applied sciences

MDPI

Perspective

Privacy-Preserving Aggregation and Authentication of Multi-Source Smart Meters in a Smart Grid System

Dongyoung Koo [1], Youngjoo Shin [2,*] and Junbeom Hur [3,*]

[1] Department of Electronics and Information Engineering, Hansung University, 116 Samseongyo-ro 16-gil, Seongbuk-gu, Seoul 02876, Korea; dykoo@hansung.ac.kr

[2] School of Computer & Information Engineering, Kwangwoon University, 20 Kwangwoon-ro, Nowon-gu, Seoul 01897, Korea

[3] Department of Computer Science and Engineering, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 02841, Korea

* Correspondence: yjshin@kw.ac.kr (Y.S.); jbhur@korea.ac.kr (J.H.); Tel.: +82-2-940-5130 (Y.S.); +82-2-3290-4603 (J.H.)

Received: 31 July 2017; Accepted: 26 September 2017; Published: 29 September 2017

Abstract: The smart grid is a promising electrical grid paradigm for enhancing flexibility and reliability in power transmission through two-way communications among grid entities. In the smart grid system, the privacy of usage information measured by individual smart meters has gained significant attention, owing to the possibility of personal information inference. Moreover, efficient and reliable power provisioning can be seriously impeded through illicit manipulations of aggregated data under the influence of malicious adversaries. Due to such potential risks, it becomes an important requirement for the smart grid to preserve privacy of metering data by secure aggregation and to authenticate the aggregated result in an efficient manner within large scale environments. From this perspective, this paper investigates the current status of security and privacy in smart grid systems and representative state-of-the-art studies in secure aggregation and authentication of metering data for future directions of a smart grid.

Keywords: smart grid; privacy; aggregation; authentication; efficiency

1. Introduction

With the advancement of power grids, the *smart grid* concept was introduced to provide sustainable and affordable electricity in an efficient and stable manner. To explain the concept's schematic operation, smart meters record individual user's electricity consumption information and periodically report it to a control center, enabling adaptive and flexible transmission with minimal imbalances between generators and suppliers of energy. This next-generation power grid seamlessly integrates energy and information networks, in the direction of self-healing systems capable of controlling power generation and fluctuations in consumption. According to an IDC report [1], the worldwide smart grid market in 2017 is expected to be about $56 billion for electricity, gas and water technology.

The term *smart grid* has been defined by several national organizations such as NIST [2], IETF [3], and ETSI [4], as well as the research community [5–10]. Although there are subtle differences in their definitions and characteristics, a smart grid has the following common advantages over traditional electric grid systems:

- Energy awareness: By providing users with periodic energy usage patterns, pre-planned power consumption can be enabled. This can lead to consumer power-saving behavior through the implementation of energy-aware systems. In addition, CO_2 emissions can be reduced, and the need for surplus power generation in backup plants can be avoided, which is beneficial to the environment and economics, through continuous electrical load balancing.

- Increased power consumer selectivity: By allowing choices among various electricity generators, suppliers, and communication services, more options can be given to energy consumers. It imposes a more active role on consumers of new products, services and markets.
- Improved reliability of power generation and consumption: Based on historical records of power usage, automatic power generation and consumption can be adjusted according to expected electricity demand. It also improves the resilience of the grid to natural disasters.

Despite these benefits, increased attention has been paid to security and privacy issues threatening the successful deployment of smart grid systems [11]. Specifically, cyber security issues arise in information exchange, monitoring and controlling of electrical components. Hahn and Govindarasu [12] presented economic incentives obtainable by adversaries from electricity supply and demand, billing, and control information. For instance, measurement information can be used by adversaries for inference of users' behavioral patterns, implying privacy invasion [13]. Therefore, reliable aggregation of power usage information in a secure manner should be preceded because adaptive and adjustable power provisioning can be achieved only when metering information is aggregated reliably in advance.

In this paper, we review the current status of the smart grid in terms of industrial and governmental activities for its distribution and popularization followed by state-of-the-art research trends focusing on aggregation and authentication of metering information. We then discuss our perspective on the smart grid market and future directions for the secure management of metering information, focusing on privacy-preserving data aggregation and authentication. Since the metering data integrity and its authentication are one of the most important security requirements in smart grid systems, this paper focuses on the authenticated aggregation in smart grid systems, which has not been profoundly surveyed in the previous works, such as [14] (covering only aggregation) and [15] (addressing a broad categorization about smart grid systems according to communication techniques, management objectives, etc.). Thus, contributions of this paper reside in investigating the current status of the development process and provisioning admirable future directions for reliable data aggregation in smart grid systems.

The rest of this paper is organized as follows. Section 2 is an overview of the current status of smart grid system distribution and governmental efforts. In Section 3, state-of-the-art studies for more reliable and stable smart grid systems are recapitulated as regarding privacy-preserving aggregation, authentication, and other topics. Finally, our perspectives on advisable directions for upcoming smart grid systems are discussed in Section 4 as the conclusion of this paper.

2. Status of Smart Grids

A phased development plan with the primary goal of spreading the advanced metering infrastructure (AMI) is a fundamental early step for putting a smart grid in place. The AMI is an entire measurement and collection system that includes meters at customers' premises, communication networks between customers and service providers, and data receiving and management systems that allow service providers to use the gathered information. It enables detailed time-based information measurements and provides frequent collection and transmission of such information.

As depicted in Figure 1, there are broadly two kinds of systems: transmission and distribution. Electrical power is generated by power stations such as thermoelectric, nuclear, wind, hydroelectric, and geothermal power plants (namely, generators), and then transported to a substation (namely, suppliers) that splits high capacity power into smaller units and distributes them to customers' premises according to their requirements. Based on customers' power usage patterns, the central controller residing with the supplier determines transmission capacity, requests an amount of power based on expected demand from generators, and distributes it to its customers. To achieve this functionality, the central controller receives power usage information from smart meters in individual smart homes directly or indirectly (through an accumulation of usage information on the path from the furthermost to the nearest customers).

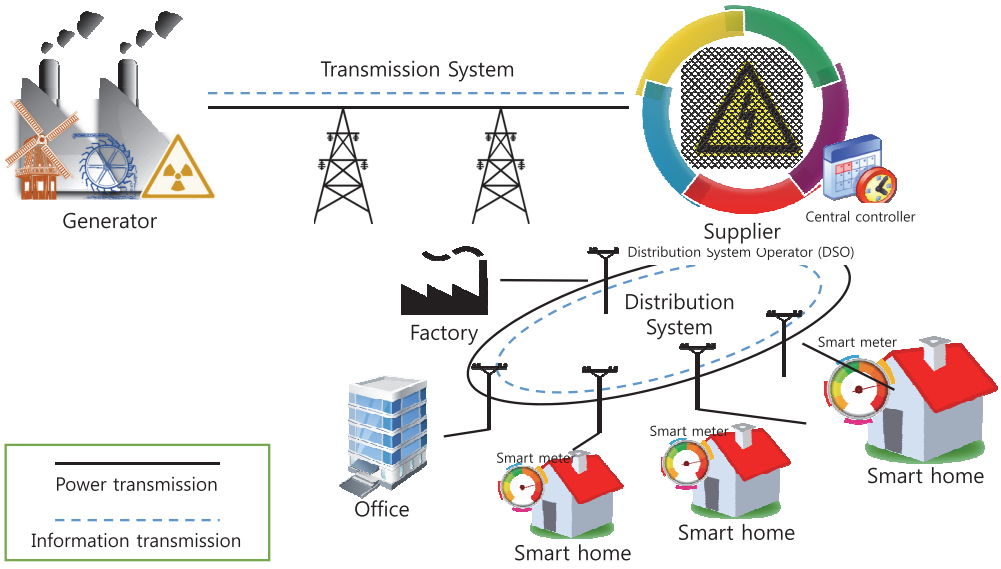

Figure 1. An overview of Smart Grid Architecture.

In particular, we explore the information aspect of the distribution system. Specifically, we investigate in depth how the central controller aggregates the metering information in a privacy-preserving and reliable manner. Since metering information can be gathered from multiple independent smart meters apart from the central controller, we denote them as multi-source smart meters. Henceforth, we refer to them as smart meters or just meters for simplicity throughout the paper. (There are several interesting and innovative researches dealing with microgrid construction by formulating a probabilistic model of power generation and pollutant emission [16], and adaptive scheduling specific to vehicular network where vehicular clients frequently change their locations [17]. However, these issues are beyond the scope of our focus, which is secure aggregation and verification of metering information in smart grid systems.)

2.1. Popularization of the Smart Grid

2.1.1. Europe

One of the largest deployments of a smart grid system was initiated by Enel Distribuzione, an Italian multinational producer and distributor of electricity and gas. The Telegestore project, by Enel and completed in 2005, was regarded as the first commercial scale use of smart grid technology to the home at an investment expense of €2.1 billion, including R&D, production and distribution of smart meters and concentrators, and construction of IT systems. It was considered unusual at that time, when independent companies designed and manufactured their own systems including metering and integrating devices without considering compatibility with ones manufactured by other companies. Since the liberalization of the electricity market in Italy, Enel has built its first smart grid capable of adjusting the two-way flow of electricity generated from renewable sources. Enel also established a strategic partnership agreement with the NEC Corporation for the development of new technologies and solutions in this field.

InovGrid, an innovative project in Évora Portugal, aims to equip the electricity grid devices with information to automate grid management, improve service quality, reduce operating costs, improve energy efficiency for building sustainable environments, and develop renewable energy. By allowing energy suppliers and companies to use this technology platform to offer consumers value-added energy products and services, the status of the entire distribution grid can be controlled and managed at any given moment of time. Portugal and Electricidade de Portugal (EDP) are at the cutting edge of

technological innovation and service provisioning in Europe through this project to install an intelligent energy grid.

In Germany, the city of Mannheim used real-time broadband over power lines (BPL) communications in its Model City Mannheim (moma) project. A government sponsored E-energy technology competition identified six model regions, including Mannheim, to carry out research and development activities with the main objective of creating an Internet of Energy.

2.1.2. North America

In the United States, private companies are leading the way in technical development with regulations, laws and finances from the government. Various research and development projects including IntelliGrid and the Modern Grid Initiative have been led by the Electric Power Research Institute (EPRI).

In 2003, for the first time in the world, Grid 2030, driven by Department of Energy (DOE), planned a next-generation 100-year investment starting with $4.5 billion in a power network. It was a declarative start for the smart grid industry, with about 50 electric power companies and research institutes participating, aiming at replacing old facilities and improving the infrastructure for two-way facilities. Since replacing the utility mesh with a smart meter communicating over a wireless mesh network in 2003, Texas has worked to build a smart grid that can manage 200,000 devices (sensors in smart meters, smart thermostats, and sensor service areas). It supports 50,000 devices in real-time, serving one million consumers and 43,000 companies in 2009.

The largest deployment programs in the world to date are also run by the DOE through the Smart Grid Program, which was funded by the American Recovery and Reinvestment Act (ARRA) of 2009 with matching funds from individual utilities. This program includes equipment for an advanced metering infrastructure (AMI) of more than 65 million smart meters, customer interface systems, distribution and substation automation, volt/VAR optimization systems with more than 1000 synchrophasors, dynamic line rating, cyber security projects, advanced distribution management systems, energy storage systems, and renewable energy integration projects that have been completed by 2015.

Hydro One, the largest smart grid service provider in Canada, deployed a communications infrastructure from Trilliant complying with a standard and that served 1.3 million customers in the province of Ontario at the end of 2010. Ontario has begun to build one of the most advanced power grids in the world supported by the Smart Grid Fund from the Ministry of Energy, which has been supporting innovative projects and the development of modern and intelligent electrical systems since 2011. Moreover, SmartGrid Canada promotes a modern and efficient electricity grid for its residents [18].

2.1.3. Oceania and Asia

Since its approval in December 2013, a plan to implement a localized green smart grid electricity network in the Tonsley Park redevelopment in Australia has been realized [19]. Sydney, in partnership with the Australian government, has implemented a smart grid and smart city program.

In Korea, the smart grid market got off to a slower start than in developed countries but is being promoted rapidly under government initiatives. Taking advantage of the country's small land mass, the government's objective is to build the world's first nationwide intelligent power network by 2030, spending about $6 billion on technical development and $18 billion on infrastructure. In the first phase, the government carried out pilot projects to establish base cities for each of the seven major metropolitan areas ending in 2016, plans for the second and final stages are to build a smart grid covering all of the metropolitan areas by 2021 and extend it nationwide by 2030. Specifically, the plan is to complete consumer intelligence by 2020 and a nationwide intelligent power grid by 2030.

2.2. Standardization and Regulations

2.2.1. North America

In 2004, the National Electric Delivery Technology Roadmap was established as a concrete action plan in the United States. The following year, the Energy Policy Act (EPAct2005) was enacted, setting requirements for implementation, rules for smart meters and hourly rates to customers. The government investigated the installation of smart meters, responding to demand and supply.

In 2007, the government enacted the Energy Independence and Security Act (EISA), the first legislation using smart grid terms with the aim of advancing the national transmission grid and streamlining power consumption. The Federal Energy Regulatory Commission (FERC) is focusing on smart grid-related issues to support the modernization of national electrical systems in accordance with Title XIII of the EISA. As part of it, the Grid Modernization Initiative (GMI) works with partners in industry, academia, and cities/states across the U.S. including DOE for the purpose of creating the modern grid of the future, aiming at (1) greater resilience to hazards of all types; (2) improved reliability for everyday operations; (3) enhanced security from an increasing and evolving number of threats; (4) additional affordability to maintain economic prosperity; (5) superior flexibility to respond to the variability and uncertainty of conditions; and (6) increased sustainability through energy-efficient and renewable resources. The 2017 GMI Peer Review Poster Session was the first time where all projects in the portfolio were viewed together.

In 2009, the ARRA made the single largest investment in clean energy and supported more than 100 Smart Grid projects with subsidies of approximately $4 billion. This act focused on developing and distributing new power supplies in connection with various investment support programs for transmission and distribution, power storage monitoring, and control technology, from power generator to final consumer via power operator. Regarding cyber security for critical energy infrastructure, the Cybersecurity Research, Development and Demonstration (RD&D) for Energy Delivery Systems program takes both operational technology and information technology into account in order to protect systems against malware without any slowing down of communications.

In Canada, the Canadian Smart Grid Standards Roadmap was released in October 2012 by the Standards Council of Canada [20]; CanmetENERGY was a major partner in the development of the roadmap. This document describes the recommendations for the future plan of smart grid technology to ensure efficient and effective development covering (1) smart grid policy, legislative and regulatory considerations; (2) privacy and security requirements; (3) transport and deployment standards; and (4) metering system standards.

2.2.2. Europe

Europe is promoting the smart grid as a way to implement climate agreements and a low carbon economy. The European Union (EU) aims to improve cost-effectiveness by replacing at least 80% of electricity meters with smart meters by 2020. This smart metering and smart grid adoption are expected to reduce pollutant emissions in EU by up to 9% and also reduce annual household energy consumption. To measure cost efficiency, EU countries conducted a cost-benefit analysis in accordance with the guidelines of the European Commission (EC).

In terms of security and privacy issues, the smart grid task force in EU was established in 2009 to advise the EC on smart grid deployment and development issues. Expert Group 2, one of five expert groups focusing on specific areas, aims to mitigate the security risks of personal data and the smart metering system. The EC proposed developing codes for cyber security networks to complement existing national rules and deal with cross-border issues [21].

To identify and address security challenges, several European projects have been initiated. NobelGrid [22] deals with smart grid security in a new generation of low cost smart meters through secure protocols. SEGRID [23] and SPARKS [24] aim to study known and future security threats for

the purpose of avoidance for the future realization of smart grids. HyRiM [25] is another project for risk management for utility providers.

2.2.3. Oceania and Asia

The U.S. based research institute Northeastgroup expected government regulation on the smart grid to continue to play an important role as Australia and New Zealand increase smart grid investment between 2017 and 2027. The Northeast Group is expected to invest $6.1 billion in these countries to build a smart grid infrastructure during the specified periods [26].

Since the Korea Smart Grid Institute (KGSI) was launched in August 2009, it has aimed to explore projects on developing technology that cover (1) the convergence of electric power and IT; (2) support for cooperation among industry, academia, and research institutes; (3) pursuit of international cooperation and certification; (4) standardization and security; and (5) ultimate achievement of a low carbon green society.

2.2.4. South America

The majority of South American countries are struggling with a wide range of power supply problems, including electricity theft, low reliability, and operational inefficiencies, due to the lack of systematic grid systems. To address these challenges, regional utilities in South America are looking to smart grid infrastructure and massive deployments are in progress. Including Brazil, Colombia, Ecuador, Chile, and Argentina, they will invest $38.1 billion in modernizing their grid infrastructure by 2025 with the guidance of Northeast Group [27]. Brazil has planned to promote South America's first nationwide smart meter deployment and deployed three million smart meters in 2014. However, in consideration of the financial burden of low income employees and distribution operators, Brazil will gradually promote the deployment and invest $25.6 billion during the upcoming decade from 2017.

3. Privacy-Preserving Aggregation with Authentication

In smart grid systems, millions of smart meters are controlled by a single central controller, and an aggregator collects and aggregates metering information from hundreds of smart meters at intervals ranging from a few milliseconds to several days. Under such a scenario, attacks compromising smart grid security can be divided into passive and active attacks [10,28,29]. The aims of passive attacks are to learn and use the exchanged information without affecting system resources. Thus, its objective is general privacy (i.e., confidentiality) invasion of transmitted information such as system configuration, architecture, and operation behaviors. These attacks are rarely detected by the system administrator, hence the main focus is prevention of information leakage by exploiting cryptographic primitives. On the other hand, the aims of active attacks are to modify and affect systems through modification of exchanged data and/or injection of false information into a system [30].

In order to make smart grids resilient against attacks, cryptographic primitives are widely employed. As regarding data confidentiality, encryption algorithms are exploited as an elementary approach to guarantee security in communication and storage. Especially regarding integrity, the metering information is subject to unintentional modification or intentional modification from malicious adversaries during transmission. For the purpose of integrity violation detection, several authentication mechanisms have been extensively studied. In addition, all sorts of smart grid entities are required to prove their authenticity to avoid impersonation attacks. Therefore, verification of its source is of paramount importance. Another essential feature in smart grids is computational and communicational efficiency, so that delivery and operational delays of the expected metering information should be minimized to maintain strict control of the infrastructure. To achieve the aforementioned properties, countermeasures need to be efficiently handled by participating entities in an automated fashion because many distributed entities, such as smart meters, have limited computation capabilities and have a long chain of communications in the aggregation path. Specifically,

the length of packets in a smart grid is restricted, which means that the number of messages that can be aggregated in one packet is also limited.

Energy consumption costs have been proven to be higher in data transmission than computation costs for security improvements in a single device [31]. Therefore, various integrity guarantee techniques have been studied through cryptographic operations for secure data aggregation before and after communication.

First, the aggregation can be divided into lossy and lossless approaches. In the former, the aggregator just collects the total sum or average usage of smart meters. It then takes multiple input values as input and outputs a single value (e.g., sum or average) for the purpose of statistics by exploiting a homomorphic encryption algorithm to provide data privacy. On the other hand, in the lossless approach, the aggregator collects the individual usage of distributed smart meters and stores all the data received from individual smart meters in a database for the purpose of billing [32]. Cho et al. [33] proposed privacy-preserving authentication with a lossless data aggregation scheme, called PALDA, which exploited homomorphic encryption. However, the aggregation was performed without cryptographic operations (i.e., payloads of received packets are aggregated into the payload of the output packet by removing redundant headers and tails through encapsulation and decapsulation accordingly). They provided an analysis of their scheme in a numerical manner. The majority of studies have adopted the Paillier encryption algorithm [34] as an additive homomorphic encryption, which allows for the addition of metering data in encrypted form, thus reducing the number of computations during encipherment/decipherment. Erkin and Gene [35] presented a modified Paillier (additive) homomorphic encryption. In their scheme, though a public decryption key allows everyone to access the aggregated usage, individual consumption cannot be derived because decryption can be done only after the computation of all individual information (in terms of differential privacy). All the participating smart meters must make use of the same random number during the encryption phase, which might be unstable under circumstances where a partial set of smart meters fail to upload their usage information. Borges and Mühlhäuser [36] used an additive homomorphic encryption in their proposed privacy-preserving transmission of aggregated data, called EPPP4SMS. In their scheme, the central controller receives encrypted measurements and computes aggregation on them. Mustafa et al. [37] designed a privacy-preserving selective aggregation scheme in a multi-recipient system model in concert with a bilinear pairing-based BLS short signature, aggregate signature, and additive homomorphic Paillier encryption algorithms. Garcia and Jacobs [38] proposed a privacy-preserving energy metering system based on homomorphic encryption. Li et al. [39,40] constructed an aggregation tree, each node in which calculates the sum of electricity usage of constituting smart meters in the subtree, by employing the Paillier homomorphic encryption. Wang et al. [41] used the Paillier's homomorphic encryption and verifiable secret sharing by introducing a trusted third party. Bartoli et al. [31] presented a lossless data aggregation for machine-to-machine (M2M) networks by packing multiple sensor data in a single output. However, their scheme restricted the number of input data that can be contained in a single output to four at most. Li et al. [42] proposed a lossless data aggregation scheme with improved reliability, which authenticates transmitted data and diagnoses faults in it by exploiting signature amortization and batch verification. Unfortunately, it does not guarantee data privacy.

Erkin and Gene [35] introduced collection scenarios of power usage information based on different criteria: space and time. In the spatial aggregation, usage information from a group of smart meters in a certain area is aggregated for a specific time period. Shen et al. [43] proposed a privacy-preserving multi-dimensional data aggregation considering a residential area where multiple users live. Based on Honer's rule, they constructed a user-level polynomial to store the dimensional values. On the other hand, in the temporal aggregation, the total usage of a single smart meter is aggregated. Furthermore, spatio-temporal aggregation collects total usage information of independent and other smart meters in a neighborhood at the same time [33].

When considering a decentralized (liberalized) electricity market, where electricity and data transmission are provided by different authorities heterogeneously, the subject of aggregation can be differentiated to aggregator and gateway levels. For an aggregator encompassing central controller level aggregation, Mustafa et al. [37] considered a multi-recipient model, while Ruj and Nayak [44] examined a single-recipient one. At the gateway level, Li et al. [39], He et al. [45], Deng and Yang [46], Cho et al. [33], Hur et al. [47], and He et al. [48] constructed an aggregation tree for user privacy. In each of these studies, the topology is organized into a tree, and aggregation is performed at the gateway without any knowledge of the resulting value by exploiting homomorphic encryption. In [33,45,48], independent smart meters generate and send encryption of the metering data under a public homomorphic encryption key to the gateway, after which the gateway performs a homomorphic evaluation without knowledge of the underlying metering data. The central controller receives the resulting value in encrypted form from the gateway and takes an action proper to the results, after decrypting homomorphic ciphertext. On the other hand, Li et al. [39,46,47] examined an environment where smart meters are organized in a hierarchical manner (incremental aggregation) such that a smart meter sends encrypted metering data to another until the aggregated data reaches the central controller. It is noteworthy that Hur et al. [47] designed a lightweight additive homomorphic encryption based on modular arithmetic that achieved much faster aggregation performance than others adopting variations of the Paillier encryption algorithm. Recently, Abdallah and Shen [49] adopted a lightweight lattice-based encryption algorithm where aggregation is performed by smart appliances instead of smart meters, gateways, or central controller.

Li and Lui [50] used a homomorphic signature that allowed the aggregator to check the correctness of the aggregated data in order to address the malleability of the Paillier encryption. He et al. [45] adopted authentication of the control message in downlinks to guarantee the identity of the central controller when aggregated data is not considered to be the target of integrity verification. On the other hand, Deng et al. [46,47] put their main focus on the integrity of aggregated metering data by identifying the source of received metering data. To do so, integrity verification is performed at each smart meter, and the signature of verified aggregated data is again signed by the verifying smart meter before sending it to the parent node in the tree.

For efficiency in authentication, various approaches have been taken such as the short signature scheme [37] for communication overhead and the batch signature scheme [43], which looks to shorten computation time. Lu et al. [32] presented a modified Paillier encryption in which they pack multiple measurements into a single ciphertext of a smart meter, which then signs the ciphertext and sends it to the local gateway aggregating ciphertext measurements. After validation of the signatures, the aggregation is computed and the results are sent to the supplier.

Other criteria in smart grid systems include identity anonymization as a way to conceal users' real identities by exploiting zero knowledge proof, pseudonyms, and various kinds of signature schemes [32,51–57]. Wang et al. [57] proposed an anonymous aggregation scheme in a fog computing environment by exploiting the Castagnos-Laguillaumie cryptosystem. Zhang et al. [58] proposed a secure data aggregation scheme under the range segmentation model SEDAR (SEcure Data Aggregation scheme under the Range segmentation model). They also presented two extended versions of SEDAR through randomization (REDAR) and compression (CEDAR), achieving a significant reduction in communication costs with a trade-off in security and accuracy, respectively. Ni et al. [59] considered operation centers as curious entities in reality and pointed out privacy issues that can arise at the aggregator site. To address information leakage, they extended Lifted-ElGamal encryption to aggregate end users' consumption reports at the gateway. By leveraging zero-knowledge range proof, their scheme is proven secure against false data injection attacks without the disclosure of individual measurements. Similarly, Nandgaonkar and Kamble [60] assumed that the aggregator is untrustworthy, potentially a powerful eavesdropper. Li et al. [61] presented a fine-grained aggregation model which enables a central controller to evaluate the multi-subset data aggregation of different ranges. Their proposed scheme, called PPMA (Privacy-Preserving Multi-subset Aggregation), introduced

a trusted third party to guarantee privacy protection with the aid of the Paillier homomorphic encryption algorithm.

Very interesting research is also being conducted in various other directions. For example, Gong et al. [62] introduced a concept of incentive by proposing a demand response program in the smart grid system that allows the demand response provider to compute individual demand curtailments and demand response rewards in a privacy-preserving manner. Ford et al. [63] presented an anonymization mechanism supporting fine-grained data analysis in a comprehensive manner.

3.1. Efficiency and Scalability

As mentioned in [64], smart meters can collect metering information at varying intervals (as an example, for the Hydro One project, the reading intervals can be 5 to 60 min). With technology evolution, measurement even can be done at interval of less than every minute [65]. In Europe, as a result of the Powerfox project, customers can directly access consumption information via an Android app in 2017 [66]. The provided information is displayed by hourly with 15 min aggregations for a week based on the collected data every minute. Across the U.S., the advanced metering information (AMI) infrastructure records 15 min consumption data [67]. World Energy Council also mentioned that smart meters send metering information at pre-defined intervals from hourly to every 15 min [68], while Japanese smart meters are supposed to provide metering information in 30 minute intervals [69].

As metering information increases, the cost of aggregation based on accumulated data also increases. In addition, an aggregation technique should take into account the computing power of a smart meter with limited computing resources. According to the comparison of computation time in [70], the schemes using existing (or modified versions of) public key encryption algorithms supporting additive homomorphic properties such as Paillier, ElGamal, and RSA require a considerably larger amount of computing resources than the additive homomorphic encryption performing only simple modular additions presented by Hur et al. [47], which was designed with smart grid system efficiency as a priority.

However, this kind of somewhat homomorphic encryption supports only limited arithmetic operations due to its limited plaintext space. When the plaintext space increases, so does the corresponding computation time. A more serious limitation is that these studies provide only simple aggregation manipulations, such as addition, and do not support more comprehensive operations. To derive more meaningful metering information, it is necessary to consider the use of fully homomorphic encryption (FHE), which gives a high degree of freedom in operations.

In another aspect, scalability depends on the intervals between gathering metering information. As the acquisition interval is shortened, the amount of information obtainable from the smart meter increases. This might enable more accurate predictions for efficient resource management. However, when the data communication cost and computation capability are overloaded, the expected output cannot be collected. Therefore, it is desirable to establish a systematic deployment plan and an appropriate collection interval in consideration of the performance that smart meters and their central controller can afford.

4. Conclusions and Discussion on Future Directions of Smart Grids

In the above, we have looked at the latest trends in smart grid and state-of-the-art research for secure data aggregation. The majority of countries around the world are implementing and realizing deployment policies for the popularization of the smart grid to meet the goals of low carbon emissions, efficient and reliable supply chains, and the liberalization of choices. At the same time, they are promoting interoperability in industry through standardization and regularization. There might arise various disputes over replacing existing power grid systems with intelligent smart grid counterparts in the present transition stage. However, considering current and future developments, it is necessary to recognize the tremendous advantages of the smart grid.

The research on privacy-preserving data aggregation in smart grid environments is evolving in various aspects with respect to:

- Privacy preservation: To achieve privacy protection during data transmission, semantically secure encryption algorithms are employed. Additionally, (additive) homomorphic encryption supporting evaluations on encrypted data such as ElGamal, Paillier, and lattice-based cryptosystems are being adopted in order to protect user privacy. Depending on the subject to be protected, all kinds of participating entities such as smart appliances, smart meters, (intermediate) gateways, and central controllers are taken into account.
- Authentication: To produce accurate aggregate results, various kinds of authentication algorithms are being adopted. According to the situation, sender authentication that validates data origin is considered. Some algorithms are used in upstream directions to check forwarding entities during the process of transferring metering data to the central controller, while others are used to identify the central controller in downstream directions during delivery of decisions made from aggregate data. On the other hand, data authentication is combined with the above approaches to avoid false data injection attacks from malicious adversaries or unintended malfunctions.
- Efficiency: In terms of computational efficiency, lightweight encryption algorithms are designed through modification of the existing homomorphic encryption schemes. Batch verification algorithms are also considered in the validation of received data authenticity. In terms of communication efficiency, data aggregation itself is devised to minimize the size of transmitted data with the modification of internal data structures. Furthermore, short signature schemes are also adopted in authentication mechanisms.

In the metering data aggregation schemes presented so far, erroneous insertions by external intervention such as false data injection can be detected through authentication. However, not only the validation of smart meters participating in aggregation but also the validation of aggregated information should be considered at the same time for secure smart metering because metering data can be threatened by both the insider and outsider adversaries during the aggregation and transmission in the grid network. Although most of the state-of-the-art schemes adopted additive homomorphic encryption such as the Paillier cryptosystem, fully homomorphic encryption (FHE) would be more appropriate for complex statistical analysis at the central controller. However, since the current FHE requires computationally infeasible overheads for resource-limited smart meters in practice; designing more practical aggregation algorithms that satisfy both the security and scalability requirements will be an open problem in the smart grid system.

Additionally when it comes to the authenticated aggregation, majority of state-of-the-art studies handle message authentication and data origin authentication assuming that smart meters are trustworthy. However, in practice, we need to consider more practical threat models. For example, the smart meters may be compromised easily without revealing their identities on a smart grid infrastructure. However, unfortunately, some studies just provide transmission integrity under the somewhat unrealistic and strong security assumption. In other words, when a compromised smart meter inserts erroneous metering information in the process of adding its own metering information to the aggregation before sending the correctly signed aggregated data on to the next meter, there are possibilities that the central controller misbehaves triggering power outage or surplus power generation. The issue of how to ensure reliability with the existence of compromised smart meters needs to be taken into account.

As smart grid technology improves, the performance of terminal devices, including sensors, is expected to improve significantly, while the functionalities performed in the terminal will be diversified according to their purposes. Thus, it is expected that more efficient and stable techniques will be researched to improve the relevant situations in smart grids.

By the way, for smart grids, standard development is more important than in other industries because their interoperability must be established for combination of the various technologies involved from initial power generation to delivery to the consumer. International standards are led by U.S.

organizations, such as the IEEE and NIST, while each country also presents its own national standards. The EU has formed the SGCG (Smart Grid Coordination Group-CEN, CENELEC, ETSI) for sustainable processes, reference architecture, and information security and data privacy. South Korea has established the KSGA (Korea Smart Grid Association) and Japan the JSCA (Japan Smart Community Association), and they have signed MOUs for a civil-government joint organization in response to international standards. Although efforts are being made to expand the infrastructure in individual countries, it is expected that the standardization of international standards for global interoperability, as well as the standards in each country, will be a more important goal.

There might be non-negligible issues, such as in the Tonsley innovation district in Australia, due to financial burdens on residents and utilities, or as in the Netherlands where development is suspended by a security issue in a smart grid system that has not yet matured. However, at the present stage, which is the first phase of widespread deployment, research and the systemization of measures to maximize the positive effects of the smart grid is required based on the development of systematic planning and harmonious solutions to conflicting issues, rather than aborting its progress. The future of the smart grid is bright, but new threats will arise in new environments. Therefore, it is necessary to make continuous efforts to minimize the potential side effects while reviewing the various issues that arise as the smart grid is established, along with ongoing research on possible future situations.

Acknowledgments: This research was financially supported by Hansung University for Dongyoung Koo. This work was also supported by an Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korean government (MSIT) (No.2017-0-00143, Development on countermeasure against cache side-channel attacks for Youngjoo Shin; and No.2017-0-00380, Development of next generation user authentication for Junbeom Hur).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. International Data Corporation (IDC). Worldwide Spending on the Internet of Things Forecast to Reach Nearly $1.4 Trillion in 2021, According to New IDC Spending Guide. Available online: https://www.idc.com/getdoc.jsp?containerId=prUS42799917 (accessed on 27 September 2017).
2. Pillitteri, V.Y.; Brewer, T.L. Guidelines for Smart Grid Cybersecurity. *NIST Interagency/Internal Report (NISTIR)-7628 Rev 1*, 25 September 2014; pp. 1–668. Available online: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (accessed on 29 September 2017)
3. Baker, F.; Meyer, D. Internet Protocols for the Smart Grid. *No. RFC 6272*; June 2011, pp. 1–66. Available online: https://tools.ietf.org/html/rfc6272.txt.pdf (accessed on 27 September 2017).
4. European Telecommunications Standards Institute (ETSI). Machine-to-Machine Communications (M2M); Threat Analysis and Counter-Measures to M2M Service Layer. *ETSI TR 103 167 V1.1.1 (2011-08)*, Sophia Antipolis, France, 4 August 2011; pp.1–62. Available online: http://www.etsi.org/deliver/etsi_tr/103100_103199/103167/01.01.01_60/tr_103167v010101p.pdf (accessed on 27 September 2017).
5. McDaniel, P.; McLaughlin, S. Security and Privacy Challenges in the Smart Grid. *IEEE Secur. Priv.* **2009**, *7*, 75–77.
6. Khurana, H.; Hadley, M.; Lu, N.; Frincke, D.A. Smart-grid security issues. *IEEE Secur. Priv.* **2010**, *8*, 81–85.
7. Liu, J.; Xiao, Y.; Li, S.; Liang, W.; Chen, C.L.P. Cyber Security and Privacy Issues in Smart Grids. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 981–997.
8. Erol-Kantarci, M.; Mouftah, H.T. Smart grid forensic science: Applications, challenges, and open issues. *IEEE Commun. Mag.* **2013**, *51*, 68–74.
9. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 21–38.
10. Delgado-Gomes, V.; Martins, J.F.; Lima, C.; Borza, P.N. Smart grid security issues. In Proceedings of the International Conference on Compatibility and Power Electronics (CPE), Lisbon, Portugal, 24–26 June 2015; pp. 534–538.

11. The Global Smart Grid Federation (GSGF). Smart Meter Security Survey. Available online: http://www.globalsmartgridfederation.org/wp-content/uploads/2016/08/smart_meter_security_survey.pdf (accessed on 27 September 2017).
12. Hahn, A.; Govindarasu, M. Cyber Attack Exposure Evaluation Framework for the Smart Grid. *IEEE Trans. Smart Grid* **2011**, *2*, 835–843.
13. Greveler, U.; Glösekötterz, P.; Justusy, B.; Loehr, D. Multimedia content identification through smart meter power usage profiles. In Proceedings of the International Conference on Information and Knowledge Engineering (IKE), Las Vegas, NV, USA, 16–19 July 2012.
14. Erkin, Z.; Troncoso-pastoriza, J.R.; Lagendijk, R.L.; Perez-Gonzalez, F. Privacy-preserving data aggregation in smart metering systems: An overview. *IEEE Signal Process. Mag.* **2013**, *30*, 75–86.
15. Fang, X.; Misra, S.; Xue, G.; Dajun, Y. Smart Grid—The New and Improved Power Grid: A Survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980.
16. Pooranian, Z.; Nikmehr, N.; Najafi-Ravadanegh, S.; Mahdin, H.; Abawajy, J. Economical and environmental operation of smart networked microgrids under uncertainties using NSGA-II. In Proceedings of the International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 22–24 September 2016; pp. 1–6.
17. Shojafar, M.; Cordeschi, N.; Baccarelli, E. Energy-efficient Adaptive Resource Management for Real-time Vehicular Cloud Services. *IEEE Trans. Cloud Comput.* **2016**, *PP*, 1–14.
18. SmartGrid Canada. Available online: http://www.sgcanada.org/ (accessed on 27 September 2017).
19. Department of Planning, Transport and Infrastructure, Government of South Australia. Adelaide's New Suburb—TONSLEY. Available online: https://dpti.sa.gov.au/tonsley (accessed on 27 January 2017).
20. Standards Council of Canada. The Canadian Smart Grid Standards Roadmap: A Strategic Planning Document. Available online: https://www.scc.ca/sites/default/files/publications/Smart_Grid_Report_FINAL_EN_3.pdf (accessed on 27 September 2017).
21. European Commission. Minutes—High level Roundtable on Main Challenges for Cyber Security in the Energy System. Available online: https://ec.europa.eu/energy/sites/ener/files/documents/detailed_minutes_rome_24.3_final.pdf (accessed on 27 September 2017).
22. NobelGrid. Available online: http://nobelgrid.eu/ (accessed on 27 September 2017).
23. SEGRID. Available online: https://segrid.eu/ (accessed on 27 September 2017).
24. The SPARKS Project. Smart Grid Protection Against Cyber Attacks. Available online: https://project-sparks.eu/ (accessed on 27 September 2017).
25. HyRiM. Hybrid Risk Management for Utility Providers. Available online: https://hyrim.net/ (accessed on 26 April 2017).
26. Metering & Smart Energy International. Smart Grid Investments in Australia and New Zealand to Read $6.1bn. Available online: https://www.metering.com/news/smart-grid-investments-australia/ (accessed on 27 September 2017).
27. Northeast Group, LLC. Smart Grid Infrastructure Investment in South America: $38.1bn by 2025. Available online: http://www.prnewswire.com/news-releases/smart-grid-infrastructure-investment-in-south-america-381bn-by-2025-300125709.html/ (accessed on 27 September 2017).
28. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129.
29. Khatoun, R.; Zeadally, S. Cybersecurity and Privacy Solutions in Smart Cities. *IEEE Commun. Mag.* **2017**, *55*, 51–59.
30. Salinas, S.; Li, M.; Li, P. Privacy-Preserving Energy Theft Detection in Smart Grids: A P2P Computing Approach. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 257–267.
31. Bartoli, A.; Hernandez-Serrano, J.; Soriano, M.; Dohler, M.; Kountouris, A.; Barthel, D. Secure Lossless Aggregation Over Fading and Shadowing Channels for Smart Grid M2M Networks. *IEEE Trans. Smart Grid* **2011**, *2*, 844–864.
32. Liang, X.; Li, X.; Lu, R.; Lin, X.; Shen, X. UDP: Usage-Based Dynamic Pricing with Privacy Preservation for Smart Grid. *IEEE Trans. Smart Grid* **2013**, *4*, 141–150.
33. Cho, S.; Li, H.; Choi, B.J. PALDA: Efficient privacy-preserving authentication for lossless data aggregation in Smart Grids. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 914–919.

34. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Advances in Cryptology—EUROCRYPT*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 223–238. Available online: https://www.researchgate.net/publication/221348062_Public-Key_Cryptosystems_Based_on_Composite_Degree_Residuosity_Classes (accessed on 4 February 2016).
35. Erkin, Z.; Tsudik, G. Private Computation of Spatial and Temporal Power Consumption with Smart Meters. In Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS); Singapore, 26–29 June 2012; pp. 561–577.
36. Borges, F.; Muhlhauser, M. EPPP4SMS: Efficient Privacy-Preserving Protocol for Smart Metering Systems and Its Simulation Using Real-World Data. *IEEE Trans. Smart Grid* **2014**, *5*, 2701–2708.
37. Mustafa, M.A.; Zhang, N.; Kalogridis, G.; Fan, Z. DEP2SA: A Decentralized Efficient Privacy-Preserving and Selective Aggregation Scheme in Advanced Metering Infrastructure. *IEEE Access* **2015**, *3*, 2828–2846.
38. Garcia, F.D.; Jacobs, B. Privacy-Friendly Energy-Metering via Homomorphic Encryption. In Proceedings of the International Workshop on Security and Trust Management (STM); Copenhagen, Denamrk, 27–28 June 2011; pp. 226–238.
39. Li, F.; Luo, B.; Liu, P. Secure Information Aggregation for Smart Grids Using Homomorphic Encryption. In Proceedings of the IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 327–332.
40. Li, H.; Lin, X.; Yang, H.; Liang, X.; Lu, R.; Shen, X. EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 2053–2064.
41. Wang, X.F.; Mu, Y.; Chen, R.M. An efficient privacy-preserving aggregation and billing protocol for smart grid. *Secur. Commun. Netw.* **2016**, *9*, 4536–4547.
42. Li, D.; Aung, Z.; Williams, J.R.; Sanchez, A. Efficient and Fault-Diagnosable Authentication Scheme for Advanced Metering Infrastructure. *Data and Network Analytics Research Group, Tech. Rep.*; January 2013. Available online: https://pdfs.semanticscholar.org/9fe3/d9aafc0e3017d768391c97d481fc4f960fa7.pdf (accessed on 27 September 2017).
43. Shen, H.; Zhang, M.; Shen, J. Efficient Privacy-Preserving Cube-Data Aggregation Scheme for Smart Grids. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1369–1381.
44. Ruj, S.; Nayak, A. A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids. *IEEE Trans. Smart Grid* **2013**, *4*, 196–205.
45. He, X.; Pun, M.O.; Kuo, C.C.J. Secure and efficient cryptosystem for smart grid using homomorphic encryption. In Proceedings of the IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012; pp. 1–8.
46. Deng, P.; Yang, L. A secure and privacy-preserving communication scheme for Advanced Metering Infrastructure. In Proceedings of the IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012; pp. 1–5.
47. Hur, J.B.; Koo, D.Y.; Shin, Y.J. Privacy-Preserving Smart Metering with Authentication in a Smart Grid. *Appl. Sci.* **2015**, *5*, 1503–1527.
48. He, D.; Kumar, N.; Zeadally, S.; Vinel, A.; Yang, L.T. Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid against Internal Adversaries. *IEEE Trans. Smart Grid* **2017**, *8*, 2411–2419.
49. Abdallah, A.; Shen, X. A Lightweight Lattice-based Homomorphic Privacy-Preserving Data Aggregation Scheme for Smart Grid. *IEEE Trans. Smart Grid* **2016**, *PP*, 1–10.
50. Li, F.; Luo, B. Preserving data integrity for smart grid data aggregation. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 366–371.
51. Rial, A.; Danezis, G. Privacy-preserving Smart Metering. In Proceedings of the Annual ACM Workshop on Privacy in the Electronic Society (WPES), Chicago, IL, USA, 17 October 2011; pp. 49–60.
52. Jawurek, M.; Johns, M.; Kerschbaum, F. Plug-In Privacy for Smart Metering Billing. In Proceedings of the International Symposium on Privacy Enhancing Technologies (PETS), Waterloo, ON, Canada, 27–29 July 2011.
53. Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K.; Mui, T.W.; Tsang, Y.H.; Kwok, C.K.; Yu, K.Y. Selling Power Back to the Grid in a Secure and Privacy-Preserving Manner. In Proceedings of the International Conference on Information and Communications Security (ICICS), Hong Kong, China, 29–31 October 2012; pp. 445–452.

54. Cheung, J.C.L.; Chim, T.W.; Yiu, S.M.; Li, V.O.K.; Hui, L.C.K. Credential-Based Privacy-Preserving Power Request Scheme for Smart Grid Network. In Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), Houston, TX, USA, 5–9 December 2011; pp. 1–5.
55. Chu, C.K.; Liu, J.K.; Wong, J.W.; Zhao, Y.; Zhou, J. Privacy-preserving Smart Metering with Regional Statistics and Personal Enquiry Services. In Proceedings of the ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIA CCS), Hangzhou, China, 8–10 May 2013; pp. 369–380.
56. Zargar, S.H.M.; Yaghmaee, M.H. Privacy preserving via group signature in smart grid. In Proceedings of the Electric Industry Automation Congress (EIAC), Mashhad, Iran, 13–14 February 2013; pp. 1–5.
57. Wang, H.; Wang, Z.; Domingo-Ferrer, J. Anonymous and secure aggregation scheme in fog-based public cloud computing. *Future Gener. Comput. Syst.* **2017**, pp. 1–8.
58. Zhang, P.; Li, W.; Sun, H. Cost-Efficient and Multi-Functional Secure Aggregation in Large Scale Distributed Application. *PLoS ONE* **2016**, *11*, e0159605.
59. Ni, J.; Zhang, K.; Alharbi, K.; Lin, X.; Zhang, N.; Shen, X. Differentially Private Smart Metering with Fault Tolerance and Range-Based Filtering. *IEEE Trans. Smart Grid* **2017**, *8*, 2483–2493
60. Nandgaonkar, K.; Kamble, S. A survey on privacy-preserving data aggregation without secure channel. *Int. Res. J. Eng. Technol. (IRJET)* **2016**, *3*, 133–136.
61. Li, S.; Xue, K.; Yang, Q.; Hong, P. PPMA: Privacy-Preserving Multi-Subset Aggregation in Smart Grid. *IEEE Trans. Ind. Inform.* **2017**, *PP*, 1–10.
62. Gong, Y.; Cai, Y.; Guo, Y.; Fang, Y. A Privacy-Preserving Scheme for Incentive-Based Demand Response in the Smart Grid. *IEEE Trans. Smart Grid* **2016**, *7*, 1304–1313.
63. Ford, V.; Siraj, A.; Rahman, M.A. Secure and efficient protection of consumer privacy in Advanced Metering Infrastructure supporting fine-grained data analysis. *J. Comput. Syst. Sci.* **2017**, *83*, 84–100.
64. Mohassel, R.R.; Fung, A.; Mohammadi, F.; Raahemifar, K. A survey on Advanced Metering Infrastructure. *Int. J. Electr. Power Energy Syst.* **2014**, *63*, 473–484.
65. Murrill, B.J.; Liu, E.C.; Thompson, R.M. Smart meter data: Privacy and cybersecurity. *Congressional Research Service, Library of Congress*. 3 March 2012. Available online: http://marylandsmartmeterawareness.org/wp-content/uploads/2012/07/Congress-Research-Service-SM-privacy-and-cybersecurity.pdf (accessed on 27 September 2017).
66. European Commission. My Energy Data—European Smart Grids Task Force Expert Group 1—Standards and Interoperability. Available online: https://ec.europa.eu/energy/sites/ener/files/documents/report_final_eg1_my_energy_data_15_november_2016.pdf (accessed on 1 September 2017).
67. U.S. Energy Information Administration. An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling. Available online: https://www.eia.gov/consumption/residential/reports/smartmetering/pdf/assessment.pdf (accessed on 27 September 2017).
68. World Energy Council. Energy Efficiency: A Recipe For Success. Available online: https://hub.globalccsinstitute.com/publications/energy-efficiency-recipe-success/ (accessed on 1 September 2017).
69. Metering & Smart Energy International. Smart Grid Trends in Japan: 7 Things to Know. Available online: https://www.metering.com/smart-grid-trends-in-japan-7-things-to-know/ (accessed on 4 March 2015).
70. Farah, S.; Javed, Y.; Shamim, A.; Nawaz, T. An experimental study on performance evaluation of asymmetric encryption algorithms. Recent Advances in Information Science. In Proceedings of the Proceeding of the 3rd European Conference of Computer Science, (EECS-12), Paris, France, 2–4 December 2012; pp. 121–124.