records limits the precision and flexibility of intrusion detection with conventional NIDSs. To tackle this issue, they present a model that utilizes multimodal data, integrating elements such as network traffic, user behaviour, and system logs to offer a comprehensive perspective on potential risks.

Liu et al. thoroughly examined intrusion detection, emphasizing rule-learning-based IDSs in smart grids, as reported in another survey [66]. They effectively investigated the potential alternatives of several artificial neural networks for rule induction in intrusion detection systems. However, their future direction for developing IDSs in AMI needs more detailed specifications. Jacob et al. employed a graph-based learning model utilizing graph neural networks (GNNs) to design an IDS for power grids, where multimodal data fusion combined cyber and physical features for improved detection [124].

Another study [125] highlights that multimodal cyber-physical fusion significantly improves IDS effectiveness. However, reducing vulnerabilities in smart grid intrusions and addressing cyber-physical attacks on distributed grid-edge devices (e.g., PV panels, smart loads, EVs) remain significant challenges in energy system cybersecurity. A distributed, multimodal anomaly detection system is developed to address this, integrating multiple time-series data sources and leveraging unsupervised machine learning to detect deviations from normal behaviour.

On the other hand, along with a wide range of data-driven tools, the data interdependencies computed through Indicators of Compromise (IoC) in Industrial Control Systems (ICS), such as SCADA, SG, and AMI systems, are crucial in detecting attacks, identifying malicious activities early, and mitigating loss [126]. The incident responders can detect attack triggers and respond swiftly to prevent further intrusions by analyzing IoC [127]. However, the concept of IoC needs to be understood before implementing it based on the requirements and context of the critical infrastructure. Despite their significance in the detection mechanism, the research on IoC in ICS environments is limited. This study examines the potential IoCs for ICS cyber-attacks alongside their representation standards, associated challenges, and evaluates their effectiveness by mapping them to common ICS threats. The article also identifies research gaps and addresses future directions for improving IoC-based security in industrial sectors.

In addition, this article provides an overview of a range of contemporary and pertinent studies that can serve as a resource for further research for developing and implementing IDSs for AMI. An analysis is conducted on the attack surfaces, strategies, and implications in AMI. Next, an analysis is conducted of current scholarly methods for intrusion detection systems and AMI procedures. A thorough IDS architecture suitable for AMI, along with some principles for designing and implementing workable IDSs, is suggested. Table 3 presents the key differences among various IDS approaches for the AMI, based on several significant features and techniques of the IDSs.

doi:10.20944/preprints202604.1188.v1

Table 3. Comparison of major features of IDSs focusing on AMI among different papers

Ref #	Application domain	Type of IDSs	Type of Dataset	Type of Attack	Using Multi Modal Data	Using IoC Metric
Sun et al. [13] 2020	AMI	Hybrid IDS	Network Traffic Meter Data	✗	✗	✗
Radoglou et al. [87] 2020	SG	Anomaly Based IDS	Network Traffic Modbus Data Operational Data	DoS Brute Force Port Scanning	✓	✗
Zaboli et al. [128] 2025	Scada	✗	Energy Consumption Data	Energy Theft	✗	✗
Korba et al. [129] 2020	AMI	Anomaly Based IDS	Energy Consumption Data	Power overloading cyberattacks	✗	✗
Sun et al. [82] 2022	AMI	Hierarchical Federated Learning IDS (HFed-IDSs)	Network Traffic Data	DoS Probing scanning (Probe) Remote to local (R2L) User to root (U2R)	✗	✗
Atef et al. [81] 2023	AMI	Federated Learning Based (FL-IDS)	Energy Consumption Data	Evasion Attacks	✗	✗
Bhattacharjee et al. [32] 2021	AMI smart meters	Context-aware Anomaly Based IDS	Power consumption time-series Data	FDI Attack	✗	✗
Kiflay et al. [123] 2024	✗	Network Based IDS	Flow-based & Payload-based Data	Various Cyber Attack	✓	✗
Asiri et al. [126] 2023	SCADA	Network Based IDS	✗	Various Cyber Attacks	✗	✓
Jacob et al. [124] 2023	SG	Graph Neural Networks Based IDS	CPS Testbed	FDI, Backdoor Brute Force Reverse Shell Ransomware	✓	✗
Rajesh et al. [127] 2023	SCADA	Network Based IDS	Flow-based & Payload-based Data	Various Cyber Attacks	✗	✓
Li et al. [84] 2020	CPS	DeepFed Based IDS	Network Traffic Data	Response Injection Reconnaissance Attack Command Injection	✗	✗

doi:10.20944/preprints202604.1188.v1

Table 3. *Cont.*

Ref #	Application domain	Type of IDSs	Type of Dataset	Type of Attack	Using Multi Modal Data	Using IoC Metric
Dong et al. [130] 2025	Energy Management System	Deep Multimodal Anomaly Based IDS	Energy Consumption Data	✗	✓	✗
Xia et al. [131] 2025	AMI	Federated Semi-Supervised IDS	Network Traffic Data	Cyber Network-level Attacks	✗	✗
Kenneth et al. [132] 2024	AMI	ML Based IDS	Network Traffic Data	DoS DDoS	✗	✗
Dong et al. [130] 2025	Energy Management System	Deep Multimodal Anomaly Based IDS	Energy Consumption Data	✗	✓	✗
SMH et al. [133] 2024	AMI	Anomaly Based IDS	Meter Data	FDI Attack	✗	✗

Note: [✓: Examined or specified; ✗: Neither examined nor specified].

 doi:10.20944/preprints202604.1188.v1

5. Research Trends and Direction

AMI possesses numerous unique characteristics that differentiate it from a conventional IT environment. Implementing a robust IDS solution for the AMI presents numerous challenges, including diverse communication networks and protocols, limited computational and processing capabilities in field devices, and elevated implementation costs. In particular, after surveying the various security aspects of AMI and multiple categories of current IDS for AMI, the following research questions need further exploration to design future intelligent IDS:

1. Can the current IDS capture and integrate all the relevant data, that is, the multi-modality of data from the AMI system, in a scalable way?
2. Can the IDS identify an actual assault by analyzing the fused features collected among different layers of AMI data?
3. Do the chosen multimodal features enhance the ability of IDS to detect intrusion?
4. How can the scalability issues be addressed by the architectural design of the proposed MIDS?
5. If the system is under attack, can it determine the type of attack and the layer from which it originated?

Answering these research questions requires an experimental framework that supports experimentation of both the intrusion detection algorithms and their scalability. Therefore, in this paper, an experimental framework of a tailored MIDS for AMI is presented to address the above challenges.

5.1. An Experimental Framework for Developing Scalable IDS

Answering the aforementioned research questions requires experimental research, and hence, an experimental framework is necessary. Typically, such experimental frameworks for IDS enable the exploration of various machine learning algorithms and techniques for intrusion detection. However, no existing IDS framework targets the full scope of scalable AMI and therefore lacks support for experiments that leverage its seminal characteristics, such as its hierarchical architecture, diverse modalities, and distributed resources. For example, much work has been done on federated learning. However, federated learning focuses on privacy issues rather than performance in a distributed, hierarchical system. Consequently, existing work on federated multimodal learning does not consider scale in light of the heterogeneous, hierarchical system's computational and networking capabilities, such as those in AMI. Consequently, such frameworks are poorly suited as a basis for research and discovery of IDS for AMI. Based upon the gaps we have identified, there are two most impactful features of AMI: i) scalability for its hierarchical and distributed architecture, and ii) the capability to handle rich datasets in terms of quantity and types or modality generated from heterogeneous devices and protocols across AMI infrastructure.

Therefore, an experimental framework must support data-driven experiments of various IDS techniques that are scalable in such a distributed system, as shown in the Figure 6, The proposed framework supports a flexible approach to developing and testing IDSs for AMI, thereby filling this gap. This framework supports the hierarchical architecture of AMI and focuses on a data-driven, yet architecture-aware, approach to experimentation. The framework's architecture consists of multiple layers. The lower layers typically consist of simple IDSs that are connected to low-power devices. At the lowest layers, an IDS is typically signature-based. These IDSs require minimal computational power and primarily send alarms to other IDSs, indicating that an intrusion event may have occurred. Upper-layer IDSs are more sophisticated and utilize machine learning methods to determine if a potential intrusion alarm is a true positive. The architecture can support multiple upper layers. At each layer, the IDSs have a more inclusive view of the distributed system than those at the layer below. They may be able to determine more accurately whether intrusion alarms are true positives. The algorithms shown in the Figure 6 are generalized to utilize functions provided by pluggable modules, thereby providing flexibility. The framework's salient features are as follows.

Hierarchical and distributed: AMI is hierarchical, comprising protocols and devices that operate at various levels. These range from simple, low-powered devices with few task-oriented features, such

 doi:10.20944/preprints202604.1188.v1

as smart meters, which use simple protocols like point-to-point RF, to centralized systems that run complex software over sophisticated long-haul networks. The hierarchical and distributed nature of AMI presents both opportunities and challenges when designing effective intrusion detection systems. Developing IDS technology that is effective in such an environment requires testing and evaluation in this environment, or at least using a testbed that simulates it.

Flexible support for heterogeneous devices and protocols: In addition, AMI's hierarchical architecture of heterogeneous devices, sensors, and communications networks provides a rich set of data having various modalities, such as smart meter data, communication network data, and sensor data. There should be flexible APIs to support heterogeneous devices and protocols across the AMI network; i.e., the experimental framework should supply such APIs to simplify the integration of different devices and protocols.

Flexible support for Distributed Intrusion Detection: Our proposed framework is a multi-layered structure, as shown in the Figure 6. It consists of lower-layer UMIDS and upper-layer IDS, which can be **Central IDS (C-IDS)** or **Multimodal IDS (MIDS)**. IDSs in the lower layers will be responsible for detecting *possible* intrusions and notifying upper-layer IDS. The IDS at lower layers of the AMI may have only local data and leverage only one modality, such as the values in the meters' holding registers, to detect a possible intrusion. Therefore, intrusion detection at lower layers may yield a higher degree of false positives than IDS at upper layers and may miss intrusions occurring there. However, when notified of a possible intrusion by a lower-layer IDS, an IDS in an upper layer may leverage multiple modalities, resulting in fewer false positives. Unfortunately, upper-layer MIDS cannot continuously fetch the various data modes from lower layers without overloading the communication network and burdening simple, low-power devices. Therefore, the framework architecture must incorporate the following modules that enable control over data transfer, including the timing of transmission, the format and encoding of the exchanged data, and the volume of data transferred across layers.

Research has shown that using diverse modalities can enhance machine learning techniques [134], thereby improving the effectiveness of IDS. The goal of multimodal IDS (MIDS) is to integrate data modalities to become intelligent enough to more precisely identify anomalies, discern patterns of compromise, and differentiate between normal behaviour and prospective attacks.

Developing intelligent MIDS is highly complex for a critically distributed CPS such as AMI, given its numerous cyber-physical features. To address the challenges of detecting intrusions and determining their types, our proposed framework is hierarchical and distributed, supporting various network architectures via simulation or hardware-in-the-loop. This enables the efficient transfer of data in a distributed environment of diverse devices.

To support the large distributed AMI system, the experimental framework of MIDS should include the following features:

Alert Generation and Aggregation: In AMI, as a multi-layered complex system, security threats can originate from different sources, including cyberattacks on smart meters, communication channels, and data processing units. For instance, when anomalies are detected at lower levels of the distributed system, an alert can be generated by the Distributed Intrusion Detection Systems (HD-IDSs), which are deployed across the system; however, for a large system, relying solely on isolated alerts can lead to false positives and an incomplete threat assessment. This is why alert generation and alert aggregation generated from HD-IDSs are considered to be one of the building components of our suggested MIDS, which plays a crucial role in determining the true source and type of attack targeting AMI. Thus, alert generation and aggregation from Distributed IDSs is critical because it allows the C-IDS to:

- Validate if an attack is real by correlating multimodal data.
- Detect large-scale, coordinated cyber attacks that individual HD-IDSs might miss.
- Reduce false positives & improve accuracy using historical attack patterns[135,136].
- Classify the attack type and trigger an appropriate response to protect the AMI network.
- Continuously improve its detection model through learning from aggregated alerts.

 doi:10.20944/preprints202604.1188.v1

Without alert aggregation from distributed IDSs or HD-IDSs and correlation within the C-IDS, the MIDS cannot discern the true nature of false-positive and false-negative alarms, thereby compromising the security of the AMI system against multilayered cyber-physical vulnerabilities posed by cyber threats or intrusions.

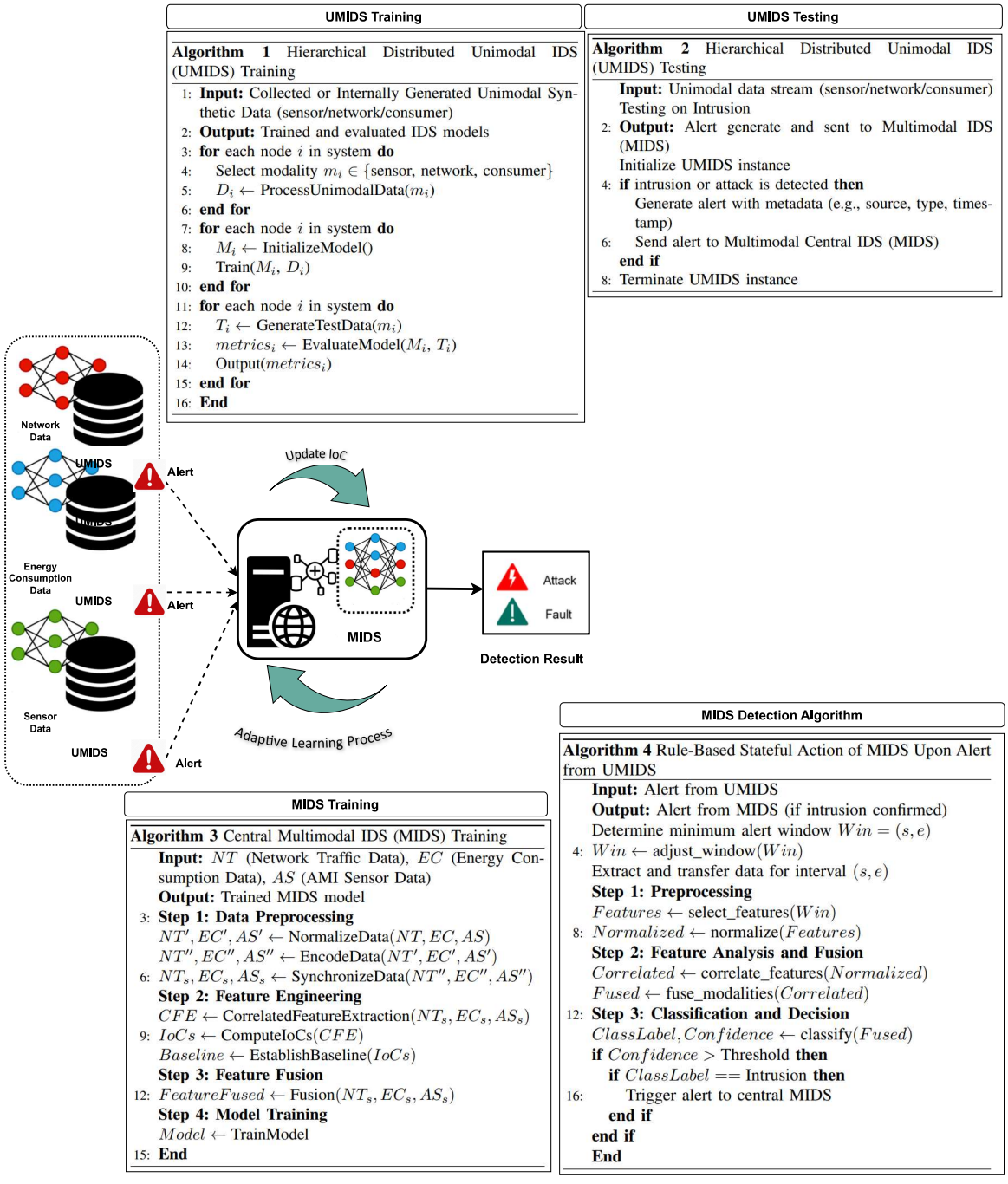

Figure 6. Schematic diagram of the experimental IDSs framework.

Support Adaptive Machine Learning Techniques. Given the complexity of the data types and availability in an AMI, the framework should support modules and APIs for integrating advanced ML techniques. These techniques include the following, as well as others mentioned in our literature survey.

- *Multimodal IDS:* The framework should include tools for selecting and fusing multimodal features. A *modality* refers to a distinct type of data or signal, including network statistics, sensor data, log data, etc. Multimodal systems combine these modalities to increase the effectiveness of IDS [9].

 doi:10.20944/preprints202604.1188.v1

Kiflay et al. presented the potential of multimodal data in the Network Intrusion Detection System (NIDSs) by integrating flow-based and payload characteristics to address the shortcomings of conventional machine learning-based NIDSs by improving detection accuracy and reliability [123]. In another study, Farhan et al. employed a multimodal approach to develop effective IoT-based NIDSs by combining trained text and texture features to classify various attacks targeting SG [121]. Federated Learning (FL), an emerging ML technique, can also leverage multimodal data and maintain data privacy [137,138]. Unfortunately, federated multimodal IDS does not scale well, particularly in such a hierarchical system.

- *Correlation-Based Feature Extraction (CFE):* is a technique utilized in machine learning and data analysis to discern and extract the most relevant features for a model by analyzing the correlations among variables (features) inside the dataset. The objective is to identify features that exhibit strong correlations with the target variable (the output or label) while discarding redundant or less useful features. The proposed IDSs feature IoC that can prevent AMI from severe cyber threats and protect the system from further disruption. Li et al. employed correlation-based feature selection (CFS) for developing ML-based classifiers for IDSs targeting SG [139]. Correlation-based feature extraction is an effective technique for identifying the most pertinent features by examining their connections to the target variable and their interrelationships with other features. It streamlines models, enhances accuracy, and minimizes the likelihood of overfitting. The CFE works on with an evaluation function to choose a subset of features where the linear correlation coefficient for two continuous random variables, X and Y, is defined as:

$$r_{XY} = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2 \sum_i (y_i - \bar{y})^2}}$$

- *Feature Fusion:* Feature fusion implies the process of combining features of multiple types or modalities extracted from different data sources (modalities) with an aim to improve the accuracy and robustness of IDS in AMI. Feature fusion in an MIDS for AMI in SG involves integrating various data modalities—such as network traffic, energy consumption, and sensor data—into a cohesive representation to enhance the identification of cyber-physical attacks. This approach identifies communication anomalies by utilizing network data, reveals irregular usage patterns from abnormal energy consumption data, and detects physical invasions or environmental anomalies from the sensor data, thereby creating a comprehensive view of the system. To enhance detection accuracy and robustness of this type of IDS, fusing features can be a robust technique that detects potential attack routes and reduces false positives and negatives through cross-modal validation. Feature fusion allows MIDS to utilize temporal patterns, such as energy usage spikes caused by network abnormalities, and spatial correlations, like sensor readings from nearby meters. Using fused features, deep learning, attention processes, and graph-based models can reveal intricate interactions among modalities. This enables the identification of complex assaults, including DoS, MitM attacks (detected by network and energy data anomalies), electricity theft (via inconsistencies in energy, meter, and sensor data), and replay attacks. Feature fusion creates robust IDSs that protect AMI [140,141].
- An *Indicators of Compromise (IoC):* is a metric or forensic evidence indicating a system or network has been infiltrated by a cyberattack or security incident, and calculating IoCs from relevant features and including them in both the training set and the detection set. One such example of useful IoCs is correlation-based statistics, which have been shown, in some cases [127], to improve intrusion detection and classification.
- *Co-Learning:* Co-learning or training is the methodology for generating additional labelled training samples when labelled data are scarce in a multimodal context[142]. This implies a collaborative learning method in which multiple modalities (e.g., network traffic, system logs, sensor data, user behaviour) are concurrently or cooperatively analyzed. This approach enhances MIDSs with improved detection efficacy, robustness, and flexibility by intelligently integrating heterogeneous

 doi:10.20944/preprints202604.1188.v1

inputs. Particularly, it is a crucial technique for MIDSs which aim at real-time, high-stakes systems where dependence on a single data stream poses significant risks. The basic IDS algorithm constructs weak classifiers on the basis of each modality, mutually enhancing one another using labels for unlabeled inputs.

Rule-based Stateful IDS: A Rule-based Stateful Intrusion Detection System (Stateful IDS) for an AMI in SG is a security tool that employs state-based monitoring and analysis to detect potential cyber threats within the AMI network. Moreover, it provides improved insights into communication patterns and behaviours, enabling more accurate detection of anomalies or malicious activities. This is a type of sophisticated IDS that would utilize various use cases as criteria to detect aberrant behaviour and identify the underlying cause regardless of whether an intrusion occurs. This set of rules has four categories: a)threshold-based, b) range-based, c) anomaly-based, and d) stateful behaviour-based. Where the stateful analysis serves as an augmented plugin of this type of IDS, functioning as a formidable security measure to accomplish the following objectives: 1) Interoperability, 2) long-term stability, and 3) recognition of diverse cyberattacks, including DoS, ARP spoofing, GPS spoofing, FDIA, replay attacks, port scanning, and physical assaults. Subsequently, the state manager is involved to analyze and detect which records are probable alerts or warnings in the database server [8].

Thereafter, the event manager connects to the management server, whose functionality was previously discussed, where users are allowed to modify the functionality of designated components through the console functions, either through a command-line or a graphical user interface. The rule-based stateful plugin of the IDSs comprises three functional components, including detection rules: a) the decoder for application and communication layer protocols, b) the engine for rule matching and verification, and c) the state manager and administrator. On the other hand, the content inspection rules assess specific criteria for each data application layer. Based on correlation and IoC, the state inspection regulations identify the presence of specified flags to distinguish between normal and aberrant pattern variations. Consequently, the state manager plays the role of establishing resilient protection for AMI by revitalizing the statuses and modifying the IDS model by revising and refining regulations . A stateful analysis for Intrusion Detection Systems for SG is introduced by Kang et al. by observing and recording network and system behaviours over time to enhance detection accuracy. The proposed framework facilitates the definition and execution of stateful rules using open-source Suricata IDSs, improving the efficient detection of abnormalities by comparing incoming traffic with specified states of smart grid devices. Applying IEC 61850 demonstrates the framework's effectiveness in conducting stateful analysis for enhanced security [143].

Modularity and interfaces that support maximum flexibility: The framework makes use of pluggable modules that determine data collection, feature extraction and selection, data cleaning and normalization, feature fusion, alarm generation, feature transmission, training, training set generation, classification methods, and analysis. This modular feature of the framework enables flexible experimentation, not only to evaluate effective intrusion detection, but also to assess scalable network communication and computation.

6. Conclusions

This paper summarizes recent research on intrusion detection systems for AMI systems. Due to the complexity, heterogeneity, and inter-connectivity of the wide range of AMI system components, implementing and deploying MIDS, which combines UMIDSs and MIDS within the AMI paradigm, is more challenging than in other systems. An advanced IDS must be able to identify attacks in real time for such a highly distributed and hierarchical system. In this paper, the limitations, strengths, and most common methodologies of existing IDSs are highlighted. Furthermore, a proactive approach is recommended as a future research direction for detecting intrusions targeting the AMI of the SG system. The proposed MIDS approach would enable an extensive analysis of multimodal data correlations and the detection of intrusions using IoC, rule-based stateful analysis, and decision-making algorithms

 doi:10.20944/preprints202604.1188.v1

from the IDS deployed in the AMI. Furthermore, it would facilitate experimentation to discover scalable methods for applying intrusion detection to the AMI.

Nomenclature

AMI	Advanced metering infrastructure
SM	Smart meter
IoT	Internet of Things
FDIA	False data injection attack
DoS	Denial of Service
ICT	Information and communication technologies
SG	Smart Grid
MitM	Man-in-the-Middle
TPR	True Positive Rate
SCADA	Supervisory Control and Data Acquisition
CIA	Confidentiality, Integrity, and Availability
FL	Federated Learning
CPS	Cyber-physical system
IDS	Intrusion detection system
DSM	Demand side management
DNP3	Distributed network protocol version 3.0
APT	Advanced persistent threat
MIDS	Multimodal intrusion detection system
UMIDS	Unimodal intrusion detection system
NIDS	Network intrusion detection system
ICS	Industrial control system
TTPs	Tactics, Techniques, and Procedures
IoC	Indicator of Compromise
HIDS	Host intrusion detection system

References

1. Karnouskos, S.; Da Silva, P.G.; Ilic, D. Assessment of high-performance smart metering for the web service enabled smart grid era. In Proceedings of the Proceedings of the 2nd ACM/SPEC International Conference on Performance engineering, 2011, pp. 133–144.
2. Gope, P.; Sikdar, B. Privacy-aware authenticated key agreement scheme for secure smart grid communication. *IEEE Transactions on Smart Grid* **2018**, *10*, 3953–3962.
3. Jokar, P.; Arianpoo, N.; Leung, V.C. Electricity theft detection in AMI using customers' consumption patterns. *IEEE Transactions on Smart Grid* **2015**, *7*, 216–226.
4. McDaniel, P.; McLaughlin, S. Security and privacy challenges in the smart grid. *IEEE security & privacy* **2009**, *7*, 75–77.
5. Lázaro, J.; Astarloa, A.; Rodríguez, M.; Bidarte, U.; Jiménez, J. A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid. *Electronics* **2021**, *10*, 1881.
6. Otuoze, A.O.; Mustafa, M.W.; Larik, R.M. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology* **2018**, *5*, 468–483.
7. Merlino, J.C.; Asiri, M.; Saxena, N. Ddos cyber-incident detection in smart grids. *Sustainability* **2022**, *14*, 2730.
8. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *Ieee Access* **2019**, *7*, 46595–46620.
9. He, H.; Sun, X.; He, H.; Zhao, G.; He, L.; Ren, J. A novel multimodal-sequential approach based on multi-view features for network intrusion detection. *IEEE Access* **2019**, *7*, 183207–183221.
10. Agrafiotis, G.; Kalafatidis, S.; Giapantzis, K.; Lalas, A.; Votis, K. Advancing cybersecurity with ai: A multimodal fusion approach for intrusion detection systems. In Proceedings of the 2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom). IEEE, 2024, pp. 51–56.
11. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering* **2018**, *67*, 469–482.

 doi:10.20944/preprints202604.1188.v1

12. Coelho, P.; Gomes, M.; Moreira, C. Smart metering technology. *Microgrids Design and Implementation* **2019**, pp. 97–137.
13. Sun, C.C.; Cardenas, D.J.S.; Hahn, A.; Liu, C.C. Intrusion detection for cybersecurity of smart meters. *IEEE Transactions on Smart Grid* **2020**, *12*, 612–622.
14. Carpenter, M.; Goodspeed, T.; Singletary, B.; Skoudis, E.; Wright, J. Advanced metering infrastructure attack methodology. *InGuardians white paper* **2009**.
15. Foreman, J.C.; Gurugubelli, D. Identifying the cyber attack surface of the advanced metering infrastructure. *The Electricity Journal* **2015**, *28*, 94–103.
16. Shein, R. Security measures for advanced metering infrastructure components. In Proceedings of the 2010 Asia-Pacific Power and Energy Engineering Conference. IEEE, 2010, pp. 1–3.
17. Banik, S.; Banik, T. Survey on Simulation and Vulnerability Testing in Smart Grid. *preprints.org* **2024**.
18. Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Li, J. A denial of service attack in advanced metering infrastructure network. In Proceedings of the 2014 IEEE International Conference on Communications (ICC). IEEE, 2014, pp. 1029–1034.
19. Diovu, R.; Agee, J. A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks. In Proceedings of the 2017 IEEE PES PowerAfrica. IEEE, 2017, pp. 28–33.
20. Shokry, M.; Awad, A.I.; Abd-Ellah, M.K.; Khalaf, A.A. Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. *Future Generation Computer Systems* **2022**, *136*, 358–377.
21. Khattak, A.M.; Khanji, S.I.; Khan, W.A. Smart meter security: Vulnerabilities, threat impacts, and countermeasures. In Proceedings of the Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM) 2019 13. Springer, 2019, pp. 554–562.
22. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE communications surveys & tutorials* **2012**, *14*, 998–1010.
23. Wang, J.; Shi, D.; Li, Y.; Chen, J.; Ding, H.; Duan, X. Distributed framework for detecting PMU data manipulation attacks with deep autoencoders. *IEEE Transactions on smart grid* **2018**, *10*, 4401–4410.
24. Guo, Y.; Ten, C.W.; Hu, S.; Weaver, W.W. Modeling distributed denial of service attack in advanced metering infrastructure. In Proceedings of the 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT). IEEE, 2015, pp. 1–5.
25. Banik, S.; Rogers, M.; Mahajan, S.M.; Emeghara, C.M.; Banik, T.; Craven, R. Survey on Vulnerability Testing in the Smart Grid. *IEEE Access* **2024**.
26. Foreman, J.C.; Gurugubelli, D. Cyber attack surface analysis of advanced metering infrastructure. *arXiv preprint arXiv:1607.04811* **2016**.
27. Banik, S.; Banik, T.; Banik, S. Using Virtual Environment to Analyze Cyber-Attacks on Smart Grid Protocol. *Preprints* **2023**. https://doi.org/10.20944/preprints202309.0984.v1.
28. Banik, S.; Banik, T.; Hossain, S.; Saha, S.K. Implementing Man-in-the-Middle Attack to Investigate Network Vulnerabilities in Smart Grid Test-bed. *arXiv preprint arXiv:2306.00234* **2023**.
29. Kulkarni, S.; Rahul, R.; Shreyas, R.; Nagasundari, S.; Honnavalli, P.B. MITM intrusion analysis for advanced metering infrastructure communication in a smart grid environment. In Proceedings of the Trends in Computational Intelligence, Security and Internet of Things: Third International Conference, ICCISIoT 2020, Tripura, India, December 29-30, 2020, Proceedings 3. Springer, 2020, pp. 256–267.
30. Banik, S.; Manicavasagam, R.; Banik, T.; Banik, S. Simulation and Analysis of Cyber-Attack on Modbus Protocol for Smart Grids in Virtual Environment. In Proceedings of the Science and Information Conference. Springer, 2024, pp. 384–401.
31. Pavithra, L.; Rekha, D. Prevention of replay attack for isolated smart grid. In Proceedings of the Next Generation Information Processing System: Proceedings of ICCET 2020, Volume 2. Springer, 2021, pp. 251–258.
32. Bhattacharjee, S.; Madhavarapu, V.P.K.; Silvestri, S.; Das, S.K. Attack context embedded data driven trust diagnostics in smart metering infrastructure. *ACM Transactions on Privacy and Security (TOPS)* **2021**, *24*, 1–36.
33. Khan, Z.A.; Adil, M.; Javaid, N.; Saqib, M.N.; Shafiq, M.; Choi, J.G. Electricity theft detection using supervised learning techniques on smart meter data. *Sustainability* **2020**, *12*, 8023.
34. Ismail, M.; Shahin, M.; Shaaban, M.F.; Serpedin, E.; Qaraqe, K. Efficient detection of electricity theft cyber attacks in AMI networks. In Proceedings of the 2018 IEEE wireless communications and networking conference (WCNC). IEEE, 2018, pp. 1–6.

 doi:10.20944/preprints202604.1188.v1

35. Na, L.; Xiaohui, X.; Xiaoqin, M.; Xiangfu, M.; Peisen, Y. Fake data injection attack detection in AMI system using a hybrid method. In Proceedings of the 2021 IEEE Sustainable Power and Energy Conference (iSPEC). IEEE, 2021, pp. 2371–2376.
36. Bi, J.; Luo, F.; Liang, G.; Yang, X.; He, S.; Dong, Z.Y. Impact assessment and defense for smart grids with FDIA against AMI. *IEEE Transactions on Network Science and Engineering* **2022**, *10*, 578–591.
37. Wei, L.; Rondon, L.P.; Moghadasi, A.; Sarwat, A.I. Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid. In Proceedings of the 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). IEEE, 2018, pp. 1–9.
38. Nabil, M.; Ismail, M.; Mahmoud, M.; Shahin, M.; Qaraqe, K.; Serpedin, E. Deep learning-based detection of electricity theft cyber-attacks in smart grid AMI networks. *Deep learning applications for cyber security* **2019**, pp. 73–102.
39. Jokar, P.; Leung, V.C. Intrusion detection and prevention for ZigBee-based home area networks in smart grids. *IEEE Transactions on Smart Grid* **2016**, *9*, 1800–1811.
40. Anderson, R.; Fuloria, S. Who controls the off switch? In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications. IEEE, 2010, pp. 96–101.
41. Anwar, A.; Mahmood, A.N.; Tari, Z. Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid. *Information Systems* **2015**, *53*, 201–212.
42. Banik, S.; Saha, S.K.; Banik, T.; Hossain, S. Anomaly Detection Techniques in Smart Grid Systems: A Review. *arXiv preprint arXiv:2306.02473* **2023**.
43. Aburomman, A.A.; Reaz, M.B.I. A survey of intrusion detection systems based on ensemble and hybrid classifiers. *Computers & security* **2017**, *65*, 135–152.
44. Zhou, C.V.; Leckie, C.; Karunasekera, S. A survey of coordinated attacks and collaborative intrusion detection. *computers & security* **2010**, *29*, 124–140.
45. Arshad, J.; Azad, M.A.; Amad, R.; Salah, K.; Alazab, M.; Iqbal, R. A review of performance, energy and privacy of intrusion detection systems for IoT. *Electronics* **2020**, *9*, 629.
46. Berman, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L. A survey of deep learning methods for cyber security. *Information* **2019**, *10*, 122.
47. Tong, W.; Lu, L.; Li, Z.; Lin, J.; Jin, X. A survey on intrusion detection system for advanced metering infrastructure. In Proceedings of the 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC). IEEE, 2016, pp. 33–37.
48. Mirzaee, P.H.; Shojafar, M.; Cruickshank, H.; Tafazolli, R. Smart grid security and privacy: From conventional to machine learning issues (threats and countermeasures). *IEEE access* **2022**, *10*, 52922–52954.
49. Grochocki, D.; Huh, J.H.; Berthier, R.; Bobba, R.; Sanders, W.H.; Cárdenas, A.A.; Jetcheva, J.G. AMI threats, intrusion detection requirements and deployment recommendations. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm). IEEE, 2012, pp. 395–400.
50. Marchese, D.; Jin, A.; Fox-Lent, C.; Linkov, I. Resilience for smart water systems. *Journal of Water Resources Planning and Management* **2020**, *146*, 02519002.
51. Aravinthan, V.; Namboodiri, V.; Sunku, S.; Jewell, W. Wireless AMI application and security for controlled home area networks. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting. IEEE, 2011, pp. 1–8.
52. Faisal, M.A.; Aung, Z.; Williams, J.R.; Sanchez, A. Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study. *IEEE Systems journal* **2014**, *9*, 31–44.
53. Zhang, K.; Hu, Z.; Zhan, Y.; Wang, X.; Guo, K. A smart grid AMI intrusion detection strategy based on extreme learning machine. *Energies* **2020**, *13*, 4907.
54. Attia, M.; Sedjelmaci, H.; Senouci, S.M.; Aglzim, E.H. A new intrusion detection approach against lethal attacks in the smart grid: temporal and spatial based detections. In Proceedings of the 2015 Global Information Infrastructure and Networking Symposium (GIIS). IEEE, 2015, pp. 1–3.
55. Albuquerque Filho, J.; Brandão, L.C.; Fernandes, B.J.; Maciel, A.M. A review of neural networks for anomaly detection. *IEEE Access* **2022**.
56. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems* **2018**, *99*, 45–56.
57. Denning, D.E. An intrusion-detection model. *IEEE Transactions on software engineering* **1987**, pp. 222–232.
58. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. *ACM computing surveys (CSUR)* **2009**, *41*, 1–58.

 doi:10.20944/preprints202604.1188.v1

59. Yen, S.W.; Morris, S.; Ezra, M.A.; Huat, T.J. Effect of smart meter data collection frequency in an early detection of shorter-duration voltage anomalies in smart grids. *International journal of electrical power & energy systems* **2019**, *109*, 1–8.
60. Prabhakar, P.; Arora, S.; Khosla, A.; Beniwal, R.K.; Arthur, M.N.; Arias-Gonzáles, J.L.; Areche, F.O.; et al. Cyber Security of Smart Metering Infrastructure Using Median Absolute Deviation Methodology. *Security and Communication Networks* **2022**, *2022*.
61. Berthier, R.; Sanders, W.H. Specification-based intrusion detection for advanced metering infrastructures. In Proceedings of the 2011 IEEE 17th Pacific rim international symposium on dependable computing. IEEE, 2011, pp. 184–193.
62. Jokar, P.; Nicanfar, H.; Leung, V.C. Specification-based intrusion detection for home area networks in smart grids. In Proceedings of the 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, 2011, pp. 208–213.
63. Ruan, H.M.; Yeap, G.W.; Lei, C.L. Hybrid intrusion detection framework for advanced metering infrastructure. In *Intelligent Systems and Applications*; IOS Press, 2015; pp. 894–903.
64. Khan, R.; Albalushi, A.; McLaughlin, K.; Laverty, D.; Sezer, S. Model based intrusion detection system for synchrophasor applications in smart grid. In Proceedings of the 2017 IEEE Power & Energy Society General Meeting. IEEE, 2017, pp. 1–5.
65. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications* **2017**, *84*, 25–37.
66. Liu, Q.; Hagenmeyer, V.; Keller, H.B. A review of rule learning-based intrusion detection systems and their prospects in smart grids. *IEEE Access* **2021**, *9*, 57542–57564.
67. Farooqi, A.H.; Khan, F.A. Intrusion detection systems for wireless sensor networks: A survey. In Proceedings of the International Conference on Future Generation Communication and Networking. Springer, 2009, pp. 234–241.
68. Kasinathan, P.; Pastrone, C.; Spirito, M.A.; Vinkovits, M. Denial-of-Service detection in 6LoWPAN based Internet of Things. In Proceedings of the 2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob). IEEE, 2013, pp. 600–607.
69. Wallgren, L.; Raza, S.; Voigt, T. Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks* **2013**, *9*, 794326.
70. Jithish, J.; Alangot, B.; Mahalingam, N.; Yeo, K.S. Distributed anomaly detection in smart grids: a federated learning-based approach. *IEEE Access* **2023**, *11*, 7157–7179.
71. Tariq, N.; Alsirhani, A.; Humayun, M.; Alserhani, F.; Shaheen, M. A fog-edge-enabled intrusion detection system for smart grids. *Journal of Cloud Computing* **2024**, *13*, 43.
72. Faisal, M.A.; Aung, Z.; Williams, J.R.; Sanchez, A. Securing advanced metering infrastructure using intrusion detection system with data stream mining. In Proceedings of the Intelligence and Security Informatics: Pacific Asia Workshop, PAISI 2012, Kuala Lumpur, Malaysia, May 29, 2012. Proceedings. Springer, 2012, pp. 96–111.
73. Zhang, Y.; Wang, L.; Sun, W.; Green II, R.C.; Alam, M. Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid* **2011**, *2*, 796–808.
74. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems* **2020**, *77*, 103201.
75. Le, A.; Loo, J.; Chai, K.K.; Aiash, M. A specification-based IDS for detecting attacks on RPL-based network topology. *Information* **2016**, *7*, 25.
76. Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad hoc networks* **2013**, *11*, 2661–2674.
77. Pongle, P.; Chavan, G. Real time intrusion and wormhole attack detection in internet of things. *International Journal of Computer Applications* **2015**, *121*.
78. Thanigaivelan, N.K.; Nigussie, E.; Kanth, R.K.; Virtanen, S.; Isoaho, J. Distributed internal anomaly detection system for Internet-of-Things. In Proceedings of the 2016 13th IEEE annual consumer communications & networking conference (CCNC). IEEE, 2016, pp. 319–320.
79. Lo, C.H.; Ansari, N. CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid. *IEEE Transactions on Emerging Topics in Computing* **2013**, *1*, 33–44.
80. Sahani, N.; Zhu, R.; Cho, J.H.; Liu, C.C. Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey. *ACM Transactions on Cyber-Physical Systems* **2023**, *7*, 1–31.

 doi:10.20944/preprints202604.1188.v1

81. Bondok, A.H.; Mahmoud, M.; Badr, M.M.; Fouda, M.M.; Abdallah, M.; Alsabaan, M. Novel evasion attacks against adversarial training defense for smart grid federated learning. *IEEE Access* **2023**.
82. Sun, X.; Tang, Z.; Du, M.; Deng, C.; Lin, W.; Chen, J.; Qi, Q.; Zheng, H. A hierarchical federated learning-based intrusion detection system for 5g smart grids. *Electronics* **2022**, *11*, 2627.
83. Khraisat, A.; Alazab, A.; Singh, S.; Jan, T.; Jr. Gomez, A. Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions. *ACM Computing Surveys* **2024**, *57*, 1–38.
84. Li, B.; Wu, Y.; Song, J.; Lu, R.; Li, T.; Zhao, L. DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems. *IEEE Transactions on Industrial Informatics* **2020**, *17*, 5615–5624.
85. Vijayanand, R.; Devaraj, D.; Kannapiran, B. A novel deep learning based intrusion detection system for smart meter communication network. In Proceedings of the 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS). IEEE, 2019, pp. 1–3.
86. Song, K.; Kim, P.; Tyagi, V.; Rajasekaran, S. Artificial immune system (AIS) based intrusion detection system (IDS) for smart grid advanced metering infrastructure (AMI) networks. Technical report, Virginia Tech, 2018.
87. Radoglou Grammatikis, P.; Sarigiannidis, P.; Efstathopoulos, G.; Panaousis, E. ARIES: A novel multivariate intrusion detection system for smart grid. *Sensors* **2020**, *20*, 5305.
88. Pan, S.; Morris, T.H.; Adhikari, U. A specification-based intrusion detection framework for cyber-physical environment in electric power system. *Int. J. Netw. Secur.* **2015**, *17*, 174–188.
89. Mohan, S.N.; Ravikumar, G.; Govindarasu, M. Distributed intrusion detection system using semantic-based rules for SCADA in smart grid. In Proceedings of the 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). IEEE, 2020, pp. 1–5.
90. Kwon, Y.; Kim, H.K.; Lim, Y.H.; Lim, J.I. A behavior-based intrusion detection technique for smart grid infrastructure. In Proceedings of the 2015 IEEE Eindhoven PowerTech. IEEE, 2015, pp. 1–6.
91. Fadel, E.; Gungor, V.C.; Nassef, L.; Akkari, N.; Malik, M.A.; Almasri, S.; Akyildiz, I.F. A survey on wireless sensor networks for smart grid. *Computer Communications* **2015**, *71*, 22–33.
92. Longe, O.M.; Ouahada, K.; Ferreira, H.C.; Rimer, S. Wireless sensor networks and advanced metering infrastructure deployment in smart grid. In Proceedings of the e-Infrastructure and e-Services for Developing Countries: 5th International Conference, AFRICOMM 2013, Blantyre, Malawi, November 25-27, 2013, Revised Selected Papers 5. Springer, 2014, pp. 167–171.
93. Banik, S.; Banik, T.; Banik, S. Intrusion detection system in smart grid-a review, 2023.
94. Ioulianou, P.; Vasilakis, V.; Moscholios, I.; Logothetis, M. A signature-based intrusion detection system for the internet of things. *Information and Communication Technology Form* **2018**.
95. Efstathopoulos, G.; Grammatikis, P.R.; Sarigiannidis, P.; Argyriou, V.; Sarigiannidis, A.; Stamatakis, K.; Angelopoulos, M.K.; Athanasopoulos, S.K. Operational data based intrusion detection system for smart grid. In Proceedings of the 2019 IEEE 24th international workshop on computer aided modeling and design of communication links and networks (CAMAD). IEEE, 2019, pp. 1–6.
96. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. An anomaly-based intrusion detection system for the smart grid based on cart decision tree. In Proceedings of the 2018 global information infrastructure and networking symposium (GIIS). IEEE, 2018, pp. 1–5.
97. Khoei, T.T.; Aissou, G.; Hu, W.C.; Kaabouch, N. Ensemble learning methods for anomaly intrusion detection system in smart grid. In Proceedings of the 2021 IEEE international conference on electro information technology (EIT). IEEE, 2021, pp. 129–135.
98. Rose, T.; Kifayat, K.; Abbas, S.; Asim, M. A hybrid anomaly-based intrusion detection system to improve time complexity in the Internet of Energy environment. *Journal of Parallel and Distributed Computing* **2020**, *145*, 124–139.
99. AlHaddad, U.; Basuhail, A.; Khemakhem, M.; Eassa, F.E.; Jambi, K. Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks. *Sensors* **2023**, *23*, 7464.
100. Pan, S.; Morris, T.; Adhikari, U. Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Transactions on Smart Grid* **2015**, *6*, 3104–3113.
101. Chavez, A.; Lai, C.; Jacobs, N.; Hossain-McKenzie, S.; Jones, C.B.; Johnson, J.; Summers, A. Hybrid intrusion detection system design for distributed energy resource systems. In Proceedings of the 2019 IEEE CyberPELS (CyberPELS). IEEE, 2019, pp. 1–6.
102. Abou-Elasaad, M.M.; Sayed, S.G.; El-Dakroury, M.M. Smart Grid intrusion detection system based on AI techniques. *Journal of Cybersecurity & Information Management* **2025**, *15*.

 doi:10.20944/preprints202604.1188.v1

103. Vigna, G.; Kemmerer, R.A. NetSTAT: A network-based intrusion detection system. *Journal of computer security* **1999**, *7*, 37–71.
104. Liu, M.; Xue, Z.; Xu, X.; Zhong, C.; Chen, J. Host-based intrusion detection system with system calls: Review and future trends. *ACM computing surveys (CSUR)* **2018**, *51*, 1–36.
105. Gassais, R.; Ezzati-Jivan, N.; Fernandez, J.M.; Aloise, D.; Dagenais, M.R. Multi-level host-based intrusion detection system for Internet of things. *Journal of Cloud Computing* **2020**, *9*, 62.
106. Sen, O.; Hassan, T.; Ulbig, A.; Henze, M. Enhancing scada security: Developing a host-based intrusion detection system to safeguard against cyberattacks. *arXiv preprint arXiv:2402.14599* **2024**.
107. Li, B.; Lu, R.; Wang, W.; Choo, K.K.R. Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. *Journal of Parallel and Distributed Computing* **2017**, *103*, 32–41.
108. Hu, Z.; Liu, S.; Luo, W.; Wu, L. Intrusion-detector-dependent distributed economic model predictive control for load frequency regulation with PEVs under cyber attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers* **2021**, *68*, 3857–3868.
109. Rani, M.; et al. A review of intrusion detection system in cloud computing. In Proceedings of the Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India, 2019.
110. Abdelkhalek, M.; Ravikumar, G.; Govindarasu, M. Ml-based anomaly detection system for der communication in smart grid. In Proceedings of the 2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2022, pp. 1–5.
111. Sen, P.; Waghmare, S. Machine learning based intrusion detection system for real-time smart grid security. In Proceedings of the 2021 13th IEEE PES Asia Pacific Power & Energy Engineering Conference (APPEEC). IEEE, 2021, pp. 1–6.
112. Prasad, G.; Huo, Y.; Lampe, L.; Leung, V.C. Machine learning based physical-layer intrusion detection and location for the smart grid. In Proceedings of the 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE, 2019, pp. 1–6.
113. Otoum, S.; Kantarci, B.; Mouftah, H.T. Mitigating False Negative intruder decisions in WSN-based Smart Grid monitoring. In Proceedings of the 2017 13th International wireless communications and mobile computing conference (IWCMC). IEEE, 2017, pp. 153–158.
114. Cárdenas, A.A.; Baras, J.S.; Seamon, K. A framework for the evaluation of intrusion detection systems. In Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06). IEEE, 2006, pp. 15–pp.
115. Bai, K.Z.; Fossaceca, J.M. EM-AUC: A Novel Algorithm for Evaluating Anomaly Based Network Intrusion Detection Systems. *Sensors* **2024**, *25*, 78.
116. Puccetti, T.; Ceccarelli, A. Detection Latencies of Anomaly Detectors-An Overlooked Perspective? In Proceedings of the 2024 IEEE 35th International Symposium on Software Reliability Engineering (ISSRE). IEEE, 2024, pp. 37–48.
117. Sedik, A.; Faragallah, O.S.; El-sayed, H.S.; El-Banby, G.M.; El-Samie, F.E.A.; Khalaf, A.A.; El-Shafai, W. An efficient cybersecurity framework for facial video forensics detection based on multimodal deep learning. *Neural Computing and Applications* **2022**, pp. 1–18.
118. Raza, A.; Munir, K.; Almutairi, M. A novel deep learning approach for deepfake image detection. *Applied Sciences* **2022**, *12*, 9820.
119. Khalid, H.; Kim, M.; Tariq, S.; Woo, S.S. Evaluation of an audio-video multimodal deepfake dataset using unimodal and multimodal detectors. In Proceedings of the Proceedings of the 1st workshop on synthetic multimedia-audiovisual deepfake generation and detection, 2021, pp. 7–15.
120. Zhou, F.; Wen, G.; Ma, Y.; Geng, H.; Huang, R.; Pei, L.; Yu, W.; Chu, L.; Qiu, R. A comprehensive survey for deep-learning-based abnormality detection in smart grids with multimodal image data. *Applied Sciences* **2022**, *12*, 5336.
121. Ullah, F.; Turab, A.; Ullah, S.; Cacciagrano, D.; Zhao, Y. Enhanced Network Intrusion Detection System for Internet of Things Security Using Multimodal Big Data Representation with Transfer Learning and Game Theory. *Sensors* **2024**, *24*, 4152.
122. Zhang, Y.; Wang, J.; Chen, B. Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach. *IEEE Transactions on Smart Grid* **2020**, *12*, 623–634.
123. Kiflay, A.; Tsokanos, A.; Fazlali, M.; Kirner, R. Network intrusion detection leveraging multimodal features. *Array* **2024**, *22*, 100349.
124. Sweeten, J. Multi-Modal Intrusion Detection in Cyber-Physical Smart Power Grids. Master's thesis, Tennessee Technological University, 2023.

 doi:10.20944/preprints202604.1188.v1

125. Shilay, D.M.; Lorey, K.G.; Weiz, T.; Lovetty, T.; Cheng, Y. Catching anomalous distributed photovoltaics: An edge-based multi-modal anomaly detection. *arXiv preprint arXiv:1709.08830* **2017**.
126. Asiri, M.; Saxena, N.; Gjomemo, R.; Burnap, P. Understanding indicators of compromise against cyber-attacks in industrial control systems: a security perspective. *ACM transactions on cyber-physical systems* **2023**, *7*, 1–33.
127. Manicavasagam, R. Identifying and Detecting Network Indicators of Compromise (IOCs) for Demand Response Programs. PhD thesis, Tennessee Technological University, 2023.
128. Zaboli, A.; Hong, J.; Ştefanov, A.; Liu, C.C.; Hwang, C.S. Large Language Models for Power System Security: A Novel Multi-Modal Approach for Anomaly Detection in Energy Management Systems. *IEEE Access* **2025**, *13*, 203558–203585.
129. Korba, A.A.; Tamani, N.; Ghamri-Doudane, Y.; et al. Anomaly-based framework for detecting power overloading cyberattacks in smart grid AMI. *Computers & Security* **2020**, *96*, 101896.
130. Dong, Y. Correlation-Driven Multi-Level Multimodal Learning for Anomaly Detection on Smart Electric Grid. In Proceedings of the 2025 2nd International Conference on Smart Grid and Artificial Intelligence (SGAI). IEEE, 2025, pp. 254–257.
131. Xia, Z.; Tang, H.; Hu, Z.; Zhou, H. Efficient intrusion detection in ami systems based on federated semi-supervised learning. *IEEE Transactions on Network Science and Engineering* **2025**.
132. Broni, K.; Mills, G. Intrusion Detection for Advanced Metering Infrastructure using Machine Learning. In Proceedings of the 2024 IEEE 9th International Conference on Adaptive Science and Technology (ICAST). IEEE, 2024, Vol. 9, pp. 1–8.
133. SMH, S.S.F. Real-time implementation of IoT Enabled Cyber Attack Detection System (IoT-E-CADS) in Advanced Metering Infrastructure (AMI) using Machine Learning Technique (MLT). *IoT* **2024**.
134. Abdullakutty, F.; Elyan, E.; Johnston, P. A review of state-of-the-art in Face Presentation Attack Detection: From early development to advanced deep learning and multi-modal fusion methods. *Information fusion* **2021**, *75*, 55–69.
135. Hadi, H.J.; Cao, Y.; Hussain, F.B.; Ahamad, N.; Alshara, M.A.; Ullah, I.; Javed, Y.; He, Y.; Jamil, A.M. Reducing False Positives in Intrusion Detection System Alerts: A Novel Aggregation and Correlation Model. In Proceedings of the International Conference on Digital Forensics and Cyber Crime. Springer, 2025, pp. 153–167.
136. Alserhani, F.M. Alert correlation and aggregation techniques for reduction of security alerts and detection of multistage attack. *International Journal of Advanced Studies in Computers, Science and Engineering* **2016**, *5*, 1.
137. Huang, W.; Wang, D.; Ouyang, X.; Wan, J.; Liu, J.; Li, T. Multimodal federated learning: Concept, methods, applications and future directions. *Information Fusion* **2024**, *112*, 102576.
138. Zhao, Y.; Barnaghi, P.; Haddadi, H. Multimodal federated learning on iot data. In Proceedings of the 2022 IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, 2022, pp. 43–54.
139. Li, X.J.; Ma, M.; Sun, Y. An adaptive deep learning neural network model to enhance machine-learning-based classifiers for intrusion detection in smart grids. *Algorithms* **2023**, *16*, 288.
140. Andresini, G.; Appice, A.; Di Mauro, N.; Loglisci, C.; Malerba, D. Multi-channel deep feature learning for intrusion detection. *IEEE Access* **2020**, *8*, 53346–53359.
141. Upadhyay, D.; Manero, J.; Zaman, M.; Sampalli, S. Gradient boosting feature selection with machine learning classifiers for intrusion detection on power grids. *IEEE Transactions on Network and Service Management* **2020**, *18*, 1104–1116.
142. Baltrušaitis, T.; Ahuja, C.; Morency, L.P. Multimodal machine learning: A survey and taxonomy. *IEEE transactions on pattern analysis and machine intelligence* **2018**, *41*, 423–443.
143. Kang, B.; McLaughlin, K.; Sezer, S. Towards a stateful analysis framework for smart grid network intrusion detection. In Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016. BCS Learning & Development, 2016.