Computer Networks 70 (2014) 312–329

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Cloud Computing for Smart Grid applications

Melike Yigit [a,*], V. Cagri Gungor [a,b], Selcuk Baktir [a]

[a] Department of Computer Engineering, Bahcesehir University, Faculty of Engineering, Ciragan Cad. Osmanpasa Mektebi Sok. No: 4-6, 34353 Besiktas, Istanbul, Turkey

[b] Department of Computer Engineering, Abdullah Gul University (AGU), Faculty of Engineering, Barbaros Mahallesi, Erkilet Bulvari, Kocasinan, Kayseri, Turkey

ARTICLE INFO

Article history:
Received 6 August 2013
Received in revised form 29 November 2013
Accepted 12 June 2014
Available online 20 June 2014

Keywords:
Smart Grid
Cloud Computing
Smart Grid and Cloud Computing architecture
Cloud Computing based Smart Grid applications and projects

ABSTRACT

A reliable and efficient communications system is required for the robust, affordable and secure supply of power through Smart Grids (SG). Computational requirements for Smart Grid applications can be met by utilizing the Cloud Computing (CC) model. Flexible resources and services shared in network, parallel processing and omnipresent access are some features of Cloud Computing that are desirable for Smart Grid applications. Even-though the Cloud Computing model is considered efficient for Smart Grids, it has some constraints such as security and reliability. In this paper, the Smart Grid architecture and its applications are focused on first. The Cloud Computing architecture is explained thoroughly. Then, Cloud Computing for Smart Grid applications are also introduced in terms of efficiency, security and usability. Cloud platforms' technical and security issues are analyzed. Finally, cloud service based existing Smart Grid projects and open research issues are presented.

1. Introduction

The Smart Grid (SG) is used by electric power utilities to track and control power usage of consumers. In SGs, the governance of energy usage is done in real time with the ability of smart meters' bidirectional communication [1]. A more reliable and secure communication is guaranteed with the SG's distributed energy management feature which is called as load balancing. Electric power utilities achieve preferable operation and management of their electric power systems by monitoring their energy usage. When consumed energy reaches peak levels, signals are sent to consumers to reduce energy consumption. In this way, the SG balances its energy load [2]. Entire power supply system and protection devices are monitored by control centers for providing security of SG's load balancing system during communication. Cloud Computing (CC) is used to perform this communication process between substations and power supply companies' power plants. Built-in redundancy is utilized to increase the reliability, security and robustness of this communication [3]. In this context, scalable platforms are needed to run many SG applications when data intensity is high. Over the time of the day, the resource requirement varies as the utilization differentiates between day (peak operation) and night (lower level operation). CC platforms can be utilized for obtaining scalable, elastic, secure, robust and sharable resources in order to build and operate a functional SG architecture [3].

Utilities and consumers take the security and privacy of their data very seriously. This affects the acceptance of SGs provided by cloud platforms, i.e. the privacy issues for the users should be addressed by the utilities [4,5]. CC platforms chosen for SG applications should realize high assurance in their communication systems. There are some performance issues related to the use of cloud platforms for SG applications

* Corresponding author. Tel.: +90 5542403593.
E-mail addresses: melike.yigit@stu.bahcesehir.edu.tr (M. Yigit), cagri.gungor@agu.edu.tr (V.C. Gungor), selcuk.baktir@bahcesehir.edu.tr (S. Baktir).

http://dx.doi.org/10.1016/j.comnet.2014.06.007
1389-1286/

as well, e.g. the requirement for supporting real time services to give rapid response to consumers. Internet congestion and server failure are the main constraints in this respect [6]. Consistency and fault tolerance services are necessary for cloud systems. In order to ensure these features, some consistency models such as database guarantees, replication behavior of state machine and virtual synchrony must be applied to cloud platforms. An important advantage of cloud systems for SG applications is their highly qualified Internet routing capability that is supplied by providing multi-path Internet routes between access points and cloud services. In this manner, connection losses are prevented and communication is reliably achieved between the SG and cloud hosted services.

The next generation computing paradigm, provided by CC, satisfies the requirements of SG applications [7]. Cloud providers facilitate CC and offer services with their huge servers for computations and with their big data centers for storage. Many resources shared in the network, such as software and information, are provided to the power grid utility's devices through CC. Therefore, it is preferable for many SG applications to use CC for information management and distributed energy management.

There have been several studies on how SG applications can exploit CC to increase their reliability and performance. In the study by Simmhan et al. [8], a SG's demand response is optimized by using CC. This is achieved by CC with a flexible and scalable model of Cloud virtual machines. These Cloud virtual machines perform computations to determine the availability of resources to be used on demand and to be discharged when not in use. Also, redundancy is achieved for critical SG applications by these Cloud virtual machines by adding extra virtual machines to duplicate computations and replicate the data. In the work by Rusitschka et al. [9], a different CC model is proposed for real time data retrieval and parallel processing for SG applications. In another research, conducted by Bai et al. [10], CC provides efficient and secure storage management for a Smart Grid condition monitoring application. CC also offers many other advantages to a SG in terms of affordability and scalability. Kim et al. offered a CC based demand response architecture which aims at giving fast response to customers by providing direct communication between consumers and utilities [11]. Grid aware CC routing algorithms, which solve service request routing problems, are implemented by Mohsenian-Rad et al. [12], Fayyaz et al. [13] and Alcaraz and Lopez In [14], the authors focused on addressing the security and reliability issues in combining SG applications with CC. In addition to research conducted on the application of CC for SGs, there are also some products, already in the market, implementing SG applications utilizing CC. Hohm, Microsoft's energy management tool, is hosted on a cloud platform proposed to be used by special residential buildings [15]. Proprietary power saving suggestions are procured by Hohm [15]. Google's PowerMeter is another tool utilizing CC for SG applications and was ended in September 26, 2011 [16]. It is a scalable platform and facilitates monitoring the energy usage of consumers. There are also many other applications for testing and observing the performance of CC on SG applications [17–19]. Some of these applications are already in use and some are still being researched. All these studies are summarized in Table 1.

The remainder of this paper is organized as follows. In Sections 2 and 3, the SG and CC architectures are presented, respectively. In Section 4, opportunities and challenges to apply CC in SG is discussed. In Section 5, the use of CC for SG applications is analyzed in technical and security perspectives. In Section 6, an overview of CC based SG applications and projects are given. Open research issues in CC for SGs are presented in Section 7. Finally, this paper is concluded in Section 8.

2. The Smart Grid (SG) architecture

An electric grid with the information and communications technology (ICT) is called a Smart Grid. In SG, information about consumers' electricity consumption behavior is collected automatically with the use of the ICT [1]. This helps increase the efficiency, reliability and performance of the electric grid. The European Technology Platform is preparing a SG policy to overcome many challenges in current electricity supply, in terms of reliability, flexibility, efficiency, load adjustment, peak power cut, permanency, market supply and demand response support [20]. Reliability is provided by a SG with its features such as the ability for fault detection and self-healing. In SG applications, bidirectional energy flow allows for flexible network topology with distributed generation. The demand side management feature of the SG ensures efficiency in energy consumption. The load adjustment feature helps balance loads in spite of their variations. If a user's load exceeds an average threshold, power can be cut for this user to control electricity usage in high-cost/peak-usage periods.

The SG conceptual model, identified by the National Institute of Standards and Technology (NIST) [21], gives the characteristics, requirements, operations and services that should be provided by a SG. It also specifies communication ways from top level to lower levels for SG applications. The conceptual model includes seven domains such as bulk generation, transmission, distribution, customer, service provider, operations and markets [21] as given in Fig. 1. The conceptual model begins with bulk generation. In this domain, electricity generation and protection procedures are realized. The second domain is the markets which perform load balancing by analysing and optimizing energy pricing to help control energy consumption of customers. Business processes of energy producers, customers and transmission companies are performed by a service provider, which is the third domain of the SG conceptual model [21]. Operations in the network such as monitoring of network operation, network control, fault detection and reporting are realized with the fourth operations domain. Transportation of electricity from sources to distribution are achieved by using the transmission domain. Service providers optimize flows by the agency of the transmission domain and connect with customers via the distribution domain which achieves real time monitoring of electricity consumption. The last SG domain is the customers who let their energy usage be managed. All of these domains make up the SG architecture and result in many benefits

Table 1
Related works about how to use Cloud Computing for managing Smart Grid applications.

CC for SG studies	Subject
Simmhan et al. [8] and Kim et al. [11]	Demand response optimization with cloud platforms
Rusitschka et al. [9]	Increasing SG applications performance with parallel processing
Bai et al. [10]	SG condition monitoring with secure storage management
Hohm by Microsoft [15]	Providing power savings for SG applications
Google PowerMeter Tool [16]	Monitoring real time energy usage
Mohsenian-Rad et al. [12]	A routing algorithm that solves SG routing problems with CC
Fayyaz et al. [13] and Alcaraz and Lopez [14]	Obtaining more secure systems for SG applications with CC

including efficiency, low cost, fault tolerance and renewable energy generation.

3. Cloud Computing (CC) architecture

The usage of resources in the manner of a service over the network is called Cloud Computing (CC) [22]. CC has many types such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Data as a Service (DaaS). [23]. Implementation and maintenance costs, and system complexity of CC are reduced with the utilization of information technology. With CC, computations are achieved over the Internet. Resources such as software and information are shared through the network and retrieved by computers and devices on demand.

Distribution of services to a large number scattered computers is the main principle of CC [23]. Thus, companies or systems such as the SG, which use CC, can use the available services easily as they need. CC has an Enterprise Data Center which enables to shift resources to meet applications' requirements and provides access to all storage systems when needed. On a CC platform, there may be also other resources such as firewalls used for security, network devices for increased performance and storage area networks to enhance capacity.

The SG offers many features and applications to consumers, however it needs to be improved to handle more secure, efficient and scalable systems. This can be carried out by using the power of CC. Operations can be done at low cost with CC because sharing and automation are widespread within these systems. Also, real time response is very important for SG applications for giving immediate demand response. In cloud platforms, when a client request comes to the cloud operation system, a response is sent to the client in real time. In addition, CC provides a power efficient self-healing system which is crucial for SG applications to recover from faults and give instant response to customers. Communication in the SG is achieved via the Internet, therefore there should be no Internet outages to provide consistent transmission. This is handled in CC by assigning two or more IP addresses to a client which is called *multi homing* [6].

CC has many characteristics that can yield improved SG applications. These CC characteristics are listed below:

- Reconstruction of SG technological infrastructure is provided with the **agility** characteristic of CC [20].
- Communication between the machine and cloud software is done via CC **application programming interface (API)** [20].
- Public cloud delivery model provides **lower cost** for SG customers.
- Any device by a consumer/customer that needs to access the systems can do this from anywhere via the Internet. This is the **device and location independence** feature of CC [23].
- **Maintenance and virtualization** are other properties of CC. Installation is not required for running applications and performing computations. This provides easy access to CC services from anywhere and at anytime. Servers and storage devices can be shared and carried easily from one server to another using the virtualization property of CC [23].
- Large number of users use shared resources, which are located in a pool. This is enabled by the CC **multitenancy** characteristic. In this way, infrastructure is centralized with lower cost, without needing extra device load capacity and utilization increase [10].
- CC provides disaster recovery capability and this assures **reliability** [24].
- Some architectures are constructed for increasing system **performance** in CC platform by using web services [24].
- **Reliability** is improved by using private cloud platforms which prevents connection losses [25].

Characteristics of CC, which are summarized in Fig. 2, are suitable for SG applications in terms of security, reliability, scalability and performance. Therefore, CC has been already used in many SG applications, as described in Section 2.

4. Opportunities and challenges to apply CC in SG

SG can benefit from all aspects of CC, however there are some barriers to the adoption of CC by SG utilities. Although these barriers, real-time computing and storage capacity are required for the SG applications immediately. Therefore, CC is the best and simplest way to meet the SG requirements in spite of its challenges. In this respect, this section investigates opportunities and challenges in the integration of the CC technology within the SG for efficient SG management.

4.1. Opportunities to apply CC in SG

Power industry is interested in CC mainly for business reasons, i.e. the increased efficiency, reduced price, improved robustness, higher security and scalable capacity are attractive features of the CC in performing the SG

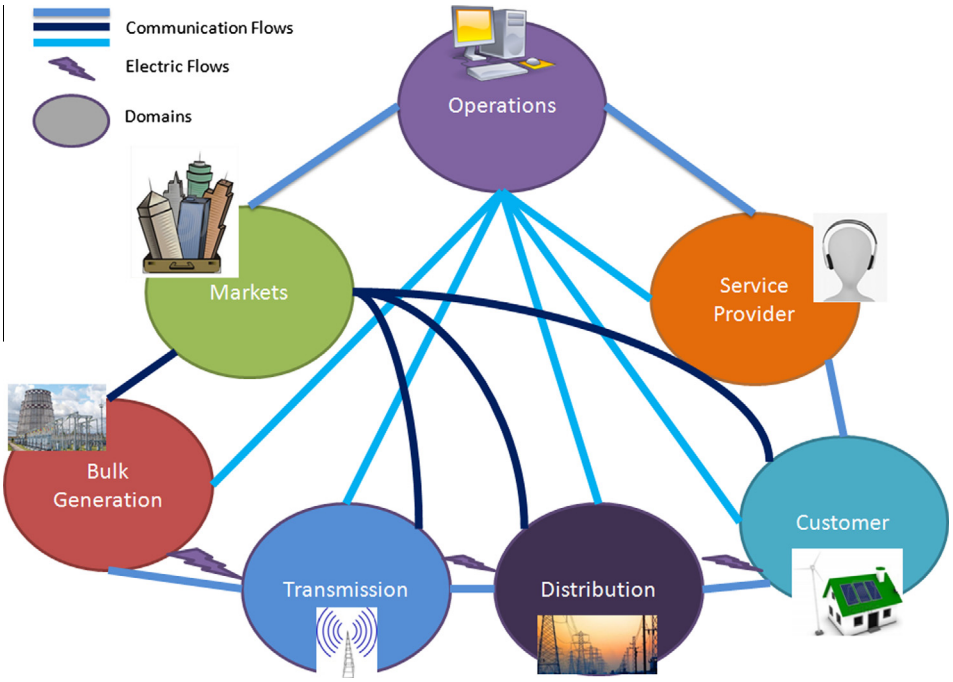


Fig. 1. Smart Grid conceptual model.

Fig. 2. Cloud Computing characteristics.

capabilities [26]. CC offers low cost computing with respect to older models. Furthermore, its robustness is intrinsically provided with the geographic replication of services. In this way, when power outages or failures occur in a region, a replicated service immediately starts running. Security in CC is guaranteed with the automatic management of cloud services which provides easier and better protection against attacks [27]. Capacity of CC is high with the used data centers, and redeployment of services in CC ensures elasticity by shifting loads [28]. All of these advantages of CC can be used in SG applications. In this respect, drivers to use the CC in a SG are shown in Fig. 3 and listed below:

- **Scalability:** Early SG applications are derelict because of the scalability problem for SG components that are deployed on a large scale. CC solves this scalability problem by deploying storage devices geographically and expanding them vertically or horizontally [29]. Therefore, the needs of a SG, such as new devices, and data storage capacity, become unnecessary when CC is used. In this way, SG utilities can react to the market changes including new state of the art technology product, expeditiously when they have data intensive [30].
- **Cost Efficiency:** Electric utilities use the SG network to switch from coal and nuclear plants to renewable energy sources such as solar, wind farms and hydroelectric. In this network, all devices are connected to each other and send status information to utilities to be controlled by them. Also, information exchange is done to check power generation by producers and consumption by consumers. This information exchange is provided at low cost over the Internet by cloud platforms and dedicated lines are used for the SG [30].
- **Central Data Storage:** SG applications are high performance computing (HPC) applications that need special computing hardware and the ability for parallel processing. However, these hardware devices are very expensive. Sufficient storage and performance can be provided by a single cloud data center with lower cost compared to deploying special computing hardware. Therefore, HPC applications such as the SG migrate to

the Cloud Computing platform to deal with the affordability issue [31]. This also helps with the set up in the communication standards in the SG, easily. Ubiquitous network access in the cloud also guarantees the access of everyone to the cloud and procure interpretability between the SG systems. A common communication platform that is offered by the cloud provides data flow in SG and avoids the use of multiple middleware software and interfaces to access the data by SG systems. Data consistency is also supplied with standardization of data formats on one central platform [30].

- **Security:** Data security and privacy are the most crucial issues for the SG environment, and therefore a detailed analysis of the security issues of CC for the SG environment are presented in Section 5.2. In this respect, a private cloud environment can be used in a SG to provide privacy, access rights, data encryption, etc. This can be achieved if a service level agreement is done with the cloud provider. Thus, utilities can provide reliance on their own by using different ways and CC ensures more security for SG applications with ironclad barriers when utilities have much more experience to meet requirements of SG applications. In CC, multiple applications are managed and run in a single data center. With these ironclad barriers, users of the same cloud cannot see each others' data and traffic in this shared environment [32].
- **Real-time Response:** Huge amounts of data, such as energy control/consumption and market data, is processed synchronically by CC with its distributed data processing centers which provides a scalable load balancing technology in the SG. Control systems in a SG need the real-time response feature of CC to give rapid reaction against an outage. However, Advanced Metering Infrastructure (AMI) also needs low delay for transferring and displaying control signals and pricing information for demand management in the grid environment. This indicates that CC provides opportunity to monitor, process and verify coming data streams from many SG sources in real-time through its storage and processing capabilities. Using CC, time critical applications of a SG is efficiently realized and not affected from changing conditions [31].

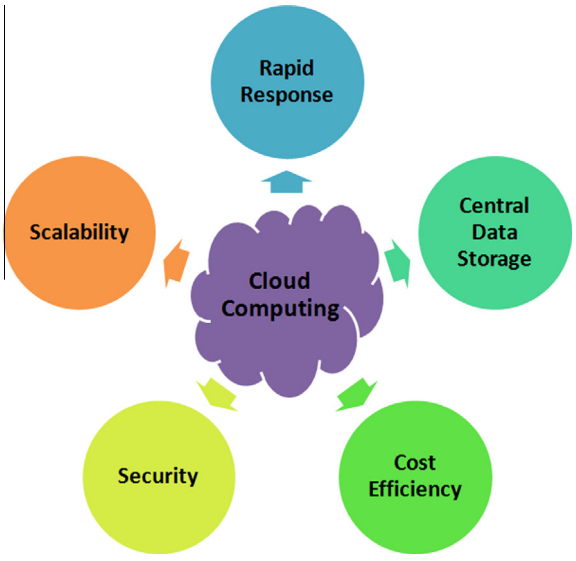


Fig. 3. Cloud Computing enhancers to use them in a Smart Grid.

The use of CC for SG applications enables new services and business models. However, a SG application has some requirements that must be addressed by a CC design and there are some challenges in using CC for SG. These challenges are discussed in Section 4.2.

4.2. Challenges in using Cloud Computing for Smart Grids

The current espousing of CC is also associated with some challenges contrary to the motivation of applying it on SG systems because SG utilities still have negative thoughts about CC's authenticity. This can be challenges ahead regarding inefficiencies for SG and therefore, while designing CC for SG systems, these challenges must be considered and analyzed carefully. On that note, major challenges of applying CC for SG applications can be outlined as follows.

- **Location of data:** Cloud servers are placed in any location, so location of these servers that store and process SG applications are not known by the business enterprise. This is very critical issue to meet the requirements of data management in SG. Therefore, defining the data location by Cloud Service Providers (CSPs) has a vital importance for the security of SG applications [33].
- **Mixing of data:** CC enables a model to access the applications through a location independent resource pool. There are many multi-user applications in CSPs however, security and scalability of them is an open issue for enterprises. Therefore, some security methods such as data encryption algorithms must be applied on CSPs for reliability and confidentiality in SG applications [33].
- **Inefficient cloud security policy:** Some CSPs apply weaker security policies than others. These differences may be specific to utilities, therefore they may cause disagreements between SG utilities. Utilities can solve this problem by putting service level agreements into effect between each others to provide required security levels for SG applications [30].
- **Term of agreement:** If contract agreement includes commercial papers that posses stored data in CC, SG utilities can pay huge amount of charge to CSPs for their requested data after service level agreement end date [33].
- **Dependence of CSP's Application Programming Interfaces (APIs):** Many applications in CC are implemented by Cloud Service Providers and they are compatible with the utility specific APIs. Therefore, passing of SG services in CC from one CSP to another CSP becomes difficult and takes longer time [33].

- **Compatibility:** CC does not comply any audit requirements. This is the most critical issue that must be overcome by CC for meeting SG auditing compliance requirements. However, CC has many challenges due to location of data, inefficient security policy, etc. Therefore, it is difficult for CC to become compatible with auditing requirements including privacy laws [34].
- **Redundant Data Management and Disaster Recovery:** Recovery in emergency situation is the biggest concern of SG utilities because CC distributes data to multiple servers in different geographical areas. Therefore, enough reliability cannot be provided by CC for SG applications when data in a certain time is not defined. In the current situation, SG utilities know the location of their data and access it eventually when a disaster recovery happens. However, in CC system, CSPs can outsource benefits, services and also recovery processes from other parties and this situation causes a complicated problem when data is not hold by the main CSP [34].

SG utilities that are under pressure have to enhance their practices to deal with high workload. However, very few of these utilities aware of safety critical events despite the SG applications' authentication, accuracy, availability and compatibility requirements. Therefore, it is important for the SG utilities to comprehend their current risks and CC challenges that are listed above while designing and implementing CC on the SG current system. All of these challenges and opportunities that is described in Section 4.1 are shown on the right side and left side respectively in Fig. 4.

5. Analysis of Cloud Computing for Smart Grid applications

This section analyzes the integration of the CC technology with the SG. Based on the findings in the previous sections, this section presents the technical and security analyzes of CC for SG applications, and shows how CC can be used in SG applications meeting the security requirements.

5.1. Technical analysis of CC for SG applications

Three levels of services are offered to SG utilities by CC. Devices and other utilities such as operating system, storage device and database are deployed on a cloud platform and are presented as a SG service according to demand from SG customers. As described in Section 3, all of these CC SG services are divided into three categories as SaaS, IaaS and PaaS, explained as follows:

- **Software as a Service (SaaS):** One to many application delivery to customer is provided by the SaaS model [26]. This means that only the SG customer can access the service that is installed on the utility's hardware via an Internet connection. Customers get permission to access the services by using their software licenses and, therefore, they pay for each service that is used [26]. In this way, only authorized users can access the services through their installed APIs. This provides security, reliability and efficiency to SG systems.
- **Platform as a Service (PaaS):** Service provider provides the development environment if required in this service model. Some of the SG utilities can use this model if they do not want to invest in the environment or when they want to especially focus on the functionality of services. In this way, concentrate applications can be built by SG utilities without considering development environment [33].
- **Infrastructure as a Service (IaaS):** In this model, infrastructure can be offered as a service by CC to SG utilities. CC platforms can share or devote infrastructure to SG utilities who pay for their hardware usage. Computational and storage capabilities are provided by this model with the CC virtualization concept. IaaS can run SG applications that need high performance by handling workloads. Therefore, using this service model can be efficient for SG utilities. IaaS performance can also be increased significantly if SG utilities outsource CC, resources and the infrastructure from other parties [35]. In this way, CSPs become only responsible for its maintenance and repair, and disaster recovery can be handled immediately. Scalability is also one of the advantages of this model that is useful for meeting a SG's huge demand response requirements by easily adding new data storage devices as the demand increases [33].

CC offers different deployment models for the implementation of SG services. There are three cloud deployment models that are public, private and hybrid. SG utilities must select the most appropriate model according to the requirements of their SG services. In this respect, in Table 2, all these models are explained and rated in terms of their usability in SG systems.

- **Public Cloud:** This cloud deployment model is the primary model of CC. In this model, users pay per use of SG services. There is not any limitation about which user can or cannot use cloud service because it is a public cloud. Service providers can make different offers, therefore SG services can be charged or not charged based on the offered conditions. Cloud Provider manages the cloud in the SG and users access the SG through the Internet [36]. All the services in this cloud are standardized to meet comparability requirements of SG applications [37].
- **Private Cloud:** This is an internal deployment model that works like a private network. However, it can differ depending on the SG application's requirements. If a basic private cloud is used in a SG, each SG utility has its own data center and provides services by itself. Thus, high security, reliability and confidentiality are ensured. But, this model prevents other utilities from accessing services and if an interrelationship is required between SG services that are located in different utilities, it is difficult to give access permission to utilities. This problem can be solved in two ways; one of them is by letting an external service provider realize the operation of the

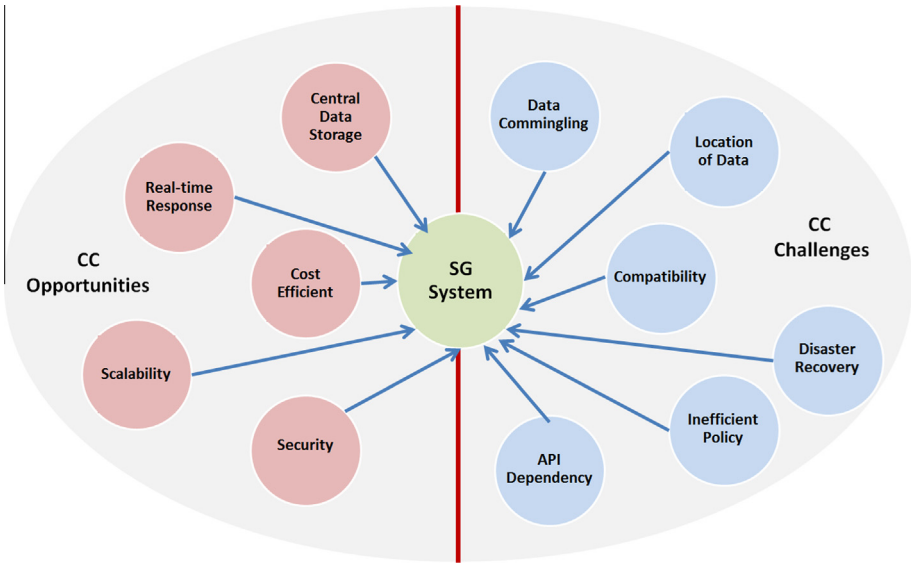


Fig. 4. Opportunities and challenges of Cloud Computing for Smart Grid utilities.

private cloud according to a Service Level Agreement (SLA) without taking data and infrastructure; the second way is to outsource the private cloud by giving all infrastructure and its management to another service provider [36].

- **Hybrid Cloud:** SG utilities that take advantage of CC with a cost efficient way can use the hybrid cloud deployment model. This model combines private and public cloud deployment models for SGs by making a SG utility a cloud provider that holds its own data center and uses a private cloud model. A SG utility processes, analyze and combines data in the private cloud and builds services. Then, all of these services are published to all other utilities by using public clouds [36].

These different deployment models described above are scored according to their usability for SG applications in Table 2. They are analyzed to find the best suitable CC model to use CC with SGs. Assessments show that public cloud offers a good solution for SG utilities which need less complex and high standardized services. A private cloud is also very efficient in terms of security for SG applications, however, it is restrictive for SG utilities due to its internal access limitation feature. Although an external service cloud can perform the cloud operation in a private cloud, it is difficult to integrate all SG utilities with respect to an SLA. Hybrid cloud is another approach for SG utilities as discussed above. It provides benefits for utilities in a SG by combining public and private clouds. This CC deployment model is the best model for SG utilities due to its countrywide scalability feature by giving a dominant role to CSPs.

As illustrated in Fig. 5, multiple services are provided in a SG cloud based on the SaaS service model that is used to charge customers by a monthly fee. The IaaS model is also used for hosting data storage and processing power. The cloud provider provides services by using the PaaS model through its data center that classify data for data storage and processing power. Utilities and customers call the services from the SG cloud and response is sent them via the IaaS model. Inputs such as power consumption data are required to call some services, therefore customers and utilities have to send these inputs to subscribe these services. The data center inside the cloud environment is very modular and established on a virtualized operating system. There are many CPUs in the clusters, and thus the processing time decreases and real time response is achieved. Security is also provided with this hybrid cloud by processing, analyzing and aggregating data in the private cloud and publishing the computed services to utilities and customers through the public cloud.

The state of the art in CC for SG applications is described above where data centers with large computation and storage capacities and the hybrid cloud model are analyzed. Results show that CC presents many advantages that must be considered by SG utilities. SG applications can be implemented with several CC services and deployment models. The main advantages of CC for SG applications are scalability, real time response, cost efficiency and security, which are all the most critical and crucial issues for SG applications.

5.2. Security analysis of CC for SG applications

Power Grid systems are cyber-physical systems which combine the physical electricity infrastructure and the cyber infrastructure. The communication line between the two is however blurred and, as a consequence, operations' control and consumer applications' communication in SG systems have critical vulnerabilities against cyber-attacks. Therefore, some standards must be developed to avoid these attacks for SG applications. However, there is no standard for privacy. Cloud platforms can be used by utilities to provide security and safety for SG applications. Consumers' information such as theirpower usage data is collected by smart meters and this data is sent to operators

Table 2
Assessment of the usability of Cloud Computing deployment models in the Smart Grid.

Smart grid requirements	Public cloud	Private cloud	Hybrid cloud
Low complexity	✓	✗	✗
Cost efficient	✓	✗ ✗	✗
Scalability	✓	✗ ✗	✓ ✓
High security	✗ ✗	✓ ✓	✓ ✓
Compatibility	✗	✗ ✗	✓ ✓
Easy access to services	✓ ✓	✗ ✗	✓
SG usability	✓	✗	✓ ✓

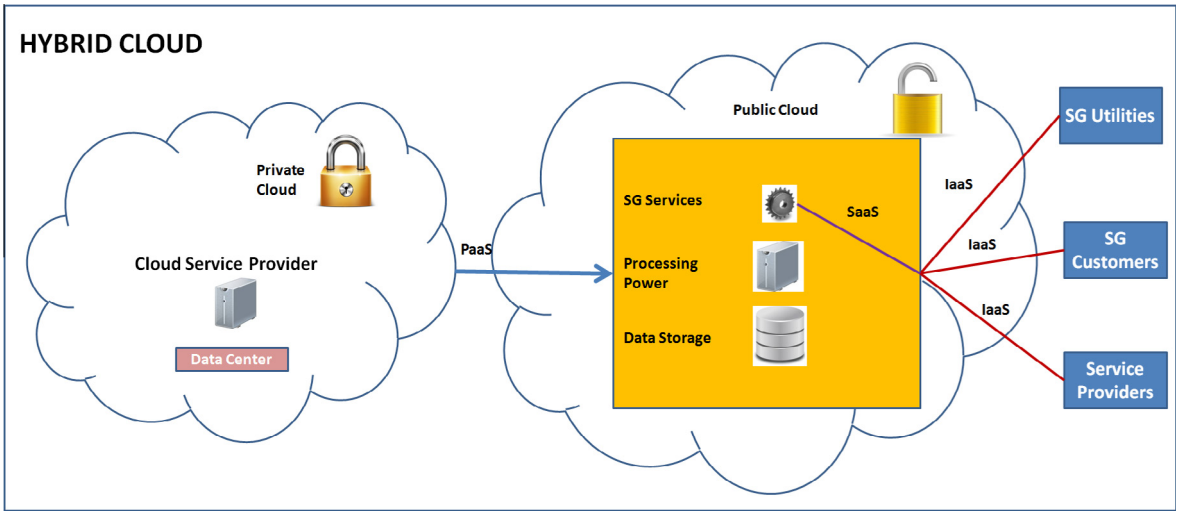


Fig. 5. Cloud Computing hybrid cloud architecture for Smart Grid.

in real time in SG systems. To obtain security and privacy, this data is encrypted with each customer's own key [2]. Data sizes and time constraints change according to the SG application and CC provides secure and reliable transmission control and access to data and utilities. Cloud platforms provide long term data conservation with not only the customer's private consumption data but also with the energy pricing data. A CC platform assures the reliability and security for SG services through the distribution of its data centers globally.

Cloud platforms differ for different applications. Some run on shared platforms while others operate on privileged platforms. Therefore, cloud platforms are severed in three types as public clouds, private clouds and hybrid clouds [38]. Public clouds provide services, running on the same hardware, to their customers. In this cloud type, a cloud fabric is used to separate the data of different organizations. Even though public clouds seem efficient, they are unreliable and not secure because of possible cyber attacks. Therefore, they are not suitable for SG applications. On the other hand, private clouds provide more secure systems for SG applications since a single organization uses a hardware alone. Visualization and storage services are provided by a cloud fabric to monitor data access. Hence, SG applications use private clouds for monitoring and transmitting customer data. The third cloud type, hybrid clouds, can also be preferred by SG systems since advantages of both public and private clouds are enjoyed by hybrid clouds [38]. With stable work load, hybrid clouds work with private clouds for reliability. However, at peak work loads, it switches to operation with public clouds to increase performance. Therefore, in certain cases, hybrid clouds are favored by a SG to meet the customer requirements for high performance or high security [39,40].

Safety management control is provided by especially private Cloud Computing for SG applications. In private clouds, computing is separated from the storage and shared areas of users. The necessity for solving the risks in data access, information management, data insulation and transfer is the main issue for private clouds. Private clouds overcome this issue with the ability of security control in the operating system level. Information security in the SG system is guaranteed through the cloud's authentication and encryption strategy [41]. In this respect, a SG using the private cloud architecture has five layers that facilitate secure SG applications. These layers are identified as the grid application layer, the database and middle-ware layer, the cloud operating system layer, the visualization layer and the data center layer. The data center layer is located at the bottom and it is responsible for data storage. The virtualization layer is the second layer and has the main functionality of protecting against unreliable node faults [41]. The distribution of the data center layer's resources to the database and middleware layer is performed by the cloud operating system layer. The database in the database and middle-ware layer is used for the

storage of data that comes from the application layer. The application layer includes complex applications whose complexity is handled by middle-ware. SG applications, such as fault diagnosis and system monitoring, run on the application layer. The application layer runs these SG applications by sending request to the lower layers and retrieving information from these layers in a secure way. All of these private cloud layers are illustrated in Fig. 6.

Another security approach is to use a protection policy for cloud service based Smart Grid information management [7]. Any SG system can potentially collapse due to node failures. Therefore, quality of service and security for SG systems must be ensured in cloud platforms. To this end, in [7] a protection policy manager (PPM) is proposed. The PPM is located in the SG system and ensures an interface between the SG system and the CC platform. In the CC platform, quality of service, privacy and security are forced by the PPM as SG services. The PPM provides security according to the requirements of SG applications by using three different strategies as described below.

- **Selection of reliable CC service providers [8]:** Provisioning of SG information management requirements are done by the selection of the correct private cloud by the PPM. This results in trustable data storage, transmission and computation.
- **Information and computation ciphering [42]:** PPM encrypts information that is held in CC storage devices for providing data security in the SG domain. PPM also checks whether data is changed during transmission and makes necessary corrections if it is altered. Privacy can be achieved by using a homomorphic encryption scheme which allows for computations over encrypted data [42].
- **Enhancing redundancy of data storage and computation [43,44]:** Virtualization technology is developed by PPM to increase redundancy of the data item. Redundancy is increased by storing different parts of the data item in separate CC service providers and when the redundancy design is made well, the missing parts of a data item can be recovered.

All of the above features of PPM indicate that using CC facilitates robust, reliable and secure transmission in SG applications. Similar to PPM, there are also other approaches that help secure the SG by using the CC technology. These approaches are described as follows.

The data access and privacy issues in SG technologies are studied by the Department of Energy (DOE) and the National Institute of Standards and Technology (NIST) which publishes standards for cryptographic algorithms that must be used by the US government [45–47]. In [45], the key findings are summarized for the data safety, consumer access and confidentiality issues in Smart Grid technologies. These provide a detailed overview to assess the state of existing SG security policies. From these findings, [45] especially focuses on the development of legal and regulatory regimes [45] and the development of proper privacy and security standards, as investigated by the NIST [46,47], to increase the success of security efforts. In [46], the privacy concerns of SG users are dealt with in terms of personal data, personal confidentiality, behavioral confidentiality and personal communications confidentiality. Recommendations such as transparent installation of SG technologies, providing training and awareness programs for employees responsible for SG users' personal information security are included in the NIST guideline to improve the privacy of users in the SG [46]. For a detailed risk analysis, the vulnerabilities of the electric grid technology, which adversely affect the operation of the SG, are listed in [47]. These vulnerabilities are categorized in five classes such as people related vulnerabilities, policy and procedure vulnerabilities, platform software/firmware vulnerabilities, platform vulnerabilities and network vulnerabilities. The guidelines by the NIST [46,47] and DoE [45] provide consistent security mechanism for the SG technology.

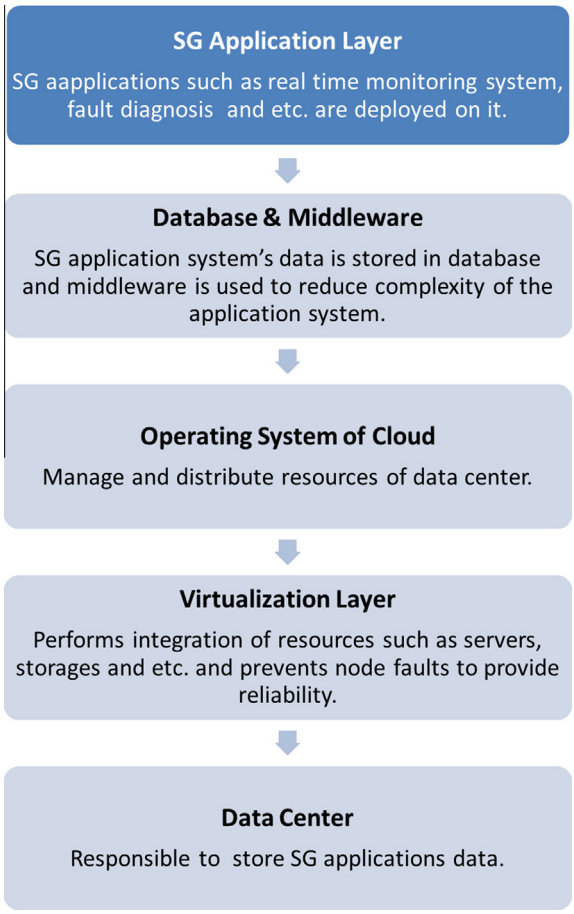


Fig. 6. Smart Grid private cloud layers.

Another SG security approach includes using a public key infrastructure (PKI) and techniques as proposed by [48]. In this study, an integrated solution including PKI technologies, which are certificate life-cycle management tools, reliance anchor security and attribute certificates, and trusted computing elements has been implemented to provide the highest level of security for Smart Grids. The aim of using trusted computing elements is to form a

secure environment for complex Cloud Computing and Internet applications which need extensive deployment of mobile code such as Flash, PDF, and Java. To this end, in [48], a remedy is proposed with standards that are exposed, adhered and signed by operators and suppliers. All the critical components of a Smart Grid must be covered by these standards to construct a trust management framework. In this way, secure and more reliable environments can be realized for a Smart Grid.

Integrated Security System (ISS) is proposed by [49] for protection of the Smart Grid against cyber attacks. ISS includes three components including manager module, switch & agent module and assessed module. All of these modules help increase the security of the SG control system architecture and legacy control devices by securing the Supervisory Control and Data Acquisition (SCADA) system. The layered structure of ISS prevents intruders and offers scalable, expandable and inter-operable solutions for grid security [49].

In [50], a privacy preserving protocol, based on secure multi-party computation (SMC), is proposed for real-time demand management. Using the SMC computation framework for secure communication between multiple parties via a secured protocol including homomorphic encryption, the proposed architecture meets the smart meter requirements such as the protection of the end user's personal data, load management, providing a sustainable billing method and removing the need of third party applications for security. In this method, computations can be performed on encrypted data and thus privacy of data is conserved.

Other studies focus on issues related to the privacy of collected smart metering data by using basic cryptographic techniques [51]. They present protocols to aggregate smart meter measurements [52], and construct authentication mechanisms to define anonymous smart meter readers [53]. All of these techniques are designed for addressing the security and privacy challenges in the Smart Grid such as consumer fraud and malicious hackers [54].

6. Cloud Computing based Smart Grid projects and applications

Electric power systems consist of three subsystems that are power generation, power delivery and power utilization. In recent years, CC has been known as a hope-inspiring technology that strengthens all these SG subsystems and therefore, it becomes a crucial component for SG applications. Within this context, many CC based SG projects including Globus [59], EGI-InSPIRE (Integrated Sustainable Pan-Europe an Infrastructure for Researchers in Europe) [60], Information Power Grid from NASA [61], OpenNebula [62] and TClouds [63] have been implemented and they are summarized in Table 4. Additionally, existing SG applications run on cloud platforms are presented in this section to demonstrate the effectiveness and trustworthiness of applying CC in SG. Concordantly, CC architecture for each application varies depending on the SG application requirements, so other technologies, such as cognitive radio, MapReduce, and Hadoop, are also evaluated in some of the CC based SG applications.

6.1. Generation scheduling with demand response optimization

Real-time consumer power usage tracking is done by power utilities with smart meters [8]. But, after retrieving, analyzing and processing millions of consumer data, transforming them to significant decisions are so much difficult and hard to manage for SG meters. Therefore, different kinds of solutions such as information and software system techniques, which include pattern mining, machine learning, semantic information, distributed stream processing and CC platforms, are used to reduce complexity of the SG events, to give rapid response to customers and to provide scalable and reliable communication environment. This solution is applied in Los Angeles Smart Grid Demonstration Project that has been already finished and used in city [8]. The goal of this project is that optimizing the power consumption with managing huge amount of data and demand upward by combining stream processing, semantic complex event processing and CC platforms with SG systems. In this respect, they propose a system architecture model that is shown in Fig. 7 to achieve SG demand response optimization [8]. This model has two layers as shown in Fig. 7. The top layer performs demand response tasks including in order retrieving real time smart meter information, detecting abnormalities in a short period of time for decreasing latency to give critical response, enriching smart meter data by using semantic information, updating demand forecast according to latest coming information and giving targeted response when peak load happens by communicating with customers, and the second layer of the model includes technologies that are used to realize these tasks. All these technologies inside the second layer are explained below:

- **Scalable stream processing:** retrieves SG meter readings streaming via communication protocols and when emergency situation occurs, detects it and gives rapid response.
- **Semantic information integration:** combines information that is taken from online services with AMI data.
- **Data mining and complex event processing:** uses some models to estimate a mismatch in supplier and demand sites.
- **Machine learning:** finds the most efficient technique for load cutting according to customer response.
- **Natural language processing:** translates a chosen response into a workable form for sending it to a customer.
- **Cloud infrastructure:** all tools that are mentioned above run on cloud platforms that share information by using Web services with respect to data privacy rules.

6.2. Cloud based smart meter

Bidirectional communications is one of the important features of the SG. This provides to control devices and their operations with smart meters that collect information from SG users' devices and check their status. However, if a new application needs to be added on this SG

application, the whole system must be reconstructed [64]. This can be avoided by using the cloud smart meter framework [7]. System architecture of this framework is shown in Fig. 8 [7]. As shown in Fig. 8, all the SG services that perform an advanced metering application are placed into the smart meter application cloud. These services are developed, maintained and updated by the utilities inside this cloud. A smart meter accesses these services through a public interface and controls the devices with respect to coming response from the cloud. For instance, a smart application cloud includes a smart heater control service that learns the heat balance to equalize billing and warming. A smart meter requests this service and controls the heat according to coming information. If the service provider updates this service such as changing the heat balance, the smart meter does not need to know this change, it does the same thing with respect to a service response. This framework provides efficient solutions with these features for the SG Advanced Metering Infrastructure (AMI) with the ability of scalability, dependency and reliability because all appliances requests are met from one and shared cloud platform.

6.3. Cloud based Machine to Machine (M2M) communications applications for SG systems

Communication technology is provided by M2M communications for ensuring communication between systems and devices without needing humans. Therefore, many SG applications use M2M technology for smart meters and its energy management systems to interchange information. CC is combined with M2M communications because of its low cost, efficiency and high performance. In this respect, a SG's energy management system is supported by M2M with CC. In [55], intelligent cloud based energy management system (iCEMS) is proposed. iCEMS general system architecture, shown in Fig. 9, consists of three layers: consumer, iCEMS middleware and physical resources. iCEMS middleware and physical resources are located inside the cloud platform to utilize cloud CC methods. In this respect, iCEMS provides four main benefits to SG systems by using these CC features. The first one is the management of local renewable energy. Integration of renewable energy with existing SG is difficult, therefore load demand management cannot be done efficiently. iCEMS solves this problem with dynamic load demand management that is performed by its load demand manager. The load demand manager includes a demand forecasting engine and a battery monitor inside the iCEMS middleware [55]. Thus, continuous power can be supplied for users. The second feature is balancing energy for processing and storage by selecting suitable energy sources with respect to SG service requirements. Therefore, iCEMS uses CC platform to increase energy efficiency by clustering resources efficiently. iCEMS performs CC task with a cloud manager that is located inside the middleware for collecting consumer requirements, measuring energy consumption of resources, providing security and managing resources. The third property of iCEMS is that it increases the energy efficiency by decreasing monitoring, processing and communication operations of M2M devices. That is achieved by using power monitoring and environment monitoring sensors as shown in Fig. 9. These sensors always send information about consumed power, device profile, and environment and user profiles, periodically. According to these information, the knowledge repository that is located in iCEMS middleware is updated and the situation based adaptive resource allocation information is sent by iCEMS to improve energy efficiency [55]. The fourth feature of iCEMS is that it provides user friendly energy management services for increasing energy efficiency with user interaction [55]. This offers user specific information, location and situation dependent energy management services to customers [55].

6.4. Cyber Physical System (CPS) for SG

Cyber Physical System (CPS) is a CC application for the power grid. The integration of computing power, communication capability and self governing control ability is done by CPS [56]. SG monitoring applications need to control the environment in real time and CPS facilitates this by controlling situations of information, processes, transmissions and environment in real time. CPS also provides SG security with Microgrid that is combined to SG system and is called as Microgrid CPS framework. The system

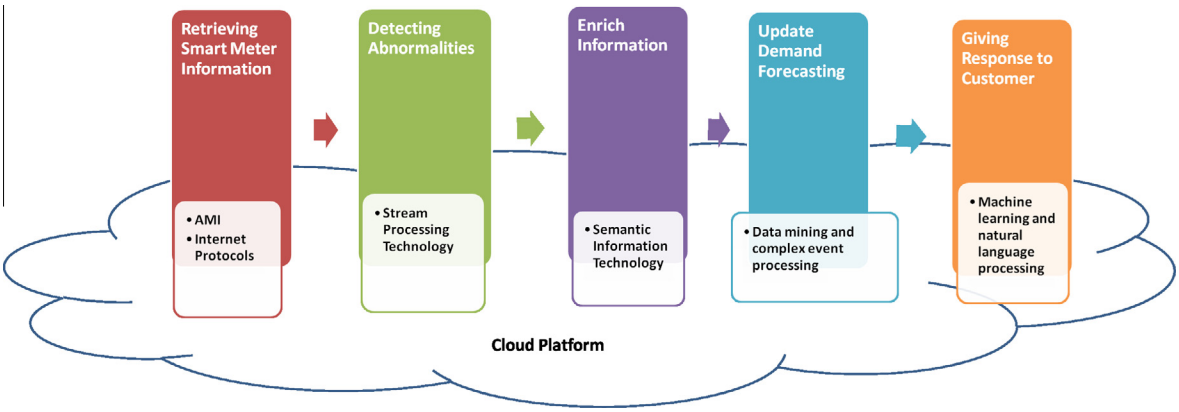


Fig. 7. System architecture model of demand response optimization [8].

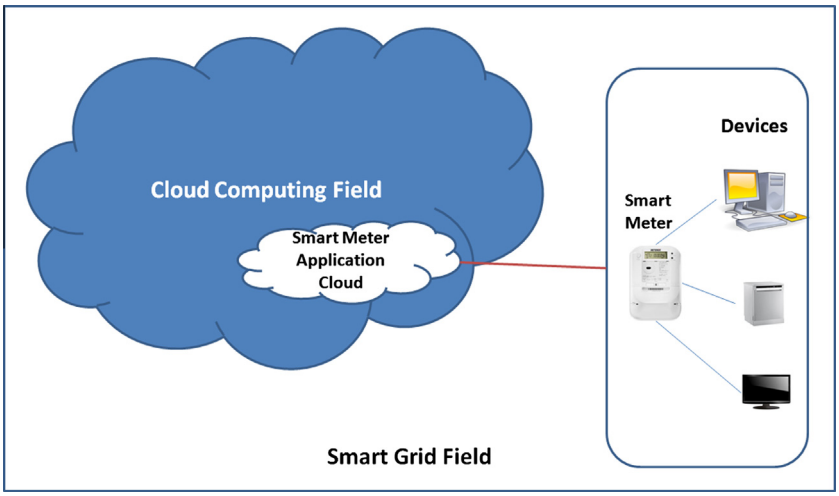


Fig. 8. System architecture of Cloud Smart meter framework [7].

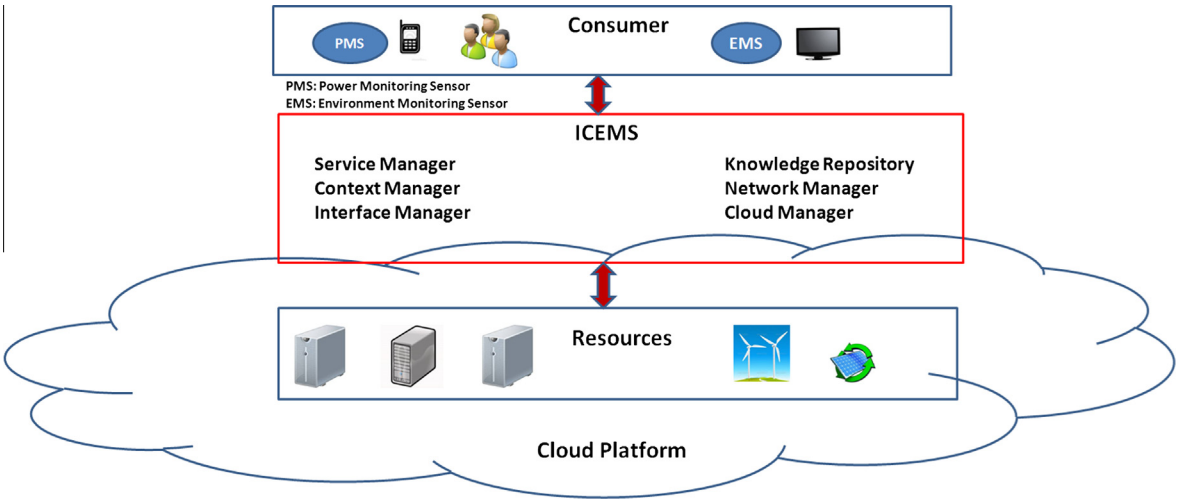


Fig. 9. System architecture of iCEMS [55].

architecture of this framework is shown in Fig. 10. Both the information and power networks are controlled by this Microgrid CPS in SG applications using physical and information processing equipments such as distributed power supply devices, sensors and servers. All power equipments are connected with each other via transmission lines. As shown in Fig. 10, CPS forms a local area network for the SG communication network and connects with the SG network via a CPS router. In this system, the distribution network combines all data that are retrieved from the CPS environment. This information is analyzed and processed in real-time. User information is also checked by the distribution network to legitimate the user. Power distribution, control system, energy storage and load are also all included in this CPS local area network and in CPS architecture these loads are balanced with respect to three cases. These are adjustable load, interruptible load and sensitive load. Microgrid performs all of these load adjustments by interacting with the CPS local area network to retrieve information about the network and gives response to users' demand according to data analysis via an actuator node [56].

6.5. SG condition monitoring with CC platforms

SG systems process large amount of data including real time information, operating data, test data, etc., and the size of this data increases every day. Therefore, SG condition monitoring becomes more difficult in terms of reliability and security. In this manner, [10] proposes the system architecture, shown in Fig. 11, for cloud platforms that hold status information of a SG. This technology provides efficient and real time SG condition monitoring with big data. [10] combines different kinds of technologies to ensure high performance, efficient and robust SG condition monitoring systems. Hadoop is one of the used technologies to

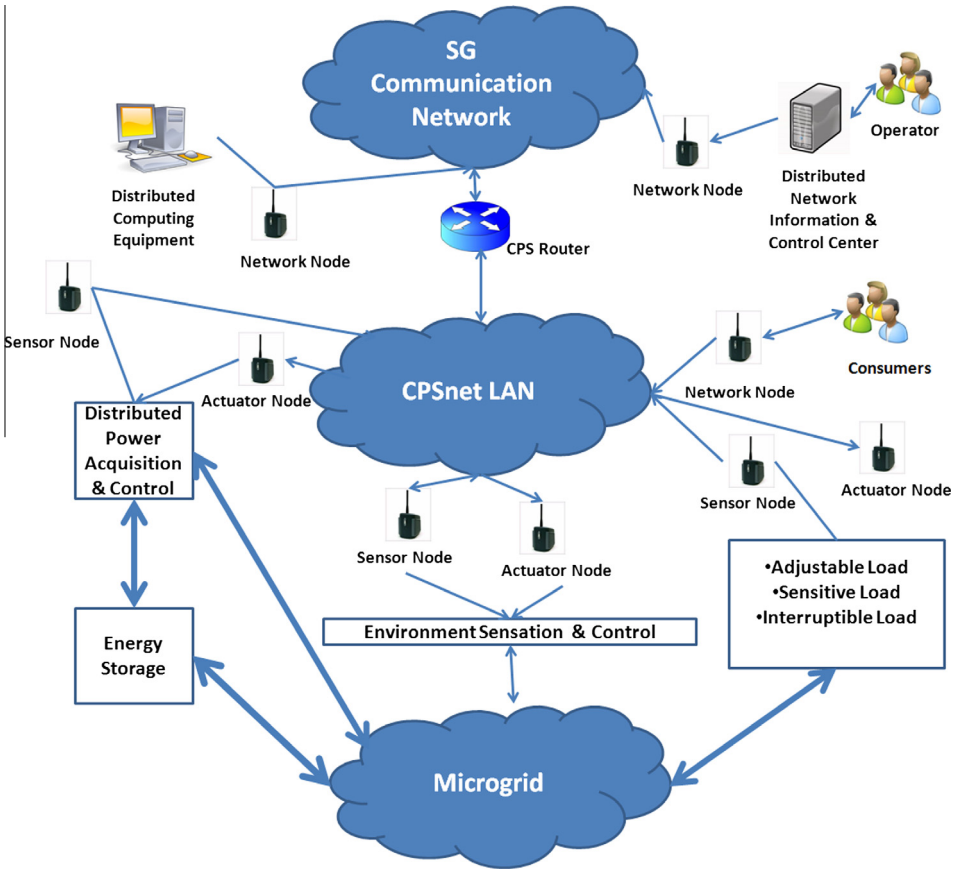


Fig. 10. System architecture of CPS in Smart Grid [56].

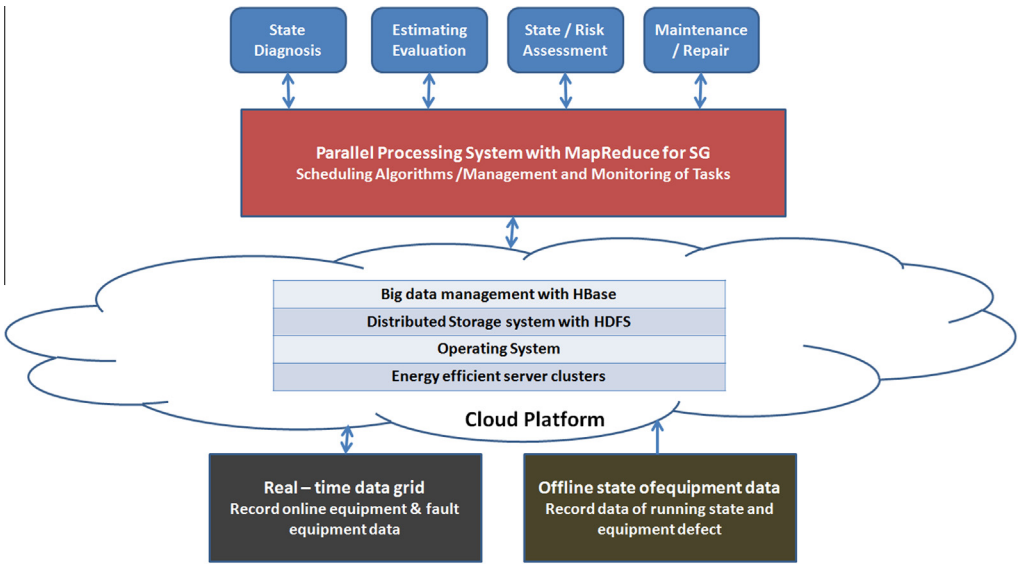


Fig. 11. System architecture of Cloud Computing platform for Smart Grid condition monitoring [10].

increase the productivity by running idle servers. In this way, hardware utilization increases and equipment cost decreases because of the reduced number of the required devices. Another technology that is used for SG condition monitoring is the Hadoop Distributed File System (HDFS) that is located inside the cloud platform as shown in

Fig. 11. The HDFS is preferred because it is fault tolerant and its deployment is realized by using low cost hardware. SG applications that have large data sets and need high throughput access can use the HDFS for efficiency [65]. The third technology that is used for [10]'s SG condition monitoring tool is HBase that is a fault tolerant relational database and used for dealing with big tables [66]. Therefore, [10] uses HBase to deal with large data sets retrieved from SG applications. MapReduce, another tool provided by Hadoop, is used in the proposed architecture for parallel processing across huge datasets. It achieves high performance with the ability of fault diagnosis and channel condition monitoring by retrieving data from the online data grid and the offline state of the equipment data grid, as shown in Fig. 11, and spreads the operations across the channels [25]. As a result, the CC based SG condition monitoring tool provides high performance with MapReduce, more security with the HDFS's fault detection feature and more storage with HBase. Integration of these technologies offers resistant solutions with fault diagnosis to CC based SG applications, as summarized in Table 3. Hence, it is preferable for a SG to a cloud platform to increase its performance, reliability and efficiency [10].

6.6. Dynamic Internet Data Centers (IDCs) operations with SG and CC

In this application Internet Data Centers (IDCs), that are the parts of a CC platform for computing many operations with big data, are used for minimizing electricity cost in the Smart Grid environment [57]. Electricity price in a Smart Grid changes according to demand response, and when demand increases, the cost also increases. Therefore, dynamic workload becomes an important subject for both clients and power suppliers. In this respect, Wang et al. [57] proposes a model for minimizing the electricity cost by using dynamic power supply. Their proposed method is based on two operations. One of these operations is to achieve electricity cost minimization in the SG environment with IDC operators that manage dynamic workload by becoming price maker instead of being price taker in the proposed system. The second operation is by designing and using an algorithm, called Corrected Marginal Cost (CMC), for solving the optimization problem to procure marginal cost by distributing workload between IDCs.

Wang et al. [57] firstly formulates the energy cost minimization problem by deploying IDCs that are inside the separate electricity market regions and front-end Web portals to retrieve user requests. In this respect, when requests of clients are captured by Web portals, it sends them to a IDC for processing. Electric cost of all these IDCs are tried to be minimized by estimating each IDC machines workload that is assigned by front-end Web portal server. In second phase, marginal cost of each IDCs are computed according to proposed algorithm of CMC. This algorithm computes the marginal cost by comparing each IDCs cost. However, marginal cost shows that total cost always changes due to demand change in electricity usage. Therefore, CMC algorithm decreases the power consumption of IDC that has big marginal cost and increases the power consumption of IDC that has low marginal cost. In this way, total cost decreases and electricity cost minimization is achieved with handling interaction between SG and IDCs, adaptively [57]. However, dynamic workload and variable electric prices cause instabilities in IDCs. Therefore, Rao et al. [67] propose a scheme and model to minimize the operation risk and design the most suitable algorithm to provide quality of service against irregular electricity market and overcome uncertainties of IDCs under SG environment.

Rao et al. [67] firstly study with a single IDC location to handle instabilities. They propose electricity cost and risk minimization formulas with a new metric unit to measure the electricity cost. In the second phase, they study the use

Table 3
Cloud Computing service-based Smart Grid applications.

CC based SG applications	Benefit feature for SG by CC
Generation scheduling with demand response optimization [8]	Visualized resource pool to store all data in one place
Cloud based Smart Meter [7]	Easy integration of new applications to Smart Meter
iCEMS [55]	Providing efficiency, high performance with using renewable resources for SG
CPS for SG [56]	Offer Load balancing and increase security
SG Condition Monitoring with CC Platforms [10]	Used of Hadoop, HDFS, HBase, MapReduce to enhance SG performance
Dynamic Internet Data Centers Operations with SG and CC [57]	Reduce electricity price with dynamic workload by using IDCs and CMC algorithm
NET-AMI with the Integration of Cognitive Radio and CC [58]	Providing cost-efficient platform for AMI meters by using CC energy services and cognitive radio services

Table 4
Cloud Computing for Smart Grid projects.

SG and CC Projects	Domain	Mission
Globus [59]	SG	Resolving distributed resource sharing with a one source framework
EGI-InSPIRE [60]	SG	Constitution of European Grid Infrastructure (EGI) for Distributed Computing Infrastructure (DCI)
Information Power Grid from NASA [61]	SG	High Performance Computing, Data Management in Large-Scale
OpenNebula [62]	CC	CC management with developing scalable, highly adaptable software
TClouds [63]	CC	Constructing cloud platforms with the ability of low cost, reliable and scalable for providing secure and resilient operations

of distributed IDC locations. Energy usage problem of IDCs are tried to be solved by modeling risk minimization problem and with an hedging algorithm. A hedging algorithm provides the certainty by solving the deregulation problem that is the variation of electricity price change at each time at different IDC locations. [67] formulates this deregulation of IDC locations at time t with a vector and provides hedging with buying electricity from power market before electricity price fluctuations and dynamic workload happen to minimize operation risk. However, an IDC operator needs to know how much electricity to buy which is decided with an optimal hedging algorithm. Proposed hedging algorithm figures the amount of electricity to buy for each IDC location by specifying the time interval that is used to determine for how long the electricity is bought. These are defined with the hedging algorithm which computes the variance and covariance of price and load for each IDC location and in the end calculates electricity cost of each IDC. As a result, Rao et al. [67] test their systems' suitability by using real work loads and by retrieving real energy price fluctuations. According to test results, Rao et al.'s [67] recommended scheme becomes successful to reduce IDCs operations' risks by solving instabilities of electricity price. This solves SG applications' problems that mostly occur due to surging power usage.

6.7. NET-AMI with the integration of cognitive radio and CC

Netbook advance metering infrastructure (NET-AMI) is one of the applications which uses a Cloud Computing data center to provide central communication and optimize the network infrastructure. Cost efficient platform is provided for AMI meters by Net-AMI with wireless transceiver that is used to access cloud data center's energy services, cognitive radio services and wireless communication services through cognitive radio channels [58]. This low cost platform is achieved by Net-AMI by reutilizing the cell towers and using low frequency bands. In this way, deployment of Net-AMI becomes easy and speedy while it performs communication with the metropolitan wide network. It also provides communication based on universal wireless standards and protocols and is attenuated to oncoming standards by improving software. In addition, Net-AMI proposes a persistent communication against power line failures during power information transmission between utilities and hosts. All of these features of NET-AMI are performed with an efficient wireless cloud data center system architecture that enables communication between utilities and NET-AMI via cognitive radio transmission.

Fig. 12 shows the procedure about how NET-AMI performs communication between a utility and the Home Area Network (HAN). In this infrastructure, instead of registering NET-AMI to a Wireless Service Provider, wireless transmission between NET-AMI and the utility is enabled by adopting a new universal interface style. Wireless connectivity between utility and NET-AMI is supplied by Cognitive radio through deployment of cognitive radio antenna and cellular provider antenna on the base transceiver station on both the utility and NET-AMI sites. This reduces the infrastructure cost and path loss because existing base transceiver stations are used and the height of cognitive radio antenna, that is important to make reliable communication, remains same [58]. Communication between utilities, NET-AMI and cloud data center is

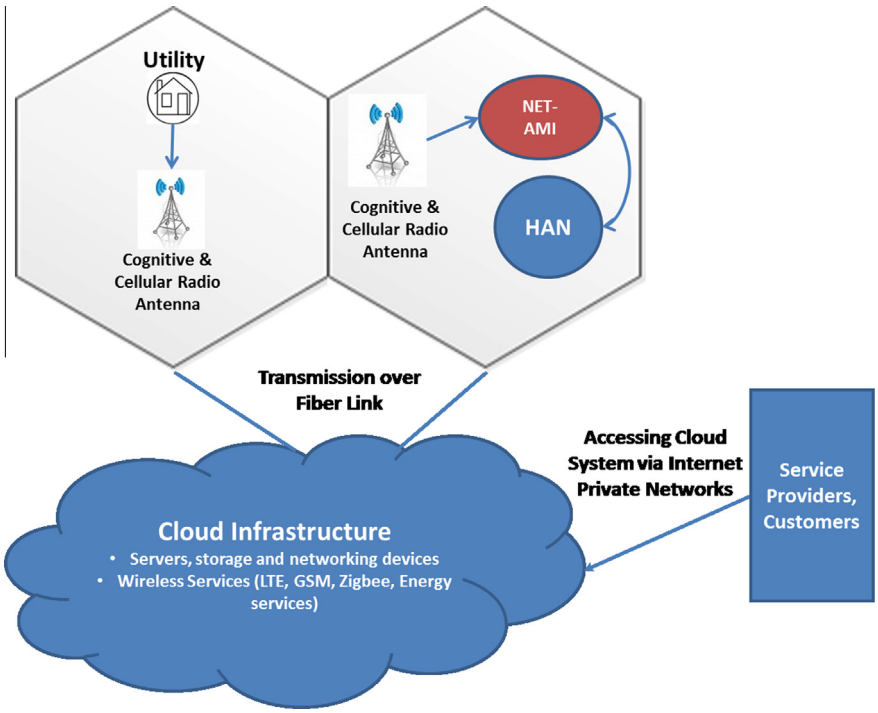


Fig. 12. NET-AMI cloud data center system architecture with cognitive radio transmission feature [58].

performed by cognitive radio that senses the spectrum in the cell and finds unused bands. The cognitive radio's sensed information is sent to cloud data center through fiber, and cloud data center opens all services, i.e. cognitive radio service, waveform service, protocols service, security service, microgrid information packet and air-interface service and microgrid energy optimization service [58]. These services are used by the cloud data center to prepare and send response to NET-AMI by accessing cognitive radio antenna through radio over fiber. NET-AMI realizes some tasks such as getting information from HAN according to coming request and sending response to cloud data center with cognitive radio antenna through radio over fiber. Cloud data center analyzes this coming data from NET-AMI and prepares a control signal to send NET-AMI in order to use control devices in HAN [58].

7. Open research issues in CC for SGs

Many projects and applications exist for the purpose of using CC to service the information management in the SG. However, there are still some open research issues that must be solved to realize this aim. These open research issues are listed below.

- **Security Framework for SG Applications:** Security is a major issue for electric companies. If the data in the cloud is compromised, cloud companies can suffer from this situation. This risk increases when hackers obtrude into the internal system. How to provide security against these hackers is a challenging question for cloud services. Therefore, a security framework based on the SG authentication is needed to improve security when CC is applied for SG applications. This authentication mechanism can work by blocking non-authorized devices. Device blocking can be achieved with cloud platforms, and thus only SG users can use the SG applications and others cannot access these applications. This can improve a SG's performance and reliability. This framework can also increase security when data located in the private cloud is moved to the public storage space with authorization control for the stored data and separate access levels assigned to each user and software agent [36].
- **Increasing Robustness:** There is a huge amount of data and information flow between SG utilities. Therefore, when failures occur in these utilities, the network connectivity is lost and, as a result, all data and analysis centers fail in their operations. If such a disaster occurs, the cloud provider needs to have an efficient recovery mechanism to restore all the data. Robustness of cloud platforms must also be increased for critical SG applications that need to share information trustfully in real-time and large scale. This can be achieved by using an advanced distributed communication framework which traces state of the SG network [36].
- **Defining Communication Protocols and a Model for Network Utilization:** The coupling between the energy components and the CC system must be provided. There are massive amount of objects and all of them need synergy between each other. However, in the current system it cannot be provided with the traditional methods. Therefore, protocols should be defined to provide interpretability between cloud platform and SG systems. In this way, CC service providers and users can efficiently work with each other. In addition, network utilization must be also increased with a model that provides only the subscribers, who needed, can access the SG services and remaining of them are blocked to access.
- **Economic Data Centers and Large Scale Cloud Platforms:** Large amount of electric power is consumed by cloud data centers. Cloud platforms are important to support many SG applications. Therefore, energy efficient cloud platforms must be designed to reduce power consumption for SG applications and carbon emission for the environment. This can be achieved by strengthening cloud virtual machines according to the utilization of resources. In this respect, a CC model must be constructed to strength these virtual machines by reallocating them dynamically to a new place where energy is cheaper according to the required CPU performances of SG applications. Global cloud platforms must be also built to increase SG applications scale in market. This cost efficient model must also increase scalability and improve resource utilization by eliminating redundancies and by adjusting resource usage according to SG applications' requirements.
- **Timely Demand Response:** The requirements of SG applications for timely demand response must be met with cloud platforms. SG applications need optimized and adaptive/real time demand response management. Therefore, cloud platforms require a scheduling mechanism and a distributed infrastructure to increase communication speed and to provision time critical SG applications. This can be achieved by distributing Cloud virtual machines to locations where there is high demand.
- **Efficient Streaming with Clouds:** Stream operations are needed for SG audio and video applications using CC. There is a heterogenous network in the SG domain and efficient streaming must be supported in this environment. For this reason, private and public clouds need stream processing for data integration. A dynamically adjustable multimedia streaming (DAMS) algorithm, which adjusts encoding method dynamically for multimedia applications with respect to bandwidth availability and power [68], can be applied inside cloud platforms for decreasing load and reducing power consumption.

These are the open research issues for cloud platforms. All these issues raised should be addressed to realize more efficient and reliable SG applications.

8. Conclusion

In this paper, the SG and CC architectures, and related works on SG applications with cloud platforms are reviewed. Opportunities and challenges of cloud platforms for SG applications are described. Cloud platforms are analyzed from technical and security perspectives, and their

compatibility with SG systems is investigated. Cloud service based SG applications and projects are presented to make the case for the suitability of CC for SG applications. Finally, some open research issues are described.

Acknowledgement

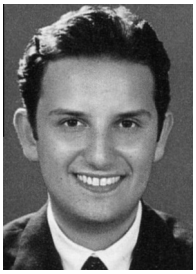
The work of V.C. Gungor has been supported by Abdullah Gul University Foundation.

References

[1] V. Gungor, B. Lu, G. Hancke, Opportunities and challenges of wireless sensor networks in smart grid, IEEE Trans. Ind. Electron. 57 (2010) 3557–3564.
[2] Y. Simmhan, A. Kumbhare, B. Cao, V. Prasanna, An analysis of security and privacy issues in smart grid software architectures on clouds, in: IEEE International Conference on Cloud Computing, IEEE, 2011, pp. 582–589.
[3] W. Wang, A. Rashid, H. Chuang, Toward the trend of cloud computing, J. Electron. Comm. Res. 12 (2011).
[4] A. Beloglazov, J. Abawajy, R. Buyya, Energy-aware resource allocation heuristics for efficient management of data centers for cloud computing, Future Gener. Comput. Syst. 28 (2012) 755–768.
[5] V. Chang, G. Wills, R. Walters, W. Currie, Towards a Structured Cloud roi: The University of Southampton Cost-Saving and User Satisfaction Case Studies, 2012.
[6] K. Birman, L. Ganesh, R. Renesse, Running smart grid control software on cloud computing architectures, in: Workshop on Computational Needs for the Next Generation Electric Grid, Ithaca, New York.
[7] X. Fang, S. Misra, G. Xue, D. Yang, Managing smart grid information in the cloud: opportunities, model, and applications, IEEE Network 26 (2012) 32–38.
[8] Y. Simmhan, S. Aman, B. Cao, M. Giakkoupis, A. Kumbhare, Q. Zhou, D. Paul, C. Fern, A. Sharma, V. Prasanna, An informatics approach to demand response optimization in smart grids, Natural Gas 31 (2011) 60.
[9] S. Rusitschka, K. Eger, C. Gerdes, Smart grid data cloud: a model for utilizing cloud computing in the smart grid domain, in: First IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2010, pp. 483–488.
[10] H. Bai, Z. Ma, Y. Zhu, The application of cloud computing in smart grid status monitoring, Internet Things (2012) 460–465.
[11] H. Kim, Y. Kim, K. Yang, M. Thottan, Cloud-based demand response for smart grid: architecture and distributed algorithms, in: IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2011, pp. 398–403.
[12] A. Mohsenian-Rad, A. Leon-Garcia, Coordination of cloud computing and smart power grids, in: First IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2010, pp. 368–372.
[13] S. Fayyaz, M. Nazir, Handling security issues for smart grid applications using cloud computing framework, J. Emerging Trends Comput. Inf. Sci. 3 (2012).
[14] C. Alcaraz, J. Lopez, Addressing situational awareness in critical domains of a smart grid, Network Syst. Secur. (2012) 58–71.
[15] M. Hohm, Microsoft hohm Fact Sheet, 2009. Microsoft Corp. <http://www.microsoft-hohm.com>.
[16] Google.org, Google PowerMeter – Save Energy. Save Money. Make a Difference, 2011. <http://www.google.com/powermeter/about/>.
[17] V. Bernardo, M. Curado, T. Staub, T. Braun, Towards energy consumption measurement in a cloud computing wireless testbed, in: First International Symposium on Network Cloud Computing and Applications (NCCA), IEEE, 2011, pp. 91–98.
[18] M. Bjelica, B. Mrazovac, V. Vojnovic, I. Papp, Gateway device for energy-saving cloud-enabled smart homes, in: Proceedings of the 35th International Convention MIPRO, IEEE, 2012, pp. 865–868.
[19] I. Hong, J. Byun, S. Park, Cloud computing-based building energy management system with zigbee sensor network, in: Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), IEEE, 2012, pp. 547–551.
[20] J. Popeang, Cloud computing and smart grids, ERP E-Business Appl. Deployment Open Source Distrib. Cloud Syst. III (2012) 57–66.
[21] D. Von Dollen, Report to nist on the smart grid interoperability standards roadmap, in: Prepared by the Electric Power Research Institute for NIST (June 2009), 2009.
[22] B. Ugale, P. Soni, T. Pema, A. Patil, Role of cloud computing for smart grid of india and its cyber security, in: Nirma University International Conference on Engineering (NUiCONE), IEEE, 2011, pp. 1–5.
[23] L. Zheng, S. Chen, Y. Hu, J. He, Applications of cloud computing in the smart grid, in: 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), IEEE, 2011, pp. 203–206.
[24] E. Brynjolfsson, P. Hofmann, J. Jordan, Cloud computing and electricity: beyond the utility model, Commun. ACM 53 (2010) 32–34.
[25] D. Wang, Y. Song, Y. Zhu, Information platform of smart grid based on cloud computing, Dianli Xitong Zidonghua(Automation of Electric Power Systems) 34 (2010) 7–12.
[26] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., A view of cloud computing, Commun. ACM 53 (2010) 50–58.
[27] K. Birman, D. Freedman, Q. Huang, P. Dowell, Overcoming cap with consistent soft-state replication, Computer 45 (2012) 50–58.
[28] Q. Zhang, L. Cheng, R. Boutaba, Cloud computing state of the art and research challenges, J. Internet Serv. Appl. 1 (2010) 7–18.
[29] P. Mell, T. Grance, The nist definition of cloud computing draft, NIST Spec. Pub. 800 (2011) 145.
[30] R.M. Ward, R. Schmieder, G. Highnam, D. Mittelman, Big data challenges and opportunities in high-throughput sequencing, Syst Biomed. 1 (2013) 0–1.
[31] A. Iosup, S. Ostermann, M. Yigitbasi, R. Prodan, T. Fahringer, D. Epema, Performance analysis of cloud computing services for many tasks scientific computing, IEEE Trans. Parallel Distrib. Syst. 22 (2011) 931–945.
[32] M. Jensen, J. Schwenk, N. Gruschka, L. Iacono, On technical security issues in cloud computing, in: IEEE International Conference on Cloud Computing, CLOUD'09, IEEE, 2009, pp. 109–116.
[33] W. Deng, F. Liu, H. Jin, B. Li, D. Li, Harnessing renewable energy in cloud datacenters: opportunities and challenges, IEEE Network Mag. (2013).
[34] N. Hasan, M.R. Ahmed, Cloud computing: opportunities and challenges, J. Modern Sci. Technol. 1 (2013).
[35] H.R. Motahari-Nezhad, B. Stephenson, S. Singhal, Outsourcing business to cloud computing services: opportunities and challenges, IEEE Internet Comput. Palo Alto 10 (2009).
[36] D.S. Markovic, D. Zivkovic, I. Branovic, R. Popovic, D. Cvetkovic, Smart power grid and cloud computing, Renew. Sust. Energy Rev. 24 (2013) 566–577.
[37] A. Ojala, V. Puhakka, Opportunity discovery and creation in cloud computing, in: 46th Hawaii International Conference on System Sciences (HICSS), IEEE, 2013, pp. 4296–4305.
[38] F. Luo, Z. Dong, Y. Chen, Y. Xu, K. Meng, K. Wong, Hybrid cloud computing platform: the next generation it backbone for smart grid, in: IEEE Power and Energy Society General Meeting, IEEE, 2012, pp. 1–7.
[39] R. Buyya, C. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging it platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Gener. Comput. Syst. 25 (2009) 599–616.
[40] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, D. Zagorodnov, The eucalyptus open-source cloud-computing system, in: 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, CCGRID'09, IEEE, 2009, pp. 124–131.
[41] L. Zheng, Y. Hu, C. Yang, Design and research on private cloud computing architecture to support smart grid, International Conference on Intelligent Human–Machine Systems and Cybernetics (IHMSC), vol. 2, IEEE, 2011, pp. 159–161.
[42] C. Wang, K. Ren, J. Wang, Secure and practical outsourcing of linear programming in cloud computing, in: Proceedings IEEE INFOCOM, IEEE, 2011, pp. 820–828.
[43] R. Basmadjian, H. De Meer, R. Lent, G. Giuliani, Cloud computing and its interest in saving energy: the use case of a private cloud, J. Cloud Comput.: Adv. Syst. Appl. 1 (2012) 5.
[44] I. Egwutuoha, S. Chen, D. Levy, B. Selic, A fault tolerance framework for high performance computing in cloud, in: 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), IEEE, 2012, pp. 709–710.
[45] Data Access and Privacy Issues Related to Smart Grid Technologies, 2010. <http://energy.gov/gc/downloads/department-energy-data-access-and-privacy-issues-related-smart-grid-technologies>.

[46] NISTR 7628 Guidelines for Smart Grid Cyber Security, Privacy and the Smart Grid, vol. 2, 2010. <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf>.
[47] NISTR 7628 Guidelines for Smart Grid Cyber Security, Supportive Analyses and References, vol. 3, 2010. <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf>.
[48] A.R. Metke, R.L. Ekl, Security technology for smart grid networks, IEEE Trans. Smart Grid 1 (2010) 99–107.
[49] D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, An integrated security system of protecting smart grid against cyber attacks, in: Innovative Smart Grid Technologies (ISGT), IEEE, 2010, pp. 1–7.
[50] A. Rial, G. Danezis, Privacy-preserving smart metering, in: Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, ACM, pp. 49–60.
[51] F.D. Garcia, B. Jacobs, Privacy-friendly energy-metering via homomorphic encryption, in: Security and Trust Management, Springer, 2011, pp. 226–238.
[52] K. Kursawe, G. Danezis, M. Kohlweiss, Privacy-friendly aggregation for the smart-grid, in: Privacy Enhancing Technologies, Springer, pp. 175–191.
[53] C. Efthymiou, G. Kalogridis, Smart grid privacy via anonymization of smart metering data, in: First IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2010, pp. 238–243.
[54] H. Lam, G. Fung, W. Lee, A novel method to construct taxonomy electrical appliances based on load signaturesof, IEEE Trans. Consum. Electr. 53 (2007) 653–660.
[55] J. Byun, Y. Kim, Z. Hwang, S. Park, An intelligent cloud-based energy management system using machine to machine communications in future energy environments, in: IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2012, pp. 664–665.
[56] X. Jin, Z. He, Z. Liu, Multi-agent-based cloud architecture of smart grid, Energy Procedia 12 (2011) 60–66.
[57] P. Wang, L. Rao, X. Liu, Y. Qi, D-pro: dynamic data center operations with demand-responsive electricity prices in smart grid, IEEE Trans. Smart Grid 3 (2012) 1743–1754.
[58] K. Nagothu, B. Kelley, M. Jamshidi, A. Rajaee, Persistent net-ami for microgrid infrastructure using cognitive radio on cloud data centers, IEEE Syst. J. 6 (2012) 4–15.
[59] N. Sadashiv, S. Kumar, Cluster, grid and cloud computing: a detailed comparison, in: 6th International Conference on Computer Science & Education (ICCSE), IEEE, 2011, pp. 477–482.
[60] A. Di Meglio, M. Riedel, S. Memon, C. Loomis, D. Salomoni, Grids and clouds integration and interoperability: an overview, in: Proceedings of the International Symposium on Grids and Clouds and the Open Grid Forum (ISGC 2011 & OGF 31), vol. 1, Academia Sinica, Taipei, Taiwan, March 19–25, 2011, p. 112. <http://pos.sissa.it/cgi-bin/reader/conf.cgi?confid=133,id.112>.
[61] G. Towns, J. Ferguson, D. Fredrick, G. Myers, Grid User Support Best Practices, 2009.
[62] D. Milojičić, I. Llorente, R. Montero, Opennebula: a cloud management tool, IEEE Internet Comput. 15 (2011) 11–14.
[63] P. Verissimo, A. Bessani, M. Pasin, The tclouds architecture: open and resilient cloud-of-clouds computing, in: IEEE/IFIP 42nd International Conference on Dependable Systems and Networks Workshops (DSN-W), IEEE, 2012, pp. 1–6.
[64] T. Singh, P. Vara, Smart metering the clouds, in: 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, WETICE'09, IEEE, 2009, pp. 66–71.
[65] K. Shvachko, H. Kuang, S. Radia, R. Chansler, The hadoop distributed file system, in: IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST), IEEE, 2010, pp. 1–10.
[66] S. Zhang, J. Wang, B. Wang, Research on data integration of smart grid based on iec61970 and cloud computing, Adv. Electron. Eng. Commun. Manage. 1 (2012) 577–582.
[67] L. Rao, X. Liu, L. Xie, Z. Pang, Hedging against uncertainty: a tale of internet data center operations under smart grid environment, IEEE Trans. Smart Grid 2 (2011) 555–563.
[68] S.-Y. Chang, C.-F. Lai, Y.-M. Huang, Dynamic adjustable multimedia streaming service architecture over cloud computing, Comput. Commun. 35 (2012) 1798–1808.

Melike Yigit received her B.S. and M.S. degrees in computer engineering from Bahcesehir University, Istanbul, Turkey, in 2010 and 2012, respectively. Currently, she is a Ph.D. student in Bahcesehir University, Istanbul, Turkey and works at Turkish Airlines (THY), which is a national airlines in Turkey, as a Business Analyst. Before starting THY, she worked in Huawei Technologies Co. Ltd. and Alcatel-Lucent Teletas as a software developer and San-Tez Project student, respectively. Her current research interests are smart grid communications, power line communications and wireless adhoc and sensor networks.



Vehbi Cagri Gungor received his B.S. and M.S. degrees in Electrical and Electronics Engineering from Middle East Technical University, Ankara, Turkey, in 2001 and 2003, respectively. He received his Ph.D. degree in electrical and computer engineering from the Broadband and Wireless Networking Laboratory, Georgia Institute of Technology, Atlanta, GA, USA, in 2007 under the supervision of Prof. Ian F. Akyildiz. Currently, he is an Associate Professor and Chair of Computer Engineering Department, Abdullah Gul University (AGU), Kayseri, Turkey. His current research interests are in smart grid communications, machine-to-machine communications, next-generation wireless networks, wireless ad hoc and sensor networks, cognitive radio networks, and IP networks. Dr. Gungor has authored several papers in refereed journals and international conference proceedings, and has been serving as an editor, reviewer and program committee member to numerous journals and conferences in these areas. He is also the recipient of the IEEE Trans. on Industrial Informatics Best Paper Award in 2012, IEEE ISCN Best Paper Award in 2006, the European Union FP7 Marie Curie IRG Award in 2009, Turk Telekom Research Grant Awards in 2010 and 2012, and the San-Tez Project Awards supported by Alcatel-Lucent, and the Turkish Ministry of Science, Industry and Technology in 2010.

Selcuk Baktir received the B.Sc. degree in electrical engineering in 2001, from Bilkent University, Ankara, Turkey, and the M.Sc. and Ph.D. degrees in electrical and computer engineering in 2003 and 2008, respectively, from Worcester Polytechnic Institute, MA, USA. Currently, he is an Assistant Professor at the Department of Computer Engineering, Bahcesehir University, Istanbul, Turkey. Before joining Bahcesehir University, he was working as a research scientist at TUBITAK BILGEM, Kocaeli, Turkey. His current research interests include applied cryptography and data security. He is the recipient of the IBM Research Pat Goldberg Memorial Best Paper Award in 2007 and the European Union FP7 Marie Curie IRG Award in 2010.