Received 17 September 2020; revised 19 October 2020; accepted 2 November 2020. Date of publication 11 November 2020; date of current version 15 December 2020.

Digital Object Identifier 10.1109/OJCOMS.2020.3037517

The Challenges of Privacy and Access Control as Key Perspectives for the Future Electric Smart Grid

ANNA TRIANTAFYLLOU[1], JOSE ANTONIO PEREZ JIMENEZ[2], ALEJANDRO DEL REAL TORRES[2], THOMAS LAGKAS[3] (Senior Member, IEEE), KONSTANTINOS RANTOS[3], AND PANAGIOTIS SARIGIANNIDIS[1] (Member, IEEE)

[1]Department of Electrical and Computing Engineering, University of Western Macedonia, 50100 Kozani, Greece

[2]Research and Development Department, IDENER, 41300 Seville, Spain

[3]Department of Computer Science, International Hellenic University, 65404 Thessaloniki, Greece

CORRESPONDING AUTHOR: P. SARIGIANNIDIS (e-mail: psarigiannidis@uowm.gr)

This work was supported by the European Unions Horizon 2020 Research and Innovation Programme under Grant 833955.

ABSTRACT The Electric Smart Grid (ESG) is referred to as the next generation electricity power network. The ESG is an intelligent critical infrastructure subject to various security vulnerabilities and especially data privacy breaches. This study presents a comprehensive overview of the latest privacy-preserving mechanisms and policies in the ESG, while promoting the employment of modern access control techniques towards preventing personal data disclosure, affecting both utility companies and consumers. Efficient categorization is provided regarding the proposed privacy preserving methods and characteristics, while focus is also given on the use of the Blockchain technology and the Multi Authority Access Control paradigm in the ESG infrastructure. The study concludes with a discussion upon privacy and access control challenges, as well as future work concerning the ESG.

INDEX TERMS Electric smart grid, AMI, privacy, access control, blockchain, data anomymization, encryption.

I. INTRODUCTION

ENERGY transition in Europe has become a major issue, filled by significant and far-reaching challenges. Nowadays, more than ever, transportation, communications, resource management (water and air) and even agriculture are enabled by modern Electrical Power and Energy Systems (EPESs) promoting automation. The future of energy is electric and this is a great chance to move towards integrating higher share of renewables, promoting a more efficient and decentralized energy system, by involving advanced digital technologies. The era of Internet of Things (IoT) paves the way for a number of promising applications in various industry sectors and especially the Electric Smart Grids (ESGs) [1]. The ESG promotes efficient electricity generation, transmission and distribution to industrial and residential networks. It utilizes the benefits of a Supervisory Control and Data Acquisition (SCADA) system and Advanced Metering Infrastructures (AMI) towards enabling multi stakeholder interactions.

A SCADA system is an industrial automation system that controls and monitors the transmission network based on data collection acquired from instruments and sensors located throughout the field [2]. SCADA systems enable ESGs to provide an appealing scheme for remote control and observation of electric microgrids. Based on SCADA systems, supervision and control of the electric network equipment is enabled towards safeguarding reliability and promoting desired efficiencies for the whole utility. On the other hand, AMI is the system that collects and analyzes data from smart meters in order to deploy various powerrelated applications and services in an intelligent way based on that data [3]. An AMI consists of the AMI Control Center (ACC), which enables automated twoway communications between smart utility meters and the Meter Data

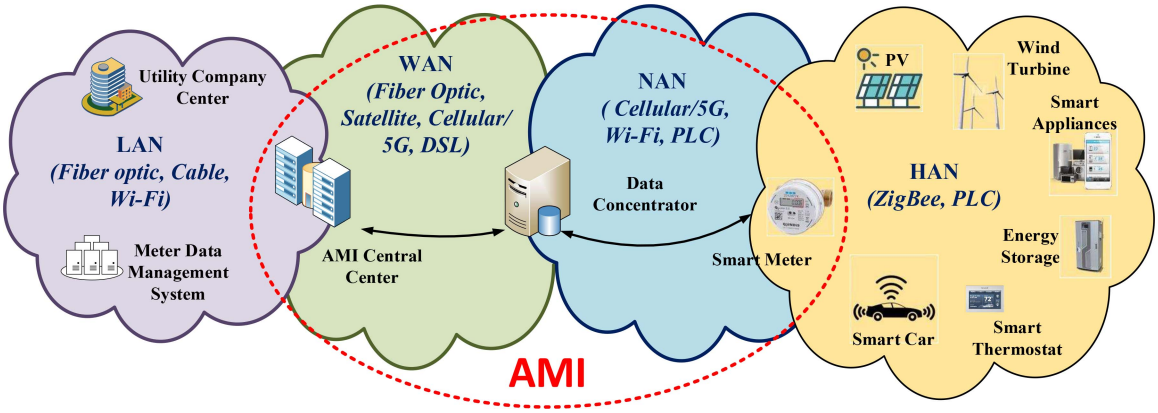

FIGURE 1. Advanced Metering Infrastructure.

Management System (MDMS), which aggregates, stores and permits the editing of meter data [4]. Smart meters provide utility companies with detailed information regarding consumers' power consumption, focusing on load monitoring and billing. As presented in Figure 1, the AMI network infrastructure interconnects the following networks: the Wide Area Network (WAN), which connects companies' utility centers to the ACC, the Neighborhood Area Network (NAN), which connects the ACC to the smart meters and the Home Area Network (HAN), which connects the home appliances with customers smart meter. Nonetheless, enormous challenges and initiatives are risen concerning the transition to a modernized electrical infrastructure in both industry and academia. Despite the economic benefits this modernisation brought, the employment of futuristic and upcoming technologies in the ESG's cyber-physical infrastructure has risen various security concerns. In the present day, cyber attacks have become increasingly sophisticated, stealthy, targeted and multi faceted. As a result, incidents like power outages, brownouts and blackouts are likely to happen and they may affect not only the energy domain but all the interconnecting devices and infrastructure. According to the European Network and Information Security Agency (ENISA) [5], a cyber security incident occurred to an ESG infrastructure can severely impact the confidentiality, integrity or availability of the system, including all its domains and organisations involved regarding the functioning of the power system.

As the ESG paradigm is reaching realization, it is more likely for cyber-attackers to get access to the underlying systems and networks. Attractive access points for cyber attacks are created by the ESG's tendency to rely on consumer behavioural data in order to provide its corresponding beneficial services. The manipulation of energy usage data towards extracting private and sensitive information about the customers is considered as privacy breach. Privacy breaches are a major concern in ESGs, disfavoring the employment of smart meters in every day life. In addition, it is a fact that consumer privacy strongly depends on authentication and authorization mechanisms. It is essential to enable secure and smart metering operations, while performing the efficient aggregation of data regarding billing operations and dynamic billing with high security protection and access control.

Furthermore, data analytics are now playing a more important role in the modern ESG, handling different types of unstructured data including messages, social media conversations, digital images, sensor data, video or voice recordings, and bring them together with more traditional, structured data [6]. Big data and machine learning can greatly benefit the prediction of energy on a short and medium term basis. However, unforeseen challenges to the field of data privacy are risen, due to their ability to derive actionable insights from large multidimensional data sets.

A. CONTRIBUTION

The current work aims to highlight all aspects of data privacy disclosure that may be encountered in the ESG. Moving towards a generation of decentralized and distributed technologies, the ESG infrastructure will require modifications and novel security technologies in order to adapt in this new era of autonomous programming, while also safeguarding data privacy. Motivated by the evolution of communication technologies in the ESG domain, as well as the major security and privacy concerns that have risen over the years, the contributions of this study include the following:

- A detailed overview of data privacy definitions, requirements and security concerns in the ESG is presented. Due to the fact that privacy-preserving mechanisms are data-centric, it is important to define all corresponding data types and procedures.
- A chronological taxonomy of privacy preserving standards and frameworks for the ESG is provided, as found in the literature up until now.
- A comprehensive presentation as well as context-aware categorization of techniques and algorithmic models regarding the protection of data privacy in the ESG is included.
- The use of authentication and authorization or else access control mechanisms is strongly promoted towards the safeguarding of data privacy in the ESG. Towards this direction, a detailed review is also

presented regarding the evolution and requirements of access control in the ESG aiming to discover potential technological gaps in existing schemes and mechanisms.
- An introduction to distributed artificial intelligence for the ESG is also being made, where focus is given on potential privacy preserving mechanisms with authentication capabilities as well.
- An extended discussion is conducted regarding state of the art mechanisms and techniques to be employed in the ESG infrastructure towards enhancing consumer privacy, while also authenticating participating networking entities.
- Our goal is to draw attention on existing vulnerabilities and in parallel emphasize the need for the implementation of an efficient collaboration between existing privacy-preserving schemes and access control mechanisms.
- The conducted survey can be of significant importance to scholars and professionals regarding the implementation of new and more efficient privacy and access control techniques, motivated by current technological gaps and deficiencies.

Furthermore, to our knowledge, during the last five years, there has not been a survey work discussing modern access control and authentication techniques as a combined solution for dealing with the ESGs privacy issues and its future challenges as a decentralized infrastructure. More specifically, various approaches were presented in order to protect the privacy of customers in [7] and [8], while still using smart metering. However, no authentication policies or standards were discussed. Moreover, regardless the state-of-the-art research work presentation on privacy preservation issues in Vehicle-to-Grid (V2G) networks, no privacy standards or authentication standards were included in [9]. The increased need for more efficient privacy-preserving schemes for ESG is highlighted in [10]. Nevertheless, no focus is given on privacy and authentication standards, as well as authentication policies in decentralized infrastructures. During the same year, a thorough discussion was conducted in [11] regarding the security and privacy issues of data fusion in different IoT application domains. In this work, privacy-preserving data fusion requirements and solutions were presented regarding the ESG infrastructure. However, the authors did not discuss authentication or access control mechanisms in depth. In 2019, [4] and [12] discussed a variety of non-cryptographic and cryptographic solutions for ensuring consumer privacy in AMI, without drawing the attention on the enhancement of access control and authentication policies. In the same year, an extended survey was conducted on security and privacy research in ESG metering networks [13]. However, no insight was provided regarding privacy standards and decentralized authentication policies in the next generation ESG infrastructure. Later on, an extended review was presented on differential privacy techniques for cyber-physical systems in [14]. Authors have managed to cover all dimensions and aspects of differential privacy implementation in energy systems. Nevertheless, no discussion was conducted regarding authenticating and controlling the access rights of entities involved in novel decentralized ESG architectures, while also preserving the privacy of sensitive information. In 2020, another work was presented giving an in-depth overview on the fundamental knowledge and frameworks of local differential privacy [15]. In this study mainstream privacy mechanisms were introduced, but no focus was given on the ESG application domain. Furthermore, during the same year, a survey of IoT privacy and security was conducted in [16]. The authors highlighted a number of solutions regarding privacy protection and access control systems in the IoT, but no mention was provided regarding the protection of the ESG infrastructure in related matters of security and privacy preservation. Similarly, a taxonomy of privacy enhancing technologies was presented in [17]. Nevertheless, the ESG paradigm and its vulnerabilities on privacy protection were not part of the discussion in the manuscript. Last but not least, an overview of privacy leakage issues in the ESG infrastructure was provided in [18]. However, authors only discussed privacy aware machine learning-based detection mechanisms and did not emphasize on privacy preservation standards, authentication mechanisms or the deployment of decentralized blockchain in the ESG.

In contrast to the aforementioned works, the current survey provides a thorough overview of the challenges of privacy and access control as key perspectives for the evolution of the ESG infrastructure. A detailed comparison of our work with related studies is provided in Section II.

The remainder of this article is organized as follows. Section II is dedicated to related work, while Section III describes the meaning, the requirements and various concerns of privacy in the ESG. Section IV provides a categorization regarding ESG privacy policies, standards, techniques and mechanisms. Section V presents the authentication and authorization mechanisms appropriate for the ESG infrastructure, while Section VI focuses on access control mechanisms and the use of Blockchain technology for the ESG. Section VII presents an overview on federated learning for privacy preservation in the ESG. In Section VIII a discussion is conducted regarding data privacy challenges in the ESG and current technological gaps. Finally, Section IX concludes the study.

II. RELATED WORK

A variety of surveys have already been published regarding the technologies and security concerns in the ESG. However, there is a few literature reviews regarding privacy [4], [7], [8], [9], [10], [12], [13]. More specifically, the work in [7] is focused on the problem of customer privacy-protection in the ESG. The authors present a categorization of various schemes in order to safeguard metering data for billing and other AMI operations. They also stated that consumer's privacy can be easily endangered, due to

TABLE 1. Related work contributions regarding the ESG privacy.

Contribution	Finster et al [7]	Han et al [9]	Asghar et al [8]	Ferrag et al [10]	Desai et al [4]	Sultan S. [12]	Kumar et al [13]	This survey
Privacy policies	x	x	x	x	x	x	-	x
Privacy standards	-	-	x	-	-	-	-	x
Privacy-Aware Smart Metering	x	x	x	x	x	x	x	x
Authentication policies	-	-	-	-	-	-	-	x
Authentication standards	-	-	-	-	-	-	-	x
AMI Authentication	-	x	-	x	-	-	x	x

the ability of ESG billing companies to acquire necessary information based on frequent metering. Moreover, the authors in [9] study a wide variety of research works focusing on state-of-the-art techniques regarding the preservation of privacy. Considerable focus is given on data aggregation, confidentiality, billing operations and identification in Vehicle-to-grid (V2G) networks. Furthermore, in 2017 a review was presented regarding the utilization of metering data in ESGs and the related privacy concerns [8]. In this work, privacy-preserving meter data delivery and management were discussed and various research directions were proposed for suitable security solutions. In addition, the work in [10] covers issues regarding security and privacy in the ESG. In more detail, a classification of attacks regarding leaking privacy in ESG is proposed, while focus is also given on standardization requirements and needs. A number of countermeasures regarding privacy breaches and game theoretic approaches are proposed as well via the presentation of different application scenarios. In 2018 another survey was published presenting a detailed analysis regarding privacy problems and their suitable solutions in ESG's AMI. The work in [4] focused on presenting various privacy preserving approaches and highlights technological gaps of existing schemes regarding privacy preservation. In the same year, the authors in [13] propose a taxonomy of cyber-security threats towards the smart metering network. Several threats are discussed regarding system-level security and services. Operational requirements are described and several schemes are presented regarding privacy protection as well. Last but not least, the author in [12] describes and categorizes works on privacy-preserving smart metering. The proposed categorization is based on attribution, the main cause for privacy issues in smart metering, and also on the maintainability of billing operations.

All of the aforementioned surveys are related to privacy preservation for ESGs and are published between 2014 and 2019. Nevertheless, as presented in Table 1, none of the above has presented or discussed modern access control and authentication techniques as a combined solution for dealing with the ESG's privacy issues and its future challenges as a decentralized infrastructure.

In literature, the term "privacy" is easily confused or associated with encryption regarding the ESG infrastructure. The current study aims to provide a better understanding of ESG operations regarding privacy concerns and in contrast to previous studies. It proposes the cooperation of privacy preserving models with state-of-the-art access control techniques towards enhancing data confidentiality and integrity. In addition, a discussion is conducted regarding the causes of data breaches, how they affect consumers and ways to be dealt with. Furthermore, a helpful categorization of privacy preserving and access control policies, standards, techniques and mechanisms is presented in order to raise the readers awareness regarding the current state and technological gaps of the ESG innovation. The current ESG privacy survey demonstrates a new viewpoint on smart grid history and promotes a challenging perspective on the future of smart grid.

III. PRIVACY IN THE ESG

Privacy is a term that applies to one's ideas, belongings, activities or decisions. Such is the dimension of privacy in the ESG as well, most commonly known as information or else data privacy. In particular, data privacy concerns an entity's ability to control the use, exposure or even acquisition of its own information [19]. Nowadays, the evolution of information systems raises major ethical challenges and concerns regarding the safeguarding and control over personal information. In ESGs, **private data** are considered the electricity consumption data, billing information, subscribers' profile information, types of devices operating at home and prosumer general characteristics. A prosumer is an important stakeholder role of the ESG referring to consumers who produce and share surplus energy with grid and other users [20]. Capturing such data by attackers usually means violation of privacy. On the other hand, the ESG involves different kinds of **operational data** containing instructions and commands for multiple procedures in the grid. Such data to be captured by attackers can lead to significant power disruptions and possibly damage the operation of the whole system. Table 2 summarizes all types of data found in the ESG.

As an intelligent infrastructure manipulating data of both energy and information, the ESG manages data from various processes including electricity generation, transmission, distribution and consumption. Based on these operations, electrical information from smart meters, power distribution stations and information that does not concern electricity measurements like meteorological data, marketing information and regional economic data are considered in the

TABLE 2. Types of data in the ESG.

Type	Category	Form
User data	Private data	Structured
Subscribers' profile information	Private data	Semi-structured
Reporting data	Private data	Unstructured
Log data	Private data	Structured
Types of devices operating at home	Private data	Unstructured
Electricity consumption data	Private data	Structured
Customer service information	Private data	Unstructured
Current loads of transformer feeders and capacitors	Operational data	Structured
Current on fault locations	Operational data	Structured
Status of relays	Operational data	Structured
Real-time current and voltage values	Operational data	Structured
Status of circuit breakers	Operational data	Structured
Running state of equipment	Operational data	Structured
Regional economy information	Private and Operational data	Semi-Structured
Marketing information	Private data	Structured
Meteorological information	Private and Operational data	Unstructured

system. The utilization of such information can help manage participating power plants, schedule the maintenance of according power equipment and the operation of subsystems, as well as organize business behavior in marketing. Data can be of various forms. ESG manages *a variety of data including structured, unstructured, probabilistic and multi-factor*.

Information − Theoretic Privacy (**ITP**) is a form of privacy in the ESG involving the ability to access, edit and share personal information given to others, while ensuring it is appropriately protected and discarded [21]. In addition, maintaining the integrity of the provided information is up to the owner, as well as, any actions concerning the disclosure of certain personal data to others. More specifically, users should ensure that data controller entities follow specific rules for collecting personal data, particularly with regard to proportionality of collection to the purpose of processing and legal basis. In the ESG, this kind of data privacy is noted in the smart-metering system, focusing on the regular reports of electricity usage delivered to the utility provider in real-time. Based on this procedure, the involved utility providers can easily acquire private user information. Smart meters acquire and distribute electricity usage information, providing a rich flow of information that reveals customers' behaviors and habits that stem from appliances usage. Furthermore, this category also refers to the exposure and management of a participating organization's confidential information regarding potential customers, profit statistics, future product designs, transaction details, current trends in the market, etc.

On the other hand, **Behavioral Privacy** (**BP**) is another form of privacy in the ESG associated with the right to exchange information without restrictions, while keeping any knowledge of personal activities and choices, from being shared with others [22]. In the ESG, each consumer should be free to benefit from the real-time energy monitoring in his HAN towards enabling remote load surveillance, automation in energy controlling and dynamic billing. These assets can be enabled by a in-home device for the consumer to purchase or prepay for electricity. The utility companies are interested in gathering the metering data periodically in order to efficiently manage and provide energy to the consumer. In case the collection time interval varies, a cyber attack can be considered to have taken place aiming to monitor the exchanged information. Moreover, BP encloses the consumer's rights to utilize energy according to his preferences and habits without being held accountable for. This kind of personal information could be revealed to public media or law enforcement endangering the consumers towards harassment or embarrassment.

A. ESG PRIVACY REQUIREMENTS

Objectives and requirements regarding the development of the ESG are closely related to the safeguarding of authentication, confidentiality and integrity of the data exchanged. *Authentication* refers to the need for proving the legitimacy of utility companies, consumers and smart devices. *Integrity* focuses on the possible alteration or modification of data and control commands without authorization. Guaranteeing the integrity of meter commands is essential towards safeguarding sensitive customer information and avoid potential privacy breaches, while *confidentiality* refers to the prevention of data disclosure by unauthorized users [23]. Potential privacy and legal consequences may arise if the exchange of sensitive data within the AMI, MDMS and the HAN stays unprotected. Due to the diverse nature of data exchanged in the ESG, the National Institute of Standards and Technology (NIST) proposed the employment of a Privacy Impact Assessment (PIA) report [23]. The report facilitates the discovery of privacy risks in the ESG, the documentation of the findings, and then the recommendation of solutions regarding the mitigation of the privacy risk findings. Furthermore, European Commission has also initiated a Data Protection Impact Assessment (DPIA) for smart grid and smart metering environment [24]. The DPIA template refers to smart grid stakeholders involving generators, metering operators and energy service companies, distribution system operators and suppliers. ESG stakeholders value the collection and use of personal data, since they are very

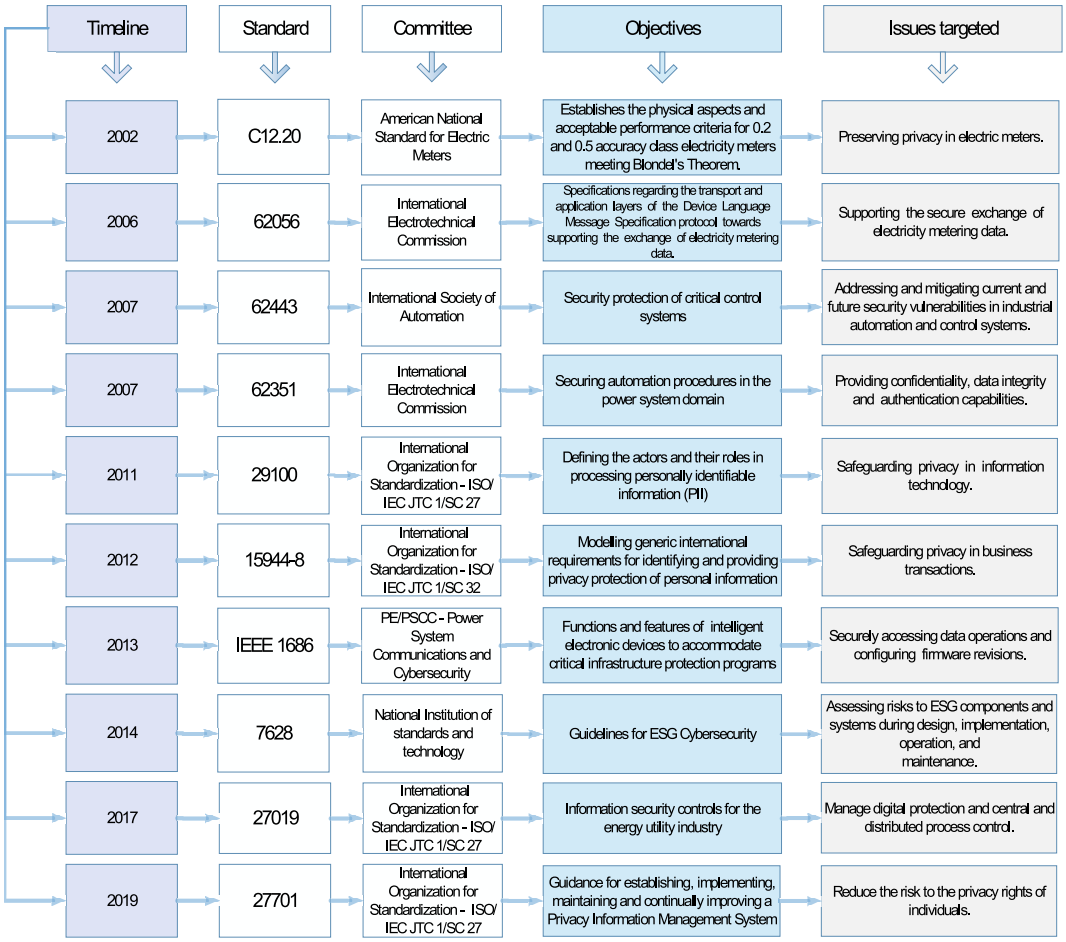

FIGURE 2. A taxonomy of privacy standards in the ESG.

likely to be subject to General Data Protection Regulation (GDPR) obligations as data controllers.

B. ESG SECURITY ISSUES

The AMI system handles various types of data regarding control information about the ESG, energy consumption and dynamic energy pricing making it an attractive target for adversaries [13]. Due to existing security vulnerabilities, consumer's privacy can be breached by the misuse of private data, possible eavesdropping attempts or interceptions in the backhaul IP network and possible forwarding node compromise. Eavesdropping, relay and man-in-the-middle (MITM) attacks are based on the unauthorized interception of wireless packets concerning the communication between the utility companies and the consumer [25]. On the other hand, the interception of the backhaul IP network technique is focused on the tampering of exchanged packets [26]. In more detail, the backhaul IP network is utilized by utility companies in order to aggregate data and operation commands. However, due to minimal or non-existent authentication of network control mechanisms and the tendency of relying on IP source addresses for authentication, the backhaul IP network is vulnerable to cyber attacks [27]. Due to this fact, an adversary has the ability to manipulate the participating devices and exchanged data packets regarding the payload, operation commands or even the source and destination addresses. Moreover, the compromise of a forwarding node in the AMI system, such as a demand response automation server, can reveal confidential information to an attacker by providing him with smart meter packets [28]. Last but not least, the blindfolded trust to the distribution network entities/energy suppliers can also cause severe cases of data breaches [29]. Despite the fact that an energy supplier entity is characterized as trustworthy, consumption information should not be permitted to be directly exchanged between the consumer and the utility companies. Such an act is necessitated in order to prevent consumers' private data misuse towards unfair business strategies or unwanted advertising promotions initiated by electric power companies in cooperation with the according energy suppliers.

IV. DATA PRIVACY MECHANISMS FOR THE SMART GRID

ESG data privacy can be safeguarded by revealing only the necessary information for the system's operation. It is essential for both consumers and participating organizations in the ESG to develop privacy-preserving policies regarding

TABLE 3. Existing privacy standards for the ESG.

Privacy standards	Applicability	Type	Relevance
ISO/IEC 27701:2019	Information Security Management System (ISMS)	General	High
ISO/IEC 27019:2017	Industrial control and automation systems	General	High
NISTIR 7628	All ESG components	Technical	Moderate
ISO/IEC 29100	All ESG components	General	Moderate
ISO/IEC 15944-8	Business transactions	General	Low
ANSI C12.20	Electricity meters	Technical	Low
IEC 62056	AMI	Technical	Low
IEEE 1686-2013	Substations	Technical	High
IEC 62351	All ESG components	Technical	Moderate
ISA/IEC 62443	Industrial control and automation systems	Technical	High

information storage, exchange and identification. This way sensitive information distributed internally, would be safely shared with other parties and secured against breaches. There is a variety of existing privacy standards and frameworks that can be applied to secure privacy in ESG use cases [30], as presented in Table 3. Figure 2 presents a chronological taxonomy of these privacy preserving standards as found in the literature up until now. The design of possible use cases can support the development of embedded protection rules regarding privacy into the ESG. Grid architects and engineers can enable grid entities to monitor data flows and accordingly acquire and use data by privacy preserving regulations [22]. Moreover, data privacy in the ESG has drown the interest of many researchers, proposing different kinds of anonymization and aggregation techniques.

A. EXISTING PRIVACY STANDARDS AND FRAMEWORKS

1) PRIVACY ORIENTED STANDARDS

There is a variety of existing privacy frameworks and standards for the ESG. Recently, the *ISO/IEC 27701:2019* [31] was published as a privacy extension of the ISO/IEC 27001, focusing on the deployment of Privacy Information Management Systems (PIMSs). More specifically, the standard outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals. In addition, *ISO/IEC 27019:2017* [32] provides guidance based on the ISO/IEC 27002:2013 standard aiming to manage energy utility industry′s control systems regarding the generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes. Furthermore, *ISO/IEC 29100* [33] and *ISO/IEC 15944-8* [34] are other standards describing helpful considerations that can be employed to safeguard privacy in the ESG infrastructure. The international *ISO/IEC 29100* standard provides the specification of a common privacy terminology, regarding the involved actors and the definition of their roles towards privacy safeguarding considerations in information technology. On the other hand, the *ISO/IEC 15944-8* standard defines the required descriptive techniques on business semantics and business transactions modelling aiming to safeguard privacy. Moreover, information privacy principles and rules are presented by the European Union in [35], the Asia-Pacific Economic Cooperation (APEC) in [36], the Federal Trade Commission in [37] and the NIST in [38]. In addition, specific directions are also provided in the *Consumer Privacy Bill of Rights* document [39], released by the Obama Administration, towards improving consumers privacy protection and helping businesses adapt in the rapidly changing digital environment by maintaining consumer trust and grow.

2) NETWORK ORIENTED ASPECTS

In a more technical level, smart meters can safely operate by utilizing the *ANSI C12.20* standard [40], an American National Standard for Electricity Meters regarding accuracy and performance, while intelligent electronic devices can be safeguarded by employing the *IEEE 1686-2013* standard [41], regarding data access operations,configuration of firmware revision and various data retrieval issues. The *IEC 62056* [42] defines a set of specifications regarding the transport and application layers of the Device Language Message Specification (DLMS) protocol towards supporting the exchange of electricity metering data. Moreover, the ESG infrastructure can be based on the *IEC 62351* [43] industry standard towards efficiently securing automation procedures in the power system domain. The standard includes ten different sub-standards that deal with different areas providing in part confidentiality, data integrity and authentication capabilities. The IEC 62351-1 standard includes an overview of security in power systems, focusing on a variety of threats and the according countermeasures towards mitigation in such systems. The IEC 62351-2 standard provides an extensive glossary, more specifically a list of terms regarding security in power systems, while the IEC 62351-3 standard focuses on power system automation protocols based on TCP/IP towards enhancing protection in message integrity and confidentiality. Moreover, the IEC 62351-4 standard involves the safeguarding of Manufacturing Message Specification (MMS) on application and TCP/IP based level, while the IEC 62351-5 standard describes a hash-based response authentication mechanism for safeguarding data integrity by utilizing pre-shared secret keys. The IEC 62351-6 standard specifies security procedures and messages for protocols derived form the IEC 61850 standard, such as Generic Object Oriented Substation Events (GOOSE) and Sampled Values (SV). The IEC 62351-7 standard is refereed to power system operations and defines the appropriate

network and system management (NSM) data object models. These models are useful in observing the state and health of networks and systems, while also detecting potential intrusions in the information infrastructure. The IEC 62351-8 standard defines the use of Role-Based Access Control (RBAC) in power systems, while the IEC 62351-9 standard specifies cryptographic key management. Last but not least, the IEC 62351-10 standard aims to describe a security architecture for power systems. It involves the coordination of essential security controls with system components and their interaction towards securely deploying power generation, transmission, and distribution. Despite its benefits, IEC 62351 contains some inaccuracies and does not promote modern cryptographic algorithms providing lower cost performance (e.g., elliptic curve cryptography). Similarly, the ISA/IEC 62443 series of standards [44] can assist in addressing future security vulnerabilities, while also mitigating current technological gaps in industrial automation and control systems. In particular, the ANSI/ISA-62443-4-2-2018 [45] specification provides detailed requirements regarding technical control system components aiming to efficiently secure industrial automation and control systems.

B. PRIVACY SCHEMES AND TECHNIQUES IN THE ESG

Despite the existing guidelines and standards against data disclosure, researchers have come up with various solutions to enhance privacy protection in ESG architecture, focusing mainly on data modification techniques. As displayed in Figure 3, there are various approaches towards safeguarding the privacy of end users during data aggregation processes in the ESG. Furthermore, data anonymization and data obfuscation are well known privacy preservation methods involving different kinds of techniques for data management and transformation. Literature has also been focused on the preservation of privacy in battery-based data masking schemes.

1) PRIVACY PRESERVATION DURING DATA AGGREGATION

Data aggregation refers to the collection of power measurements concerning a specific number of consumers in order to mask individual consumption. It has been proven that private user information, signifying the presence at home based on the behavior of electricity, is connected to data in the form of measurements or pricing evaluations and is not likely to be leaked if aggregated over a certain area [46]. This assumption is supported by the work in [47], which proposes an Integrated Authentication and Confidentiality (IAC) scheme so as to secure AMI communications. The IAC protocol is based on hop-by-hop data aggregation towards grouping intermediate nodes and also encryption so as to achieve data integrity and confidentiality. However, it was noted that intermediate nodes remained vulnerable to attacks and could jeopardize the privacy of the whole network. According to literature there are three ways for privacy preservation performed on data aggregation processes. The first category involves *data aggregation schemes utilizing trusted third parties (TTPs)*. The second category includes *data aggregation schemes using perturbation*, while the third category deals with *data aggregation schemes using cryptography*.

A **Trusted Third Party** (**TTP**) is an intermediate utility that differentiates identity information from the detailed usage information. In the AMI, smart meters rely on the TTP not to send the individual values but their aggregation (i.e., sum of all smart meters readings during the period) to the aggregator/electricity supplier. This way the energy supplier can not analyse the individual energy consumptions against statistical patterns. However, relying on one supposedly trustworthy entity for the entire process enhances the fear of compromise. Due to this fact pseudonyms were proposed as a possible solution. A **pseudonym** is a mask name that concerns a person or group for a particular purpose. Based on this technique, the work in [48] presents the use of a third-party escrow mechanism so as to secure the frequent transmissions of energy consumption data. In this scheme, two integrated pseudonyms are utilized by smart meters for monthly billing data and fine-grained data respectively. The energy supplier is associated with the pseudonym for monthly billing. Nevertheless, previous studies noted that the use of pseudonyms can efficiently protect only a portion of the households identities, as smart metering data characteristics can be used in the de-pseudonymization process [49].

In the light of eliminating the drawbacks brought by the TTP technique, data aggregation by the use of perturbation was proposed. The **perturbation technique** focuses on adding noise or some means of randomness to the metering data of each smart meter so that the aggregating node or entity does not infer the metering data [50], [51], [52]. One major drawback of aggregation protocols by means of perturbation is that due to the randomness added to each smart meter, the aggregated data can not reflect exactly the aggregated real metered data. Furthermore, in order to provide a good approximation of the real aggregated data, all noisy metering data should be successfully delivered to the aggregating node.

Encryption is the technique of concealing information and commonly in aggregation protocols. In ESG applications, encryption exists in the form of *asymmetric cryptography, symmetric cryptography, hash functions and homomorphic encryption*. It is often utilized in privacy preserving data aggregation schemes in cooperation with TTPs. **Symmetric key cryptography** is an encryption technique that requires the sharing of a single private key between the communicating entities for encryption and decryption. On the other hand, in **asymmetric key cryptography** the use of a private key enables data decryption and sign. A public key is also required in order to encrypt and verify the data exchanged. Confidentiality is the key asset of this technique regarding the definition of the private key, while the public key can be published freely. The TTP stands as the certificate authority for key management. Each communication

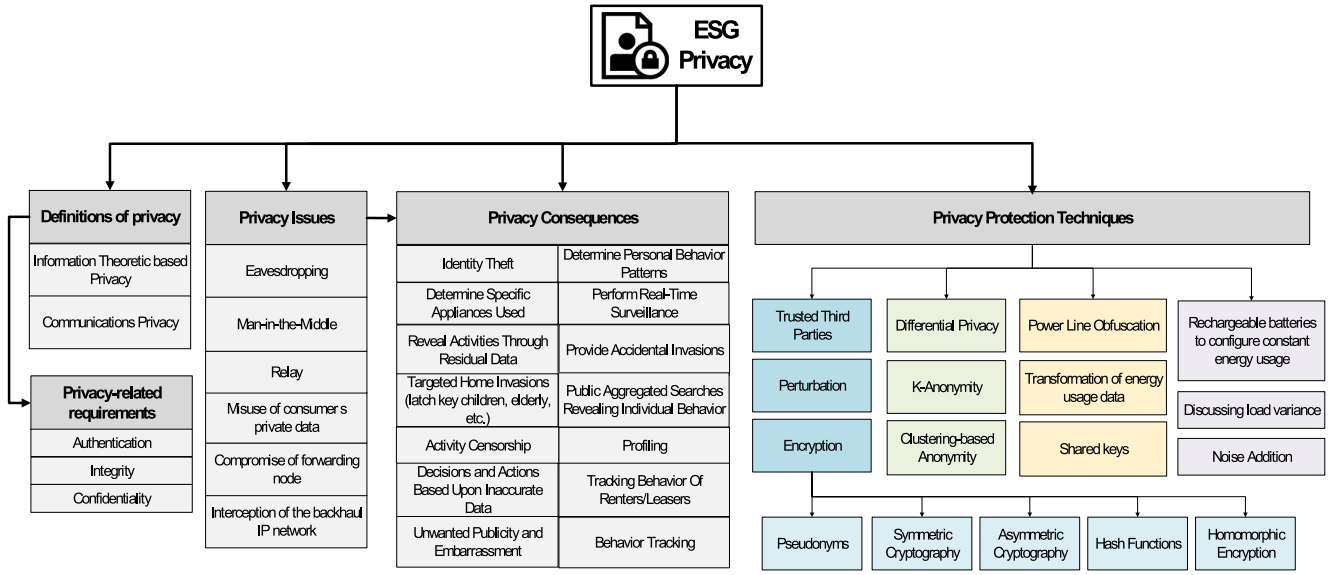

FIGURE 3. Privacy overview in the ESG.

entity needs to obtain the certified public keys from the certificate authority before the communication is initiated [53]. There has been a lot of research based on key management procedures concerning the ESG [54], [55], [56], [57], [58]. In [59] several encryption algorithms are presented, concluding to Advanced Encryption Standard (AES) algorithm as the most appropriate for ensuring security in the ESG.

Moving on, a **hash function** is another cryptographic algorithm with the ability to produce small fixed size data from large random size data. It is a special mathematical function which maps a given input to a certain output with a fixed size [60]. Hash functions cannot produce the same output for two different inputs. Also, their main advantage lies on the fact that one cannot get back to the input with just the output given. A well-known member of the family of cryptographically secure hashes is the Secure Hash Algorithm-2 (SHA-2). The work in [61] is based on cryptographic hash functions towards deploying a lightweight and privacy-preserving data aggregation (LPDA) scheme for dynamic electricity pricing. Moreover, a lightweight fault-tolerant privacy preserving data aggregation scheme, named EPDAS is proposed in [62] utilizing the advantages of elliptic curve cryptography and hash chain technique to provide confidentiality, anonymous authentication, autonomy and integrity. Furthermore, a hash-based authentication code was utilized in [63] so as to support the design of a privacy preserving AMI for fine-grained metering data collection. According to this scheme metering data are transmitted via a random multi-hop path anonymously to a MDMS. The utility's public key is utilized for the encryption of metering data. A TTP is considered as the verification entity responsible for managing of smart meters utilizing the Diffe-Hellman algorithm for symmetric key sharing. This method is known to be susceptible to the computationally intensive Man-In-The-Middle (MITM) attack.

Homomorphic encryption is another cryptographic technique widely used in data aggregation schemes in order to provide sufficient level of privacy to the smart meters. Based on this particular technique, the authors in [64] propose a privacy-preserving data aggregation scheme for the ESG, which enables smart meters to report their measurements periodically , while preventing private information from being leaked. Furthermore, homomorphic encryption is used in [65] as a part of a Privacy Preserving Fog-Enabled Aggregation (PPFA) scheme. Based on this scheme, efficient and concentrated Gaussian noise is required to be added by smart meters to their data and encrypt the noisy results with an efficient stream cipher. Similarly, in [66] the proposed Ring Triangulation Communication Architecture utilizes homomorphic encryption to relieve transmission congestion during data aggregation. Another privacy preserving scheme utilizing the homomorphic encryption for identity-based data aggregation is introduced in [67]. However, the authors in [68] proved that this particular scheme is not practical since it can only resist two colluding attacks. Recently, an efficient privacy-preserving scheme for Line-loss Calculation, named EPLC was proposed [69]. Based on this scheme, homomorphism was utilized so as to safeguard residential data according to line-loss representation. Despite the fact that homomorphic encryption enables the decrease of energy consumption, the mitigation of bandwidth bottleneck and helps to prolong the network lifetime, most of the existing aggregation protocols utilizing it have one major drawback. This is because they were designed for a single entity recipient system which is not ideal for a real ESG environment [66]. Moreover, the authors in [70] presented an Elliptic Curve Based Data Aggregation (ECBDA) based on

ElGamal encryption. This scheme utilizes a TTP, but which does not participate in data reporting or aggregation so as to reduce overhead. Smart meters take charge of signing the encrypted data and then send them to the aggregator. Last but not least, a Learning With Errors over Rings (R-LWE) based encryption scheme is presented in [71] for prosumers' privacy protection in the ESG. The proposed scheme is focused on reducing messaging overhead and computation overhead.

Summing up, despite the benefits of existing approaches, it has been shown that data aggregation continues to suffer from privacy risks. An adversary has the ability to monitor a residence either by impersonating a legal smart meter, or by shifting the electricity usage information, or even by migrating virtually the location of the metering device to an area with higher charges [13]. TTP authorities alone can prevent the malicious monitoring of the network traffic. Moreover, noise addition in order to mask the transmitted data can result to a low approximation of the real aggregated data. Last but not least, data encryption techniques can raise compatibility issues with existing programs and applications, as well as be quite costly for maintenance. Without capable systems, the reduction of systems operations can be significantly compromised.

2) DATA ANONYMIZATION FOR PRIVACY PRESERVATION

Data anonymization is another solution towards preventing the disclosure of personal information in the ESG infrastructure. This technique focuses on encrypting data sets to remove any personally identifiable information. Different kinds of anonymization techniques have been presented until now to guarantee privacy such as *differential privacy [14], k-anonymity [72], and clustering-based anonymity [73]*. In order to shield individual privacy in the context of big data, different anonymization techniques have conventionally been used.

The approach of **Differential privacy**, introduced by Dwork [74] is different and focuses on minimizing the amount of data disclosed. This approach controls the effect of any single individual on any information that can be extracted from the database, either by being absent or present [75]. In more detail, the main idea behind differential privacy [76], [77] is that it uses random noise to bound the publicly visible information that can be acquired about a user in the dataset. Up until now various studies have provided novel privacy preserving mechanisms based on differential privacy for the ESG. The basic logic of differential privacy in an ESG scenario is presented in Figure 4. In 2015, a novel Multifunctional Data Aggregation (MuDA) scheme was presented, supporting multifunctional aggregations and flexibility while utilizing differential privacy with limited noises [78]. Another technique utilizing a randomized response algorithm based on sparse coding was also presented in [79]. This technique is able to achieve differential-privacy and provides utility guarantees for consumers behaviours, while processing a batch of data at each time.

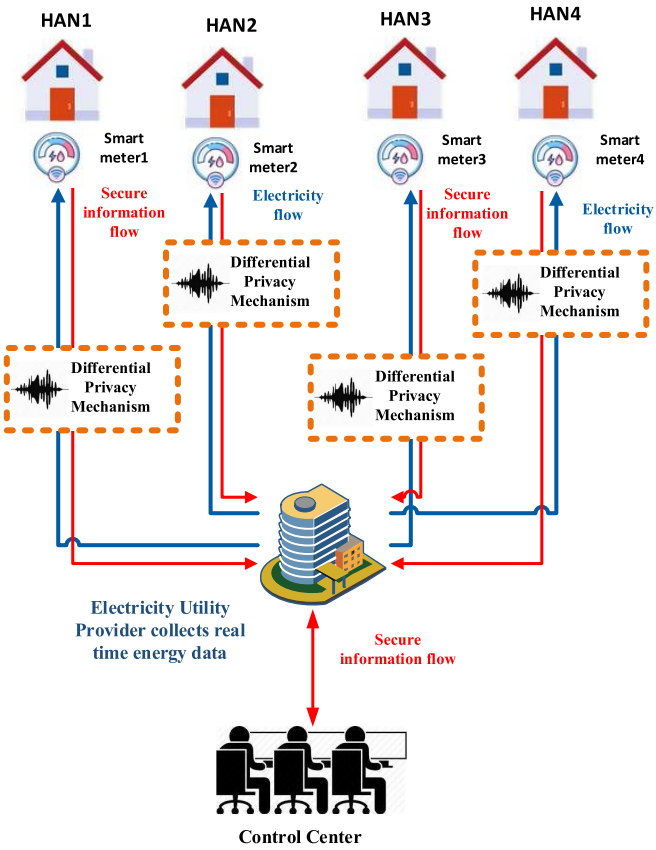

FIGURE 4. Differential privacy logic in the ESG.

On the other hand, **k-anonymity** approach [72] is based on grouping samples according to their sensitive information. The identification of individual samples would be impossible for an attacker if the group released is large enough. However, if the adversary had obtained information about some of these sensitive features from another source, then identifying individual samples would be possible. K-anonymity guarantees the protection of privacy by defining each released dataset entry in a way that relates to at least k individuals. This procedure is possible even if the entries released are directly connected to external information [80]. The work in [81] proposed the utilization of this method in cooperation with a trusted data aggregator. This entity guarantees the aggregation of energy consumption data from the smart meters. Nevertheless, access to unprotected data is highly possible due to the disclosure of individual energy consumption readings to the data aggregator.

Clustering-based anonymity is a very commonly used method for privacy preserving. Research has shown that clustering algorithms regarding privacy can also be adopted in the smart grid environment. K-means method is one of the most used partitional cluster analysis methods. k-means clustering targets the separation of a number of observations into k clusters in a way that each cluster contains observations similar to the mean value. This privacy technique is adopted in [82] to be evaluated under residential smart meter measurements. Another privacy preserving clustering algorithm

used in the process of mining large data-sets of smart grid is proposed in [83]. This algorithm can prevent all participants' privacy data leakage without increasing limited time complexity and decreasing the accuracy of mining results. The work in [84] takes advantage of clustering algorithms for profiling individuals' power consumption. A multi-layered clustering model for ESG applications is proposed examining each consumer's data as a part of the microgrid the user belongs to and on a second level as a part of the wider ESG. It is configured so that the privacy of consumers is enhanced as the local power consumption profiles are transferred to the central processor of the ESG. Last but not least, the concept of distributed anonymization is discussed in [85]. In this study, the authors present a novel Collaborative Anonymity Set Formation (CASF) method that forms different groups of smart metering data and utilizes the Blind Digital Signature (BDS) method [86] in order to hide the associated pseudonyms against any internal and external adversaries. However, this new method results in additional communication overhead when increasing the number of collaborating smart meters.

Nevertheless, the most common drawback of anonymization techniques is being sensitive to the background knowledge attack [87]. Since it is not possible to predict the level of background knowledge an attacker possesses about an individual, compromise has to be made with a higher distortion to the data and consequently higher information loss [88]. Furthermore, anonymous data aggregation can result in limitations regarding deriving insight from the data for marketing efforts, or towards personalizing the user experience.

3) DATA OBFUSCATION FOR PRIVACY PRESERVATION

Data obfuscation refers to the perturbation of metering data by *adding noise* or employing specific *algebraic tranformation formulas to energy usage data* [89]. The authors in [90] utilized data obfuscation so as to preserve consumer privacy in an IEEE 802.11 based ESG AMI network. Based on the proposed scheme the assigned gateway receives the obfuscated power measurements by the smart meter. Next, the gateway verifies the data and forwards the measurements to the utility center aiming to support billing operations, while achieving consumer privacy. Furthermore, in study [91], random data obfuscation was deployed, by utilizing the *Laplace distribution*, so as to mask real-time data in the ESG infrastructure. The proposed scheme manages to balance the utility-privacy trade off by employing homomorphic encryption. It also takes into consideration the signal-to-noise ratio in order to estimate the level of entropy concerning the utility and the provided data regarding the level of privacy. Moreover, Tonyali *et al.* [92] presented a data obfuscation approach for safeguarding consumer privacy, while also estimating the state of distribution. Based on this approach, the obfuscation vectors are estimated by the AMI network gateway, which then multiplies each one of them with a random number. A shared key is utilized for the distribution of the results to the smart meters. The proposed scheme estimates the state of distribution and simultaneously supports secure third-party billing. In addition, the study in [93] presents a privacy-preserving scheme which utilizes the error-free state estimation technique. The basic idea of the proposed scheme is that the generated obfuscation measurements are utilized by a *third party* towards generating state estimators. The utility provider acquires the state estimators so as to calculate distributed state estimation. Despite its benefits against automatic attacks, the proposed scheme requires specific statistical measures towards evaluating the level of obfuscation in the metering data. Last but not least, a latest research in [94] proposed a *Power Line Obfuscation (PLO) mechanism* to obfuscate the line parameters in a power system network. The authors utilise differential privacy so as to hide the network sensitive values, while also maintaining the fundamental properties of the obfuscated network.

Summing up, despite their advantages, data obfuscation techniques can be burdensome. By adding more noise to the data may render the data useless. Employing a sufficient level of data masking for privacy preservation, while also maintaining the usefulness of the raw data still remains a challenge.

4) PRIVACY PRESERVATION IN BATTERY-BASED DATA MASKING TECHNIQUES

The **Battery-based Data Masking** (**BDM**) are well known approaches that consider the manipulation of smart meter measurements towards disguising the real energy consumption values. For this purpose, a rechargeable battery is used to partially supply the energy demand. According to [21], in the ESG data privacy can be estimated based on the information leakage rate. This parameter signifies a connection between the user's real energy consumption and the energy requested from the grid. A single-letter expression is utilized to express the minimum information leakage rate in cases of infinite or zero battery capacity. It is proven that the availability of a renewable energy source greatly depends on the information leakage rate. A characteristic method of the BDM category is the *Best Effort (BE*) power management model proposed in [95]. The proposed scheme is described as a load signature moderation system that safeguards the exchanged smart meter measurements in an independent way, without restricting the ESG functionalities. It is based on a power mixing algorithm and different privacy metrics in order to evaluate its protection levels. Results show that the scheme succeeds in hiding the home load identity, since the rechargeable battery manages to mask the consumers real energy consumption. However, it was noted that the customers privacy may be endangered by utilizing a BE scheme. The batteries' required capacity and charging rate may be the cause of privacy breaches during the effort of maintaining the masking process. A similar method, named *Non-Intrusive Load Levelling (NILL)* was proposed in [96] in order to protect the privacy of the consumer by utilizing an in-residence battery, as presented in Figure 5. The NILL approach safeguards privacy by hiding the variance

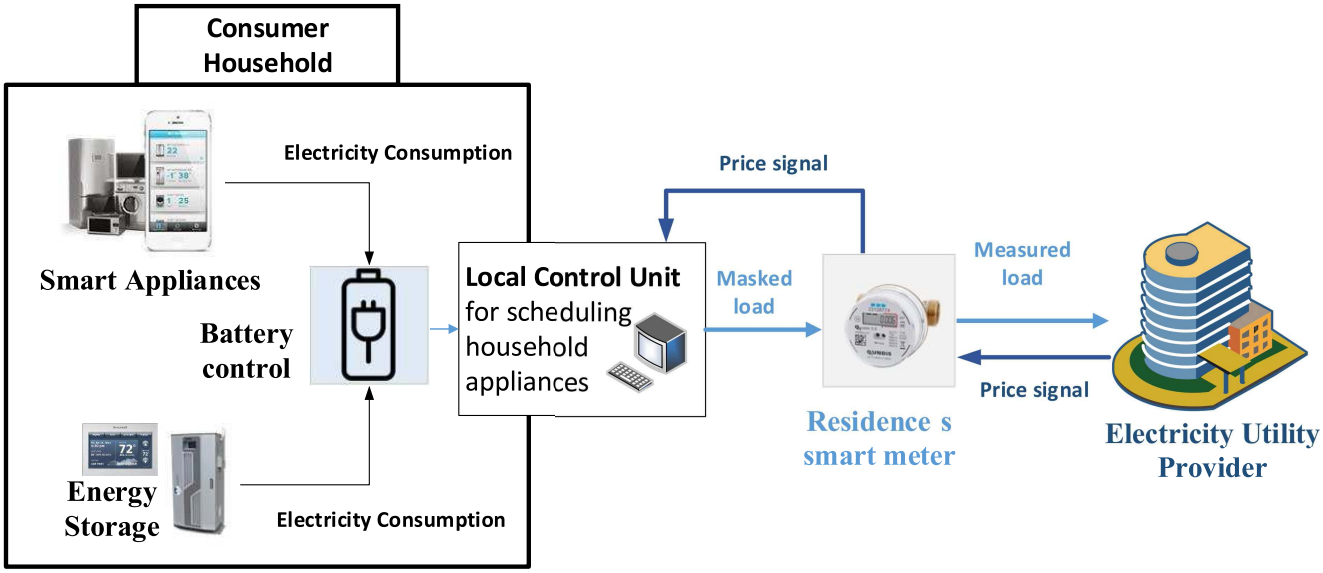

FIGURE 5. Battery-based privacy preserving logic in the ESG.

in load. Based on this method, in order to disguise the appliance activities, a removal of most of the energy usage transitions takes place referring to load events. This way the consumers energy usage profiles can be revealed. Later on, the work in [97] came to present the faults of the previous method. As a solution, the *Lazy Stepping (LS)* scheme was proposed, as another BDM approach. Its basic advantage was noted to be the prevention of precise load change recovery attacks. However, despite the method's superiority against the ones in [95] and [96], the lack of differential privacy metrics sentenced it as less efficient compared to the one in [98]. The authors in [98] focused on the capabilities of *differential privacy* and proposed a randomized Battery-based Load Hiding (BLH) algorithm. A multitasking-BLH-Exp3 algorithm was also utilized for adding noise and adaptively update the proposed BLH method based on the context and the constraints. The context involved battery energy consumption, while also focused on the way appliances tend to consume energy. Moreover, a battery based method towards hiding sensitive power consumption information is proposed in [99]. The presented scheme was based on *adding or subtracting noise via cascading method*. This method utilizes a function specified on the amount of recharged energy. The proposed function is based on adding noise. Despite the fact that differential privacy is achieved, noise generation continues to impact the battery life. That is why a secondary battery was also used to recharge the first one and remained unknown to the adversary in order to achieve the desired privacy. Last but not least, the authors in [100] presented a battery based differential privacy preserving (BDP) scheme aiming to safeguard the disclosure of smart meter measurements of the customers, while also promoting cost saving. The proposed scheme utilizes two cost-friendly *differential privacy-preserving (CDP)* schemes under static and dynamic pricing policies.

Despite theirs benefits, BDM approaches are greatly affected by the capacity, the charging and discharging of the corresponding battery. Due to this fact, such data masking may result to the irreversible transformation or even the loss of sensitive metering data.

V. ENHANCING CONSUMER PRIVACY VIA AUTHENTICATION AND AUTHORIZATION

The protection of the consumer data is essential for achieving a compliant and secure ESG infrastructure which is based on a privacy-by-design and privacy-by-default approach [101]. According to the NIST Guidelines for Smart Grid Cybersecurity [22], **Authentication** refers to the verification of a user′s identity as a requirement for accessing the ESG information system. On the other hand, **Authorization** is the process which is adjacent to the authentication mechanism in the Smart Grid communications where the access to restricted resources is allowed based on different aspects and rules (e.g., access policies). Authorization also involves the denial or revocation of access regarding a malicious actor. In the context of the ESG, this is more challenging to achieve than in a normal Information Technology (IT) environment due to the distributed component of the nodes and assets present in the ESG networks. To that end, the proper authentication and authorization procedures and technologies have to be adopted and implemented through access control mechanisms present in several devices of the Smart Grid network. Node authentication and authorization has a huge impact on backhaul network protection, ensuring the legitimacy of participating devices. It is also important to retain logs of the different access control requests and approvals in order to maintain the non-repudiation principle across the communication flow of the networks. However, the traditional access control protocols are not suitable for

IoT mainly due to a massive scale, ubiquitous connectivity and distributed nature.

A. AUTHORIZATION AND AUTHENTICATION CHALLENGES IN THE ESG

In general, confidentiality, integrity, and availability are the three main security requirements of the ESG. More specifically, the major security requirements of the AMI include message authentication for meter reading and load control messages, as well as confidentiality for user privacy and user behavior. Encryption is the basic technique towards safeguarding confidentiality and integrity, while cryptographic keys are utilized to secure employed authentication protocols.

The authentication and authorization of users is a crucial challenge for the future ESG, since access in field or home or substation equipment should be granted only by following specific policies for authentication and information concerning each user separately and without being known to other participants. Following the same principles, the substations and the utilitys central station should in charge of hierarchically managing all authentication and authorization procedures in the ESG. This way, only authenticated users are allowed to execute the granted authorized actions upon the intended devices in a verified and scalable manner.

In the traditional power network, authentication and authorization are executed as two separate processes. However, it is essential to deploy them as one process in the ESG aiming to manage dynamic user-role authorizations for a large number of users, as well as multiple and frequent authentications among billions of devices [102]. The total execution time will also be reduced, enhancing the system's efficiency. Consequently, users should be mutually authenticated with the substations server in a role-based authorization manner so as to gain access to devices and enable the mitigation of insider attacks in the ESG network.

In the ESG, mutual authentications can be considered between:

- A device and another device (e.g., smart meter and the gateway, RTU and the control center)
- A device and the network (e.g., appliances in a Home Area Network)
- A user and the network/device (home appliances and network)

It is a fact that current authentication protocols faces numerous challenges in terms of efficiency, delay, cost, overhead and privacy. Up until now, none of the proposed technologies has managed to deploy mutual authentication among the energy provider, Home Area Networks, Neighbor Area Networks and AMI network. Furthermore, another challenge lies upon the user's involvement during the authentication of home appliances. The set-up procedure of smart devices is very important and should be handled carefully, since they generate and send data that belong to a particular user. Moreover, none of the proposed authentication protocols has managed to satisfy all the proposed security and performance objectives in the ESG network until now [103].

Authentication protocols rely mainly on cryptographic mechanisms for the AMI. Key management is process that defines the use of cryptographic keys in a given environment, as well as specific rules and types for their deployment [104]. Inadequate key management can endanger the security of AMI communications and also provoke possible key disclosure to attackers. Key management systems are of critical importance for a large number of devices and pose a great challenge in the ESG infrastructure towards sustaining the security concerns in AMI. Hence, considering all these challenges and security requirements of sub-component procedures, we can conclude that developing a sustainable and efficient access control system for the ESG is not a trivial task. Such a system will enforce authentication of all participating networking entities and subnetworks in the grid in distributed and scalable manner, while also avoiding private information disclosure and enabling high quality demand response management. More specifically, *low execution and protocol delay is expected, low computational cost and overhead, as well as resistance to attacks and failures are required. Trust among the ESG network entities is essential, verifying the fact that authentication and authorization mechanisms have a huge impact on privacy protection*.

B. AUTHENTICATION MECHANISMS IN ESG

Towards ensuring and strengthening the security of the AMI for a large number of devices, well-tailored key management techniques should be employed. A key management system involves procedures of key generation, refreshing, distribution and storage policies for achieving participants authentication. Recently, different kind of approaches have been proposed for ensuing efficient key management in the ESG, as well as privacy protection.

In 2019, Zhang *et al.* presented a multi-factor authenticated key establishment (PMAKE) scheme with privacy-preserving properties based on a reverse fuzzy extractor, a physical unclonable function and a cryptographic one-way hash function for achieving secure ESG communication [105]. Based on this scheme, two phases were specified. At first, the service provider should allow the enrollment of new consumers at the network via a request and then an anonymous authentication procedure takes place. In addition, the proposed scheme was proven to withstand all known passive and active attacks.

In the same year, Zhu *et al.* proposed a data aggregation scheme for fog-based ESG communications with privacy-preserving authentication properties [106]. The techniques of short randomizable signature and blind signature were utilized for anonymous authentication of the fog nodes. After that, fog nodes were able to be involved in billing procedures securely. In addition the homomorphic Paillier cryptosystem was deployed in order to safeguard data aggregation. Kumar *et al.* focused on providing a novel elliptic curve cryptography-based authentication protocol for preserving demand response in the ESG [107]. Secret session keys between the ESG devices and a utility center were deployed.

The utilization of this key, enabled sensitive information to be exchanged in a secure way. Security analysis showed that ECCAuth was able to deal with several known attacks.

Recently, Yu *et al.* presented a privacy-preserving lightweight authentication protocol for the ESG system [108] aiming to deal with the weaknesses of Kumar's scheme [107]. The proposed protocol utilized pseudo-identity and secret parameters in order to be resilient against session key disclosure, MITM, masquerade and replay attacks, as well as enable secure mutual authentication and anonymity. The authors created a more efficient and secure scheme by utilizing only hash and XOR operations.

A lightweight anonymous authentication and key agreement scheme for the ESG was also proposed in [109]. Based on this scheme smart meters and the service provider were able to authenticate each other and maintain a shared session key between them. Compared to other authentication models for the ESG, the presented solution ensured smart meter anonymity and untraceability, while achieving fast mutual authentication between networking entities.

Furthermore, the work in [110] focused on achieving smart meter anonymity and preserving data privacy, while also enforcing identity authentication. In this scheme, pseudonym certificates were issued by a TTP authority in order to prevent identity disclosure of smart meters. The Advanced Encryption Standard algorithm is also utilized during the data aggregations process.

Another scheme for preserving demand-response security in the ESG was presented by Alfakeeh *et al.* [111] promoting a group authentication technique. Based on this technique, a single public key operation is employed in order for the utility server to authenticate the ESG smart devices. Once a device enters the group, no public key operation is required in order to be authenticated again. This way communication overheads as well as, the overall computation aiming to deploy a secret key session is significantly reduced. The proposed algorithm was proven to be resilient against various attacks.

Last but not least, DRMAS, an authentication scheme for demand response management for the ESG is proposed in [112]. DRMAS leverages a mutually agreed session key between ESG smart devices and the utility center in order to safely exchange sensitive information. In addition, the proposed scheme was able to deal with several known attacks, to complete authentication and be cost-free of any pairing based operations.

VI. ACCESS CONTROL MECHANISMS IN ESG

An access control mechanism defines the admittance in certain kind of resources or services, promoting security and privacy. Such a mechanism determines the system's communication rights, as well as the authorization of all involving networking entities based on security models and policies [113]. A comprehensive access control of the ESG should be able to deal efficiently with authentication and authorization procedures.

Saxena and Choi [103] reviewed the state of the art in access control mechanisms (ACMs) for the ESG in 2015 and identified three types of access control mechanisms: **user-based access control** (**UBAC**), **role-based access control** (**RBAC**), **and attribute – based access control** (**ABAC**). Other variants have been identified within this review. There is also another classification of ACMs, *centralised and decentralised*. The UBAC technique requires permissions to be defined for each user by a system administrator, based on the individual's needs. On the other hand, RBAC enables to configure permissions according to the different roles in an organizational hierarchy. Each role is defined by a set of access permissions regarding the network's resources. According to RBAC, a user can acquire access permissions defined by one or more roles.

Regarding ABAC technique, policies are defined based on existing attributes in order to provide the desired access rights. This technique utilizes the defined attributes to produce effective rules and requests regarding access control. This is done through a structured language called the extensible Access Control Markup Language (XACML).

On the one hand, the **centralised ACMs** provide a single point of failure but they are easier to maintain as an infrastructure where all the data and access policies are stored. On the other hand, **the decentralised** are more resistant to outages and attacks as they are distributed and provide a more flexible approach for introducing new rule-based policies. In addition to this classification, the schemes that use *attribute-based encryption* can be classified in two groups: *single authority and multi authority* schemes. A **multi authority scheme** manages the attribute keys by multiple authorities in comparison with the single point of failure of single authority schemes.

A. ACCESS CONTROL REQUIREMENTS IN ESG

In 2008, the US Department of Energy released the first AMI System Security Requirements for the ESG environments [114]. In this initial requirements document, thirteen requirements are envisioned for tackling the access control mechanisms technically. The target of these requirements are not technical but oriented to the management and governance of the organisation's security in ESG environments. In addition, according to NIST [22], a list of twenty-one high-level cybersecurity technical requirements are detailed, accompanied by an impact level allocation towards performing risk assessment over the Smart Grid environments. The technical issues that are explored in the document range from access control policies, account management, remote access management to notification systems. More cybersecurity requirements for ESG are presented in [115]. In this article, the authors present a list of technical cybersecurity requirements for access control in ESG service-oriented architectures (SOA). Within this article, it is demonstrated that the use of Web technologies simplifies and enable a flexible way of managing authentication and authorization procedures. This flexibility provides an efficient approach

TABLE 4. Access control requirements for the ESG.

Requirement	Category
Access control security policy and procedures	Common Governance, Risk, and Compliance
Remote Access	Common Governance, Risk, and Compliance and Unique Technical Requirements
Account Management	Common Governance, Risk, and Compliance
Access Enforcement	Common Governance, Risk, and Compliance
Information Flow Enforcement	Unique Technical Requirements
Separation of Duties	Common Governance, Risk, and Compliance
Least Privilege	Common Governance, Risk, and Compliance
Unsuccessful Login Attempts	Common Technical Requirements
Smart Grid Information System Use Notification	Common Technical Requirements
Session Control	Unique Technical Requirements, Availability
Permitted Actions without Identification or Authentication	Unique Technical Requirements
Wireless Access Restrictions	Common Governance, Risk, and Compliance
Access Control for Portable and Mobile Devices	Common Governance, Risk, and Compliance
Use of External Information Control Systems	Common Governance, Risk, and Compliance
Control System Access Restrictions	Common Technical Requirements
Publicly Accessible Content	Common Governance, Risk, and Compliance

for enabling third parties authentication systems to control the access to the data in a fine-grained way. Sato *et al.* [116] in his book review the different standards, requirements and technologies for the Smart Grids, dedicating a whole chapter for Smart Grid security. An analysis of the IEC 62351 series is also detailed, including, in this case, the IEC 62351-8 dedicated to the role based access control standards of this IEC series. Table 4 presents a summary of the proposed access control requirements recommended for the ESG infrastructure.

B. CENTRALISED ACCESS CONTROL IN ESG

Bobba *et al.* [117] developed a *Policy-Based Encryption System (PBES)*. This mechanism encourages the use of sharing information across competing companies by using *a centralized key distribution centre (KDC)*. As a single KDC point of failure (single authority), this is raised as a security issue limiting the implementation of this mechanism.

Wu *et al.* [118] suggested a new issue in the ACMs regarding the transaction of information on noisy communications channels. To that end, Wu *et al.* proposed *fuzzy identity-based encryption (IBE) with lattice-based access control(LBAC)* in a fine-grained access control scheme design.

After that, Yeo *et al.* [119] proposed a *new dynamic ACM based on RBAC mechanisms and context awareness control (CAAC) model*. The security of this model lies in the use of both mentioned mechanism (RBAC and CAAC) for enabling role-based access control while allowing a dynamic measuring of the current context of the user, then, based on the context, an access policy is executed.

Moving forward, Wen *et al.* [120] introduced a new data aggregation scheme for fine-grained access control. In this article, *a data aggregation scheme based on attributes decision tree (DABA)* is proposed.

Similarly, a *Multidimensional-data Tight Aggregation scheme* which supports Privacy-preserving and fine-grained Access control (MTAPA) has been proposed recently by B. Lang *et al.* [121]. MTA-PA is based on Boneh-Goh-Nissim (EBGN) homomorphic encryption scheme and KP-ABE for the access control at the dimension level. The security analysis is reasonable and it is noteworthy that it is not necessary with this mechanism to de-crypt and re-encrypt in middleware nodes of the AMI reducing the threat surface for data leaks. No details about the authority model are covered in this work.

C. DECENTRALIZED ACCESS CONTROL IN THE ESG

The evolution of the ESG necessitates the deployment of decentralized access control systems where access rights are granted by the requested smart meters or other authorized network entities rather than a centralized entity. The traditional access control models lack the ability of dynamic permission management. In its current state the ESG is based on a centralized management mode, with low adaptive ability. Due to its vast scale, it is essential to address any constrains regarding information storage and resource access in order to improve reliability and quality of service. Therefore, a novel access control environment should be deployed leveraging both access control and authorization.

In order to address this matter, a *role attribute-based access control (RABAC)* is introduced in [122]. Scalability and multi authority is provided by following a domain of domains (DoD) concept while flexibility and interoperability are ensured by using an heterogeneous communication model for heterogeneous networks. No benchmark or analysis of the security of this proposed ACM is presented in this article.

Later, Ruj and Nayak [123] proposed an *offline multi authority decentralized ACM*. *Homomorphic encryption* is used for achieving confidentiality of customer data and attribute-based encryption (ABE) is used for access control. Although the use of this mechanism is more robust than Bobba *et al.* [117] as being decentralised and more privacy-oriented, one drawback is the performance penalty introduced by the use of homomorphic encryption as it is first seen in this article. Simultaneously, Liu *et al.* [124] proposed *a Multi Authority Access Control with Efficient Attribute Revocation (MAAC-AR) scheme*. This scheme is based on attribute-based encryption for achieving fine-grained access control.

TABLE 5. Access control mechanisms in the ESG.

Scheme	Topology	Authority model	Mechanism(s)	Relevance
Bobba et al.	Centralised	Single authority	PBES	Low
Kim et al.	Decentralised	Multi authority	RABAC	High
Ruj et al.	Decentralised	Multi authority	ABE	High
Wu et al.	N/A	N/A	IBE/LBAC	Low
Yeo et al.	N/A	N/A	RBAC	Medium
Liu et al.	Decentralised	Multi authority	ABE	High
Mutsvangwa et al.	Decentralised	Multi authority	CP-ABE	High
Wen et al.	N/A	N/A	DABA	Medium
Guan et al.	Decentralised	Multi authority	KP-ABE	High
B.Lang et al.	N/A	N/A	KP-ABE	Medium

A new implementation based on a *CP-ABE(Ciphertext-Policy Attribute-Based Encryption)* based access control is proposed by Mutsvangwa *et al.* [125]. This scheme follows *a multi-KDC (multi authority) approach* allowing a positive decentralisation of the key distributions. In addition, moderate performance in terms of the computational load is expected by using this implementation. Simultaneously, Guan *et al.* [126] proposed *a delay-tolerant flexible data access control mechanism based on a Key-Policy Attributed-Based Encryption (KP-ABE) on a multi authority basis*. One aspect of the proposed scheme is the delay-tolerant processing of encrypted information sent by Residential Units (RUs).

Later on, the authors in [127] proposed a new access control model for distributed management. The proposed authorization mechanism manages dynamically the access rights, while providing the opportunity to all participating nodes to be involved in the execution of access and control. Similarly, the work in [128] presents a new decentralized access control system, which empowers the users to control the access to their resource, while also leveraging the Masked Authenticated Messaging (MAM) data communication protocol in order to safeguard user privacy. Table 5 presents a summary of existing access control mechanisms for the ESG.

Following the same direction, *Blockchain and Distributed Ledger Technologies (DLT)* have burst into the catalogue of technologies for ensuring access in modern decentralized architectures. This is all due to the principles of the Blockchain technologies, which are: (a) fault tolerance to attacks (e.g., DDoS, device malfunctioning or data loss) due to the decentralized nature of Blockchain technologies, (b) confidentiality and integrity by design, which is typically adopted by many applications, for the exchange of information at Blockchain level by the use of cryptographic mechanisms (c) the use of smart-contracts, which enables the use of advanced logic rules on the transaction of information.

D. BLOCKCHAIN IN ESG

The distributed architecture of nodes and machines in the ESGs demands resilience and fault-tolerance to outages and attacks. Blockchain is one of the most promising research fields to handle these challenges. It was first presented by Nakamoto Satoshi in 2008 towards deploying effective bitcoin decryption [129]. The basic concept of a blockchain is that it enables the participation of all users in the network towards autonomous data storing and distribution. In Bitcoin cryptocurrency Blockchain was implemented in the form of a public ledger in a peer-to-peer network, where nodes replicated and stored continuous and cross-depended blocks of information. The distribution of the blocks is based on a consensus algorithm. The blocks' encryption utilizes a hash which is produced based on the data of the previous block in the chain. This method can guarantee the integrity and confidentiality of the data on the chain. In addition, chain operations can be constantly monitored and tracked, while avoid imitations. Data for all transactions completed in the Blockchain is safeguarded, since anonymous information sharing takes place by the users involved.

The tamper-proof and trace-ability-oriented design of the Blockchain makes them interesting in some use cases for the ESG environment.

Di Francesco Maesa *et al.* [130] introduced the use of Blockchain as a *generic access control mechanism*. In this novel implementation, the underlying mechanism is an ABAC through the Bitcoin Blockchain. The policies are expressed in XACML and there is public visibility of the policies in the Blockchain. However, some drawbacks are identified, the first one is the size of the policies which are heavy for a Blockchain, this could incur in high use of computational resources. The second one is the used technology for the Blockchain, in this case, the authors used Bitcoin which is a public Blockchain. This is considered a privacy and security issue because an attacker could have access to the authentication and authorization procedures in the Blockchain. Ouaddah *et al.* [131] proposed *FairAccess, a Blockchain-based access control framework* for IoT. This framework features an identity-based access control with permissioned access policy based on Bitcoin testnet and an Organization-based Access Control (OrBAC) model. It is worth highlighting from this work the proof of concept implementation yet the use of Bitcoin as a public Blockchain is negative for privacy-oriented environments. Following this research, Laurent *et al.* [132] proposed another access control scheme based on Blockchain technology, in this case, the *Ethereum Blockchain*. This mechanism features an access control list (whitelist) approach for

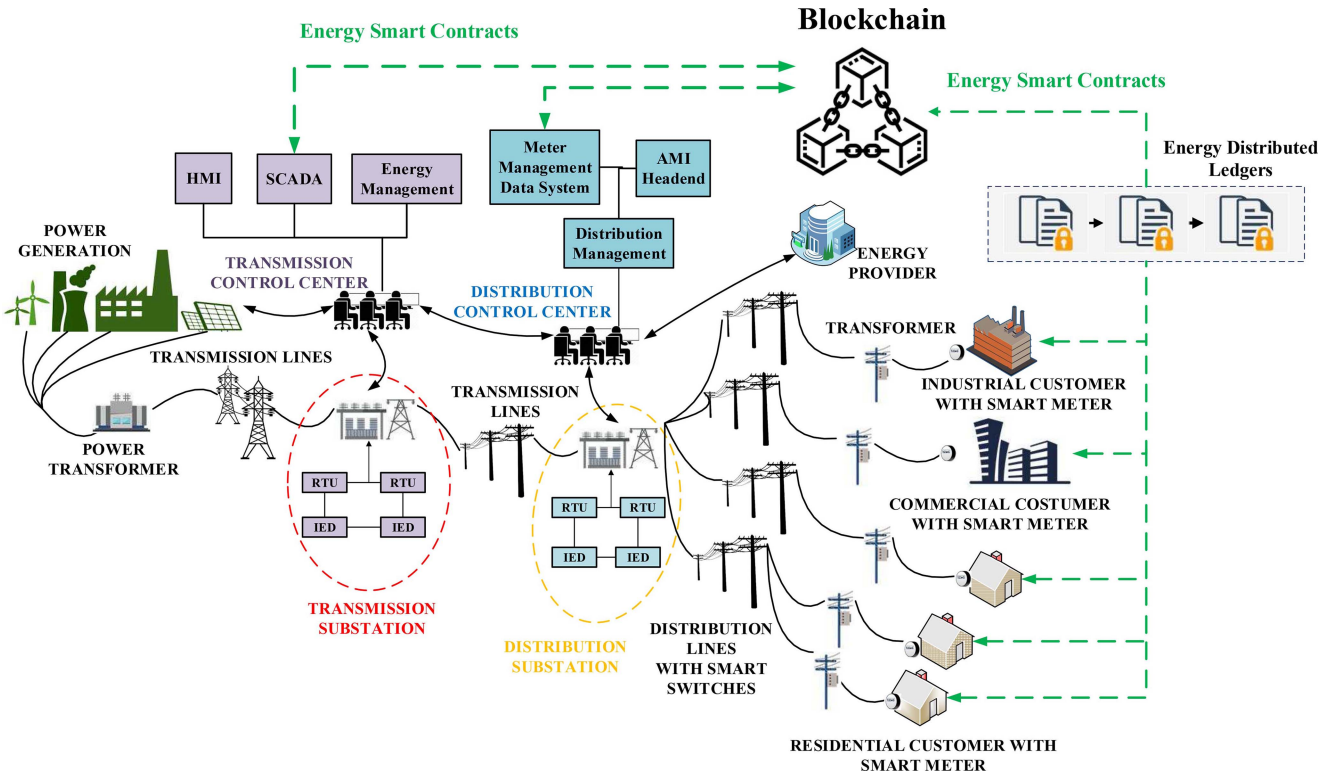

FIGURE 6. Blockchain application in the ESG.

the different restricted resources and the authorization is handled by the Blockchain infrastructure. In contrast with Di Francesco Maesa *et al.* [130], *Smart Contracts* are introduced in this scheme for managing the whitelist. A threat model is also presented in the security analysis of this implementation yet it lacks advanced access control mechanisms such as RBAC, ABAC or other variants. Lin *et al.* [133] proposed *a new Blockchain-based secure mutual authentication with fine-grained access based on Attribute-based signature (ABS)*. Recently, Maesa and colleagues have revisited their work [134], this time the Blockchain technology was changed from Bitcoin to Ethereum, which have private Blockchain capabilities. In this new approach, XACML is again used as a data format for the policies and proof of concept is provided. The use of Ethereum was performed in the public testnet raising security and privacy issues yet the authors acknowledge that the use of a permissioned (private) Blockchain could reduce costs and improve trust.

All the mentioned work above this paragraph is not focused on ESG exclusively. To that end, a novel Blockchain-based access control scheme for the ESGs has been proposed recently by Zhou *et al.* [135]. This scheme features *identity-based cryptography (IBC)* for the access control mechanism. A performance analysis is provided yet the details and performance implications of using a Blockchain are not fully detailed. Simultaneously, Zhang *et al.* [136] have developed *a Blockchain-based decentralized keyless signature scheme for the ESG*. To do so, Zhang and colleagues developed a new consensus method for deploying authentication procedures in the Blockchain based on the Merkle hash tree. This scheme is well detailed in terms of computational costs and performance implications. A comparison against similar schemes is also provided.

Another implementation regarding the Distributed IoT was proposed in [137] designing a blockchain-based access control scheme called BacS. Based on BacS, a redefinition of the access control permissions of the data services is deployed and stored on the blockchain, once the data has accessed the management server of current domain. In parallel, Shi *et al.* utilized a lightweight symmetric encryption algorithm (SEA) to achieve privacy-preserving for Distributed IoT system.

Figure 6 demonstrates the role of Blockchain in the ESG infrastructure. Blockchain based smart energy contracts can be quite useful for safeguarding the operations of the ESG infrastructure. They are based on the distribution of cryptographically signed ledgers towards maintaining the integrity of data, leveraging trustworthiness and securing the system′s resilience at the edge. Furthermore, based on this technique autonomous anomaly detection can be employed in the infrastructure, delivering any potential unauthorized attempts to modify critical EDS data in a real-time basis. Moreover, Blockchain can be used to manage the versioning of time, user and data transactions, while providing unchangeable crypto signed ledgers for data protection.

Despite the fact that the ESG produces and supplies electricity from various sources of primary energy, like

TABLE 6. Blockchain schemes for the ESG.

Scheme	Authority model	Mechanism(s)	Special features
Zhou et al.	Decentralised	IBC	confidentiality, integrity, authentication and non-repudiation of data
Zhang et al.	Decentralised	Merkle hash tree	Key management without TTP
Shi et al.	Decentralised	SEA	Credible experimental model on Ethereum private chain
Firoozjaei et al.	Decentralised	k-anonymity	Credit-sharing information, Subnets
Gai et al.	Decentralised	Group signatures	Covert channel authorization
Zhang et al.	Decentralised	ABAC	Reliability, flexibility
Liu et al.	Decentralised	CBAC	Overhead balance and fault tolerance strategy

hydroelectric power plants, the ability of producing electricity will also be provided to each house or building by employing its own solar panels. Based on this assumption, all members of the ESG, such as factories, bulk generation operators , renewable energy power plants, energy consumers and producers will utilize smart contracts towards exchanging real-time energy data in a two-way method. More specifically, when the consumer buys electricity, a unique timestamped block for verification will be created in a distributed ledger by the blockchain enabled AMI.

This way, energy transaction data can be securely transferred by system operators to consumers in order to charge their network costs via the Blockchain mechanism. Moreover, modifications on data requirements will be required towards increasing the speed of clearing transactions between the various transmission system operators. Transactions will be managed and executed on the basis of actual consumption. In order to protect data from possible cyber-attacks, encrypted blocks will be utilized in order to store information and provide a connection to a blockchain towards constructing a database in real time.

Based on the trustful end-to-end functionality of the blockchain, Hy-Bridge, a hybrid blockchain-based billing and charging framework was recently presented in [138]. In Hy-Bridge, due to the blockchain-distributed consensus, a credit-sharing feature for participants is provided regarding the energy and utility market. Credit-sharing information is exchanged based on a local block framework for service management, while user privacy is preserved by isolating peer-to-peer transcations in subnetwork blockchains, where k-anonymity is utilized. All transactions are then connected to the main blockchain based on a hybrid model. An alternative permissioned blockchain edge model for ESG network is also presented in [139]. This model utilizes covert channel authorization techniques to safeguard the validity of participants, as well as group signatures. In addition, the authors included an optimal strategy for security awareness based on smart contracts running on the blockchain. Another interesting approach regarding decentralized, flexible, and fine-grained authorization for smart devices is proposed in [140]. The authors utilize blockchain, as well as attribute-based access control capabilities for their model. It was shown that collaboration of these techniques achieves enhanced reliability and flexibility in cases of controlled access authorization in emergencies.

Furthermore, a blockchain-based communication protocol is realized in [141] for overhead balance strategy and fault-tolerance strategy. In order to deal with access control gaps in blockchains, this work proposed a digital control scheme of certicate-based data access (CBDA). Additionally, a public anonymous authentication method is utilized for preserving user privacy and identifying malicious anonymous users that might have managed to obtain any of the distributed certificates. Table 6 summarizes the Blockchain-enabled mechanisms for the ESG infrastructure employing efficient access control and authorization in a privacy preserving manner.

VII. FEDERATED LEARNING FOR PRIVACY PRESERVATION IN THE ESG

The ESG handles a large and complex volume of generated data on different network entities towards deploying real-time processing. In order to provide reliable and high quality services, the ESG infrastructure utilizes Machine learning (ML) techniques that enable secure information analysis and storage for all generated data. ML is a process of pattern identification, prediction and decision making based on previously acquired information towards addressing different kind of tasks. Moving towards the vision of a decentralized ESG infrastructure, the design and development of such technologies is essential. Such techniques will enable the dynamic integration of ESG components, as well as the secure exchange of all generated data and behavioural patterns. Long-term load forecasting can greatly benefit from the evolution of ML. However, such an ESG essential service can raise privacy concerns, since the load profiles reveal a lot of sensitive information about consumers [142]. Towards addressing this security issues, without degrading data volume and variety, Federated Learning (FL) was recently proposed as an on-device solution [143].

FL is a promising technique in edge computing, focused on model training for multiple parties, where the ML algorithm is run locally by data holders and only model parameters are exchanged [144]. This way participants can learn a global model collaboratively while preserving their privacy. FL outperforms conventional ML, in which a centralized curator collects all training data, by reducing privacy concerns and transmission costs, since the training work is distributed amongst all participants. In the ESG infrastructure, FL can be performed on the edge equipment, such as a smart meter in each house, posing as an interface between the customer and the electric power supply. Based on FL, the

ESG can exploit the capabilities of secure distributed intelligence and also utilize Blockchain technology to develop an efficient collaboration among untrusted entities for reliable data sharing [145].

Based on this assumption, a novel blockchain-enabled federated learning (FL-Block) scheme is proposed in [146]. FL-Block utilizes blockchain to verify miner participants, so as to allow local learning updates on each participating end-device. Based on this collaborative scheme, the global model is not kept in centralized entity and autonomous machine learning is enabled.

Similarly, in [147] the authors presented a Federated Capability-based Access Control model (FedCAC) for large scale IoT systems. Based on the proposed scheme, FL is utilized in order to propagate access permission amongst participants, while an identity-based management strategy is employed in order to handle the access rights. By decentralizing the authorization decision-making policy, the service provider can locally perform the access authorization process leveraging situational awareness.

Moreover, the work in [148] realized a novel architectural model for data transmission based on permissioned blockchains. Based on this model, the authors focused on deploying secure connections between all IoT nodes. By utilizing permissioned blockchains and FL capabilities security was shown to improve during data transfer, as well as data privacy to be efficiently preserved.

Regarding the field of Fog Computing, a privacy preserving system based on FL was also proposed in [149]. The utilization of FL improves the training capabilities of the proposed scheme, while the security of the IoT device data is enforced. In order to prevent the interference of third-party malicious parameters, authors deploy differential privacy accompanied by the Paillier homomorphic encryption as well. A secure parameter aggregation method is also presented in this work, based on blinding and Paillier homomorphic encryption, aiming to safeguard participants against infected Fog nodes.

Last but not least, an efficient and privacy enhanced federated learning (PEFL) scheme for industrial artificial intelligence was proposed in [150], guaranteeing aggregation oblivious security. The PEFL scheme was shown to provide a high privacy-protection level, while preventing privacy leakage from the local gradients as well as the shared parameters.

FL has yet to be employed or even practically tested in the ESG infrastructure. Nevertheless, all recent research points to promising results regarding its performance on privacy preservation. FL is a useful tool that can be combined with Blockchain technology in order to design and develop a novel access control mechanism that utilizes secure and decentralized block-chains with privacy preserving capabilities for the ESG. FL is a framework that is not designed to fill in the technological gaps of access control by itself. However, in collaboration with the capabilities of other authentication and access control schemes can produce significant improvements in the overall security of ESG.

VIII. DISCUSSION AND CHALLENGES

The ESG infrastructure provides different kinds of services ranging from real-time control processes to dynamic pricing and detailed state estimation of the various distributed operations in smart metering. These services require the collection of fine-grained data with different levels of metering frequency and data accuracy. As presented in the previous sections, a variety of privacy preserving approaches have already been proposed for the ESG, aiming to satisfy the basic privacy requirements and follow the guidelines established by organizations. The AMI is considered as the brain of the ESG. Data privacy breaches are more likely to occur in this section of the grid compared to others in various forms. Up until now privacy was attempted to be secured either while the data was in transit, involving services like on-demand metering, billing and real-time pricing, or at the smart meter level by hiding a part of them. However, due to the fact that most of existing literature works evaluate the proposed approaches via simulation and not via real-world devices, the ESG domain suffers from reproducibility of research results. Table 7 summarizes the aforementioned privacy-preserving techniques for the ESG according to the type of the protected data. ESG protected data may involve (a) electricity consumption data aggregated from smart meters, (b) billing information regarding electricity costs and contract data requirements of the corresponding utility company, (c) subscriber profile information referring to residents' personal information such as name, surname, age, address, social security number etc., (d) prosumer general characteristics including information regarding electricity network balancing operations, as well as electricity production and consumption and (e) types of devices operating at home according to amounts of energy consumed.

A. DATA MISUSE

The challenge of preventing the misuse of consumption data is currently focused on the utilization of trusted remote entities. Based on consumption data, consumer electronics companies may promote appliances, leading to consumers' privacy intrusion. Due to this fact, the leakage of sensitive information results as an inevitable fact in the AMI system. Currently, trusted remote entities are promoted to ensure the privacy of consumption usages and prevent utilities from misusing them. However, such techniques are proven to be vulnerable to eavesdropping cyber-attacks. Additionally, despite the fact that symmetric cryptography based schemes perform well in terms of energy cost and timing, further research is needed for the efficient employment of such anonymization techniques in the future decentralized ESG.

Homomorphic cryptosystems are another popular privacy-preserving solution providing security against information leakage attacks. Nevertheless, the exchange of large messages between the involved devices required in such

techniques degrades network performance and makes it vulnerable to other kinds of cyber-attacks.

Moreover, battery-based Data Masking mechanisms were presented in various forms by researchers throughout the years considering the manipulation of smart meter measurements towards disguising the real energy consumption values. For this purpose, a rechargeable battery is used to partially supply the energy demand. However, despite theirs benefits, BDM approaches are greatly affected by the capacity, the charging and discharging of the corresponding battery.

Novel and advanced privacy-preserving mechanisms producing a high level of trustfulness in transactions are essential to be implemented in order for consumers to be able to control and protect their information, while satisfying the desired requirements of the AMI services.

Existing solutions may ensure consumer privacy on some level via data anonymization, but there is a risk of preventing utilities from providing consumer specific services since specific parts of consumption information are concealed. Moving towards a decentralized management strategy of the ESG infrastructure privacy-aware machine algorithms should be implemented based on anonymization techniques. That is the only way to protect the exchange of private information, while performing machine learning training and/or testing. Challenges in this task lie on the need to re-purpose the machine learning algorithms in order to cope up with the new advances and scalability requirements, both in terms of processing and communication costs [151].

Distributed privacy in smart metering processes can also be facilitated by the utilization of advanced and secure network routing protocols, assuring high reliability on data delivery. The evolution of networking protocols for the ESG includes the employment of encryption as a common addition. However, the challenge lies on choosing the right kind of communications to be encrypted and in the right time. Such knowledge can be obtained by monitoring and studying the network traffic in the grid by utilizing intrusion detection mechanisms.

B. AUTHENTICATION, AUTHORIZATION, AND KEY MANAGEMENT

As stated in [152], limited research is being done regarding the authentication of user data and behavioral privacy in the AMI. The development of key management and authentication techniques can be based on lightweight and secure cryptography techniques such as hash functions, ECC, coding based techniques, and Merkle trees.

Another promising future direction focuses on the implementation of sophisticated key management frameworks combined with attribute-based access control qualifications. The work presented in [153] proposes a lightweight key agreement protocol, based on the IEC 62351 part 9, for increasing the security in substations and data center. The protocol minimises the vulnerabilities of IEC 62351 regarding the use of symmetric keys for communication encryption. Similarly, a novel anonymous authentication and key agreement protocol is presented in [154] providing methods of key update and revocation in aims of minimizing communication costs and employing conditional identity anonymity.

The overall ESG security and privacy goals demand a more advanced and complex security system that can seamlessly extend key management services across multiple platforms and networks of the grid, while protecting the consumers privacy. In order to provide authentication and authorization of users in the ESG, role-based passwords are utilized by smart meters, intelligent electronic devices and other outdoor field equipment. Due to the large number of devices, these passwords are often similar in each utility, transforming them to possible entry points for malicious actors. It is quite challenging to ensure user authentication and authorization in the ESG due to the fact that these devices may be accessed physically on the spot or even remotely from different locations in a wired or wireless way.

Authorization should be employed in way that each user can perform only specific actions as instructed under the access permissions granted to him/her. Based on this assumption, the resource access should be specific to each user exclusively, while enforcing a hierarchically management strategy in substations and central stations for the control of authentication and authorization. This way only authenticated users will be able to interact with the indented devices by performing assigned authorized actions in a scalable and controlled manner. By utilizing specific user-role authorization mechanisms, insider attacks can be efficiently mitigated in the ESG.

Future work should be focused on the development of decentralized authorization systems without the use of a central trusted party. Such systems would be ideal for the ESG infrastructure, since they can safeguard user privacy, be scalable enough as well as protect from malicious actors aiming to manipulate the grid network traffic.

C. ACCESS CONTROL

Designing a fully-equipped access control system for the ESG, while also safeguarding data privacy is a non trivial task. Literature shows that were several attempts towards this direction. On the one hand, centralized access control schemes were proposed, where a centralized authority is utilized in order to employ authorization policy management and policy decision making. In such systems it is easy to adapt existing security standard technologies and manage authorization rules. However, centralized access control is vulnerable to systems failures since there is only one centralized entity for management and storing. A performance bottleneck is also likely to occur towards achieving high quality of service for the users. Last but not least, privacy protection is entrusted on a TTP authority, that was proven to be inefficient towards several kinds of attacks. On the other hand, decentralized access control systems deploy authorization policy on the edge of network, enabling user to intelligently control the access to their private data,

TABLE 7. Privacy-preserving techniques in the ESG.

Techniques/Data types	Electricity consumption data	Billing information	Subscriber profile information	Prosumer general characteristics	Devices operating at home
How to preserve data privacy during data aggregation ?	1. TTPs 2. Perturbation 3. Symmetric key cryptography 4. Asymmetric key cryptography 5. Hash functions 6. Homomorphic encryption	1. TTPs 2. Symmetric key cryptography 3. Asymmetric key cryptography 4. Hash functions 5. Homomorphic encryption	1. TTPs 2. Symmetric key cryptography 3. Asymmetric key cryptography 4. Hash functions	1. TTPs 2. Perturbation 3. Symmetric key cryptography 4. Asymmetric key cryptography 5. Hash functions 6. Homomorphic encryption	1. TTPs 2. Perturbation 3. Symmetric key cryptography 4. Asymmetric key cryptography 5. Hash functions 6. Homomorphic encryption
How to perform data anonymization ?	1. Differential privacy 2. K-anonymity 3. Cluster-based anonymity	1. Differential privacy 2. K-anonymity 3. Cluster-based anonymity	1. Differential privacy 2. K-anonymity 3. Cluster-based anonymity	1. Differential privacy 2. K-anonymity 3. Cluster-based anonymity	Differential privacy
How to perform data obfuscation ?	1. Noise addition 2. Transformation energy usage data 3. Shared keys 4. TTPs 5. Power line obfuscation	1. Noise addition 2. Transformation energy usage data 3. Shared keys 4. TTPs 5. Power line obfuscation	1. Noise addition 2. Shared keys 3. TTPs	1. Noise addition 2. Shared keys 3. TTPs	1. Transformation energy usage data 2. Power line obfuscation
How to protect data privacy in battery-based schemes ?	1.Differential privacy metrics 2. Non-Intrusive Load Leveling 3. Rechargeable batteries to configure constant energy usage 4. Noise addition	1. Differential privacy metrics 2. Non-Intrusive Load Leveling 3. Rechargeable batteries to configure constant energy usage 4. Noise addition	1.Differential privacy metrics	1.Differential privacy metrics	1. Differential privacy metrics 2. Non-Intrusive Load Leveling 3. Rechargeable batteries to configure constant energy usage 4. Noise addition

while also reducing the risk of data misuse and leakage by a centralized entity. Another advantage of such systems is that there is limited influence on the network in case of a failure, as well as distributed trust relationships amongst the edge networking entities. Nevertheless, decentralized access control faces challenges regarding the implementation of authorization mechanisms on resource-constrained edge devices in terms of memory and storage. Latency and overhead are increased over the network communications. Moreover, a higher level of complexity is involved due the heterogeneity of devices in the ESG.

Another promising research direction towards enforcing privacy and efficient access control in the ESG is lead by cloud computing services. Nevertheless, this endeavour is highly dependent on authentication protocols that face several challenges towards their employment in the ESG infrastructure regarding efficiency, cost and delay. Providing mutual authentication among home area networks, industry area networks involving energy providers and the AMI network is a challenging task. Up until now, no protocol has been proven to be up for this task.

Several recent works have shown that Blockchain technology is ideal for the ESG infrastructure since it provides decentralized security and privacy. Blockchain technology enables the transfer of field measurement data and local transaction data in a peer-to-peer manner within the ESG. A decentralized manner for storage and data replication is employed on multiple devices, instead of a single data center.A variety of advantages are introduced by the Blockchain technology for the ESG including data reliability, simplicity in transactions' implementation between between untrusted peers, transparency in the distribution of resources, as well as security in establishing authorization mechanisms. A fast and public blockchain mechanism is the best choice for access control in the ESG. In such a blockhain operation, the nodes are trustless and anonymous, enforcing longer transaction approval time [155]. Still, in order to employ efficient privacy protection, modifications are required. Additionally, the public blockchain poses several challenges regarding increased network latency, energy consumption, transaction costs and computational overhead. Despite its advantages, integrating the blockchain technology may expose ESG to new types of cyber security issues, since it still suffers from several cyber security vulnerabilities [156].

Moving towards the vision of a decentralized ESG infrastructure, future research should focus on the implementation of decentralized authentication protocols and access control schemes that fulfil all the proposed security and performance objectives in the ESG. Federated learning is a novel technique that can enable privacy protection on edge-smart meters leveraging distributed intelligence in a scalable and authorized manner. Further research in this promising field is highly recommended since the collaboration between FL and Blockchain technology fills in the technological gap regarding the design and development of a novel access

control mechanism with privacy preserving capabilities for the ESG.

D. PRIVACY ECONOMIC MODELS

Another challenge regarding privacy in the ESGs focuses on the deployment of privacy economic models for smart meter data. The ESG paradigm facilitates the advancement of digital economies and privacy economics. The ESG promotes new business models and actors (aggregators) who rely on metering data so as to create portfolios and manage their assets. However, the challenges in this field are caused by the consumers′ ignorance and insecurity regarding the purpose and utilization of their personal data. A way to make customers aware of their energy behavior is the utilization of high resolution metering. This way passive (consumers) can be turned to active (prosumers) who will also be able to provide services to the grid [157]. Reliable data sharing techniques and mechanisms could be developed that would allow consumers to trust and feel safe regarding the disclosure of their private information. This anonymous data sharing could be utilized to maximize the social welfare. The deployment of such schemes would require the cooperation of privacy theoretic models and game theoretic models concerning consumer-operator interaction.

E. CASE STUDIES

The need for novel and hybrid privacy preserving approaches which follow the General Data Protection Regulation (GDPR) guidelines is essential towards the efficient deployment of ESG operations. The *Secure and PrivatE smArt gRid (SPEAR)* project is a Horizon 2020 framework research program aiming at the development of an integrated platform of methods, processes and tools for safeguarding the ESG from cyber-attacks [158]. SPEAR values the advantages of anonymous data sharing, digital certificates and hybrid privacy preserving schemes leveraging access control properties towards providing a trustful ESG communication network.

ESG privacy preservation mechanisms and access control capabilities are also being studied in the *SDN - microgrid reSilient Electrical eNergy SystEm (SDN-microSENSE)* project, another European Unions Horizon 2020 research and innovation programme [159]. SDN-microSENSE focuses on providing a platform of secure, privacy-enabled and resilient to cyber-attacks tools, towards safeguarding the efficient and reliable operation of Electrical Power and Energy Systems (EPES). Stakeholder data exchanges in modern EPESs should promote the integrity and the confidentiality of information. The SDN-microSENSE architecture utilizes Blockchain capabilities and modern anonymization techniques towards preventing potential data breaches.

These research projects are in the way of addressing the security needs and technological gaps of current networking and communication technologies for the ESG infrastructure. Their innovations in the security and privacy frameworks follow the highlights of the current survey, extending the capabilities of existing privacy preserving techniques in cooperation with efficient access control mechanisms.

IX. CONCLUSION AND FUTURE WORK

The ESG is a modern EPES. Being beneficial not only to the power industries, but also the consumers, ESG promotes efficient energy generation, distribution and monitoring, while preserving information privacy. However, due to its vast scale, many vulnerabilities are found to exist. This survey discussed how can privacy breaches and manipulation of energy consumption data be avoided in the ESG. A variety of privacy-preserving schemes and access control approaches where presented promoting different kinds of mechanisms and techniques for securing privacy in the ESG.

Smart grid privacy requires well-tailored solutions, novel hybrid approaches which follow legal and regulatory guidelines while considering a number of different interconnected stakeholders. It is essential to perform efficient metering in the AMI for every household, while safeguarding the privacy of sensitive information exchanged based on highly secured and authorized aggregation procedures. Novel authentication processes should be able to safeguard the confidential and private information of related entities and generally be able to support mutual authentication operations in the network infrastructure. A secure and reliable access control scheme can efficiently manage each entity after the authentication process.

This work presented a new viewpoint on smart grid history by promoting challenging perspectives and goals regarding the ESG's future. The identification of specified privacy needs and vulnerabilities of the ESG is vital for researchers so as to efficiently mend security gaps and propose new technologies.

REFERENCES

[1] A. Triantafyllou, P. G. Sarigiannidis, and T. D. Lagkas, "Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–24, Sep. 2018. [Online]. Available: https://doi.org/10.1155/2018/5349894

[2] K. Sayed and H. Gabbar, "Chapter 18—SCADA and smart energy grid control automation," in *Smart Energy Grid Engineering*, H. A. Gabbar, Ed. London, U.K.: Academic, 2017, pp. 481–514. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128053430000188

[3] T. N. Le, W. Chin, D. K. Truong, and T. H. Nguyen, "Advanced metering infrastructure based on smart meters in smart grid," in *Smart Metering Technology and Services—Inspirations for Energy Utilities*, M. Eissa, Ed. London, U.K.: IntechOpen, 2016. [Online]. Available: https://www.intechopen.com/books/smart-metering-technology-and-services-inspirations-for-energy-utilities/advanced-metering-infrastructure-based-on-smart-meters-in-smart-grid

[4] S. Desai, R. Alhadad, N. Chilamkurti, and A. Mahmood, "A survey of privacy preserving schemes in IoE enabled smart grid advanced metering infrastructure," *Clust. Comput.*, vol. 22, no. 1, pp. 43–69, Mar. 2019. [Online]. Available: https://doi.org/10.1007/s10586-018-2820-9

[5] "Annex II—Security aspects of the smart grid," Eur. Union Agency Cybersecurity (ENISA), Marousi, Greece, Rep., 2012. [Online]. Available: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering

[6] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *IEEE Access*, vol. 7, pp. 13960–13988, 2019.

[7] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1088–1101, 2nd Quart., 2015.

[8] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2820–2835, 4th Quart., 2017.

[9] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," *Comput. Commun.*, vols. 91–92, pp. 17–28, Oct. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366416302572

[10] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "A systematic review of data protection and privacy preservation schemes for smart grid communications," *Sustain. Cities Soc.*, vol. 38, pp. 806–835, Apr. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2210670717308399

[11] W. Ding, X. Jing, Z. Yan, and L. T. Yang, "A survey on data fusion in Internet of Things: Towards secure and privacy-preserving fusion," *Inf. Fusion*, vol. 51, pp. 129–144, Nov. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1566253518304731

[12] S. Sultan, "Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey," *Comput. Security*, vol. 84, pp. 148–165, Jul. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818303675

[13] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2886–2927, 3rd Quart., 2019.

[14] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 746–789, 1st Quart., 2020.

[15] X. Xiong, S. Liu, D. Li, Z. Cai, and X. Niu, "A comprehensive survey on local differential privacy," *Security Commu. Netw.*, vol. 2020, Oct. 2020, Art. no. 8829523.

[16] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Comput. Sci. Rev.*, vol. 38, Nov. 2020, Art. no. 100312. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574013720304123

[17] N. Kaaniche, M. Laurent, and S. Belguith, "Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey," *J. Netw. Comput. Appl.*, vol. 171, Dec. 2020, Art. no. 102807. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804520302794

[18] L. Cui, Y. Qu, L. Gao, G. Xie, and S. Yu, "Detecting false data attacks using machine learning techniques in smart grid: A survey," *J. Netw. Comput. Appl.*, vol. 170, Nov. 2020, Art. no. 102808. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804520302769

[19] J. Kang, "Information privacy in cyberspace transactions," *Stanford Law Rev.*, vol. 50, pp. 1193–1294, Apr. 1998. [Online]. Available: https://ssrn.com/abstract=631723

[20] R. Zafar, A. Mahmood, S. Razzaq, W. Ali, U. Naeem, and K. Shehzad, "Prosumer based energy management and sharing in smart grid," *Renew. Sustain. Energy Rev.*, vol. 82, pp. 1675–1684, Feb. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032117310894

[21] S. Li, A. Khisti, and A. Mahajan, "Information-theoretic privacy for smart metering systems with a rechargeable battery," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3679–3695, May 2018.

[22] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, "Guidelines for smart grid cybersecurity," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NIST IR 7628r1, Sep. 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[23] "Guidelines for smart grid cyber security: Volume 2, privacy and the smart grid," NIST Smart Grid Interoperability Panel–Cyber Security Working Group, Gaithersburg, MD, USA, Rep. NISTIR 7628, Aug. 2010. [Online]. Available: https://www.smartgrid.gov/files/Demand_Shifting_With_Thermal_Mass_in_Light_Heavy_Mass_Commer_201009.pdf

[24] "Smart grid task force 2012-14, data protection impact assessment template for smart grid and smart metering systems," Smart Grids Task Force Expert Group 2, Regulatory Recommendations for Privacy, Data Protection and Cyber-Security, Smart Grid Environment of the European Commission, Brussels, Belgium, Rep., Sep. 2018. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf

[25] S. Werner and J. Lundén, "Smart load tracking and reporting for real-time metering in electric power grids," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1723–1731, May 2016.

[26] M. M. E. A. Mahmoud, N. Saputro, P. K. Akula, and K. Akkaya, "Privacy-preserving power injection over a hybrid AMI/LTE smart grid network," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 870–880, Aug. 2017.

[27] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283–302, 1st Quart., 2014.

[28] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *J. Netw. Comput. Appl.*, vol. 59, pp. 325–332, Jan. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804515000880

[29] A. Paverd, A. Martin, and I. Brown, "Privacy-enhanced bi-directional communication in the smart grid using trusted computing," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Venice, Italy, Nov. 2014, pp. 872–877.

[30] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids—A comprehensive survey," *Comput. Stand. Interfaces*, vol. 56, pp. 62–73, Feb. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548917301277

[31] "Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines," Int. Org. Stand., Geneva, Switzerland, Rep. ISO/IEC 27701:2019, 2019. [Online]. Available: https://www.iso.org/standard/71670.html

[32] "Information security controls for the energy utility industry," Int. Org. Stand., Geneva, Switzerland, Rep. ISO/IEC 27019:2017, 2017. [Online]. Available: https://www.iso.org/standard/68091.html

[33] "Information technology—Security techniques—Privacy framework," Int. Org. Stand., Geneva, Switzerland, Rep. ISO/IEC 29100:2011, 2011. [Online]. Available: https://www.iso.org/standard/45123.html

[34] "Information technology—Business operational view—Part 8: Identification of privacy protection requirements as external constraints on business transactions," Int. Org. Stand., Geneva, Switzerland, Rep. ISO/IEC 15944-8:2012, 2012. [Online]. Available: https://www.iso.org/standard/51544.html

[35] "Data protection—Rules for the protection of personal data inside and outside the eu," Eur. Union, Brussels, Belgium, Rep., 1995. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection_en

[36] "Apec privacy framework," APE Cooper., Singapore, Rep. APEC#205-SO-01.2, 2005. [Online]. Available: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

[37] "FTC issues final commission report on protecting consumer privacy—Agency calls on companies to adopt best privacy practices," Federal Trade Commission, Washington, DC, USA, Rep., 2012. [Online]. Available: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[38] "NIST special publication (SP) 800-53 revision 4—Security and privacy controls for federal information systems and organizations—Appendix J—Privacy control catalog," NIST, Gaithersburg, MD, USA, Rep. 800-53, 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[39] "Consumer data privacy in a networked world—A framework for protecting privacy and promoting innovation in the global digital economy," The White House, Washington, DC, USA, Rep., 2012. [Online]. Available: http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights

[40] "ANSI c12.20," NEMA, Arlington, VA, USA, Rep., 2002. [Online]. Available: https://web.archive.org/web/20100526093854/http://www.nema.org/stds/c12-20.cfm

[41] "IEEE 1686-2013—Standard for substation intelligent electronic devices (IEDS) cyber security capabilities," IEEE, Piscataway, NJ, USA, Rep., 2014. [Online]. Available: https://ieeexplore.ieee.org/document/6704702/definitions#definitions

[42] *Electrcity Metering Data Exchange—The DLMS/COSEM Suite—Part 5-3: DLMS/COSEM Application Layer*, IEC Standard 62056-5-3:2016, 2016. [Online]. Available: https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/en-62056-5-32016-electricity-metering-data-exchange-dlmscosem-suite-part-5-3-dlmscosem-application

[43] R. Schlegel, S. Obermeier, and J. Schneider, "Assessing the security of IEC 62351," in *Proc. 3rd Int. Symp. ICS SCADA Cyber Security Res.*, 2015, pp. 11–19. [Online]. Available: https://doi.org/10.14236/ewic/ICS2015.2

[44] "Whitepaper industrial security based on IEC 62443," TÜV NORD Group, Hanover, Germany, White Paper. [Online]. Available: https://www.tuvit.de/fileadmin/Content/TUV_IT/pdf/Downloads/WhitePaper/whitepaper-iec-62443.pdf

[45] "ANSI/ISA-62443-4-2-2018, security for industrial automation and control systems, part 4-2: Technical security requirements for iacs components," ISA, Gurugram, Haryana, Rep., 2018. [Online]. Available: https://www.isa.org/store/ansi/isa-62443-4-2-2018,-security-for-industrial-automation-and-control-systems,-part-4-2-technical-security-requirements-for-iacs-components/62991116

[46] C. Rottondi, G. Verticale, and C. Krauss, "Distributed privacy-preserving aggregation of metering data in smart grids," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1342–1354, Jul. 2013.

[47] Y. Yan, R. Q. Hu, S. K. Das, H. Sharif, and Y. Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," *IEEE Netw.*, vol. 27, no. 4, pp. 64–71, Jul. 2013.

[48] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, Oct. 2010, pp. 238–243.

[49] V. Tudor, M. Almgren, and M. Papatriantafilou, "A study on data de-pseudonymization in the smart grid," in *Proc. 8th Eur. Workshop Syst. Security (EUROSEC)*, 2015, p. 2.

[50] W. Ren, L. Ma, and Y. Ren, "Perturbation-based schemes with ultra-lightweight computation to protect user privacy in smart grid," *Int. J. Distrib. Sens. Netw.*, vol. 9, no. 3, 2013, Art. no. 230140. [Online]. Available: https://doi.org/10.1155/2013/230140

[51] X. He, X. Zhang, and C.-C. J. Kuo, "A distortion-based approach to privacy-preserving metering in smart grids," *IEEE Access*, vol. 1, pp. 67–78, 2013.

[52] M. Savi, C. Rottondi, and G. Verticale, "Evaluation of the precision-privacy tradeoff of data perturbation for smart metering," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2409–2416, Sep. 2015.

[53] S. Iyer, "Cyber security for smart grid, cryptography, and privacy," *Int. J. Digit. Multimedia Broadcast.*, vol. 2011, p. 8, Oct. 2011.

[54] X. Long, D. Tipper, and Y. Qian, "A key management architecture and protocols for secure smart grid communications," *Security Commun. Netw.*, vol. 9, no. 16, pp. 3602–3617, 2016.

[55] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, Jun. 2014.

[56] R. Jiang, R. Lu, J. Luo, C. Lai, and X. Shen, "Efficient self-healing group key management with dynamic revocation and collusion resistance for scada in smart grid," *Security Commun. Netw.*, vol. 8, pp. 1026–1039, Apr. 2015.

[57] M. Benmalek and Y. Challal, "Eskami: Efficient and scalable multi-group key management for advanced metering infrastructure in smart grid," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 782–789.

[58] J. L. Tsai and N. W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[59] O. G. Abood, M. A. Elsadd, and S. K. Guirguis, "Investigation of cryptography algorithms used for security and privacy protection in smart grid," in *Proc. 19th Int. Middle East Power Syst. Conf. (MEPCON)*, Cairo, Egypt, Dec. 2017, pp. 644–649.

[60] S. Yip, K. Wong, R. C.-W. Phan, S. Tan, I. Ku, and W. Hew, "A privacy-preserving and cheat-resilient electricity consumption reporting scheme for smart grids," in *Proc. Int. Conf. Comput. Inf. Telecommun. Syst. (CITS)*, Jeju, South Korea, 2014, pp. 1–5.

[61] D. Ghosh, C. Li, and C. Yang, "A lightweight authentication protocol for smart grid," *Int. J. Netw. Security*, vol. 234, pp. 414–422, Dec. 2018.

[62] I. A. Kamil and S. O. Ogundoyin, "EPDAS: Efficient privacy-preserving data analysis scheme for smart grid network," *J. King Saud Univ. Comput. Inf. Sci.*, to be published. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1319157818308085

[63] M. Ambrosin, H. Hosseini, K. Mandal, M. Conti, and R. Poovendran, "Despicable me(ter): Anonymous and fine-grained metering data reporting with dishonest meters," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Philadelphia, PA, USA, Oct. 2016, pp. 163–171.

[64] Y. Chen, J.-F. Martínez, P. Castillejo, and L. López, "A privacy-preserving noise addition data aggregation scheme for smart grid," *Energies*, vol. 11, no. 11, pp. 1–17, Nov. 2018. [Online]. Available: https://ideas.repec.org/a/gam/jeners/v11y2018i11p2972-d179705.html

[65] L. Lyu, K. Nandakumar, B. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, "PPFA: Privacy preserving fog-enabled aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3733–3744, Aug. 2018.

[66] R. C. Diovu and J. T. Agee, "Data aggregation in smart grid ami network for secure transfer of energy user-consumption data," *Int. J. Eng. Res. Africa*, vol. 35, pp. 108–124, Mar. 2018.

[67] Z. Wang, "An identity-based data aggregation protocol for the smart grid," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2428–2435, Oct. 2017.

[68] Z. Wang, H. Xie, and Y. Xu, "Security analysis of an identity-based data aggregation protocol for the smart grid," in *Proc. Int. Conf. Intell. Secure Depend. Syst. Distrib. Cloud Environ.*, 2018, pp. 63–73.

[69] Z. L. H. Y. Y. Xiong, P. Zhu, and T. Deng, "EPLC: An efficient privacy-preserving line-loss calculation scheme for residential areas of smart grid," *Security Commun. Netw.*, vol. 2019, no. 9, p. 14, 2019.

[70] E. Vahedi, M. Bayat, M. R. Pakravan, and M. R. Aref, "A secure ECC-based privacy preserving data aggregation scheme for smart grids," *Comput. Netw.*, vol. 129, pp. 28–36, Dec. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128617303353

[71] A. A. Agarkar and H. Agrawal, "LRSPPP: Lightweight R-LWE-based secure and privacy-preserving scheme for prosumer side network in smart grid," *Heliyon*, vol. 5, no. 3, 2019, Art. no. e01321. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2405844018358055

[72] P. Samarati, "Protecting respondents identities in microdata release," *IEEE Trans. Knowl. Data Eng.*, vol. 13, no. 6, pp. 1010–1027, Nov./Dec. 2001.

[73] X. He, H. Chen, Y. Chen, Y. Dong, P. Wang, and Z. Huang, "Clustering-based k-anonymity," in *Advances in Knowledge Discovery and Data Mining*, P.-N. Tan, S. Chawla, C. K. Ho, and J. Bailey, Eds. Heidelberg, Germany: Springer, 2012, pp. 405–417.

[74] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds. Heidelberg, Germany: Springer, 2006, pp. 1–12.

[75] A. Agarwal, M. Herlihy, S. Kamara, and T. Moataz, "Encrypted databases for differential privacy," *Proc. Privacy Enhancing Technol.*, vol. 2019, no. 3, pp. 170–190, 2019. [Online]. Available: https://doi.org/10.2478/popets-2019-0042

[76] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation*, M. Agrawal, D. Du, Z. Duan, and A. Li, Eds. Heidelberg, Germany: Springer, 2008, pp. 1–19.

[77] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Advances in Cryptology (EUROCRYPT)*, S. Vaudenay, Ed. Heidelberg, Germany: Springer, 2006, pp. 486–503.

[78] L. Chen, R. Lu, Z. Cao, K. AlHarbi, and X. Lin, "MuDA: Multifunctional data aggregation in privacy-preserving smart grid communications," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 5, pp. 777–792, Sep. 2015. [Online]. Available: https://doi.org/10.1007/s12083-014-0292-0

[79] H. Cao, S. Liu, Z. Guan, L. Wu, H. Deng, and X. Du, "An efficient privacy-preserving algorithm based on randomized response in iot-based smart grid," 2018. [Online]. Available: http://arxiv.org/abs/1804.02781.

[80] T. Dalenius, "Finding a needle in a haystack or identifying anonymous census records," *J. Official Stat.*, vol. 2, no. 3, pp. 329–336, 1986.

[81] M. Stegelmann and D. Kesdogan, "GridPriv: A smart metering architecture offering k-anonymity," in *Proc. IEEE 11th Int. Conf. Trust Security Privacy Comput. Commun.*, Liverpool, U.K., Jun. 2012, pp. 419–426.

[82] A. Al-Wakeel and J. Wu, "K-means based cluster analysis of residential smart meter measurements," *Energy Procedia*, vol. 88, pp. 754–760, Jun. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1876610216301308

[83] Y. Yang, X. Zhang, Z. Zhu, and J. Lei, "Research on homomorphic encryption clustering algorithm for smart grid privacy preserving," in *Proc. 6th Int. Conf. Inf. Eng. Mech. Mater.*, Nov. 2016, pp. 763–767. [Online]. Available: https://doi.org/10.2991/icimm-16.2016.138

[84] O. Y. Al-Jarrah, Y. Al-Hammadi, P. D. Yoo, and S. Muhaidat, "Multi-layered clustering for power consumption profiling in smart grids," *IEEE Access*, vol. 5, pp. 18459–18468, 2017.

[85] S. Afrin and S. Mishra, "On the analysis of collaborative anonymity set formation (CASF) method for privacy in the smart grid," in *Proc. IEEE Int. Symp. Technol. Homeland Security (HST)*, Apr. 2017, pp. 1–6.

[86] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA, USA: Springer, 1983, pp. 199–203.

[87] A. Triantafyllou, P. Sarigiannidis, A. Sarigiannidis, E. Rios, and E. Iturbe, "Towards an anonymous incident communication channel for electric smart grids," in *Proc. 22nd Pan Hellenic Conf. Informat.*, 2018, p. 34–39. [Online]. Available: https://doi.org/10.1145/3291533.3291559

[88] K. El Emam and F. K. Dankar, "Protecting privacy using k-anonymity," *J. Amer. Med. Informat. Assoc.*, vol. 15, no. 5, pp. 627–637, Sep. 2008. [Online]. Available: https://doi.org/10.1197/jamia.M2716

[89] C. Xu, J. Ren, D. Zhang, and Y. Zhang, "Distilling at the edge: A local differential privacy obfuscation framework for IoT data analytics," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 20–25, Aug. 2018.

[90] A. Beussink, K. Akkaya, I. F. Senturk, and M. M. E. A. Mahmoud, "Preserving consumer privacy on IEEE 802.11s-based smart grid AMI networks using data obfuscation," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada, Apr. 2014, pp. 658–663.

[91] Z. Guan, G. Si, J. Wu, L. Zhu, Z. Zhang, and Y. Ma, "Utility-privacy tradeoff based on random data obfuscation in Internet of energy," *IEEE Access*, vol. 5, pp. 3250–3262, 2017.

[92] S. Tonyali, K. Akkaya, N. Saputro, A. S. Uluagac, and M. Nojoumian, "Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems," *Future Gener. Comput. Syst.*, vol. 78, pp. 547–557, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17306945

[93] Y. Kim, E. C. H. Ngai, and M. B. Srivastava, "Cooperative state estimation for preserving privacy of user behaviors in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Brussels, Belgium, Oct. 2011, pp. 178–183.

[94] F. Fioretto, T. W. K. Mak, and P. V. Hentenryck, "Differential privacy for power grid obfuscation," 2019. [Online]. Available: http://arxiv.org/abs/1901.06949.

[95] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, Oct. 2010, pp. 232–237.

[96] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proc. 18th ACM Conf. Comput. Commun. Security*, 2011, pp. 87–98. [Online]. Available: http://doi.acm.org/10.1145/2046707.2046720

[97] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing private data disclosures in the smart grid," in *Proc. ACM Conf. Comput. Commun. Security*, 2012, pp. 415–427. [Online]. Available: http://doi.acm.org/10.1145/2382196.2382242

[98] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Toronto, ON, Canada, Apr. 2014, pp. 504–512.

[99] M. Backes and S. Meiser, "Differentially private smart metering with battery recharging," in *Data Privacy Management and Autonomous Spontaneous Security*, J. Garcia-Alfaro, G. Lioudakis, N. Cuppens-Boulahia, S. Foley, and W. M. Fitzgerald, Eds. Heidelberg, Germany: Springer, 2014, pp. 194–212.

[100] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 619–626, Mar. 2017.

[101] A. Romanou, "The necessity of the implementation of privacy by design in sectors where data protection concerns arise," *Comput. Law Security Rev.*, vol. 34, no. 1, pp. 99–110, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0267364917302054

[102] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 907–921, 2016.

[103] N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," *Energies*, vol. 8, pp. 11883–11915, Oct. 2015.

[104] S. Renner and J. Mottok, "Towards key management challenges in the smart grid," in *Proc. ARCS Workshop 32nd Int. Conf. Archit. Comput. Syst.*, 2019, pp. 1–8.

[105] P. Gope, "PMAKE: Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid," *Comput. Commun.*, vol. 152, pp. 338–344, Feb. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366419313210

[106] L. Zhu *et al.*, "Privacy-preserving authentication and data aggregation for fog-based smart grid," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 80–85, Jun. 2019.

[107] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, "ECCAuth: A secure authentication protocol for demand response management in a smart grid system," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6572–6582, Dec. 2019.

[108] S. Yu *et al.*, "Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment," *Appl. Sci.*, vol. 10, no. 5, p. 1758, 2020. [Online]. Available: https://www.mdpi.com/2076-3417/10/5/1758

[109] L. Zhang, L. Zhao, S. Yin, C.-H. Chi, R. Liu, and Y. Zhang, "A lightweight authentication scheme with privacy protection for smart grid communications," *Future Gener. Comput. Syst.*, vol. 100, pp. 770–778, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X19310398

[110] H. Hu, X. Zhao, Y. Wu, M. Huang, Z. Zhu, and Q. Yang, "Privacy preservation of smart meters based on identity authentication," *Energy Power Eng.*, vol. 12, pp. 53–62, Jan. 2020.

[111] A. S. Alfakeeh, S. Khan, and A. H. Al-Bayatti, "A multi-user, single-authentication protocol for smart grid architectures," *Sensors*, vol. 20, no. 6, p. 1581, Mar. 2020. [Online]. Available: doi: 10.3390/s20061581

[112] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[113] R. Xu, Y. Chen, and E. Blasch, *Decentralized Access Control for IoT Based on Blockchain and Smart Contract*, Hoboken, NJ, USA: Wiley, 2020, ch. 22, pp. 505–528. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119593386.ch22

[114] *AMI System Security Requirements*, U.S. Dept. Energy, Washington, DC, USA, 2008.

[115] M. Jung, T. Hofer, S. Döbelt, G. Kienesberger, F. Judex, and W. Kastner, "Access control for a smart grid SOA," in *Proc. Int. Conf. Internet Technol. Secured Trans.*, London, U.K., Dec. 2012, pp. 281–287.

[116] T. Sato *et al.*, *Smart Grid Standards: Specifications, Requirements, and Technologies*. Singapore: Wiley, Feb. 2015.

[117] R. Bobba, H. Khurana, M. AlTurki, and F. Ashraf, "PBES: A policy based encryption system with application to data sharing in the power grid," in *Proc. 4th Int. Symp. Inf. Comput. Commun. Security*, 2009, pp. 262–275. [Online]. Available: https://doi.org/10.1145/1533057.1533093

[118] J. Wu, M. Dong, K. Ota, Z. Zhou, and B. Duan, "Towards fault-tolerant fine-grained data access control for smart grid," *Wireless Pers. Commun.*, vol. 75, no. 3, pp. 1787–1808, Apr. 2014. [Online]. Available: https://doi.org/10.1007/s11277-013-1294-6

[119] S.-S. Yeo, S.-J. Kim, and D.-E. Cho, "Dynamic access control model for security client services in smart grid," *Int. J. Distrib. Sens. Netw.*, pp. 1–7, Jun. 2014.

[120] M. Wen, X. Zhang, H. Li, and J. Li, "A data aggregation scheme with fine-grained access control for the smart grid," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Toronto, ON, Canada, Sep. 2017, pp. 1–5.

[121] B. Lang, J. Wang, and Z. Cao, "Multidimensional data tight aggregation and fine-grained access control in smart grid," *J. Inf. Security Appl.*, vol. 40, pp. 156–165, Jun. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212617306476

[122] J. Kim, Y. Kwon, Y. Lee, J.-T. Seo, and H. Kim, "Access control mechanism supporting scalability, interoperability and flexibility of multi-domain smart grid system," in *Proc. Int. Conf. Inf. Sci. Ind. Appl. (ISI)*, 2012, pp. 194–201.

[123] S. Ruj and A. Nayak, "A decentralized security framework for data aggregation and access control in smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 196–205, Mar. 2013.

[124] D. Liu, H. Li, Y. Yang, and H. Yang, "Achieving multi-authority access control with efficient attribute revocation in smart grid," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 634–639.

[125] A. Mutsvangwa, B. Nleya, and B. Nleya, "Secured access control architecture consideration for smart grids," in *Proc. IEEE PES PowerAfrica*, Livingstone, Zambia, Jun. 2016, pp. 228–233.

[126] Z. Guan, J. Li, L. Zhu, Z. Zhang, X. Du, and M. Guizani, "Toward delay-tolerant flexible data access control for smart grid with renewable energy resources," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3216–3225, Dec. 2017.

[127] F. Cai, J. He, Z. Ali Zardari, and S. Han, "Distributed management of permission for access control model," *J. Intell. Fuzzy Syst.*, vol. 38, pp. 1–10, Nov. 2019.

[128] S. Shafeeq, M. Alam, and A. Khan, "Privacy aware decentralized access control system," *Future Gener. Comput. Syst.*, vol. 101, pp. 420–433, Dec. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X18332308

[129] S. Nakamoto. (Mar. 2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://metzdowd.com

[130] D. Di Francesco Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *Distributed Applications and Interoperable Systems*, L. Y. Chen and H. P. Reiser, Eds. Cham, Switzerland: Springer, 2017, pp. 206–220.

[131] A. Ouaddah, A. Elkalam, and A. Ouahman, "Fairaccess: A new blockchain-based access control framework for the Internet of Things: Fairaccess: A new access control framework for IoT," *Security Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, Feb. 2017.

[132] M. Laurent, N. Kaaniche, C. Le, and M. V. Plaetse, "A blockchain-basedaccess control scheme," in *Proc. 15th Int. Conf. Security Cryptogr. (SECRYPT)*, Porto, Portugal, Jul. 2018, pp. 168–176, doi: 10.5220/0006855601680176.

[133] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, Aug. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804518301619

[134] D. D. F. Maesa, P. Mori, and L. Ricci, "A blockchain based approach for the definition of auditable access control systems," *Comput. Security*, vol. 84, pp. 93–119, Jul. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818309398

[135] Y. Zhou, Y. Guan, Z. Zhang, and F. Li, "A blockchain-based access control scheme for smart grids," IACR Cryptol. ePrint Archive, Lyon, France, Rep. 2019/880, 2019.

[136] H. Zhang, J. Wang, and Y. Ding, "Blockchain-based decentralized and secure keyless signature scheme for smart grid," *Energy*, vol. 180, pp. 955–967, Aug. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0360544219310096

[137] N. Shi *et al.*, "BacS: A blockchain-based access control scheme in distributed Internet of Things," *Peer-to-Peer Netw. Appl.*, pp. 1–15, Jun. 2020. [Online]. Available: https://kar.kent.ac.uk/81701/

[138] M. D. Firoozjaei, A. Ghorbani, H. Kim, and J. Song, "Hy-bridge: A hybrid blockchain for privacy-preserving and trustful energy transactions in Internet-of-Things platforms," *Sensors (Basel, Switzerland)*, vol. 20, p. 928. Feb. 2020.

[139] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.

[140] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, and X. Yang, "An attribute-based collaborative access control scheme using blockchain for IoT devices," *Electronics*, vol. 9, no. 2, p. 285, Feb. 2020. [Online]. Available: http://dx.doi.org/10.3390/electronics9020285

[141] B. Liu, L. Xiao, J. Long, M. Tang, and O. Hosam, "Secure digital certificate-based data access control scheme in blockchain," *IEEE Access*, vol. 8, pp. 91751–91760, 2020.

[142] A. Taik and S. Cherkaoui, "Electrical load forecasting using edge computing and federated learning," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dublin, Ireland, 2020, pp. 1–6.

[143] Konečný, B. McMahan, and D. Ramage, "Federated optimization:Distributed optimization beyond the datacenter," 2015. [Online]. Available: https://arxiv.org/abs/1511.03575.

[144] Q. Wu, K. He, and X. Chen, "Personalized federated learning for intelligent IoT applications: A cloud-edge based framework," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 35–44, 2020.

[145] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, Apr. 2020.

[146] Y. Qu *et al.*, "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5171–5183, Jun. 2020.

[147] R. Xu, Y. Chen, E. Blasch, and G. Chen, "A federated capability-based access control mechanism for Internet of Things (IoTs)," in *Proc. Sens. Syst. Space Appl.*, 2018, Art. no. 106410U.

[148] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020.

[149] C. Zhou, A. Fu, S. Yu, W. Yang, H. Wang, and Y. Zhang, "Privacy-preserving federated learning in fog computing," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10782–10793, Nov. 2020.

[150] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6532–6542, Oct. 2020.

[151] M. Al-Rubaie and J. M. Chang, "Privacy-preserving machine learning: Threats and solutions," *IEEE Security Privacy*, vol. 17, no. 2, pp. 49–58, Mar./Apr. 2019.

[152] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2831–2848, 3rd Quart., 2019.

[153] M. F. Moghadam, M. Nikooghadam, A. H. Mohajerzadeh, and B. Movali, "A lightweight key management protocol for secure communication in smart grids," *Elect. Power Syst. Res.*, vol. 178, 2020, Art. no. 106024. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378779619303438

[154] J. Wang, L. Wu, K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020.

[155] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 3–19, Jan. 2021.

[156] M. Saad *et al.*, "Exploring the attack surface of blockchain: A systematic overview," 2019. [Online]. Available: http://arxiv.org/abs/1904.03487.

[157] J. Rodríguez-Molina, M. Martínez-Núñez, J.-F. Martínez, and W. Pérez-Aguiar, "Business models in the smart grid: Challenges, opportunities and proposals for prosumer profitability," *Energies*, vol. 7, no. 9, pp. 6142–6171, 2014. [Online]. Available: https://www.mdpi.com/1996-1073/7/9/6142

[158] *The SPEAR Project*, Eur. Union, Brussels, Belgium. Accessed: Feb. 6, 2020. [Online]. Available: https://www.spear2020.eu/
[159] *The SDN-microSENSE Project*, Eur. Union, Brussels, Belgium. Accessed: Feb. 6, 2020. [Online]. Available: https://www.sdnmicrosense.eu/

ANNA TRIANTAFYLLOU was born in Ioannina, Greece, in 1992. She received the Diploma degree (five years) from the Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Greece, in 2017.

She is currently pursuing the Ph.D. degree with the Department of Informatics and Telecommunications Engineering, University of Western Macedonia. She is also a Research Associate with National and European Funded Research projects. She is also specialized in the mobile application development. Her main research interests are in the area of Internet of Things and mainly focus on communication technologies, networking protocols, and information security. She received the Graduation Excellence Award from the Technical Chamber of Greece in 2018.

JOSE ANTONIO PEREZ JIMENEZ was born in Mairena del Alcor, Seville, Spain, in 1994. He received the bachelor's degree in software engineering from the Universidad of Sevilla, Spain, in 2016, and the master's degree in cybersecurity from the Universidad de Sevilla in 2018.

He is currently a Research and Development Scientist with IDENER. For the last four years, he has been carrying on technical and scientific work developing new technologies with ICT and Security fields. His primary fields of study in cybersecurity are penetration testing, software security, and data privacy. His current research interests are related to the protection of software from vulnerabilities and the development of state-of-the-art technologies for detecting cyberattacks on data privacy and systems protection.

ALEJANDRO DEL REAL TORRES was born in Seville, Spain, in 1981. He received the M.Sc. degree in industrial engineering from the School of Engineering of Universidad de Sevilla in 2005, the first master's degree in start-ups and business administration from Spain's School for Industrial Organisation, the second master's degree in information technologies from Advanced Management and Technological Markets Hewlett-Packard, USA, and the Ph.D. degree in systems and automation from the School of Engineering, Universidad de Sevilla in 2010.

He has been founded IDENER in 2010, and has held its CEO position since then. Also, he has been a Lecturer with the University of Seville, since 2015. These two positions have enabled him to participate in more than 25 EU research projects, including the FP7 and H2020 programmes. He had author/coauthor nine scientific papers and 19 congress contributions. His primary field of study is framed in the advance management of smart grids and electricity markets.

THOMAS LAGKAS (Senior Member, IEEE) received the graduation degree (Hons.) from the Department of Informatics, Aristotle University of Thessaloniki in 2002, the Ph.D. degree in wireless networks from the Department of Informatics, Aristotle University of Thessaloniki in 2006, and the M.B.A. degree from Hellenic Open University in 2012.

He has been Scholar of the Aristotle University Research Committee, as well as Postdoctoral Scholar with the National Scholarships Institute of Greece. He is Assistant Professor with the Department of Computer Science, International Hellenic University. He has been a Lecturer and Senior Lecturer with the CITY College, International Faculty of the University of Sheffield, from 2012 to 2019. He also served as a Research Director with the Computer Science Department, CITY College, and a Leader with the ICT Track, South-East European Research Centre. He received a Postdoctoral certificate on Teaching and Learning from the University of Sheffield in 2017. He had participated in the Editorial Boards of respectful scientific journals. His research interests are in the areas of IoT communications, wireless networks, hybrid fiber-wireless networks, e-health data monitoring, 5G and beyond systems, flying ad hoc networks, communication security, and computer-based educational technologies with more than 70 publications at a number of widely recognized international scientific journals and conferences. He is a Fellow of the Higher Education Academy in U.K.

KONSTANTINOS RANTOS was born in Thessaloniki, Greece. He received the Diploma degree in computer engineering and informatics from the University of Patras, Greece, in 1996, and the M.Sc. and Ph.D. degrees in information security (sponsored by Marie Curie Research and Training Grant) from the Royal Holloway, University of London in 1997 and 2001, respectively.

He is an Associate Professor with the Computer Science Department, International Hellenic University (Kavala Campus), Greece, and Director with the Web Services and Information Security Lab. He has extensive research and development project involvement and substantial (more than 20 years) private- and public-sector experience in the area of information security. He has also served as a Scientific Supervisor for more than 20 development and consulting projects providing services to key private and public sector bodies. His research interests are in the areas of cybersecurity, Internet of Things security, authentication systems, and privacy.

PANAGIOTIS SARIGIANNIDIS (Member, IEEE) received the B.Sc. and Ph.D. degrees in computer science from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2001 and 2007, respectively.

He has been an Associate Professor with the Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani, Greece, since 2016. He has published over 170 papers in international journals, conferences and book chapters, including IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE INTERNET OF THINGS, IEEE TRANSACTIONS ON BROADCASTING, IEEE SYSTEMS JOURNAL, *IEEE Wireless Communications Magazine*, IEEE/OSA JOURNAL OF LIGHTWAVE TECHNOLOGY, IEEE ACCESS, and *Computer Networks*. He has been involved in several national, an European, and international projects. He is currently the Project Coordinator with three H2020 projects, namely: 1) H2020-DS-SC7-2017 (DS-07-2017), SPEAR: Secure and PrivatE smArt gRid; 2) H2020-LC-SC3-EE-2020-1 (LC-SC3-EC-4-2020), EVIDENT: bEhaVioral Insgihts anD Effective eNergy policy acTions, and H2020-ICT-2020-1 (ICT-56-2020); and 3) TERMINET: nexT gEneRation sMart INterconnectEd ioT, while he coordinates the Operational Program MARS: sMart fArming with dRoneS (Competitiveness, Entrepreneurship, and Innovation). He also serves as a Principal Investigator with the H2020-SU-DS-2018 (SU-DS04-2018-2020), SDN-microSENSE: SDN-microgrid reSilient Electrical eNergy SystEm and with the Erasmus+ KA2 ARRANGE-ICT: pArtneRship foR AddressiNG mEgatrends in ICT (Cooperation for Innovation and the Exchange of Good Practices). His research interests include telecommunication networks, Internet of Things, and network security. He have participates in the Editorial Boards of various journals, including *International Journal of Communication Systems* and *EURASIP Journal on Wireless Communications and Networking*.