Cluster Computing (2019) 22:43–69
https://doi.org/10.1007/s10586-018-2820-9

A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure

Sanket Desai[1] · Rabei Alhadad[1] · Naveen Chilamkurti[1] · Abdun Mahmood[1]

Received: 27 September 2017 / Revised: 28 March 2018 / Accepted: 17 July 2018 / Published online: 24 July 2018

Abstract

Integration of renewable resources and increased growth in energy consumption has created new challenges for the traditional electrical network. To adhere to these challenges, Internet of Everything (IoE) has transformed the existing power grid into a modernized electrical network called Smart Grid. An integral part of this transformation is the Advanced Metering Infrastructure (AMI), which enables two-way communication for flow of information consisting of energy consumption, outages, and electricity rates between smart meters and the utilities. These enhanced AMI features and privileges have resulted in a larger surface for cyber-attack, enabling remote exploitation of these smart devices without any physical access. Therefore, consumer privacy and security has become a critical issue due to the interconnection of different smart devices in various communication networks and the information they carry. In this paper, we present a comprehensive survey of privacy related research in the IoE enabled smart grid environment. The survey presents a detailed analysis of privacy problems and their corresponding solutions in AMI. Our goal is to provide an in-depth understanding of the smart grid and shed light on future research directions.

Keywords Internet of Everything (IoE) · Smart grid · Advanced Metering Infrastructure (AMI) · Security · Privacy preserving · Cryptography

1 Introduction

The recent technological trends such as communication, big data, smart infrastructure and business economics have transformed our social environment. The increased connectedness between the people, processes, data, and things, which defines Internet of Everything (IoE), is revolutionizing the way utility companies monitor, control and distribute energy over the electrical grid [20]. A recent study by Cisco predicts that IoE is projected to create $14 trillion net profit value, a combination of increased revenues and lowered costs, to private sector from 2013 to 2022. Ciscos analysis shows that most of the potential value at stake (66%, or $9.5 trillion) comes from transformation based on industry-specific use cases such as the smart grid and smart buildings [27].

Smart Grid integrates an electrical grid with information technologies for efficient power distribution and transmission between consumers and suppliers. With the help of information and communication infrastructure, smart grid enables collection and processing of various types of energy usage data through the Advanced Metering Infrastructure (AMI) consisting of different entities such as smart meters, grid sensors, phasor measurement units (PMU), fault detectors, etc. [122].

The AMI enables high speed two-way communication between the smart meters and the utility back office which allows periodic or on-demand energy consumption readings as well as fine-grained energy related data. The fine-

✉ Naveen Chilamkurti
n.chilamkurti@latrobe.edu.au

Sanket Desai
s6desai@students.latrobe.edu.au

Rabei Alhadad
R.Eludad@latrobe.edu.au

Abdun Mahmood
A.Mahmood@latrobe.edu.au

[1] Department of Computer Science and Information Technology, School of Engineering and Mathematical Science, Latrobe University, Plenty Road & Kingsbury Drive, Melbourne, VIC 3086, Australia

grained energy related data allow efficient and reliable control of the electrical grid, but also enables demand forecasting, fault detection, load balancing, dynamic pricing, demand-response, etc. However, the two-way communication has given rise to potential vulnerabilities related to consumer privacy.

1.1 Motivation

Smart Grid relies on its broad range of grid-side and consumer-side applications that enable numerous advantages in terms of energy consumption data, pricing levels and different information messages. These applications benefit by inducing a consumer behaviour in a bid to reduce load during peak time and conserve energy. However, this has resulted in breach of consumer privacy i.e. consumer profiling.

In 2009, the Federal Bureau of Investigation's Cyber intelligence investigated a widespread incident of power theft related to the smart meters. It was found that the miscreants hacked into the smart meters and reprogrammed the power consumption settings, resulting in a loss of $US400 million annually for the Puerto Rico utility [78].

Furthermore, in 2007, the Austin Energy/Austin Police conducted a warrant less surveillance program where consumer usage information was provided to find marijuana growing operations. Besides this, law enforcement agencies might use the data as real-time surveillance [62]. For instance, by remotely accessing the meter or capturing the metering data between the smart meter and the utility back office, a malicious user may acquire access to energy consumption data of a customer. This granular, fine-grained, high frequency energy usage data can be easily analyzed to derive a consumers way of living such as working hours, meal hours, vacations, house occupancy, and even living habits such as time when TV is watched.

Recent research in the Non-Intrusive Load Monitoring (NILM) field has highlighted the use of energy usage data to derive privacy-sensitive information about the customers way of living [22, 32, 51, 63, 65, 87, 120]. Such privacy issues and concerns have raised obstacles in the development and adoption of the smart grid initiative in many places in North America and Europe [33, 34, 140]. Hence, addressing these privacy issues has become a key requirement in the deployment of smart meters.

These aforementioned privacy concerns and issues have resulted in many scholars proposing various privacy preserving solutions for AMI recently. Therefore, we are motivated to analyze and highlight the potential privacy concerns, categorize and review the existing solutions and summarize future research challenges in preserving user privacy for AMI.

While various survey articles have been published in smart grid security [9, 16, 44, 48, 60, 80, 106, 115, 130, 134, 138] only a few of them address the privacy issues and concerns in depth. In this survey, we present and review in detail more than 50 privacy preserving schemes published between 2011 and 2017. Furthermore, we can summarize the main contribution of this survey paper as follows:

- We define privacy in-detail and its interweaving aspects with consumer data.
- We present a data interaction diagram simplifying the complex energy structure in terms of various interconnected stakeholders, applications, infrastructure and its highly sensitive consumer data.
- We provide a hierarchical diagram for classifications of privacy preserving approaches and identify shortcomings of existing state-of-art schemes in privacy preserving approaches in a tabular form.
- We present a discussion of technological challenges and open directions for future research.

The remainder of this paper is organized as follows. In Sect. 2, we introduce the fundamental smart grid network architecture. In Sect. 3, we present the AMI network architecture. In Sects. 4 and 5, we categorize and evaluate privacy threats and issues with the AMI data flow and use cases. In Sect. 6, we present and analyze the existing privacy related work. In Sect. 7, we evaluate the AMI privacy related work.

2 Smart Grid overview

Smart Grid also known as smart power grid or intelligent grid is an enhanced electrical grid that collaborates with information technologies for efficient power distribution and transmission between the consumers and the suppliers. With respect to traditional power systems, the smart grids are a high-speed two-way communication of information and electrical flow. The smart grid enables numerous smart assets to interact in a network infrastructure with energy management capabilities such as the AMI for the suppliers and the consumers. More specifically, the smart grid can be regarded as an electric system that uses information, two-way, cyber-secure communication technologies, and computational intelligence in an integrated fashion across electricity generation, transmission, substations, distribution, and consumption to achieve a system that is clean, safe, secure, reliable, resilient, efficient, and sustainable. Some of the benefits and requirements of the smart grid include [42, 54, 58, 96, 108]:

- Improved power reliability and quality.

- Enhancing capacity and efficiency of existing electric power networks.
- Improving resilience to disruption.
- Enabling predictive maintenance and self-healing responses to system disturbances.
- Facilitating expanded deployment of renewable energy sources.
- Accommodating distributed power sources.
- Automating maintenance and operation.
- Reducing greenhouse gas emissions by enabling electric vehicles and new power sources.
- Reducing oil consumption by reducing the need for inefficient generation during peak usage periods.
- Enabling transition to plug-in electric vehicles and new energy storage options.
- Increasing consumer choice.

To standardize the smart grid architecture and high-level conceptual reference models, a collaborative efforts have been introduced toward smart grid standardization involving noteworthy groups including: The Institute of Electrical and Electronic Engineers (IEEE) P2030, The European Commissions Mandate 490 (EU-M490) for Smart Grid with the European Telecommunications Standards Institute (ETSI), European Committee for Standardization (Comit Europen Normalisation - CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the Smart Grid Interoperability Panel (SGIP) [58]. In the following section, we will present the fundamental architecture of smart grid, which is followed by in detail review for the AMI and the data flow for AMI in smart grid.

According to NISTs conceptual model, and as shown in Fig. 1, the smart grid consists of seven logical domains: Bulk Generation, Transmission, Distribution, Customer, Markets, Service Provider and Operations [108]. The Generation, Transmission, Distribution and Customer domain perform two-way information and electricity flow while the Markets, Service Provider and Operations domain focus on information gathering.

2.1 Customer domain

The Customer domain is where the generated electricity is consumed and is considered as the main stakeholder in the smart grid. The Customer domain is electrically connected to the Distribution domain. It communicates with the Distribution, Operations, Market, and the Service Provider domains. Also, this domain enables the customers to use privileges such as: managing their electricity accounts and monitor the energy usage. In addition, the Customer domain consists of two main components which are used as a domain interface to connect with other domains using the AMI or by internet as illustrated in Fig. 1. These two components are: the utility meters and the Energy Service Interface (ESI). Also, a number of customer applications such as remote load control, monitoring the energy usage and reading of non-energy meters are available in the customer premise display unit to assist the customer in managing the electricity account and to provide a secure auditing/logging communication for the cyber security purpose.

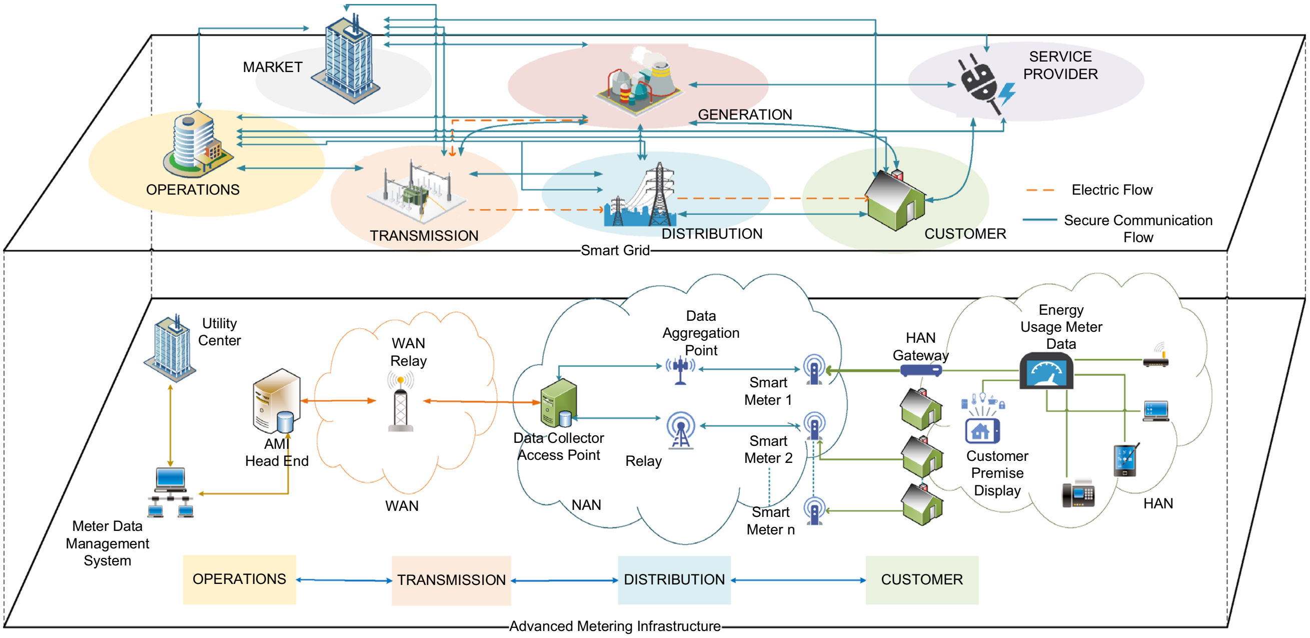


Fig. 1 Smart Grid overview

2.2 Distribution domain

The second domain the smart grid is the Distribution domain. The structure of the Distribution domain may vary in different smart grid systems depending on the entire smart grid infrastructure layout. As shown in Fig. 1, the Distribution domain is connected electrically with Customer domain and with the Transmission domain. The actors, the structure and the communication level between theses domains, contributes to the reliability of the Distribution domain. With the help of the Operation domain, the main role of the Distribution domain is to manage the real-time power flow associated with the Market domain. Also, the Market domain communicates with the Distribution domain which affects the local consumption and the generation of the power.

2.3 Transmission domain

The Transmission domain is responsible for the transmission of the energy from the Generation domain to the Distribution domain via multiple substations as appeared in Fig. 1. The primary goal of Transmission domain is to maintain the grid stability by balancing supply and demand over the network. The Transmission domain may consist of Distributed Energy Resources (DER) like power storage or generation units. Furthermore, the Supervisory and Data Acquisition System (SCADA) is used to monitor and control the transmission network.

2.4 Operations domain

The Operation domain consists of Energy Management Systems (EMS) and Distribution Management System (DMS) which analyze and control the transmission and distribution of energy supply respectively. The Operation domain is responsible for some of the critical functions of smart grid systems such as network control and monitoring, fault management and system efficiency and reliability analysis.

3 Advanced Metering Infrastructure (AMI)

With the evolution of the traditional electrical grid into the Smart Grid, Automated Meter Reading (AMR) which automatically collected the consumer data such as energy consumption was replaced by AMI. This replacement occurred due to the growing understanding of the benefits of using the two-way interactions between the utility back office and the consumers. The AMI is an integration of many technologies that provides an intelligent connection between consumers and utility back office [97]. Being an integral part of the smart grid network, the role of AMI network is to facilitate communication between the consumer's home devices such as meters and the utility center. The AMI has been assigned with various responsibilities such as periodic and on-demand energy usage readings, real-time pricing, outage alerts, firmware updates and configuration updates. In addition, AMI have security and privacy requirements due to the periodic transfer of sensitive information and command execution between the customer devices and the utility center. Integrity and confidentiality are the security objectives of high priority as compared to availability and reliability. Therefore, the AMI network design system should focus mainly on providing integrity and confidentiality.

3.1 AMI network infrastructure

To accommodate the AMI security requirements, the AMI network infrastructure has been designed in a hierarchical network architecture which includes Wide Area Network (WAN) connects utility center to the headend, Neighborhood Area Network(NAN) connects the headend to the smart meters and Home Area Network (HAN) to connect the home appliances with customer's smart meter as shown in Fig. 2.

3.1.1 Home Area Network (HAN)

The HAN comprises of all the smart appliances connected through a dedicated network to the smart metering system. HAN allows devices to be controlled and monitored using various communication protocols such as ZigBee, Ethernet, Wi-Fi, RFID, GPRS, PLC and Bluetooth. It empowers consumers by managing peak electric demand, real-time access to energy usage and monitoring device performance. In addition, HAN consist of home automation and building automation applications, which enables transfer of electrical measurement data within the home premises. Therefore, the communication requirements consist of low power consumption and cost and secure communications.

3.1.2 Neighborhood Area Network (NAN)

The NAN connects the HAN with the Wide Area Network (WAN). It offers monitoring, controlling and distribution of electricity. The NAN aggregates vast amount of metering data from thousands of meters located in different HANs. The data is gathered at a data concentrator, which acts as a gateway of the NAN. The NAN applications such as smart metering, demand response requires communication technologies which can provide a data rate of 100 kbps–10 Mbps with large coverage distance (10 km).

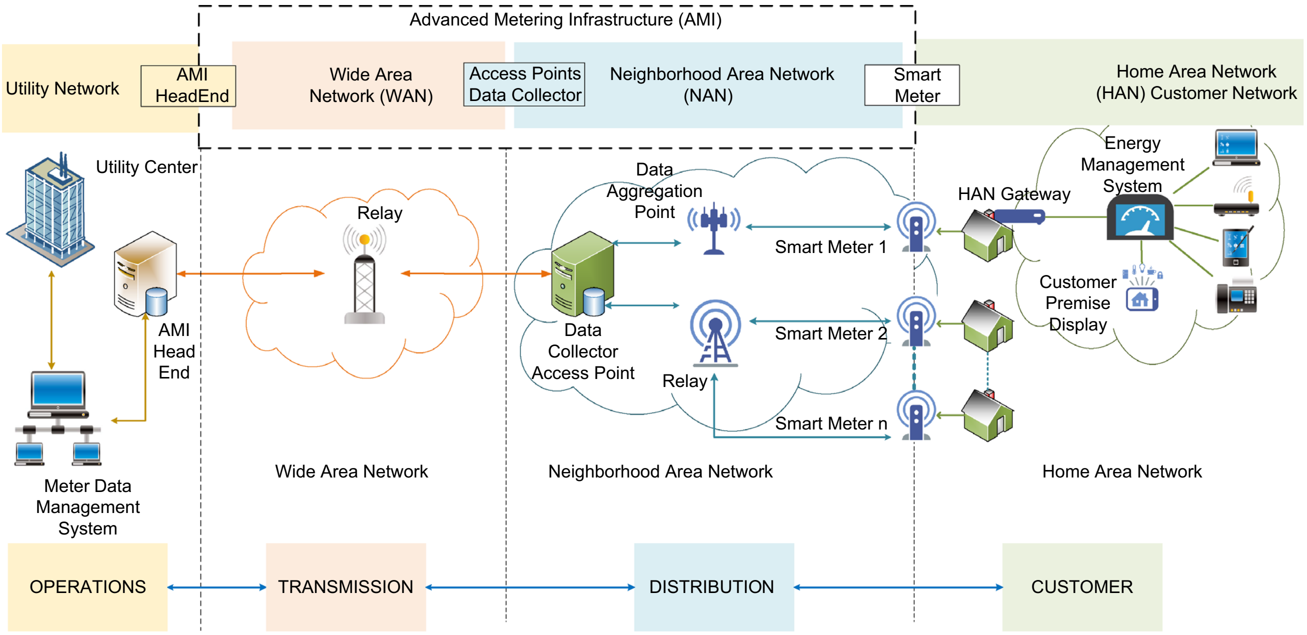


Fig. 2 AMI metering infrastructure

Different communication technologies are used in NAN such as: ZigBee mesh networks, Wi-Fi mesh networks, Power Line Communication (PLC), WiMAX, Cellular, Digital Subscriber Line (DSL) and Coaxial Cable.

3.1.3 Wide Area Network (WAN)

The WAN communicates between the NAN and the utility network. The WAN applications prioritize, control, monitoring and security of a large area of the system to assure reliability and efficiency. Due to the large volume of data transferred at a higher time frequency, a data rate of about 10 Mbps to 1 GB is required with a long coverage area of upto 100 km. Commonly used communication methods are optical communication, cellular, WiMAX and satellite communications.

3.2 AMI metering infrastructure

To facilitate the communication between the customers home devices and the utility center, AMI employ a number of different metering devices to ensure the communication flow of the energy related data. There are different AMI metering devices as described in the following section.

3.2.1 Smart Meters (SM)

One of the key component in AMI is the smart meter. Smart meters are solid state programmable devices that communicate with the utility center in a bidirectional way to transmit periodic or on-demand energy consumption readings. The smart meters are located on a consumers premise such as a home or a building, making it vulnerable to physical tampering. The smart meter acts as a gateway between the utility center and the HAN devices. In addition to the periodic or on-demand usage readings, the smart meter is performing a number of tasks such as: time-based pricing, power quality monitoring, meter tampering, energy theft detection, and communications with other intelligent home devices [97].

3.2.2 Other metering infrastructure

Other non-metering infrastructure include [129]:

- *The HAN gateway* It is an interface which communicates with the infrastructure between the Customer domain and the Distribution domain of the Smart Grid.
- *Customer premise display* An interactive interface which presents a customer with the energy usage and pricing data of the premises.
- *Energy management system* The energy management system is an interface to the utility billing and real time pricing programs. It allows easy management of the intelligent appliances enrolled in the pricing programs.
- *Data collector* A data collector aggregate data from multiple sources, i.e. smart meters and forwards it to the utility back office.
- *Metering/billing/utility center* The utility center resides in the Operation domain and is responsible for the metering and billing functionalities.

- *AMI headend* The AMI Headend communicates with other entities in the smart grid such as Meter Data Management System (MDMS) and the AMI network. The AMI Headend communicates bi-directionally with the smart meters to retrieve data and remotely execute commands, firmware updates, configuration updates, control and diagnostics and meter reading retrials in case of failure.
- *Meter data management system (MDMS)* The MDMS store the meter data and makes it readily available for other smart grid entities. The MDMS aggregates, validates, estimates and permits editing of meter data, such as energy usage, generation, and meter logs. An MDMS stores this data for a limited amount of time before it goes to a data warehouse and makes this data available to authorized systems [129].

4 AMI security requirements

For decades, availability of power for a consumer has been a priority requirement in the power grid system. With the integration of information technologies and increased customer participation in efficient energy usage, integrity and confidentiality have become a critical requirement. The NIST recognized six functional and priority areas for smart grid, namely; Electric Transportation, Electric Storage, Wide Area Situational Awareness, Demand-Response, AMI, and Distribution Grid Management. Therefore, the communication requirements and needs were vital to the power grid system depending on their functionalities, infrastructures, and architecture. Unlike traditional IT networks, the AMI has unique security requirements defined by the NISTs Smart Grid Interoperability Panel (SGIP) and has released a detailed guideline for cyber security in smart grid with three high-level security objectives, widely known as the CIA triad [49].

The CIA triad consist of Confidentiality, Integrity and Availability. Confidentiality ensures restricting unauthorized information access and disclosure in a bid to protect personal privacy and proprietary information. For instance, data confidentiality must prevent analysis of consumer’s power usage patterns using Non-Intrusive Appliance Load Monitoring algorithms which can reveal personal activities and customer profiling [102, 141].

Integrity ensures protection against inappropriate information tampering and destruction to achieve information non-repetition and authenticity. Data integrity is a pillar of information security for smart grid systems [101]. For instance, modification of data transferred in the AMI from utility to meter and vice versa, such as pricing information and commands are limited to financial losses and improper power utilization.

Availability of information is an important aspect in smart grid [79]. The goal of availability is to ensure reliable and timely access to and use of information by an appropriate actor. Based on the type of data communicated between the smart grid systems, availability concerns can vary. While dynamic pricing information and meter commands are critical with respect to financial and operational requirements and needs to be transferred in short intervals. On the other hand, availability of meter data may not be as critical as the latter can be collected at bigger intervals.

5 Privacy in AMI

The term privacy conveys numerous ideas such as privacy of belongings, activities, decisional privacy, etc. The form of privacy referred to in this section is the information privacy. More precisely, information privacy concerns an entitys control over the acquisition, disclosure and use of personal information [73, 132]. The ability of an individual to personally control their own information is considered a key ethical and human rights challenge of the information age [92, 116, 118]. Figure 3 shows the four major types of privacy and are described in the following section [59]:

- *Personal information* A formal definition of personal information is as follows Any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or one or more factors specific to his or her physical, physiological, mental, economic, cultural, locational or social identity. Privacy of personal information involves the right to control when, where, how, to whom, and to what extent an individual share their personal information, as well as the right to access personal information given to others, to correct it, and to ensure it is safeguarded and disposed of appropriately.
- *Personal privacy* The right to control the integrity of ones own body. It covers such things as physical requirements, health problems, and required medical devices.
- *Behavioural privacy* The right of individuals to make their own choices about what they do and to keep

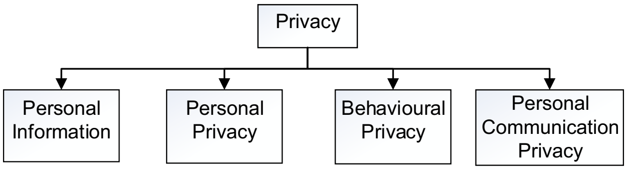


Fig. 3 Privacy in AMI

certain personal behaviors from being shared with others.

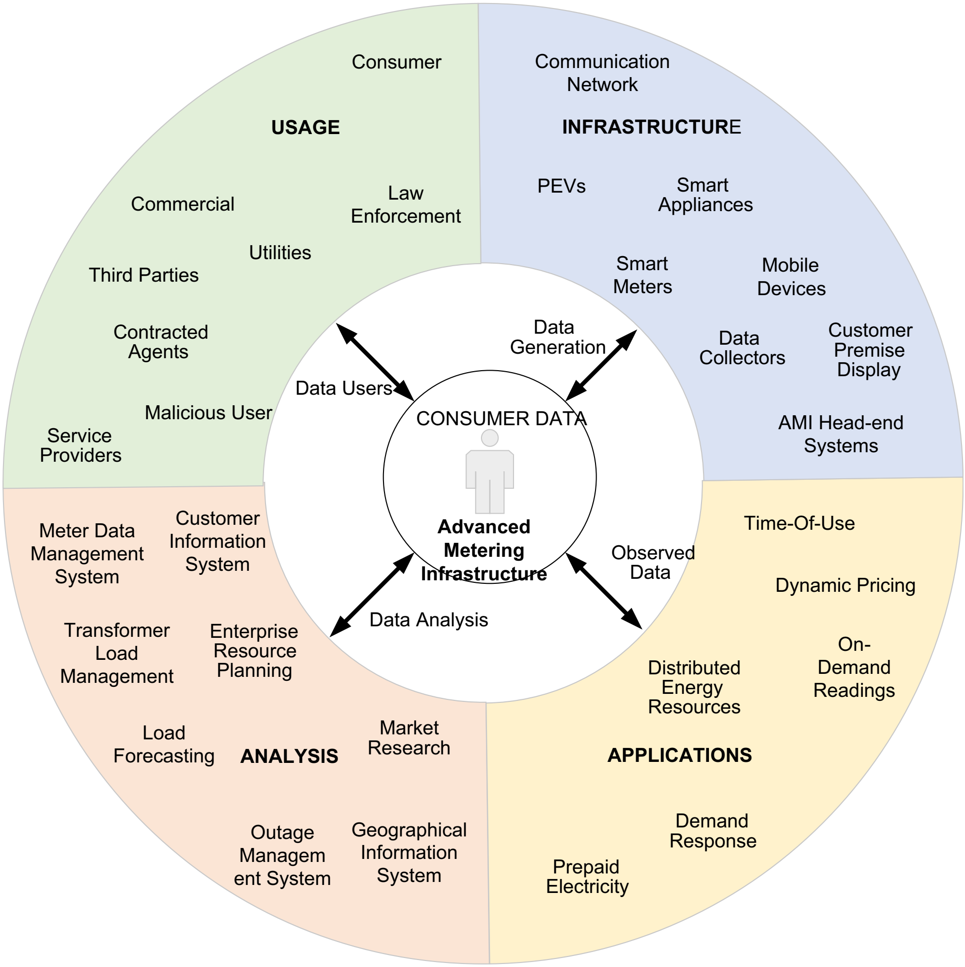
- *Personal communications privacy* The right to communicate without undue surveillance, monitoring, or censorship.

5.1 AMI data environment

There are various types of data in an AMI environment such as energy consumption data, command and control information about the smart grid, and dynamic energy pricing data. The huge amount of data in transit reflects the adoption of AMI in our daily life and its global expansion. Figure 4 shows four phases of key importance to the type of data generated and collected by AMI in Smart Grids.

- *Infrastructure* As mentioned earlier in Sects. 3.1 and 3.2, the infrastructure actors are typically the data generators and collectors in an AMI. Smart Meters are accountable for measuring the real-time energy consumption and communicating energy usage data from the customer premises to utility companies using AMI entities such as data collectors. The fine-grained sensitive data may include customer account number, consent or preferences, device IP address, location information, meter IP address, third party and service provider information, address, billing history, current bill, and presence of distributed energy resources such as on-site generation and storage [88]. Recent research has shown that sensitive information such as types of electrical home appliances used and their usage patterns can be revealed by analyzing the data collected using smart meters [65]. Recent trends in Plug-in Electric Vehicles (PEV) have also increased the potential for privacy concerns of consumer data.
- *Usage* The Usage defines the entities with an interest or concern related to the data generated and collected in the AMI. For instance, utilities can use the fine-grained energy related data to predict load forecasting, dynamic pricing, demand response etc. to efficiently use power consumption. On the other hand, certain regulations may require the utilities be transparent about energy pricing i.e., disclosing information used to set up energy pricing. This may lead to privacy concerns

Fig. 4 AMI data environment



regarding consumer energy usage data which can derive a consumers lifestyle pattern. Similarly, entities such as law enforcement agencies, government and malicious users may misuse the fine-grained data to profile a customer and jeopardize his personal privacy.

- *Analysis* Utilities and service providers use modern data analytics techniques to execute a wide range of decision-making activities such as long-term load forecasting, project financing, and efficient consumer engagement. For example, analysis of the fine-grained data collected by the AMI enable utilities to make important decisions regarding grid optimization, execute demand response programs and provide time-of-use billing with incentives to improve load balancing during peak times. Some of the components of such analysis include [95]:
  - Meter Data Management System (MDMS)
  - Consumer Information System (CIS), Billing systems and the Utility Website
  - Outage Management System (OMS)
  - Enterprise Resource Planning (ERP) Power Quality Management
  - Mobile Workforce Management (MWM)
  - Geographic Information System (GIS)
  - Transformer Load Management (TLM)

  The analyzed data may be used by utilities and service providers to benefit by building effective business strategies and profiling consumer preferences.

- *Applications* One of the key application of AMI is its facilitation of demand-response and dynamic energy pricing. For instance, demand response enables utilities to offer time based pricing such as real-time pricing, time-of-use (TOU) pricing, critical peak pricing, and variable peak pricing to reduce energy consumption without sacrificing consumer satisfaction. Moreover, prepaying of electricity through in-home device may allow access to a customer's financial information. Other applications include DER, on-demand and periodic energy usage readings, prepaid electricity.

Hence, with the amount of fine-grained data collected, processed, and analyzed, the need for addressing the privacy requirements and concerns have become a foremost priority.

5.2 AMI privacy use cases

The NIST report has highlighted over forty scenarios relating to the privacy concerns in smart grid [59]. In this literature survey, we have identified three key scenarios for AMI with potential privacy and security threats that require a high level of data privacy and integrity.

- *Meter information* The meter communicates periodic meter readings, on-demand meter readings, meter configurations and meter logs with the utility in a bi-directional way. The AMI provides an infrastructure for the customers domain devices and utility to communicate this sensitive information. A meter sends an automated power usage information through data collectors or access points to the AMI headend system periodically varying from minutes to hours. The AMI headend forwards the sensitive information to the MDMS which validates and processes the meter data. The information communicated between the meter and the utility has raised concerns regarding the integrity and confidentiality of the customer data. By eavesdropping, relay and man-in-the-middle (MITM) attacks, a malicious user may acquire access to sensitive information such as energy usage pattern for knowledge about peoples presence in their homes or may inject falsified data respectively. Moreover, accumulation of fine-granular metering data at the utility center can be used to obtain useful statistics for business strategies which would be a breach of customers privacy [30, 40, 59, 70].
- *Utility information* The utility back office resides in the Operation domain and is responsible for the various operations such as sending operational commands to meter, non-operational instructions, and batch instructions. The utility center sends the operational commands to Meter Reading and Control (MRC). The Meter Reading and Control (MRC) looks up for the specific meter and forwards the commands to the AMI headend system. The command is further sent to the designated meter and executed. Operational commands include configuration request, calibration request and remote disconnect request. Similarly, the non-operational instructions such as meter calibration, geolocation of meter, meter battery management and connectivity validation and multicasting batch instructions such as firmware updates and key management updates are executed at the meter. The integrity of the metering commands is important depending upon whether the information is sensitive or personally identifiable to the customer. For example, an attacker may use a negative connectivity ping command to trigger an OMS/Workforce Management System request for onsite repairs which requires a customer name and location to schedule a repair. Integrity of meter commands is important to prevent malicious intrusions and breach in privacy of sensitive customer information [29, 30, 59].
- *Real time pricing* The integration of AMI into smart grid has offered advanced capabilities such as demand response to in-home devices. The primary goal is to

provide customers with pricing information for current and future periods depending upon different scenarios such as TOU pricing and critical peak pricing. This has enabled customer to understand and reduce their energy consumption with real-time and historical energy data available on the in-home displays. Moreover, other advanced capabilities such as access to energy usage, DER storage status, prepaying of electricity, and changing energy plans have granted access to different types of customer and energy related information [28, 29, 59, 128].

Although availability is important to provide uninterrupted access, integrity and confidentiality of metering data have a larger impact on the smart grid objective and requirements. Confidentiality and integrity of the sensitive information communicated within the AMI, MDMS and the HAN are critical to avoid potential privacy and legal consequences.

5.3 AMI privacy issues

The Privacy Impact Assessment (PIA) was a comprehensive process of determining the privacy, confidentiality and the risk involved with data collection in the smart grid. While the scope of the PIA may vary in the entire smart grid, the Privacy subgroup conducted a PIA for consumer-to-utility process focusing on the type of information collected and how the information can be exploited. The PIA identified and addressed the Consumer-to-Utility privacy impact assessment with the following questions [59]:

- What personal information may be generated, stored, transmitted, or maintained by components and entities that are part of the smart grid?
- What are the new and unique types of privacy risks that may be created by smart grid components and entities?
- What is the potential that existing laws, regulations, and standards apply to the personal information collected by, created within, and flowing through the smart grid components?
- What could privacy practice standards look like for all entities using the smart grid so that following them could help to protect privacy and reduce associated risks?

The privacy sub-group of the Cyber Security Working Group reporting the following privacy concerns related to the consumer information [59]:

- There is no clear understanding on the privacy issues of the smart grid.
- There is a lack of standards, privacy policies, or procedures by the entities involved in the smart grid and the collection of information.
- Definitions of personally identifiable information are inconsistent in the utility industry.
- Smart meters and distributed energy systems may reveal information about residential consumers and activities within the house.
- Roaming smart grid devices (e.g., electrical vehicle recharging at other charging stations such as a friend's house) may generate more personal information.

With the integration of new technologies, functionalities, and entities into the smart grid, it brings in various types of data collection and data sharing capabilities of the power usage within the grid network which has raised privacy concerns. The recent developments in smart grid and increased functionalities of smart appliances has increased the granularity of the personal information involved. Addressing the vulnerabilities that enable exploitation through the cyber-physical infrastructure has become one of the priority concerns.

With electricity providers having access to consumers' energy usage patterns, the electric information can be used to achieve unfair business strategies ungoverned by appropriate privacy policies. An intruder may modify the current power usage, which may result in providing more energy than its required real-time consumption leading to power wastage. Smart grid requires to collect imperative data from different entities such as transformers, substations and control stations and utility back office for better efficiency and control of power usage and dynamic pricing. However, we focus on the issue of consumer information privacy.

Availability of Smart grid data such as power usage measurements and consumption reporting by individual smart devices has proven to be a new way of obtaining personal information. For example, specific smart appliances and generators can be identified from the energy patterns they generate in the power usage information available at the meter when data collections occur at a higher frequency, unlike traditional monthly smart meter readings for billing purposes. Such data can help in predicting a complete profile of user activities in a consumer premises and provide a basis for forecasting a premise activity such as when the premise was unattended, work schedules and other personal activities.

Moreover, several attacks such as eavesdropping, false data injection, spoofing, etc. have been identified by researchers that may threaten the smart grid operations such as demand-response, load forecasting, automated readings [7, 91, 112].

A typical cyber-physical system attack would involve four steps [56]:

1. Identifying weaknesses in the cyber-infrastructure.
2. Intruding into the system and gaining privileges.

3. Understand and gaining control of the control system.
4. Using the control system to launch physical attacks.

As the AMI networks are vulnerable to cyber-attacks, understanding the potential vulnerabilities of these attacks in AMI is important. Thus, we provide some of the privacy concerns related to the AMI consumer data in the following section and categorize them as shown in Fig. 5 [39, 56]:

- *Consumer identity theft* The combination of sensitive data may be misused to impersonate a utility or consumers, resulting in potentially severe threats. Sensitive data may include customer identification, name and address, financial information such as credit card number and other energy related data such as billing information.
- *Determine personal behavioral patterns and activities* Energy consumption profiles/patterns in the fine-grained metering data directly or indirectly reveal types of activities and living habits which can be used for home invasion etc.
- *Determine PEVs data* Use of PEVs on-board data logistics to determine a customers location, driving pattern and other electricity storage and consumption data.
- *Determine specific appliances used* The appliances used at specific times can be easily inferred by adversaries if they can access the fine-grained consumption data.
- *Perform real-time surveillance* The utilities collect the fine-grained metering data for energy management and value-added services development. If the time interval becomes shorter, the data collection can be considered as the real-time surveillance by potential adversaries.
- *Activity censorship* Residential activities could be revealed by the fine-grained metering data. Such information might be shared with local government, law enforcement, or public media. Then, the residents may be under risk of harassment, embarrassment, etc.
- *In-home device portal exploitation* The consumer uses in-home device to purchase or prepay for electricity based on dynamic pricing. The frequent collection of data between the in-home device and the utility can reveal sensitive information.

6 AMI privacy related works

The privacy concerns of the fine-grained sensitive energy related data have motivated several researchers to propose new privacy preserving approaches for the AMI. These privacy preserving approaches are classified into two categories: Non-Cryptography based and Cryptography based privacy preserving schemes as shown in Fig. 6 [85, 106].

Figure 7 refers to the recent trend in the number of privacy preserving schemes published by researchers from 2011 to 2017. The graph shows the number of papers published per year mainly focusing on preserving privacy of the consumer's energy consumption data. This renewed attentiveness is due to recent country-wide roll outs of smart meters and its privacy concerns [124].

6.1 Non-cryptographic approach

These approaches make clever use of non-cryptographic techniques to obfuscate the actual energy usage of a consumer. There are mainly two non-cryptographic

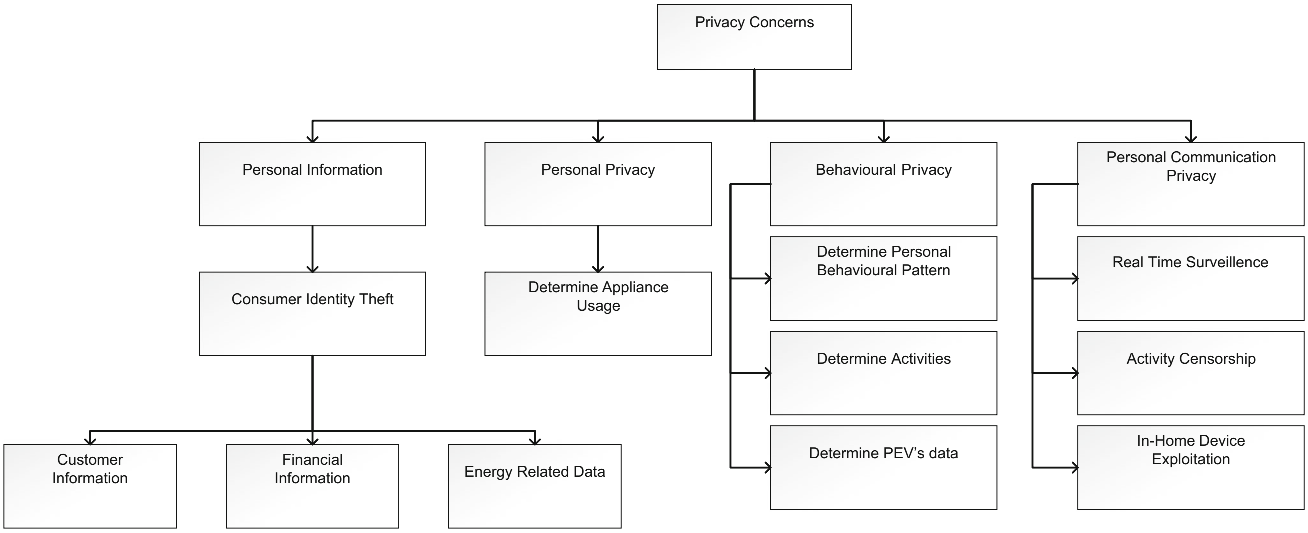


Fig. 5 Privacy concerns

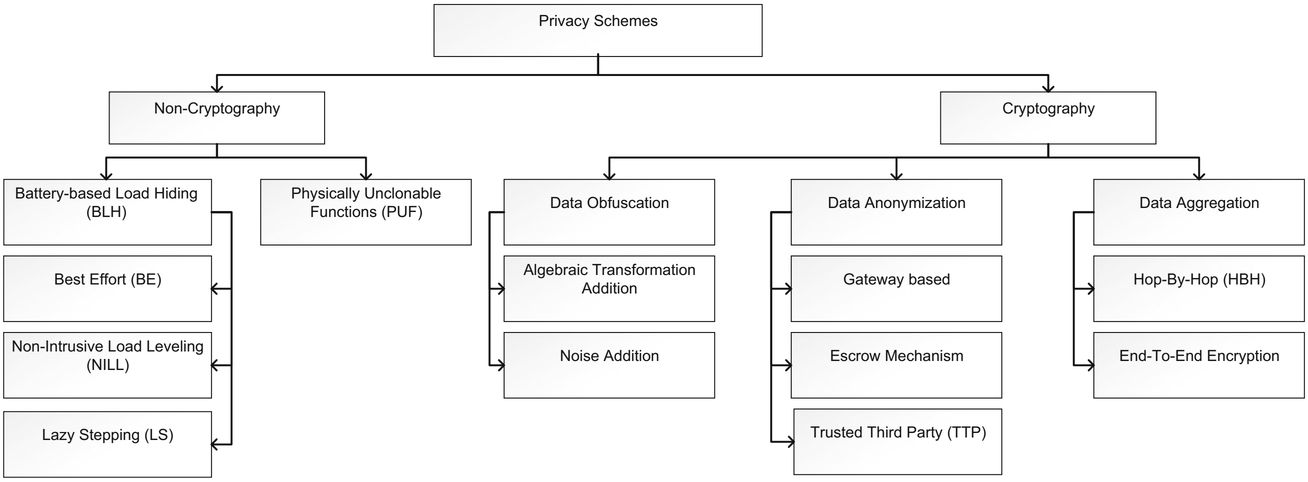
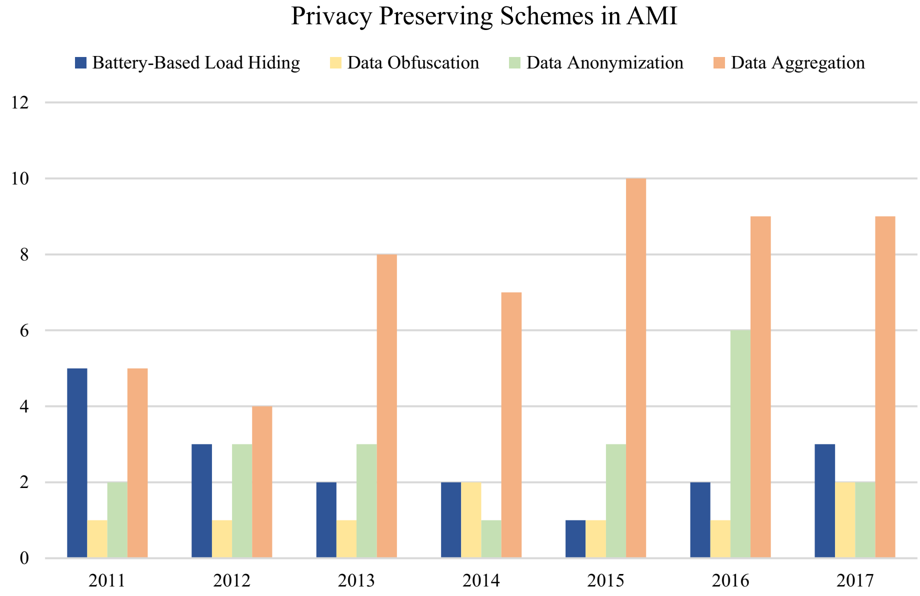


Fig. 6 Related work hierarchy

Fig. 7 Privacy preserving scheme analysis



approaches: Battery-based Load Hiding (BLH) and Physically Unclonable Functions (PUF) based.

As presented in Table 1, we have categorised the non-cryptography approach into the following categories.

6.1.1 Battery-based load hiding (BLH)

The first category of non-cryptographic approach is Battery—based Load Hiding (BLH). The BLH is a well-known approach which uses a rechargeable battery to partially supply the energy demand to manipulate meter reading in order to hide the actual energy consumption. Several BLH methods or algorithms have been recently proposed which include the Best Effort (BE) scheme [72], the Non-Intrusive Load Levelling (NILL) scheme [93] and the Lazy Stepping (LS) scheme [139] as shown in Table 1.

Koo et al. [75] proposed a Reinforcement Learning (RL) based BLH approach to preserve privacy for high-frequency and low frequency variation data. The RL–BLH algorithm learns a decision policy for choosing pulse magnitudes on the fly without prior knowledge of usage pattern. In the proposed scheme, a Q-Learning method is used to maximize the cost saving by charging the battery when the time-of-use pricing is low. Moreover, the proposed scheme uses artificially generated data to reduce the time taken to converge to an optimal policy. However, Reinforcement Learning do not estimate the actual input/output characteristic but only the desired probabilistic behaviour.

Chin et al. [26] proposed an energy management method scheme. The scheme uses Model Predictive Controller (MPC) with local energy storage devices to reduce the

Table 1 Non-cryptographic privacy preserving schemes

Author	Approach	Method	Pros	Cons
Koo et al. [75]		Reinforcement learning based algorithm	Achieves consumer privacy Energy cost saving	Estimate only the desired probabilistic behaviour
Giaconi et al. [55]		Renewable energy source (RES) with battery	Minimize energy consumption data leakage	Energy consumption leakage Wasted energy
Zhao et al. [143]		Multitasking-BLH-exp3 algorithm	Efficient and effective compared to Yang et al. (2012) Successfully assures differential privacy	Requires smart appliances connected to the battery
Backes and Meiser [10]		Integrated noise cascading method	Retains differential privacy	Effects battery life-time Requires additional battery Noise measured as energy consumption
Sankar et al. [105]		Distortion to quantify trade-off and interference-aware reverse waterfilling to achieve it	Novel utility privacy trade-off	No algorithmic approach provided for implementation Complex approach
Yang et al. [139]	Battery-based load hiding (BLH)	Lazy stepping algorithm	Prevents load change recovery attacks	Lack differential privacy Lack well defined privacy measuring metrics Less efficient compared to Zhao et al. [143] Only edge detection based NILM method attacks considered
McLaughlin et al. [93]		Non-Intrusive load levelling algorithm	Soothes energy usage transitions sensed by the smart meters	Load peak leakage Limit appliance-level load control Lack differential privacy Only edge detection based NILM method attacks considered
Kaloghdis et al. [72]		Best effort and power mixing algorithm	Achieves privacy in individual home load signature events	Load peak leakage Lack differential privacy Lack well defined privacy measuring metrics Only edge detection based NILM method attacks considered
Alam [6]	Physical unclonable functions (PUF)	Physical unclonable functions (PUF) and channel status information (CSI) technique	Achieves CIA for fine-grained sensitive data	Extra integration of PUF component Dependence on PUF for integrity and authentication

information leak and energy cost for a consumer. The MPC is an advanced control technique used to minimize the energy consumption cost in a dynamic pricing environment and reduce information leak using mutual information. This is done by predicting the effects of the controllers actions on the statistics of the consumer load and that seen by the grid using counting, and solving a Mixed-Integer Quadratic Program problems for every new meter readings available. The MPC also enables the batteries to charge during a lower pricing period to accommodate the consumer load during a higher pricing period. Although the scheme reduces the information leakage, the reduction is achieved at an expense of increased energy cost. Moreover the scheme is computationally not scalable due to use of prediction horizon and discretization levels of load.

Giaconi and Gunduz [55] proposed a scheme to address the smart meter (SM) privacy concerns using renewable energy source (RES) and a battery to partially hide the consumption pattern from the utility provider. The proposed schemes uses information theoretic approach to minimize leakage of consumers energy consumption data to the utility provider as well as the energy generated by the RES. The scheme defines the privacy problem as a Markov Decision Process (MDP) in order to optimize the energy management policy using dynamic programming. The energy management policy is responsible for requesting the amount of energy required by the utility provider at a specific time which results in information leakage. Therefore, the information leakage rate problem is presented in an additive form and is further solved numerically to identify an optimal leakage rate for the scenario where the utility provider knows the realization of RES. However, renewable energy is wasted when the battery is maximally charged or the required energy load is smaller than the generated energy.

Zhao et al. [143] proposed a randomized Battery-based Load Hiding (BLH) algorithm which ensures differential privacy. They further proposed a Multitasking-BLH-Exp3 algorithm which uses binomial distribution to add noise. The proposed algorithm adaptively updates based on the three defined context which are: energy stored at the battery, batterys energy consumption and appliances energy consumption. The algorithm also takes the constraints of these three context into account while updating the distribution. The scheme is more efficient and effective as compared to existing BLH methods in [72, 93, 139]. However, such approach can only be applied with the help of a battery, which are expensive, limited lifetime and require considerable installation and maintenance costs [107].

Backes and Meiser [10] proposed a battery based method which hides sensitive power consumption information by adding or subtracting noise, i.e. increasing or decreasing power consumption. The scheme also proposed an integrated noise generation via cascading method for on-the-fly battery recharge to retain differential privacy [36]. The noise generation via a cascading method uses the amount of recharged energy as a function. This function is made differentially private by adding noise. Although the scheme achieves differential privacy, the noise generation impacts the battery life, i.e., in practice the battery life gets reduced. The author also assumes that a secondary battery is used solely for recharge purpose, not known to the adversary. Thus the proposed scheme requires installation of two expensive batteries to achieve the desired privacy. Moreover, the scheme considers the addition of the energy consumption as an overall energy consumption, which is measured by the smart meter.

Sankar et al. [105] presented with a new framework that abstracts both the privacy and the utility requirements of smart meter data using tools from information theory and a hidden Markov model for the measurements. The proposed scheme addresses the utility privacy tradeoff which results from hiding of data for privacy purpose and sharing of data with utility for a legitimate objective. The author uses the encoding scheme based on rate distortion theory [15] to determining the minimum rate at which the data can be compressed for a desired distortion level to achieve minimum information leakage. The method presents a general approach to time series data perturbation using a battery i.e., the data perturbation cannot be eliminated by averaging. The scheme exposes high power, but less private appliance information and filters out components with a lower power to distortion threshold. However, this proposal is only limited to a framework proposal and an algorithmic approach is not detailed enough to implement it [130].

Yang et al. [139] proposed a novel stepping-based framework which prevents precise load change recovery attacks. In this scheme, four algorithms were implemented in a stepping approach to make the value dimension more coarse-grained via quantization. The authors proposed mutual-information based measurements to evaluate the algorithms in comparison with [72] and [93] (see Table 1).

McLaughlin et al. [93] proposed a Non-Intrusive Load Levelling (NILL) method to combat consumer privacy invasion using an in-residence battery. The NILL method ensures privacy by removing most of the energy usage transitions sensed by the smart meters by masking the variance in load. These energy usage transitions are load events that reflect appliance activities caused by often short-lived heavy power loads. Thus the consumers energy usage profiles revealed by NILL are futile to the NILM algorithms. However, these schemes do not work during peak voltages as explained in [139].

Kalogridis et al. [72] proposed a Best Effort scheme. The proposed scheme uses a rechargeable battery in a power management model. The scheme also proposed a power mixing algorithm and evaluated its protection levels using different privacy metrics, including relative entropy, clustering classification and correlation/regression. With regards to privacy, their technique manages to hide the home load signature, which comprises of individual consumption events. The rechargeable battery is used to fill the difference between the consumers real energy consumption and a constant meter load. Unfortunately, BE scheme may expose the customers privacy due to the capacity constraints and charging-discharging rate of the batteries. In the process of maintaining a constant load, a battery may overcharge or cause the batterys state of charge to be low or discharge completely. This results in a notable load change leaking the load-change information. Moreover, the scheme is vulnerable to attacks that leak appliance events. These attacks are based on peak load reduction and moderation algorithms which are aimed for load shifting in peak demands and on an event of a high demand load that are beyond a batterys discharge rate to maintain a constant meter load [139].

Thus, BLH approaches limit the ability of the smart grid to provide appliance-level load control and the focus is generally limited on preventing NILM attacks which deduce individual device usage from the energy consumption data with the help of load signature libraries [35, 81, 86, 136]. The BLH are also expensive and frequent charging and discharging reduces their lifespan, which make it less than ideal to both the utility company and the consumer.

6.1.2 Physically unclonable functions (PUF)

The second category of non-cryptography approach is the Physically Unclonable Functions (PUF). PUF devices are low-cost to manufacture and provide hardware based authentication and integrity mechanism resistant to impersonation attacks. The PUF is used to achieve consumer privacy by using the one-way functions embodied in the physical structure. PUFs generate random signatures based on the complex physical characteristics. The main properties of PUFs are unclonable and unpredictable.

Alam [6] proposed the use of hardware and physical layer approach. The proposed approach uses PUF to achieve integrity and authentication and Channel Status Information (CSI) technique for confidentiality of fine-grained sensitive data in Advanced Metering Infrastructure (AMI). However, the proposed scheme focuses only on data between the smart meter and the data collector and requires extra integration of expensively manufactured PUF component for integrity and authentication.

6.2 Cryptographic approach

The second approach in privacy is the Cryptographic approach. The Cryptographic approach can be defined as a way to limit the information that is leaked by the distributed computation to be the information that can be learned from the designated output of the computation [111]. The Cryptographic approach is smart grid is divided into three categories: Data Obfuscation, Data Anonymization, Data Aggregation Furthermore, from the literature we have identified the Pros and Cons of the current existing work using these cryptographic approaches in the Tables 1, 2, 3 and 4 to help understand researchers, the privacy preserving issues and concerns. In the following sections, we discuss the above three cryptographic approaches in detail.

6.2.1 Data obfuscation

Data obfuscation provides a unique opportunity to mask the original energy consumption data by applying random noise [131] or by using an appropriate algebraic transformation on the fine-grained energy usage data [19]. Table 2 lists a number of data obfuscation methods and highlights their comparative advantages and disadvantages.

Guan et al. [61] proposed utility-privacy trade off scheme based on random data obfuscation. In the proposed scheme, random data-obfuscation generated by the Laplace distribution [76] are used to mask the real-time data. The scheme uses data aggregation using homomorphic encryption and uploads the summation of the collected smart meter data to the control center. In case of a malfunctioned smart meter, there might be loss of data resulting in wrong data aggregation. Therefore, the scheme provides fault tolerance as the random obfuscation values are mutually independent and obey Laplace distribution. The proposed scheme balances the utility-privacy trade off on two metrics namely; the signal-to-noise ratio to quantify the level of utility and information entropy for level of privacy. However, the proposed scheme adds a Key Initialization Center (KIC) to the system model which initializes keys to smart meters and the control centres and has higher error rate than Privacy Preserving and Multifunctional Health Data Aggregation with fault tolerance (PPM–HAD) [64]. Moreover, in the proposed scheme, KIC uses Paillier encryption to generate encryption parameters for all the smart meters and the control center which is computationally expensive.

Tonyali et al. [125] proposed a data obfuscation approach to preserve consumer privacy and simultaneously perform distribution state estimation. In this scheme, the AMI network gateway computes the obfuscation vectors. The gateway multiplies the vector with a random number and distributes it to the smart meters using a shared key. The proposed scheme provides consumer data privacy and supports distributed state estimation and third-party billing. The author has also assessed the impact of this approach using metrics such as goodput delay and packet delivery ratio. The proposed scheme assumes only a single gateway which is not be feasible in large AMI network. On the other hand, dividing the AMI network into multiple clusters of smart meters and the distribution of obfuscation value in a cluster of smart meters is not efficient in terms of computation and transmission. Moreover the proposed scheme uses multiple gateways to distribute obfuscation value. Therefore a single compromised gateway may affect the distribution of obfuscation values to other gateways and

Table 2 Privacy preserving data obfuscation schemes

Author	Method	Pros	Cons
Guan et al. [61]	Utility privacy trade-off scheme based on random data obfuscation	Balances the utility-privacy trade off Efficient in computational cost than Han et al [64]	Addition of KDC Higher error rate than Han et al [64]
Tonyali et al. [125]	Gateway based	Provides consumer data privac Supports distributed state estimation and third party billing	Single gateway assumption Smart Meters clustering and vector distribution not efficient in terms of computation
Beussink et al. [17]		Prevents eavesdropping Supports distribution state estimation and billing	End-to-end delay Decreased throughput No comparison with other schemes
He et al. [69]	Use of random noise to distort data	Supports power demand analysis and prediction Supports privacy preserving billing operations	Original data reconstruction is difficulties Lacks billing accuracy
Kim et al. [74]	Error-free state estimation technique	Supports distributed state estimation No additional energy management facility	Less privacy guarantees Additional communication overheads No bad data detection analysis

hence result in modification of the final obfuscated meter readings. The scheme also does not consider the data falsification/injection issues.

Beussink et al. [17] presented a data obfuscation scheme for preserving consumer privacy in a 802.11s-based smart grid AMI. In the proposed scheme, the gateway is responsible for distributing the obfuscation values to the smart meters. The smart meter calculates its obfuscated power measurements and sends it to the gateway. The gateway verifies the measurement using the digital signatures and the timestamp. The gateway forwards the measurements to the utility center. The scheme supports distribution state estimation and billing operations and also achieves consumer privacy. However, the crossing of obfuscation values from gateway to the smart meters increases the traffic which increases the throughput and end-to-end delay for the proposed scheme.

He et al. [69] proposed a distortion-based privacy-preserving metering scheme that protects a customers privacy. In this scheme, a random Gaussian noise is added to the consumers energy consumption data. Further an efficient algorithm is proposed to remove the random noise for power demand analysis and prediction. The scheme also supports privacy preserving billing operations. Although the scheme conserves the computation abilities, it suffers from difficulties in reconstructing original data and billing inaccuracy [2].

Kim et al. [74] proposed a scheme which obfuscate privacy-prone data using error-free state estimation technique. The scheme selects a lead meter which generates obfuscation vectors and sends it to other meters. Each meter then generates an obfuscation measurement which are sent to a third party to generate state estimators. The state estimators are further forwarded to the utility provider to estimate distributed state estimation. The proposed scheme requires more rigorous privacy guarantees and statistical methods to determine the obfuscated meter datas indistinguishable level. Moreover, the scheme requires bad data detection analysis as there is significant meter data modification and suffers additional communication overheads.

6.2.2 Data anonymization

The second approach in cryptography privacy preserving scheme is data anonymization. The key purpose of anonymization is to separate the customers identity from the energy consumption data [119, 142]. The idea is utilities will receive enough information to compute required information but not enough to associate the data with a specific meter or a user. These approaches can also be implemented using an additional trusted infrastructure [3]. Table 3 summarizes the Pros and Cons of the current related work on the data anonymization approach.

Afrin and Mishra [3] proposed an anonymized authentication framework that consists of an authentication scheme to protect unauthorized data access and an anonymization scheme to achieve privacy. The framework is designed to prevent service providers from correlating different types of data from a smart meter and avoid single

Table 3 Privacy preserving data anonymization schemes

Author	Method	Pros	Cons
Afrin and Mishra [3]	Anonymized authentication Framework	Different types of data service Reduced single point of failure	Single point of failure The trustworthiness concern of a trusted third Party (TTP)
Afrin and Mishra [4]	Collaborative Anonymity Set Formation (CASF) method	Enhanced privacy against any internal and external adversaries	Increase in additional communication overhead with increase in smart meters collaboration
Ambrosin et al. [8]	Collaborative smart meter (SM) protocol using a random multi-hop path	Guarantees authentication and integrity Tamper proof device	Knowledge of the permanent IDs in VC Susceptible to man-In-the-middle (MITM) attack Computationally intensive
Gong et al. [57]	Privacy-preserving scheme for IDR	Computes individual incentive-basec rewards Preserves consumer privacy	Consist of a semi-trusted Proxy, a gateway or Trusted third party (TTP) for anonymization
Bao and Chen [13]	Pseudonym identity-based privacy-preserving report approach	Efficient computation and communication overhead	Insider attacks are not considered
He et al. [67]	AKD scheme using ECC	Efficient computational cost Efficien communication cost Resistant to various attacks	High assumptions are needed to understand the implementation
Rahman et al. [103]	IDR systems using cryptographic primitives	Supports incentive-based demand response (IDR)	No performance analysis No comparison with other schemes
Diao et al. [31]	Anonymous credentials using Camenisch–Lysyanskaya (CL) signature	Authenticated energy consumption readings	Ability of tracing faulty smart meter is inefficient
Finster and Baumgart [46]	Peer-to-peer protocol allowing	Anonymizing metering data Supports distributed state estimation	Billing operations not considered
Finster and Baumgart [47]	Pseudonymous smart metering protocol without trusted third party (TTP)the metering data	Lightweight anonymity network	Requires the absence of bidirectional metering communication Computationally expensive
Stegelmann Kesdogan [117]	K-Anonymity using pseudonyms	Achieve K-anonymity of smart meters	Reveals energy consumption readings
Cheung et al. [24]	Anonymous credential using Blind Signature		Distributed state estimation service not considered
Chim et al. [25]	Privacy-preserving authentication scheme (PASS) scheme	Tamper resistant HMAC based authentication Packet filtering	Device dependent pseudo identities generation Transmission delay when under attack
Bohli et al. [18]	Gaussian noise addition to metering data	Energy consumption privacy preservation	Inaccurate aggregated reading Easy to recover actual readings Smart Meters report erroneous outputs
Efthymiou and Kalogridis [37]	Securely anonymizing data and using a TTP Escrow mechanism for authentication	Supports billing and distributed state estimation using a TTP Escrow mechanism for authentication	Single point of failure The trustworthiness of the trusted service Data mining reveals usage patterns
Fhom et al. [45]	User centric privacy protection scheme	User control their privacy through a privacy manager	Use of trusted third party as privacy manager

point of failure. The scheme achieves the desired level of consumer privacy. However, the scheme has reduced single point of failure. The trustworthiness concern of the Anonymizer (AN), electricity supplier (ES) and the Data Collector (DC) colluding has not be considered. Moreover,

Table 4 Privacy preserving data aggregation schemes

Author	Approach	Method	Pros	Cons
Yan et al. [137]		IAC protocol	Efficient in terms of end-to-end delay and packet loss	Malfunctioning node not considered Energy efficiency issue not considered
Bartoli et al. [14]	Hop-By-hop	Aggregation using the concatenation operation	End-to-end security	Additional overheads No notable bandwidth saved High drop rate in lossy channel
Tonyali et al. [126]		FHE or randomly generated polynomial (secure MPC)	Preserves the actual meter readings	Significant data size and high delay
Badra and Zeadally [11]		Symmetric homomorphic encryption and key exchange methods	Low transmission and message overheads Resiliency against numerous attacks	High DH exchange and computation time
Li et al. [84]		PPMA scheme	Guarantees the privacy of individual	Dynamic pricing not supported Malfunctioned smart meters not considered High complexity
Wang [135]		Identity based data aggregation protocol	Achieves identity based signature with an aggregation	High performance cost
Ford et al. [50]		Novel data aggregation protocol for secure and efficient communication	Supports time-of-use billing Achieves desired confidentiality, integrity and consumer privacy	Assumption of TTP and UC won't collude
He et al. [68]		Lightweight data aggregation using ECC	Thwarts internal attacks and external attacks Achieves confidentiality, integrity and authentication	Higher computation cost compared to [118] Consist of aggregator and a trusted third party (TTP) Power consumption readings known by aggregator
Shen et al. [113]		Efficient privacy-preserving Cube-data aggregation	Efficient in terms of communication costs and scalable	Higher computational cost Additional pairing operation
Ferrag [43]		Bilinear pairing identity-based encryption	Achieves data and gateway privacy. Prevents data replay, modifcation, man-in-the-middle and Sybil attacks	False data injection attack not considere Partially resilient to collusion and diction attack
Bae et al. [12]		PECA	Privacy with user-specific DR services	High computational overheads High communication overheads
Abdallah and Shen [1]	End-to-end encryption	Lightweight lattice-based homomorphic cryptosystem	Prevents replay attacks and ensures data integrity	High computational cost compared to [125]
He et al. [66]		Privacy preserving data aggregation scheme against internal attackers	Efficient computational cost	Energy cost privacy not considered Location privacy not considered
Lu et al. [90]		Set-based aggregation approach	More fine-grained data aggregation result Efficient in terms of computational and communication costs	Lacks data integrity
Tahir et al. [121]		Set-based aggregation approach with data integrity	Ensures data integrity	Suffers additional overheads
Shi et al. [114]		Diverse grouping-based aggregation protocol	Supports data aggregation with error detection	Complex implementation Only malicious data mining attack is considered
Li et al. [82]		Dual-functional aggregation scheme based on Lattice Cryptographic technique	Efficient computational cost Efficient in communication overhead	Only plaintext-attack considered No comparison analysis with other schemes Internal attacks not considered
Chen et al. [23]		PDAFT	Supports fault tolerance	Lacks computation cost analysis High complexity

Table 4 (continued)

Author	Approach	Method	Pros	Cons
Jia et al. [71]		Data aggregation for time-series data	Supports high frequency metering data	Low frequency metering data not supported
Lu et al. [89]		EPPA	Resist various threats Less computation and communication overhead	Unchanged session keys Internal attacks not considered User data exposed
Garcia and Jacobs [52]		Paillier encryption on Additive Sharing	Notable leakage detection	High communication overhead Expensive encryption Non-scalability

the proposed scheme does not consider any external privacy attacks.

Furthermore Afrin and Mishra [4] proposed four variants of a distributed anonymization method for smart metering data privacy, referred to as the Collaborative Anonymity Set Formation (CASF) method. The proposed scheme adopts the network setup with an Anonymizer (AN) as mentioned in [3] from Table 3. The Anonymizer performs the anonymization and provides pseudonyms to the smart meters. The proposed scheme provides enhanced privacy against any internal and external adversaries. However, in the proposed scheme, due to the CASF request circulation and signing of pseudonym, additional communication overhead is incurred which increases with the number of collaborating smart meters. Also, the scenario of duplicate CSAF request is not considered.

Ambrosin et al [8] presented an anonymously fine-grained meter data collection scheme. A collaborative Smart Meter (SM) protocol anonymously transmits metering data to a Meter Data Management System (MDMS) using a random multi-hop path. The scheme also guarantees authentication and integrity of metering data via a group key using hash-based message authentication code (HMAC) [77]. The metering data is encrypted using the public key of the utility. Also, a tamper proof device is equipped at each meter to secure the keys. The scheme consists of Trusted Third Party (TTP) entity such as a Verification Centre (VC) responsible for proper functioning of Smart Meters (SM) which has knowledge of the permanent IDs assigned to the Smart Meters (SM). Also, the Smart Meters (SM) share symmetric keys using Diffe-Hellman Key exchange [21] which is easily susceptible to Man-In-The-Middle (MITM) attack and are computationally intensive.

Gong et al. [57] proposed a privacy-preserving scheme for Incentive-based Demand Response programs in Smart Grid (SG). The proposed scheme enables the provider to compute individual incentive-based rewards while simultaneously preserving consumer privacy by anonymizing fine-grained energy usage data. The scheme consist of a semi-trusted Proxy, a gateway or Trusted Third Party (TTP) entity responsible for anonymization of the metering data. Similarly, Tan et al. [123] proposed a pseudonym-based privacy-preserving scheme reassuring privacy, integrity, and authenticity in AMI [44].

Bao and Chen [13] presented an efficient pseudonym identity-based privacy-preserving report approach for the control center to obtain the fine-grained usage data of all the users while protecting user's privacy. Data integrity is achieved using hash tree-based mechanism. The scheme is efficient in terms of computation and communication overhead. However the scheme does not prevent insider attacks.

He et al. [67] preserves consumer privacy in the proposed AKD scheme using the elliptic curve cryptography. The AKD scheme is efficient in terms of computation cost and communication cost compared to the scheme presented in [127].The AKD scheme is resistant to impersonation attack, replay attack, modification attack, and man-in-the-middle attack, but many assumptions are needed in order to understand the implementation.

Rahman et al. [103] proposed a private and secure bidding protocol for incentive-based demand-response systems using cryptographic primitives to achieve anonymity. However, the scheme lacks performance analysis and comparison with other schemes.

Diao et al. [31] proposed a privacy preserving scheme based on linkable anonymous credentials using CamenischLysyanskaya (CL) signature [132]. Timely-based credentials are used by the Smart Meter (SM) to transmit energy consumption readings. The data collectors use credentials from the center to verify the meter signature. The energy consumption readings are authenticated using the CL signatures. However, the proposed scheme does not have the ability to trace faulty smart meter is an efficient way.

Finster and Baumgart [46] proposed a peer-to-peer protocol allowing near real-time smart metering and simultaneously preserving the consumer privacy. The privacy of consumers is preserved by anonymizing metering data within small, peer-to-peer random groups of smart meters. The proposed scheme does not consider billing operations of Advanced Metering Infrastructure.

Finster and Baumgart [47] proposed a pseudonymous smart metering protocol that does not require a Trusted Third Party (TTP). The scheme enables authenticated and anonymous pseudonyms and negates the risk of transmitting pseudonymized data using a lightweight anonymity network. However, the scheme requires unidirectional communication i.e. a peer-to-peer overlay network with probabilistic forwarding. Therefore the control center does have the functionality of acknowledging or answering the messages received. The algorithms require computationally expensive public key operation for each round of data transmission [3]. The scheme also lacks comparison on communication overhead with other Trusted Third Party (TTP) solutions.

Stegelmann and Kesdogan [117] proposed using a trusted data aggregator to collect energy consumption data from the Smart Meters (SM). K-anonymity is achieved using pseudonyms which prevent service providers from identifying specific meters. However, the individual energy consumption readings become known to the data aggregator, which can be compromised to access unprotected data.

Cheung et al. [24] presented a privacy preserving scheme using anonymous credential under the principle of bling signature. In this scheme, a customer generates a set of credentials and blinding factors which are signed by control centers private key. When the customers need more power, they send a credential to the control center anonymously and the control center will adjust the power for the area where the customer is located. However, the distributed state estimation service is not taken into consideration.

Chim et al. [25] presented a Privacy-preserving Authentication Scheme (PASS) scheme which addresses the privacy concern using tamper-resistant device and pseudo identities. The authentication process is carried out using of Hash-based Message Authentication Code (HMAC). The generation of pseudo identities depends on the lifespan of the tamper-resistant devices in each smart appliance. The scheme also suffers transmission delay when under attack due to the authentication and filtering of packets.

Bohli et al. [18] presented two design solutions to provide privacy with and without a Trusted Third Parties (TTP). The proposed scheme adds Gaussian noise to each smart meter in a bid to prevent from acquiring real energy consumption patterns. The proposed scheme has several issues such as a substantial amount of smart meters are required to ensure the accurate aggregated reading and protect the privacy of individuals, it is easy to recover true readings because the Gaussian noise added to each smart meter follows the same distribution and approximately half of the smart meters report erroneous outputs [133].

Efthymiou and Kalogridis [37] proposed a scheme to securely anonymizing frequent energy consumption data sent by a smart meter using a third-party escrow mechanism for authentication. Every Smart Meter (SM) has two integrated pseudonyms for monthly billing data and fine-grained data respectively. The Energy Supplier (ES)/Utility Back Office is associated with the pseudonym for monthly billing. The Trusted Third Party is well-known with the association of the two pseudonym pair for authentication purposes. The use of an escrow mechanism or TTP has several problems such as single point of failure, the trustworthiness of the trusted service and the data can mined for usage patterns because of the pseudonym ID.

Fhom et al. [45] proposed a user-centric privacy protection scheme which allows entities to control their privacy through a privacy manager who supports pseudonymity and data masking. The user can control his privacy preferences using a subset of infrastructure wide security policies.

6.2.3 Data aggregation

The third approach in privacy preserving cryptographic scheme is data aggregation. The basic idea behind data aggregation technique is to use aggregators in the network to concatenate and summarize data packets from several devices using functions such as sum or average. Although data aggregation reduces data transmission, it has privacy issues as the aggregation operation requires access to plaintext data. In Table 4, we have highlighted two common privacy preserving data aggregation methods namely: Hop-By-Hop [99] and End-to-End Encryption [104]. Table 4: Start of privacy preserving data aggregation schemes.The different research work outlined in Table 4 is discussed below.

Hop-by-hop concatenation In Hop-by-Hop data aggregation protocols, secure data aggregation is achieved in a hop-by-hop manner. For instance, data aggregators decrypts every message received from his neighbouring nodes. Then an aggregation is performed according to an aggregation function, and the aggregated result is encrypted forwarding it to the next node or aggregator. In Hop-by-

Hop data aggregation protocols, the aggregators share keys with their neighbouring nodes. Therefore aggregators cannot provide data confidentiality i.e. the sensitive data in transit can be revealed at every intermediate nodes. Thus hop-by-hop aggregation represents a weaker model to preserve consumers data privacy [33, 98, 144].

Yan et al. [137] presented a new protocol, Integrated Authentication and Confidentiality (IAC), to provide efficient secure AMI communications. The scheme uses hop-by-hop data aggregation and forwarding approach for efficient system security by grouping intermediate nodes. The scheme uses message authentication and encryption to achieve data integrity and confidentiality. The scheme does not consider the malfunctioning of intermediate nodes which may jeopardize transmission. The proposed protocol is also vulnerable to replay attack and forgery attack and compromising of one node will risk the whole network as the intermediate node share the same secret key.

Bartoli et al. [14] proposed a scheme to aggregate encrypted packets at an aggregator by using the concatenation operation. In the proposed scheme, a shared key and a Message Integrity Code (MIC) is used between the smart meter and the utility to provide end-to-end security. The second key is used by the aggregator and its parent node for Hop-By-Hop authentication. Although the protocol provides end-to-end security, it incurs additional overheads. The protocol does not save notable amount of data bandwidth as the saving occurs only on the head count. Also, due to the large size of the data packets, the drop rate is higher in lossy channel.

End-to-end encryption In the end-to-end secure data aggregation protocols, intermediate nodes aggregate data directly without decrypting the received data. The intermediate node apply an aggregation function on the data without decryption as they do not have access to the keys shared between the data originators. Aggregation of end-to-end encrypted data is possible using homomorphic encryption as the most commonly used encryption scheme as shown in Table 4. Even though the data is captured, an adversary cannot get the original information [94, 98, 144].

Tonyali et al. [126] proposed a secured privacy preserving protocol for smart metering systems. The proposed protocol hides the sensitive metering data using Fully Homomorphic Encryption (FHE) [53] with a randomly generated polynomial (secure MPC). Instead of using a single gateway for aggregation, the proposed scheme uses multiple aggregating smart meters who aggregate data received from a small group of meters. The aggregation at smart meters is done using a packet reassembly protocol. The encrypted data is aggregated using a hierarchical manner and without revealing the actual meter readings. However, FHE requires lattice-based cryptosystem which is very complex. Thus implementing a lattice-based cryptosystem requires significantly high and complex computations and ciphertext sizes.

Badra and Zeadally [11] proposed an efficient, lightweight privacy-preserving data aggregation approach that makes use of symmetric homomorphic encryption and DiffieHellman (DH) or Elliptic Curve DiffieHellman (ECDH) key exchange methods. Due to the implementation of DiffieHellman key exchange [21], the frequent key update makes the scheme expensive in terms of overhead and computation time.

Li et al. [84] proposed a privacy-preserving multi-subset data aggregation scheme, PPMA, in smart grid. PPMA can aggregate users electricity consumption data of different ranges respectively, while guaranteeing the privacy of individual users using the Paillier cryptosystem [100]. However, the scheme does not consider malfunctioned smart meters and does not support dynamic pricing.

Wang [135] presented an identity-based data aggregation protocol for the smart grid, which prevents unauthorized reading of fine-grained data and its analysis. The protocol is based on identity-based encryption and signature scheme [110], in which an additive homomorphic identity-based encryption scheme is combined with an identity-based signature scheme with an aggregation property. The identity-based protocol is costly in terms of performance because of the pairing operations that have to be used to deal with the identities.

Ford et al. [50] proposed a protocol for secure and efficient communication of energy consumption data. The protocol supports time-of-use billing and data mining for sensitive fine-grained measurements. Fine-grained data are encrypted by the smart meter and anonymized by the utility center before transmission to a trusted third party. The protocol achieves desired confidentiality, integrity and consumer privacy. It is assumed that the trusted third party would not collude with the utility center.

He et al. [68] presented a lightweight data aggregation scheme using Elliptic Curve Cryptography (ECC) to prevent internal attacks on the smart grid. The proposed scheme consist of three phases: initialization, registration and aggregation. In the initialization phase, the aggregator and the TTP together produce a blind factor that is used to prevent internal attacks. The aggregator registers the smart meter in the registration phase. The proposed scheme suffers from higher computational cost as compared to [41]. Moreover the power consumption readings are known by the aggregator.

Shen et al. [113] proposed an Efficient Privacy-Preserving Cube-Data Aggregation Scheme [109]. The schemes topology consist of a control center, two-level gateways namely the district gateway and a residential gateway and, the home area network. The multi-dimensional data is aggregated at the district gateway and the residential gateway. The verification of data at user level, residential gateway and the district gateway and the aggregation at the two gateways contribute to high computational cost as well as the Pailler cryptosystem. The scheme also requires additional time-consuming pairing operation.

Ferrag [43] used a bilinear pairing identity-based encryption scheme to update certificates in smart grid communications. The proposed scheme can achieve both data and gateway privacy. Although, the scheme prevents data replay, modification, man-in-the-middle and Sybil attacks, it is partially resilient to collusion and dictionary attack. Moreover, false data injection attack is not considered.

Bae et al. [12] proposed a privacy preserving scheme called PECA. The protocol assures user privacy as well as user-specific services of Demand Response programs. The scheme divides the data part into two regions: homomorphic and non-homomorphic parts. The homomorphic part is used for aggregation using three algorithms: KeyGen, Encrypt and Decrypt, while the non-homomorphic part is secured using a PKE [38]. The non-homomorphic part is used to identify user-specific services. The scheme incurs large overheads due to the two-time encryption i.e. PKE and the homomorphic encryption.

Abdallah and Shen [1] presented a lightweight privacy-preserving electricity consumption aggregation scheme that exploits lightweight lattice-based homomorphic cryptosystem. In the proposed scheme, the smart appliances are responsible for data aggregation and .The data is sent to the control center via the smart meter and the base station. The scheme prevents replay attacks and ensures data integrity via verification by smart meter or the base station. However, the scheme is has higher computational overhead compared to [5].

He et al. [66] proposed a data aggregation scheme that can achieve authentication and privacy-preserving data aggregation against internal attackers. Although the scheme is efficient in terms of computational cost, the energy cost and location privacy aspects are not considered.

Lu et al. [90] proposed a set-based aggregation scheme. The scheme divides the user data into two groups to achieve a two-subset aggregation. The scheme allows the control center to acquire more fine-grained data aggregation result for efficient controlling of the smart grid. The scheme is efficient in terms of computational and communication cost but lacks the ability to ensure data integrity. Furthermore, Tahir et al. [121] extended set-based aggregation approach by adding data integrity. The scheme uses hash chaining technique to ensure data integrity. However, hash chaining involves extra cost. The scheme suffers from additional communication overhead and aggregation time as compared to [90].

Shi et al. [114] proposed a diverse grouping-based aggregation protocol with error detection called DG-APED. The DG-APED protocol consists of three phases; data encryption and reporting, aggregation with error detection and dynamic join and leave. The scheme has complex implementation and only malicious data mining attack is considered.

Li et al. [82] proposed a privacy-preserving dual-functional aggregation scheme based on lattice cryptographic technique. The scheme consists of three phases; user report generation, privacy-preserving report aggregation and secure report reading. PDA is efficient in terms of computation cost and communication overhead. The scheme considers only plaintext-attack and does not have any comparative analysis with other schemes.

Chen et al. [23] proposes a data aggregation scheme with fault tolerance, called PDAFT. The scheme use homomorphic Paillier encryption to encrypt sensitive user data. The scheme lacks computation cost analysis. Jai et al. [71] presented a data aggregation scheme which could support efficient data aggregation for time-series metering data without leaking the individual value. The scheme consist of one aggregator which is the utility center or the grid operator and number of users i.e. smart meters. The scheme is based on meter reading reports and privacy preserving aggregation. The scheme divides the metering data for a given time slot into various small shares. Each share is encrypted and forwarded to the aggregator which aggregates the share to get an output. The scheme considers HDA attack and the aggregator to be untrusted. Therefore, binomial distribution is used to add noise by each meter which results in aggregator computing the noisy aggregation. However, the scheme does not consider low frequency metering data. The addition of noise and computation of noisy aggregated meter readings, is not suitable for low frequency metering data which require accurate readings. Therefore, the scheme is suitable only for high frequency metering data.

Lu et al. [89] proposed a privacy-preserving aggregation scheme for secure and efficient smart grid communication from user to the data center. The scheme utilizes a multi-dimensional data aggregation approach based on the homomorphic Paillier cryptosystem. This scheme performs data aggregation at the local gateway and uses batch verification for reducing authentication cost. However, the scheme assumes that the session keys between the home area network (HAN) users and the building area network gateway (BG) are unchanged. Therefore, once an adversary compromises the session keys, the adversary can decrypt any previous response messages [83].

Garcia and Jacobs [52] proposed a privacy preserving protocol for E-meters using elementary cryptographic operations. The protocol uses homomorphic properties of Paillier encryption on the additive sharing of the E-meters reading. Every E-meter helps to compute the share summation. Unfortunately, the protocol uses secret sharing, it suffers from high communication overheads between the meters and is expensive in terms of encryption. The protocol also suffers in non-scalability.

7 Conclusion and future works

The data collected in AMI plays an important role in providing services such as the periodic billing, distributed state estimation, real-time pricing, etc. These services differ in terms of the level of fine-grained data required to perform these services, the level of metering frequency and the accuracy of the data. While keeping in mind the privacy use cases and the privacy preserving aspect of consumer data, we have reviewed various non-cryptographic and cryptographic solutions for ensuring consumer privacy in AMI. According to our analysis and from the aforementioned survey papers, while some existing solutions tend to fulfil these services and simultaneously ensure consumer privacy, they suffer from several disadvantages. In the following, we highlight some of these open problems.

7.1 Privacy preserving data

Some of the privacy preserving approaches rely on providing privacy while the data is in transit, while some hide data at the smart meter level. Other approaches hide data from the utility companies by using trusted third parties. As mentioned in the non-cryptographic technique, the Battery-based Load Hiding (BLH) is a good approach, but contains severe problem which needs to be considered. The charging and discharging of the battery may conflict with the dynamic price, capacity of the battery is not considered. The existing solutions also lack the ability to provide differential privacy and cost saving simultaneously.

The reliance of data anonymization methods on escrow service or trusted third party services is not sufficient since it requires the escrow service or the trusted third party service to be trustworthy about the actual identities. While distributed anonymization can reduce this dependency, the distributed communication introduces extra overheads and requires approaches to prevent other attacks.

One of the most common approaches in data aggregation is to use homomorphic encryption. Homomorphic encryption are considered to be computationally expensive and complex, and practically infeasible for smart grids. The differential privacy and the error tolerance are two other issues related to homomorphic encryption. However, a development of computationally efficient fully homomorphic cryptosystem would result in greater acceptance.

Simple multi-party communication (SMPC) techniques can be used to ensure that the aggregator learns only the sum of the meter readings for distributed state estimation and monitoring applications. However, SMPC suffer from high computational cost and also requires the interactions between the nodes in the computational phase. Reducing the interaction cost could make it an attractive alternative.

7.2 AMI services

The AMI data in transit are used in providing services and various operations such as periodic or on-demand metering data, distributed state estimation and real-time pricing. The existing non-cryptographic and cryptographic works mentioned in Sect. 6 focus on preserving consumer privacy in one or two of the scenarios mentioned above. In most of these approaches, they do not satisfy the desired requirements for these services. For instance, data anonymization ensures consumer privacy by anonymizing the data to its original source and providing an overall energy consumption reading for the utility center. Although this approach offers privacy and allows to perform distributed state estimation, the utilities may have no access to provide consumer specific services. Therefore, there is a need to preserve both, the privacy of the consumer and the ability to perform services efficiently.

7.3 Privacy tradeoff

There exists a tradeoff that derives from the conflict between sharing metering data for operational purposes such as distributed state estimation, demand-response, billing etc. and withholding the data to ensure end-user privacy. For instance, on one hand, a utility may require energy usage data related to user privacy to perform billing, but preserving this data may affect normal billing operations. Moreover the technique of adding noise to preserve privacy can lead to an inaccurate aggregated results which may reduce the utility of the data. Therefore, it is essential to analyze and quantitatively measure these tradeoffs in the context of the information leakage and the utility retained.

Thus, from the literature survey analysis, there is a need for a novel privacy preserving schemes that will address the disadvantages of the existing work and also fulfil the requirements of the services provided by the AMI.

References

1. Abdallah, A., Shen, X.: A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. IEEE Trans. Smart Grid. (2016). https://doi.org/10.1109/TSG.2016.2553647
2. Abdallah, A., Shen, X.: Lightweight security and privacy preserving scheme for smart grid customer-side networks. IEEE Trans. Smart Grid **8**(3), 1064–1074 (2017)
3. Afrin, S., Mishra, S.: An anonymized authentication framework for smart metering data privacy. In: 2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5 (2016)
4. Afrin, S., Mishra, S.: On the analysis of collaborative anonymity set formation (casf) method for privacy in the smart grid. In: 2017 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1–6 (2017)
5. Agarkar, A., Agrawal, H.: R-lwe based lightweight privacy preserving scheme for smart grid. In: International Conference on Computing, Analytics and Security Trends (CAST), pp. 410–415. IEEE, New York (2016)
6. Alam, A.: A novel non-cryptographic security services for advanced metering infrastructure in smart grid. Commun. Appl. Electron. **3**(7), 35–39 (2015)
7. Aloul, F., Al-Ali, A., Al-Dalky, R., Al-Mardini, M., El-Hajj, W.: Smart grid security: threats, vulnerabilities and solutions. Int. J. Smart Grid Clean Energy **1**(1), 1–6 (2012)
8. Ambrosin, M., Hosseini, H., Mandal, K., Conti, M., Poovendran, R.: Despicable me(ter): anonymous and fine-grained metering data reporting with dishonest meters. In: 2016 IEEE Conference on Communications and Network Security (CNS), pp. 163–171 (2016)
9. Asghar, M.R., Dn, G., Miorandi, D., Chlamtac, I.: Smart meter data privacy: a survey. IEEE Commun. Surv. Tutorials. (2017). https://doi.org/10.1109/COMST.2017.2720195
10. Backes, M., Meiser, S.: Differentially private smart metering with battery recharging. Revised Selected Papers of the 8th International Workshop on Data Privacy Management and Autonomous Spontaneous Security, vol. 8247, pp. 194–212. Springer, New York (2014)
11. Badra, M., Zeadally, S.: Lightweight and efficient privacy-preserving data aggregation approach for the smart grid. Ad Hoc Netw. **64**, 32–40 (2017)
12. Bae, M., Kim, K., Kim, H.: Preserving privacy and efficiency in data communication and aggregation for AMI network. J. Netw. Comput. Appl. **59**, 333–344 (2016)
13. Bao, H., Chen, L.: A lightweight privacy-preserving scheme with data integrity for smart grid communications. Concurr. Comput. **28**(4), 1094–1110 (2016)
14. Bartoli, A., Hernandez-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., Barthel, D.: Secure lossless aggregation for smart grid m2m networks. In: 2010 First IEEE International Conference on Smart Grid Communications, pp. 333–338 (2010)
15. Berger, T.: Rate-Distortion Theory. Wiley, New York (2003)
16. Berthier, R., Sanders, W.H., Khurana, H.: Intrusion detection for advanced metering infrastructures: requirements and architectural directions. In: 2010 First IEEE International Conference on Smart Grid Communications, pp. 350–355 (2010)
17. Beussink, A., Akkaya, K., Senturk, I.F., Mahmoud, M.M.: Preserving consumer privacy on IEEE 802.11 s-based smart grid ami networks using data obfuscation. In: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 658–663. IEEE, New York (2014)
18. Bohli, J.M., Sorge, C., Ugus, O.: A privacy model for smart metering. In: 2010 IEEE International Conference on Communications Workshops, pp. 1–5 (2010)
19. Borden, A.R., Molzahn, D.K., Ramanathan, P., Lesieutre, B.C.: Confidentiality-preserving optimal power flow for cloud computing. In: 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 1300–1307 (2012)
20. Bradley, J., Barbier, J., Handler, D.: Embracing the internet of everything to capture your share of $14.4 trillion (2013)
21. Bresson, E., Chevassut, O., Pointcheval, D., Quisquater, J.J.: Provably authenticated group Diffie-Hellman key exchange. In: Proceedings of the 8th ACM conference on Computer and Communications Security, pp. 255–264. ACM, New York (2001)
22. Buchmann, E., Bohm, K., Burghardt, T., Kessler, S.: Re-identification of smart meter data. Pers. Ubiquitous Comput. **17**(4), 653–662 (2013)
23. Chen, L., Lu, R., Cao, Z.: Pdaft: a privacy-preserving data aggregation scheme with fault tolerance for smart grid communications. Peer-to-Peer Netw. Appl. **8**(6), 1122–1132 (2015)
24. Cheung, J.C.L., Chim, T.W., Yiu, S.M., Li, V.O.K., Hui, L.C.K.: Credential-based privacy-preserving power request scheme for smart grid network. In: 2011 IEEE Global Telecommunications Conference—GLOBECOM 2011, pp. 1–5 (2011)
25. Chim, T.W., Yiu, S.M., Hui, L.C.K., Li, V.O.K.: Pass: Privacy-preserving authentication scheme for smart grid network. In: 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 196–201 (2011)
26. Chin, J.X., Rubira, T.T.D., Hug, G.: Privacy-protecting energy management unit through model-distribution predictive control. IEEE Trans. Smart Grid **8**, 3084–3093 (2017)
27. Cisco (2017) IoE at work: smart grid | internet of everything. http://ioeassessment.cisco.com/en-gb/see/ioe-work-smart-grid-0
28. Cleveland, F.M.: Cyber security issues for advanced metering infrasttructure (AMI). In: 2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–5 (2008)
29. Darby, S.: Smart metering: what potential for householder engagement? Build. Res. Inform. **38**(5), 442–457 (2010)
30. Depuru, S.S.S.R., Wang, L., Devabhaktuni, V., Gudi, N.: Smart meters for power grid: challenges, issues, advantages and status. In: 2011 IEEE/PES Power Systems Conference and Exposition, pp. 1–7 (2011)
31. Diao, F., Zhang, F., Cheng, X.: A privacy-preserving smart metering scheme using linkable anonymous credential. IEEE Trans. Smart Grid **6**(1), 461–467 (2015)
32. Dinesh, C., Nettasinghe, B.W., Godaliyadda, R.I., Ekanayake, M.P.B., Ekanayake, J., Wijayakulasooriya, J.V.: Residential appliance identification based on spectral information of low frequency smart meter measurements. IEEE Trans. Smart Grid **7**(6), 2781–2792 (2016)
33. DoE.: Data Access and Privacy Issues related to Smart Grid Technologies. U.S. Department of Energy (2010)
34. DoE.: Smart Grid Privacy Workshop Summary Report. U.S. Department of Energy (2012)
35. Drenker, S., Kader, A.: Nonintrusive monitoring of electric loads. IEEE Comput. Appl. Power **12**(4), 47–51 (1999)
36. Dwork, C.: Differential Privacy: A Survey of Results, pp. 1–19. Springer, Berlin (2008)
37. Efthymiou, C., Kalogridis, G.: Smart grid privacy via anonymization of smart metering data. In: 2010 First IEEE International Conference on Smart Grid Communications, pp. 238–243 (2010)

38. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory **31**(4), 469–472 (1985)
39. EPIC.: The Smart Grid and Privacy. Electronic Privacy Information Center (2017)
40. Erkin, Z., Troncoso-pastoriza, J.R., Lagendijk, R.L., Perez-Gonzalez, F.: Privacy-preserving data aggregation in smart metering systems: an overview. IEEE Signal Process. Mag. **30**(2), 75–86 (2013)
41. Fan, C.I., Huang, S.Y., Lai, Y.L.: Privacy-enhanced data aggregation scheme against internal attackers in smart grid. IEEE Trans. Indus. inform. **10**(1), 666–675 (2014)
42. Fang, X., Misra, S., Xue, G., Yang, D.: Smart grid-the new and improved power grid: a survey. IEEE Commun. Surv. Tutor. **14**(4), 944–980 (2012)
43. Ferrag, M.A.: EPEC: an efficient privacy-preserving energy consumption scheme for smart grid communications. Telecommun. Syst. **66**, 671–688 (2017)
44. Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J.: A survey on privacy-preserving schemes for smart grid communications. CoRR (2016). arXiv:1611.07722
45. Fhom, H.S., Kuntze, N., Rudolph, C., Cupelli, M., Liu, J., Monti, A.: A user-centric privacy manager for future energy systems. In: 2010 International Conference on Power System Technology, pp. 1–7 (2010)
46. Finster, S., Baumgart, I.: Elderberry: a peer-to-peer, privacy-aware smart metering protocol. In: 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 37–42 (2013a)
47. Finster, S., Baumgart, I.: Pseudonymous smart metering without a trusted third party. In: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1723–1728 (2013b)
48. Finster, S., Baumgart, I.: Privacy-aware smart metering: a survey. IEEE Commun. Surv. Tutor. **17**(2), 1088–1101 (2015)
49. FIPS.: Standards for Security Categorization of Federal Information and Information Systems (2004)
50. Ford, V., Siraj, A., Rahman, M.A.: Secure and efficient protection of consumer privacy in advanced metering infrastructure supporting fine-grained data analysis. J. Comput. Syst. Sci. **83**(1), 84–100 (2017)
51. Froehlich, J., Larson, E., Gupta, S., Cohn, G., Reynolds, M., Patel, S.: Disaggregated end-use energy sensing for the smart grid. IEEE Pervasive Comput. **10**(1), 28–39 (2011)
52. Garcia, F.D., Jacobs, B.: Privacy-friendly energy-metering via homomorphic encryption. In: Proceedings of the 6th International Conference on Security and Trust Management, STM'10, pp. 226–238. Springer, Berlin (2011)
53. Gentry, C., et al.: Fully homomorphic encryption using ideal lattices. STOC **9**, 169–178 (2009)
54. Gharavi, H., Ghafurian, R.: Smart grid: the electric energy system of the future [scanning the issue]. Proc. IEEE **99**(6), 917–921 (2011)
55. Giaconi, G., Gunduz, D.: Smart meter privacy with renewable energy and a finite capacity battery. CoRR. (2016). arXiv:1605.04814
56. Goel, S., Hong, Y.: Security challenges in smart grid implementation. In: Smart Grid Security, pp. 1–39. Springer, Berlin (2015)
57. Gong, Y., Cai, Y., Guo, Y., Fang, Y.: A privacy-preserving scheme for incentive-based demand response in the smart grid. IEEE Trans. Smart Grid **7**(3), 1304–1313 (2016)
58. Greer, C., Wollman, D.A., Prochaska, D.E., Boynton, P.A., Mazer, J.A., Nguyen, C.T., FitzPatrick, G.J., Nelson, T.L., Koepke. G.H., Hefner, Jr. A.R., et al.: Nist framework and roadmap for smart grid interoperability standards, release 3.0. Special Publication (NIST SP)-1108r3 3 (2014)
59. Grid, N.S.: Guidelines for smart grid cyber security: vol. 2, privacy and the smart grid. Guideline (2010)
60. Grochocki, D., Huh, J.H., Berthier, R., Bobba, R., Sanders, W.H., Crdenas, A.A., Jetcheva, J.G.: AMI threats, intrusion detection requirements and deployment recommendations. In: 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pp. 395–400 (2012)
61. Guan, Z., Si, G., Wu, J., Zhu, L., Zhang, Z., Ma, Y.: Utility-privacy tradeoff based on random data obfuscation in internet of energy. IEEE Access. **5**, 3250–3262 (2017)
62. Guest, R.: Austin pd lawyers up over warrantless surveillance program. (2007). https://www.dallascriminaldefenselawyerblog.com/2007/11/austin-pd-lawyers-up-over-warr.html
63. Gupta, S., Reynolds, M.S., Patel, S.N.: Electrisense: single-point sensing using EMI for electrical event detection and classification in the home. In: Proceedings of the 12th ACM International Conference on Ubiquitous Computing, UbiComp '10, pp. 139–148. ACM, New York (2010)
64. Han, S., Zhao, S., Li, Q., Ju, C.H., Zhou, W.: Ppm-hda: Privacy-preserving and multifunctional health data aggregation with fault tolerance. IEEE Trans. Inform. Forensics Secur. **11**(9), 1940–1955 (2016)
65. Hart, G.: Nonintrusive appliance load monitoring. Proc. IEEE **80**(12), 1870–1891 (1992)
66. He, D., Kumar, N., Lee, J.H.: Privacy-preserving data aggregation scheme against internal attackers in smart grids. Wirel. Netw. **22**(2), 491–502 (2016a)
67. He, D., Wang, H., Khan, M.K., Wang, L.: Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Commun. **10**(14), 1795–1802 (2016)
68. He, D., Zeadally, S., Wang, H., Liu, Q.: Lightweight data aggregation scheme against internal attackers in smart grid using elliptic curve cryptography. Wirel. Commun. Mobile Comput. (2017). https://doi.org/10.1007/s11276-015-0983-3
69. He, X., Zhang, X., Kuo, C.C.J.: A distortion-based approach to privacy-preserving metering in smart grids. IEEE Access. **1**, 67–78 (2013)
70. Humayed, A., Lin, J., Li, F., Luo, B.: Cyber-physical systems security–a survey. IEEE Internet Things J. **4**, 1802–1831 (2017)
71. Jia, W., Zhu, H., Cao, Z., Dong, X., Xiao, C.: Human-factor-aware privacy-preserving aggregation in smart grid. IEEE Syst. J. **8**(2), 598–607 (2014)
72. Kalogridis, G., Efthymiou, C., Denic, S.Z., Lewis, T.A., Cepeda, R.: Privacy for smart meters: towards undetectable appliance load signatures. In: 2010 First IEEE International Conference on Smart Grid Communications, pp. 232–237 (2010)
73. Kang, J.: Information privacy in cyberspace transactions. Stanf. Law Rev. **50**, 1193–1294 (1998)
74. Kim, Y., Ngai, E.C.H., Srivastava, M.B.: Cooperative state estimation for preserving privacy of user behaviors in smart grid. In: 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 178–183 (2011)
75. Koo, J., Lin, X., Bagchi, S.: Rl-blh: Learning-based battery control for cost savings and privacy preservation for smart meters. In: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (2017)
76. Kotz, S., Kozubowski, T., Podgorski, K.: The Laplace Distribution and Generalizations: A Revisit with Applications to Communications, Economics, Engineering, and Finance. Springer, New York (2012)
77. Krawczyk, H., Canetti, R., Bellare, M.: HMAC: Keyed-hashing for message authentication. RFC. (1997). https://doi.org/10.17487/RFC2104

78. Krebs, B.: Puerto rico smart meters believed to have been and such hacks likely to spread. (2012). https://www.metering.com/puerto-rico-smart-meters-believed-to-have-been-hacked-and-such-hacks-likely-to-spread/
79. Kundur, D., Feng, X., Liu, S., Zourntos, T., Butler-Purry, K.L.: Towards a framework for cyber attack impact analysis of the electric smart grid. In: 2010 First IEEE International Conference on Smart Grid Communications, pp. 244–249 (2010)
80. Kuzlu, M., Pipattanasomporn, M., Rahman, S.: Communication network requirements for major smart grid applications in han, nan and wan. Comput. Netw. **67**, 74–88 (2014)
81. Laughman, C., Lee, K., Cox, R., Shaw, S., Leeb, S., Norford, L., Armstrong, P.: Power signature analysis. IEEE Power Energy Mag. **1**(2), 56–63 (2003)
82. Li, C., Lu, R., Li, H., Chen, L., Chen, J.: Pda: a privacy-preserving dual-functional aggregation scheme for smart grid communications. Secur. Commun. Netw. **8**(15), 2494–2506 (2015)
83. Li, H., Lin, X., Yang, H., Liang, X., Lu, R., Shen, X.: Eppdr: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. IEEE Trans. Parall. Distrib. Syst. **25**(8), 2053–2064 (2014)
84. Li, S., Xue, K., Yang, Q., Hong, P.: PPMA: privacy-preserving multi-subset aggregation in smart grid. IEEE Trans. Indus. Inform. (2017). https://doi.org/10.1109/TII.2017.2721542
85. Liao, X., Srinivasan, P., Formby, D., Beyah, A.R.: Di-prida: differentially private distributed load balancing control for the smart grid. IEEE Trans. Dependable Secure Comput. (2017). https://doi.org/10.1109/TDSC.2017.2717826
86. Lin, Y.H., Tsai, M.S.: An advanced home energy management system facilitated by nonintrusive load monitoring with automated multiobjective power scheduling. IEEE Trans. Smart Grid **6**(4), 1839–1851 (2015)
87. Lisovich, M.A., Mulligan, D.K., Wicker, S.B.: Inferring personal information from demand-response systems. IEEE Secur. Priv. **8**(1), 11–20 (2010)
88. Liu, J., Xiao, Y., Li, S., Liang, W., Chen, C.L.P.: Cyber security and privacy issues in smart grids. IEEE Commun. Surv. Tutor. **14**(4), 981–997 (2012)
89. Lu, R., Liang, X., Li, X., Lin, X., Shen, X.: EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Trans. Parallel Distrib. Syst. **23**(9), 1621–1631 (2012)
90. Lu, R., Alharbi, K., Lin, X., Huang, C.: A novel privacy-preserving set aggregation scheme for smart grid communications. In: 2015 IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2015)
91. Mahmud, R., Vallakati, R., Mukherjee, A., Ranganathan, P., Nejadpak, A.: A survey on smart grid metering infrastructures: threats and solutions. In: 2015 IEEE International Conference on Electro/Information Technology (EIT), pp. 386–391 (2015)
92. Mason, R.O.: Four ethical issues of the information age. Mis Q. **10**, 5–12 (1986)
93. McLaughlin, S., McDaniel, P., Aiello, W.: Protecting consumer privacy from electric load monitoring. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS '11, pp. 87–98. ACM, New York (2011)
94. Mlaih, E., Aly, S.A.: Secure hop-by-hop aggregation of end-to-end concealed data in wireless sensor networks. CoRR (2008) arXiv:0803.3448
95. Mohassel, R.R., Fung, A., Mohammadi, F., Raahemifar, K.: Application of advanced metering infrastructure in smart grids. In: 22nd Mediterranean Conference on Control and Automation, pp. 822–828 (2014)
96. Moslehi, K., Kumar, R.: Smart grid—a reliability perspective. In: 2010 Innovative Smart Grid Technologies (ISGT), pp. 1–8 (2010)
97. NETL.: Advanced metering infrastructure. US Department of Energy Office of Electricity and Energy Reliability (2008)
98. Ozdemir, S., Cam, H.: Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks. IEEE/ACM Trans. Netw. **18**(3), 736–749 (2010)
99. Ozdemir, S., Xiao, Y.: Secure data aggregation in wireless sensor networks: a comprehensive overview. Comput. Netw. **53**(12), 2022–2037 (2009)
100. Paillier, P., et al.: Public-key cryptosystems based on composite degree residuosity classes. Eurocrypt **99**, 223–238 (1999)
101. Pathan, A.S.K., Fadlullah, Z.M., Fouda, M.M., Monowar, M.M., Korn, P.: Information integrity in smart grid systems. Inform. Syst. **53**, 145–146 (2015)
102. Quinn, E.L.: Smart metering and privacy: existing laws and competing policies. SSRN Electron. J. (2009). https://doi.org/10.2139/ssrn.1462285
103. Rahman, M.S., Basu, A., Kiyomoto, S.: Privacy-friendly secure bidding scheme for demand response in smart grid. In: 2015 IEEE First International Smart Cities Conference (ISC2), pp. 1–6 (2015)
104. Sang, Y., Shen, H., Inoguchi, Y., Tan, Y., Xiong, N.: Secure data aggregation in wireless sensor networks: a survey. In: 2006 Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), pp. 315–320 (2006)
105. Sankar, L., Rajagopalan, S.R., Mohajer, S., Mohajer, S.: Smart meter privacy: a theoretical framework. IEEE Trans. Smart Grid **4**(2), 837–846 (2013)
106. Saputro, N., Akkaya, K.: On preserving user privacy in smart grid advanced metering infrastructure applications. Secur. Commun. Netw. **7**(1), 206–220 (2014)
107. Savi, M., Rottondi, C., Verticale, G.: Evaluation of the precision-privacy tradeoff of data perturbation for smart metering. IEEE Trans. Smart Grid **6**(5), 2409–2416 (2015)
108. SGIP.: Guidelines for smart grid cyber security. Introduction to NISTIR 7628 (2010)
109. Shah, Z., Anwar, A., Mahmood, A.N., Tari, Z., Zomaya, A.Y.: A spatio-temporal data summarization paradigm for real-time operation of smart grid. IEEE Trans. Big Data. (2017). https://doi.org/10.1109/TBDATA.2017.2691350
110. Shamir, A., et al.: Identity-based cryptosystems and signature schemes. Crypto **84**, 47–53 (1984)
111. Sharma, A., Ojha, V.: Implementation of cryptography for privacy preserving data mining. Int. J. Database Manag. Syst. **2**(3), 57–65 (2010)
112. Sharma, K., Saini, L.M.: Performance analysis of smart metering for smart grid: an overview. Renew. Sustain. Energy Rev. **49**, 720–735 (2015)
113. Shen, H., Zhang, M., Shen, J.: Efficient privacy-preserving cube-data aggregation scheme for smart grids. IEEE Trans. Inform. Forensics Secur. **12**(6), 1369–1381 (2017)
114. Shi, Z., Sun, R., Lu, R., Chen, L., Chen, J., Shen, X.S.: Diverse grouping-based aggregation protocol with error detection for smart grid communications. IEEE Trans. Smart Grid **6**(6), 2856–2868 (2015)
115. Si, G., Guan, Z., Li, J., Liu, P., Yao, H.: A Comprehensive Survey of Privacy-Preserving in Smart Grid, pp. 213–223. Springer International Publishing, Cham (2016)
116. Smith, H.J.: Managing privacy: information technology and corporate America. UNC Press Books, Chapel Hill (1994)
117. Stegelmann, M., Kesdogan, D.: Gridpriv: a smart metering architecture offering k-anonymity. In: 2012 IEEE 11th

International Conference on Trust, Security and Privacy in Computing and Communications, pp. 419–426 (2012)

118. Stone, E.F., Gueutal, H.G., Gardner, D.G., McClure, S.: A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. J. Appl. Psychol. **68**(3), 459 (1983)

119. Sun, X., Wang, H., Li, J., Zhang, Y.: Satisfying privacy requirements before data anonymization. Comput. J. **55**(4), 422–437 (2012). https://doi.org/10.1093/comjnl/bxr028

120. Suzuki, K., Inagaki, S., Suzuki, T., Nakamura, H., Ito, K.: Nonintrusive appliance load monitoring based on integer programming. In: 2008 SICE Annual Conference, pp. 2742–2747 (2008)

121. Tahir, M., Khan, A., Hameed, A., Alam, M., Khan, M.K., Jabeen, F.: Towards a set aggregation-based data integrity scheme for smart grids. Ann. Telecommun. **72**, 513–515 (2017)

122. Tan, S., De, D., Song, W., Yang, J., Das, S.: Survey of security advances in smart grid: a data driven approach. IEEE Commun. Surv. Tutor. **19**(1), 397–422 (2017)

123. Tan, X., Zheng, J., Zou, C., Niu, Y.: Pseudonym-based privacy-preserving scheme for data collection in smart grid. Int. J. Ad Hoc Ubiquitous Comput. **22**(2), 120–127 (2016)

124. Tarrant, P.: Ami global forecast: H1 2017. (2017). https://www.greentechmedia.com/research/report/ami-global-forecast-2017-2021

125. Tonyali, S., Cakmak, O., Akkaya, K., Mahmoud, M.M.E.A., Guvenc, I.: Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid ami networks. IEEE Internet Things J. **3**(5), 709–719 (2016)

126. Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A.S., Nojoumian, M.: Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems. Future Gener. Comput. Syst. (2017). https://doi.org/10.1016/j.future.2017.04.031

127. Tsai, J.L., Lo, N.W.: Secure anonymous key distribution scheme for smart grid. IEEE Trans. Smart Grid **7**(2), 906–914 (2016)

128. UCA.: UtilityAMI 2008 Home Area Network System Requirements Specification. UCA International Users Group (2008)

129. UCA.: Security Profile For Advanced Metering Infrastructure. Utility Communications Architecture International Users Group (2010)

130. Uludag, S., Zeadally, S., Badra, M.: Techniques, Taxonomy, and Challenges of Privacy Protection in the Smart Grid, pp. 343–390. Springer International Publishing, New York (2015)

131. Vukovi, O., Dn, G., Bobba, R.B.: Confidentiality-preserving obfuscation for cloud-based power system contingency analysis. In: 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 432–437 (2013)

132. Wang, H., Sun, L., Bertino, E.: Building access control policy model for privacy preserving and testing policy conflicting problems. J. Comput. Syst. Sci. **80**(8), 1493–1503 (2014). https://doi.org/10.1016/j.jcss.2014.04.017. (special Issue on Theory and Applications in Parallel and Distributed Computing Systems)

133. Wang, S., Cui, L., Que, J., Choi, D.H., Jiang, X., Cheng, S., Xie, L.: A randomized response model for privacy preserving smart metering. IEEE Trans. Smart Grid **3**(3), 1317–1324 (2012)

134. Wang, W., Lu, Z.: Cyber security in the smart grid: survey and challenges. Comput. Netw. **57**(5), 1344–1371 (2013)

135. Wang, Z.: An identity-based data aggregation protocol for the smart grid. IEEE Trans. Indus. Inform. (2017). https://doi.org/10.1109/TII.2017.2705218

136. Wichakool, W., Remscrim, Z., Orji, U.A., Leeb, S.B.: Smart metering of variable power loads. IEEE Trans. Smart Grid **6**(1), 189–198 (2015)

137. Yan, Y., Hu, R.Q., Das, S.K., Sharif, H., Qian, Y.: An efficient security protocol for advanced metering infrastructure in smart grid. IEEE Netw. **27**(4), 64–71 (2013)

138. Yan, Y., Qian, Y., Sharif, H., Tipper, D.: A survey on smart grid communication infrastructures: motivations, requirements and challenges. IEEE Commun. Surv. Tutor. **15**(1), 5–20 (2013)

139. Yang, W., Li, N., Qi, Y., Qardaji, W., McLaughlin, S., McDaniel, P.: Minimizing private data disclosures in the smart grid. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS ’12, pp. 415–427. ACM, New York (2012)

140. Zachary, G.P.: Saving smart meters from a backlash. IEEE Spectr. **48**(8), 8 (2011)

141. Zeifman, M., Roth, K.: Nonintrusive appliance load monitoring: review and outlook. IEEE Trans. Consum. Electron. **57**(1), 76–84 (2011). https://doi.org/10.1109/TCE.2011.5735484

142. Zhang, J., Li, H., Liu, X., Luo, Y., Chen, F., Wang, H., Chang, L.: On efficient and robust anonymization for privacy protection on massive streaming categorical information. IEEE Trans. Dependable Secur. Comput. **14**(5), 507–520 (2017). https://doi.org/10.1109/TDSC.2015.2483503

143. Zhao, J., Jung, T., Wang, Y., Li, X.: Achieving differential privacy of data disclosure in the smart grid. In: IEEE INFOCOM 2014—IEEE Conference on Computer Communications, pp. 504–512 (2014)

144. Zhu, S., Setia, S., Jajodia, S., Ning, P.: Interleaved hop-by-hop authentication against false data injection attacks in sensor networks. ACM Trans. Sen. Netw. **3**(3), 14 (2007)

Sanket Desai is currently pursuing a Ph.D. degree in Computer Science at Department of Computer Science and Engineering, La Trobe University, Melbourne, Australia. He holds a M.IT degree specializing in Computer Networks from La Trobe University, in 2014; the M.Sc. degree in Computer Science and B.Sc. degree in Computer Science from the University of Pune, in 2010 and 2008, respectively. He has interest in technology and privacy and the implications of technological development on the society. Currently, his research focuses on preserving privacy in IoE enabled areas, especially for Smart Grid applications. His other research interest include Cybersecurity, Vehicular Ad-Hoc Networks (VANET) and Advanced Networking.

Rabei Alhadad received his Ph.D. degree in Computer Science, from Latrobe University, Melbourne, Australia, in 2013. He also holds a M.IT degree in Computer Networks, from La Trobe University, Melbourne, Australia, in 2009 and a B.Sc. degree in Computer Science, from Western Mounting University, Libya, in 1999. He is currently working as an Associate Lecturer at the Department of Computer Science of La Trobe University. Previously he has worked as a Process Control Engineer from 2000 to 2007 at Repsol Oil Operations in Libya. His research focuses on Software Defined Networks, Internet of Things, Software Engineering and Data Networks.

Naveen Chilamkurti is currently working as an Associate Professor, Department of Computer Science and IT at La Trobe University, Australia. He received his Ph.D. from La Trobe University. He is also the Inaugural Editor-in-Chief for International Journal of Wireless Networks and Broadband Technologies launched in July 2011. He has published about 230 journal and conference papers. His current research areas include Cybersecurity, Privacy and data protection, IoT security, Fog Computing, wireless multimedia, wireless sensor networks, vehicle to infrastructure, vehicle to vehicle communications, health informatics, mobile communications, WiMAX, mobile security, mobile handover, and RFID. He currently serves on editorial boards of several international journals. He is a senior member of IEEE. He is also an Associate Editor for Wiley IJCS, SCN, Inderscience JETWI, and IJIPT.

Abdun Mahmood received the Ph.D. degree from the University of Melbourne, Australia, in 2008; the M.Sc. degree in computer science and the B.Sc. degree in applied physics and electronics from the University of Dhaka, Bangladesh, in 1999 and 1997, respectively. He has been working as an academic in Computer Science since 1999. He is currently with the La Trobe University, Melbourne where he is working as a senior lecturer in Cyber Security. Previously, he worked in the School of Engineering and IT, University of New South Wales. He has been a lecturer since 2000, an Assistant Professor since 2003 at the University of Dhaka. Between 2008 and 2011, he has been a Postdoctoral Research Fellow at the Royal Melbourne Institute of Technology. His research interests include data mining techniques for scalable network traffic analysis, anomaly detection, and industrial SCADA security. He has published his work in various IEEE Transactions and A-tier international journals and conferences.