energies

MDPI

Article

Location-Based Optimized Service Selection for Data Management with Cloud Computing in Smart Grids

Sivapragash C. [1,*], Sanjeevikumar Padmanaban [2,*], Hossain Eklas [3], Jens Bo Holm-Nielsen [2] and R. Hemalatha [4]

1 Department of Electrical and Electronics Engineering, Swarnandhra College of Engineering and Technology, Narasapuram 534275, India
2 Center for Bioenergy and Green Engineering, Department of Energy Technology, Aalborg University, 6700 Esbjerg, Denmark; jhn@et.aau.dk
3 Oregon Renewable Energy Center (OREC), Department of Electrical Engineering and Renewable Energy, Oregon Institute of Technology, Klamath Falls, OR 97601, USA; eklas.hossain@oit.edu
4 Department of Electrical and Electronics Engineering, Anna University, Chennai 600025, India; erhema@gmail.com
* Correspondence: sivadr2002@gmail.com (S.C.); san@et.aau.dk (S.P.); Tel.: +45-71-682-084 (S.P.)

Received: 21 September 2019; Accepted: 21 November 2019; Published: 27 November 2019

Abstract: To maximize the utilization, reliability and availability of power resources, some distribution strategy has to be implemented, which is possible nowadays with the support of modern information technologies (IT). To further develop power utilization, the customer should be aware of efficient power utilization, and the problem of customer management has to be resolved, where payment of electric bills could be through online solutions. A customer-aware power regulatory model is proposed that provides awareness to the consumer regarding the usage of electrical energy, in a secure and reliable solution that combines the features of electrical engineering with cloud computing to ensure better performance in notifying issues, which is done based on location and enhances the operation of smart grids. Instant electric meters are equipped with remote gadgets which communicate with a central cloud administration to produce electric bills for the client. The model provides mindfulness by showing history/notifications and suggestions for energy utilization through the smart meters. The user is provided with security keys to view the reading values and pay bills. To make the solution more accessible, the electronic data will be maintained on various servers at different locations of the cloud. Subsequently, there will be a service provider who manages service requests. A hardwired electric meter transmits the electric readings, which in turn access the particular service to make an entry for the particular connection on the cloud. The usage data will also be maintained at different locations in the cloud, which are accessible to different levels of users with appropriate security measures. The user accessibility is controlled by a Third Party Auditor (TPA) that computes the trustworthiness of users using a trust management scheme. This article also proposes a hash function, which computes and verifies the signature of the keys submitted by the users and also has a higher completeness ratio, which reaches 0.93, than typical methods. This is noteworthy, and the investigation results prove the system's proficiency in providing assured service.

Keywords: cloud services; trust management; secure computing; smart meter; LBSS; user-aware power regulatory model

1. Introduction

The Smart Grid (SG), is an enhancement of the 21st-century electrical grid, which is treated as a system that uses two-way communication. It includes information technologies (IT) and computational

intelligence in an integrated way to address electricity generation, its transmission, and distribution to achieve an electric system that is clean, secure, reliable, efficient, and sustainable. The evolution of SGs relies heavily on the utilization and integration of modern IT for the development of new applications and services that can leverage the technological upgrades that are enabled by the advanced information system. This allows electric grid systems to work in smarter ways. However, an overwhelming amount of heterogeneous information is generated in the SG, mainly due to widely deployed monitoring, metering, measurement and control devices. This calls for a dominant and cost-effective information management paradigm for data processing, analysis, and storage.

Our problem analysis is based on the situation in the regional state of Tamilnadu (India), where electric bills have to be produced for service payment, and the billing requires human intervention. In smart grids, the grid resource plays a significant role without the assistance of humans for such operations. The smart meters present in the SGs record the current energy utilization of users. Additionally, a remote gadget connected to the smart meter can send readings to a remote sink point at a specific time. The remote sink point is the cloud service, which gets the electronic reading from the gadget and creates a record in a database. Therefore, this paper suggests that the IT industry should be involved to assist in the information management of the SG. More specifically, the paper explores how cloud computing (CC), a next-generation computing paradigm, can serve the information management needs in the SG. The concept of CC is based on large data centers with massive computation and storage capacities operated by cloud providers, which deliver computing as a service. Shared resources, software, information, and storage are provided, with computers and other devices as a utility over a network. This SG information management paradigm, in which the management is (partially) accomplished via CC, is called Cloud Service (CS)-based SG Information Management [1].

Generally, the usage of electricity is measured by a human meter reader and later fed into the system manually. There can be errors during the reading process or when feeding the readings into the system, which makes the whole system error-prone. A cloud platform is one where there are multiple layers and services at different layers, which can be broken up into three primary services:

(1) Software-as-a-Service (SaaS): A service provider delivers software and applications through the internet. Users subscribe to the software and access it via the web or vendor APIs.
(2) Infrastructure-as-a-Service (IaaS): A vendor provides clients with pay-as-you-go access to storage, networking, servers and other computing resources in the cloud.
(3) Platform-as-a-Service (PaaS): A service provider offers access to a cloud-based environment in which users can build and deliver applications. The provider supplies the underlying infrastructure.

These three services make up what Rackspace calls the Cloud Computing Stack, with SaaS on top, PaaS in the middle, and IaaS on the bottom. To access the service at different layers, various restrictions can be enforced by the service provider [1]. The cloud consists of service providers who provide services in different forms like infrastructure services, platform services, and software services. Each kind of service belongs to a layer of the cloud. This paper focuses on two different layers, namely software and databases. The cloud services are a set of software interfaces through which legitimate users can access the cloud resource. The cloud is a loosely coupled environment where the cloud system does not know anything about the user and cannot trust the user easily. On a cloud platform, the data can be stored in any of the cloud servers and can be accessed through a set of available services.

The users of the cloud have been allowed to access the service, according to their trust level. Only a registered user is permitted to access the services and data. The trust in different users is managed and verified using a Third Party Auditor (TPA) who maintains the details of users and their access permissions. Only if the TPA has verified the identity of a user successfully, he can access the service or data from the cloud [2]. The TPA, using various approaches, performs the authentication or verification of the users of the cloud. Each method has its demerits and deficiencies. Any security protocol faces different network threats. However, the authentication algorithm should be more

rigid and less time-complex one. The popular key-based approaches have the problem of the higher computational complexity of keys and their higher verification time. This encourages the invention of rigid verification algorithms.

In this paper, to ensure the regular provision of power, a user-aware power regulation method is proposed, which is updated regarding the usage of current meter readings via smart meters. The entire electrical data is updated to the cloud. Depending on the power usage of a user, the proposed power regulatory model provides directions to the user to cut/reduce their power consumption. However, no such service or idea is provided in the existing literature. Additionally, the authors use a location-based service selection scheme to reduce the time complexity. The main novelty of the proposed method involves finding the users who use auditing service and have been cleared by the auditing service and then the way performs service selection, which is explained in detail in Section 3.

2. Background Survey

There exist a variety of methods for the development of cloud services and smart meters; this paper discusses a few of them that apply to our problem statement. In [3], smart meter analytics were examined from a software performance perspective and a performance benchmark design inclusive of a typical smart meter analytics tasks. This system uses both an offline model for feature extraction and online anomaly detection. Due to privacy issues, an algorithm is presented to generate large realistic datasets from a small set of real data.

In [4], a thorough analysis of 100 anonymized 5-min commercial building meter data sets was used to explore time series of electricity consumption using a simple forecast model. This method improves energy management with the support of grid control and provides a model for detecting any anomalies.

In [5], a novel design of a smart metering system was developed as a graphical user interface (GUI)-based NTL detection platform. A 3-tier model of a detection algorithm is proposed to combine three mechanisms that complement each other for enhanced performance. The triangulation technique facilitates validation of detection results through cross verification of the three sources of measurement data. Furthermore, the system also supports better flexibility with built-in or externally developed AI methods and a user-friendly GUI-based platform to monitor and analyze the NTL status of the power grid in real-time for revenue recovery.

In [6], a smart metering technique with different technologies to capture the data from smart meters is presented. In [7] the user privacy is maintained using the tools from information theory and a hidden Markov model for the measurements. It further addresses the issues due to the trade-off between privacy and utility. In [8], open-source tools are used to measure the smart meter data and data storage, and an analytics ecosystem based on publicly available test data set is studied.

There exist a variety of methods for the development of cloud services and smart meters; the paper discusses a few of them here that relate to our problem statement. Reference [9], using a tabu search algorithm, presented an efficient search algorithm to identify the locations of data and software components in data clouds. The main goal of this approach is to minimize the cost incurred in operations and emissions, modelled using mixed-integer programming. The proposed model is solved with the search algorithm discussed earlier. Virtual data center embedding (VDCE) across distributed infrastructures (DI) was introduced to make the infrastructure user-friendly and increase the revenue of providers. Reference [10], performs an analysis of different VM-based cloud environments like Eucalyptus, Open Nebula, and Nimbus. All those platforms have been evaluated with High-Level Petri Nets (HLPN).

In [11], a formal analysis, modelling, and verification of three open-source state-of-the-art VM-based cloud platforms—Eucalyptus, Open Nebula, and Nimbus—is provided. HLPN are used to model, analyze the structural and behavioral properties of the systems. Moreover, to verify the models, they have used the Satisfiability Modulo Theories Library (SMTL) and Z3 Solver.

In this article, we modelled about 100 VM to verify the correctness and feasibility of proposed original models. The results reveal that the models function correctly. Moreover, the increase in the number of VMs does not affect the working of the models, which indicates the practicability of the models in a highly scalable and flexible environment.

Reference [12] analyzes the robustness of advanced DCNs. First, the authors present multi-layered graph modelling of various DCNs, and they study the traditional robustness metrics considering different failure scenarios to perform a comparative analysis. Finally, they describe the inadequacy of the conventional network robustness metrics to appropriately evaluate the DCN robustness and propose new procedures to quantify DCN robustness. Currently, there is no detailed study available centering on DCN robustness.

Reference [13], designs a protocol to enable secure, robust, cheating-resistant, and efficient outsourcing of MIC to a malicious cloud in this paper. The main idea to protect the privacy is by employing some transformations on the original matrix to get an encrypted matrix, which is sent to the cloud; and then transforming the result returned from the cloud to get the correct inversion of the original matrix. Next, a randomized Monte Carlo verification algorithm with one-sided error is employed to successful handle result verification. Further, in this paper, the superiority of this novel technique in designing inexpensive result verification algorithm for secure outsourcing and well demonstrated. They analytically show that the proposed protocol simultaneously fulfils the goals of correctness, security, robust cheating- resistance, and high-efficiency. Extensive theoretical analysis and experimental evaluations also show its high-efficiency and immediate practicability.

In [14] Cloud Capacity Manager (CCM), a prototype system and its methods for dynamically multiplexing the computing capacity of virtualized data centers at scales of thousands of machines, for diverse workloads with variable demands are presented. Extending prior studies primarily concerned with accurate capacity allocation and ensuring acceptable application performance. CCM also sheds light on the tradeoffs due to two unavoidable issues in large scale commodity data centers: (i) maintaining low operational overhead given the variable cost of performing management operations necessary to allocate resources, and (ii) coping with the increased incidences of these operations' failures.

Reference [15] adopts the intuitive idea of High-QoS First-Replication (HQFR) to perform data replication. However, this greedy algorithm cannot minimize the data replication cost and the number of QoS-violated data replicas. To achieve these two minimum objectives, the algorithm transforms the QADR problem into the well-known minimum-cost maximum-flow (MCMF) problem. By applying the existing MCMF algorithm to solve the QADR problem, the second algorithm can produce the optimal solution to the QADR problem in polynomial time. Still, it takes more computational time than the first algorithm.

Reference [16], utilizes Voronoi partitions to determine which data center requests should be routed based on the relative priorities of the cloud operator. In [17], the ability to forecast electricity demand, respond to peak load events, and improve sustainable use of energy by consumers, are made possible by energy informatics. Information and software system techniques for a smarter power grid include pattern mining and machine learning over complex events and integrated semantic information, distributed stream processing for low latency response, cloud platforms for scalable operations and privacy policies to mitigate information leakage in an information-rich environment. Reference [18], proposes a new prototype system, in which the cloud-computing system is combined with a so-called Trusted Platform Support Service (TSS) based on a Trusted Platform Module. In this design, better effects can be obtained in authentication, role-based access and data protection in a cloud computing environment.

Reference [19] presents a pruning algorithm in which a threshold parameter is used to control the tradeoff between computation time and solution accuracy qualitatively. The algorithm is iterative with decoupled state values in each iteration, and the paper parallelizes the state estimations to reduce the overall computation time. They illustrate the proposal with examples where the pruning algorithm

reduces the computation time significantly without losing much precision in-game solutions, and that parallelization further reduces the computation time.

An interdisciplinary MIT study [20] focused on integrating and evaluating existing knowledge rather than performing original research and analysis. Besides, this study's predecessors focused on implications of national policies limiting carbon emissions, while do not make any assumptions regarding future carbon policy initiatives. Instead, they mainly consider the impact of a set of ongoing trends and existing policies. Reference [21] identifies and reviews several low-cost technology products that enable various load control functions and in an innovative prepaid power meter that will have the capacity to direct cash exchanges through remote intervention is built, keeping in mind the end goal is to empower the client to energize his record from home. The user interface comprises an LCD, which shows the power used and a measure of the bill to be paid, and will sound an alert when the balance goes beneath a specific sum utilizing GSM. Prepaid meters are now present in the market and used widely in a few African and European nations. Additionally, this will help service organizations in staying aware of power thievery.

The review concludes that interval metering is not necessary to carry out load control functions. Available technology can remotely switch loads without requiring a connection to a meter. While one-way communication is essential to carry out remote switching of loads, two-way communication is not necessary to carry out remote switching of loads. Metering, in some form, is required for the settlement of the financial transactions associated with load control programs.

Reference [22] examined uncertainty in demand response baseline models and variability in automated responses to dynamic pricing. It defined several demand response (DR) parameters, which characterize changes in electricity use on DR days, and then presented a method for computing the error associated with DR parameter estimates. In addition to analyzing the magnitude of DR parameter errors, in this article, the authors develop a metric to determine how much observed DR parameter variability is attributable to real event-to-event variability versus only baseline model error. Using data from 38 C&I facilities that participated in an automated DR program in California, it was found that DR parameter errors are significant. For most facilities, observed DR parameter variability is more likely explained by baseline model errors, not real DR parameter variability; however, and several facilities do exhibit real DR parameter variability.

Reference [23] proposes a mathematical model for the dynamic evolution where in particular supply, demand, and clearing prices under a class of real-time pricing mechanisms are characterized by passing on the real-time wholesale prices to the end consumers. The effects that such mechanisms could have on the stability and efficiency of the entire system are investigated, and several stability criteria are discussed. It is shown that relaying the real-time wholesale electricity prices to the end consumers creates a closed-loop feedback system, which could be unstable or lack robustness, leading to extreme price volatility. Finally, a result is presented, which characterizes the efficiency losses incurred when, to achieve stability, the wholesale prices are adjusted by a static pricing function before they are passed on to the retail consumers.

Fault current coefficient and time delay assignment for a microgrid protection system with a central protection unit was discussed in [24], which utilizes relays of type-distributed generators providing more protection between generators. This approach performs critical parameter assignments like fault current coefficient and relay hierarchy. This method overcomes the difficulty of the manual task of distributed generation (DG) and protection units.

Reference [25] proposed an approach for distributed network reinforcement using a time segmentation algorithm, which reduces the computation overhead. Discrete particle swarm optimization is used to overcome the problem of nonlinear and discrete optimization.

Reference [26] was focused on load models of appliances. The loads for different appliances are generated using the profiles maintained and validated with actual distribution circuits. Then on-demand sensitive load models are used to reduce the consumption of different consumer ports, introduced the improvement of such load models at the machine level, and incorporated traditional

controllable burdens, i.e., space cooling/space warming, water heater, garment dryer and electric vehicles. Approval of the machine level load models' is done by contrasting the models' output and the actual power utilization information for the related apparatus. The machine-level load models' are combined to create stack profiles for a dispersion circuit, which are approved against the load profiles of a real distribution circuit. The DR-touchy load models are utilized to examine changes in power utilization at both the household and the distribution levels, given an arrangement of client practices and additional actions by a utility.

In [27], an approach for real-time voltage-stability margin control via reactive power reserve sensitivities is proposed. In detail, a man-in-loop control method is used to boost reactive power reserves (RPRs) while maintaining a minimum amount of voltage stability margin bus voltage limits. The objective is to determine the most effective control actions to reestablish critical RPRs across the system. Initially, the concept of reactive power reserve sensitivity concerning control actions is introduced. In the sequel, a control approach based on convex quadratic optimization is used to find the minimal amount of control necessary to increase RPRs above their pre-specified (offline) levels. Voltage stability margin constraints are incorporated using a linear approximation of critical RPRs.

Reference [28], discussed an evaluation method for renewable DG in distributed networks. This approach allocates DGs to maximize the usage of connections to the local distribution company and customers. Reference [29] presents the algorithms and associated analysis, but guidelines, rules, and implementation considerations are also discussed, especially for the more complicated situations where mathematical analysis is difficult. In general, it is challenging to codify and taxonomize the scheduling knowledge because there are many performance metrics, task characteristics, and system configurations. Also, adding to the complexity is the fact that a variety of algorithms are designed for different combinations of these considerations. In spite of the recent advances, there are still gaps in the solution space, and there is a need to integrate the available solutions.

Security-aware scheduling strategy for real-time applications on clusters (SAREC) [30], proposes a security-aware scheduling strategy, or which integrates security requirements into scheduling for real-time applications by employing our security overhead model.

Scheduling real-time data-intensive applications (SARDIG) is a security-attentive dynamic real-time scheduling algorithm architecture and a dynamic grid scheduling algorithm for providing security for real-time data-intensive applications [31]. It proposes a grid architecture, which describes the scheduling framework of real-time data-intensive applications. Also, the authors introduced a mathematical model for providing security of the real-time data-intensive applications and a security gain function to quantitatively measure the security enhancement for applications running in the grid sites. They have also proved that the SARDIG algorithm always provides optimum security for real-time data-intensive applications.

It could be concluded that the system has a problem of service selection in all the above approaches when there is the considerable number of customers from different locations, so a new location-based service and selection approaches are proposed in this paper. In the following Section 3, the proposed location-based service selection approach is discussed, while Section 4 discusses the results achieved by the proposed method.

3. User-Aware Power Regulatory System with a Location-Based Service Selection Scheme

The proposed user-aware power regulatory scheme gets updates about the power usage of users through smart meters. The smart meters update the power usage details to the cloud service. Based on the power usage details, the power regulatory model provides inputs to the users to control the power usage of the connection. The selection of a location-based service selection scheme to provide additional comprehensive and consistent services has to be done in a more tactical approach where the time complexity should be reduced. The method audits the identity of the user using the auditing service, and if the user has cleared the auditing service, then the way performs service selection. The entire process is split into several stages, namely Location-Based Service Selection, Hash Function for

Key Generation, Signature Verification, Trust Management, and Profile-Based Access Restriction. In this section, we will explain each of the functional stages in detail. Figure 1 presents the architecture of the proposed user aware power regulatory model with a location-based service selection framework, and it shows the various stages of the proposed model.

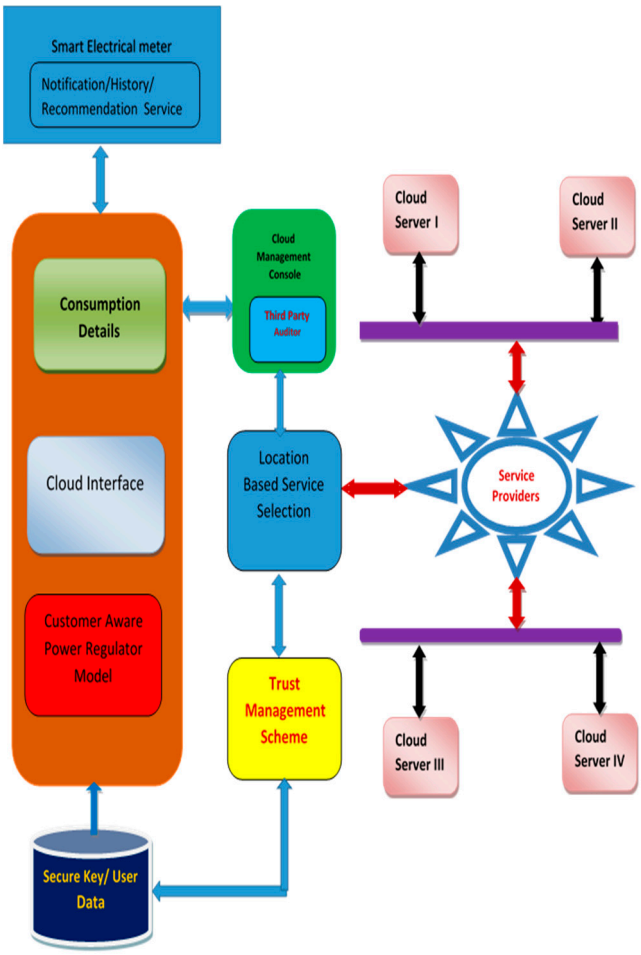

Figure 1. The architecture of the LBSS Model.

3.1. User-Aware Power Regulatory Model

The smart meter accesses the cloud service intermittently to send power use details, prior month use, cost, every month's average units, number of units utilized at peak times, number of units used during off peak-times and their relative offered price. Additionally, the shutdown date and complaints registered, number of aggregate units, number of units utilized at peak time, number of units used during the off-peak times and their relative offered cost are included, and user notifications are shown on a smart meter display. The power regulatory model controls the flow of electric supply to the user connection. At intermittent periods, the model produces electric bills and regulates the power supply. At whatever point the instalment for the electrical supply not been paid, the substation sends a control message to the smart meter to detach the electric supply. When the user pays his bills again, then the substation sends the turn-on message to the meter, which provides the power back. The power regulatory model utilizes the ZigBee convention to the correspondence between the smart meter and substation.

Algorithm 1: User-Aware Power Regulatory System

Input: User Usage Details
Output: Power to be regulated.
Start
Initialize the value of time slot Ti.
Tv = value of time slot Ti.
For each Time window Ti
Read Current usage units Cu.
Compute Number of units at peak time NPTu.
Compute Number of units at Off-Peak Time NOPTu.
Compute the cost of power usage CPU.
Compute Previous month usage Pmu.
Compute Previous month cost Pmc.
Compute Number of units on previous month Npm.
Compute No of units on peak time Nupt.
Compute No of units on off-peak time Nuopt.
Identify complaints registered Compl.
Compute shutdown date Sd.
Access Cloud Service Cs.
Cloud-Update-Service (Cu, NPTu, NOPTu, CPU,
PMU, Pmc, Npm, Nupt, Nuopt, Compl).
Display details to the smart meter.
End
If payment date Alive
Else
Access Payment-Detail Service.
If true then
Reset Payment date.
Else
Disconnect the power supply.
End
End
Stop.

Algorithm 1, above generates user awareness. It accesses the cloud service to update the cloud, so the smart meter can also show the recently registered estimations of energy utilization to the user. The model controls the power supply by checking the instalment status by accessing the cloud service. In light of the state of the instalment, the power status controls the electric supply through the smart meter.

3.2. Location-Based Service Selection

The user electronics readings are maintained at different locations of the county on different servers. Each geographic region reading is stored on separate servers located in different geographic regions. The user can view generated bills and make payment of bills through the cloud services. Upon creating a request, the cloud platform selects the respective service, according to the location of data or the server where the data is stored. To provide a more complete, and reliable service, the selection is made in a more strategic way where the time complexity should be minimized. The range of services is based on the location of the data, and then the user communicates with the selected service. The cloud management console makes the selection, and once the service is selected, then the user request is transferred to the service chosen (see Algorithm 2).

Algorithm 2: Location-Based Service Selection

LBSS(UserId Uid, UserLocation Uloc)
Output: Selected cloud service CS.
Step1: Read user-id Uid.
Step2: Read user location Uloc.
Step3: Read service details SD, service History Sh.
Step4: Select available services according to the location Uloc.
$Ss = \int_{i=1}^{N} Mx(sh) \times (Sd(Uloc))$
N = number of available services.
Mx = Minimum frequency of service
Sh = service history
Step5: Return SS.

3.3. Hash Function for Key Generation

The cloud user is assigned a secure key using which the user is identified and authenticated. The generation of the secret key is a dynamic process which is initiated for each reading, and the key is destroyed when the user completes the task. The key generation mechanism uses a hash function where the parameter of the hashing function also is changed when the existing or other users enter the system the next time. The selection of parameters and functions will also be adjusted according to the region of the user to provide more security and to avoid guessing attacks (see Algorithm 3).

Algorithm 3: Hashing Function for Key Generation

Intake: Locations loc, Schemes S.
Outcome: Secret key SecK.
Read location details LD from the database.
Compute Nl = Number of locations from Ld.
Nl = sizeof(LD).
Generate Random Number Rn.
Rn = $f(x) = \int \varnothing(1, S)$.
Selected Scheme SeS = S(Rn).
If (SeS %2) = 0 then
Generate Secret Key SecK.
Initialize SecK = $\int_{i=1}^{8} \mathrm{SecK}(i) = 0)$.// initialize the key to the size of 8 bit and set all bit to 0.
//Set the bit 1,2 = for region 1,2,3
//Set the bit 3,4 = for scheme 1-Feb no, 2-ams no, 3-Mona
//Set bit 5 and 6 = for the value -
//Set the bit 7,8 with meter no
User region ur = select the region of the user.
Select a random number for the addressing scheme RanS.
If(RanS = 1)
Ms = Select a Fibonacci number within ur.
Ms = $f(x) = \int ® \cap (\sum \mathrm{Fibanacci} \in (1, \mathrm{UR}))$
Else if (RanS = 2)
Ms = select a amstrong number within ur.
Ms = $f(x) = \int ® \cap (\sum \mathrm{Amstrong} \in (1, \mathrm{UR}))$
Else
Ms = select a manorama number within ur.
Ms = $f(x) = \int ® \cap (\sum \mathrm{Manorama} \in (1, \mathrm{UR}))$
End
Construct sk = {Ur,RanS,NS,Mr}.
Else
Create a Secret Key SecK.
Initialize SecK = $\int_{i=1}^{16} \mathrm{SecK}(i) = 0)$.// initialize the key to the size of 16 bit and set all bit to 0.
//Set the bit 1 to,4 = for region 1,2,3
//Set the bit 5 to 8 = for scheme 1-Feb no, 2-ams no, 3-Mona
//Set bit 9 to12 = for the value -
//Set the bit 13 to 16 with meter no
User region ur = select the region of the user.
Select a random number for the addressing scheme RanS.
If(RanS = 1)
Ms = Select a Fibonacci number within ur.
Ms = $f(x) = \int ® \cap (\sum \mathrm{Fibanacci} \in (1, \mathrm{UR}))$
Else if (RanS = 2)
Ms = select a amstrong number within ur.
Ms = $f(x) = \int ® \cap (\sum \mathrm{Amstrong} \in (1, \mathrm{UR}))$
Else
Ms = select a manorama number within ur.
Ms = $f(x) = \int ® \cap (\sum \mathrm{Manorama} \in (1, \mathrm{UR}))$
End
Construct SecK = {Ur,RanS,NS,Mr}.
End
Return SecK.

3.4. Signature Verification

In this stage, the user key has been verified. The verification process is performed by extracting the bit level information of the received key. If the key size is 16 bits, then a 16 bits keying mechanism is used; otherwise, an 8 bits keying mechanism is used (see Algorithm 4).

Algorithm 4: Signature Verification

Intake: SecK.
Outcome: True/False
Read Given Secret Key SecK.
Read Key Set KeyS from Key Base Kb.
Identify Key Size of SecK.
Ks = $\sum$ Bits $\in$ SecK
If Ks = 8 then
Split SecK by the 2-bit key base.
Ur = SecK(1,2).
Scheme SN = SecK(3,4).
Number Mn = SecK(5,6).
Meter No Mr = SecK(7,8).
Else
Split SecK into 4 bit Key Base.
Ur = SecK(1,2,3,4).
Scheme ScN = SecK(5,6,7,8).
Number Mn = SecK(9,10,11,12).
Meter No Mr = SecK(13,14,15,16).
End
If(ScN = 1)
Ms = Select a Fibonacci number within ur.
Ms = $\int_1^{\mathrm{Ur}} \mathrm{Feb}(1, \mathrm{Ur})$
Else if (ScN = 2)
Ms = select an amstrong number within ur.
Ms = $\int_1^{\mathrm{Ur}} \mathrm{Ams}(1, \mathrm{Ur})$
Else
Ms = select a manorama number within ur.
Ms = $\int_1^{Ur} Man(1, Ur)$
End
If Ms = Mn and Mr $\in$ Db then
Return True.
Else
Return False.
End

3.5. Trust Management

Trust management is the critical process in service selection because the user is allowed to accessing the service only if he passes the trust evaluation. The trust management is categorized based on the type of users. By identifying the user type from the request, the identity of generic users is verified based on the crucial secret mechanism. For the internal registered users, the primary public/private critical method is used. Any user is allowed to access the service based on the trust verification result.

3.6. Profile-Based Access Restriction

The cloud platform is comprised of different users and has to be restricted to minimize access by different users. For example, the internal user needs to view the readings of various users and needs to

generate reports on them, and so on. The internal users must be able to access the data more frequently, whereas the external users do not. The external user needs one-time access or access for a short time to pay the bills so that the proposed work restricts the access based on the roles. It provides role-based access restriction to offer more security to the cloud platform and thus, outsiders cannot make flooding attacks on the proposed system.

4. Results and Discussion

The proposed SG is entirely simulated using the CloudSim platform, and the coding is written using 32 bit Java language for Windows 7 or 8. The processor used is a Core i5 with 8 GB RAM for higher computational operation. The application server used is Tomcat 5.0.6. The proposed user-aware Power Regulatory Model with Location-Based Service Selection approach, is implemented and evaluated for its efficiency. The technique has been assessed utilizing different setups with a vast number of service points and numbers of users. The strategy has been tried with varying situations of re-enactment for various periods. Table 1 lists the details of the simulation parameters utilized to assess the execution of the proposed technique. Figure 2 shows a preview of the smart meter intended for the proposed system. Figure 3 is a preview of the user interface utilized by the power station staff to refresh the unit costs for an assortment of associations. Table 2 shows the completeness ratio of three different algorithms, and it shows that the proposed method has a higher completeness measure value that indicates its efficiency in providing guaranteed service.

Table 1. Simulation Parameters.

Parameter	Value
Laxity Time	100–500 s
Network Bandwidth	10 Mbps
Number of Cloud Servers	32
Number of cloud services	2
Number of service providers	2
Number of Users	1 million
Number of Insiders	10,000

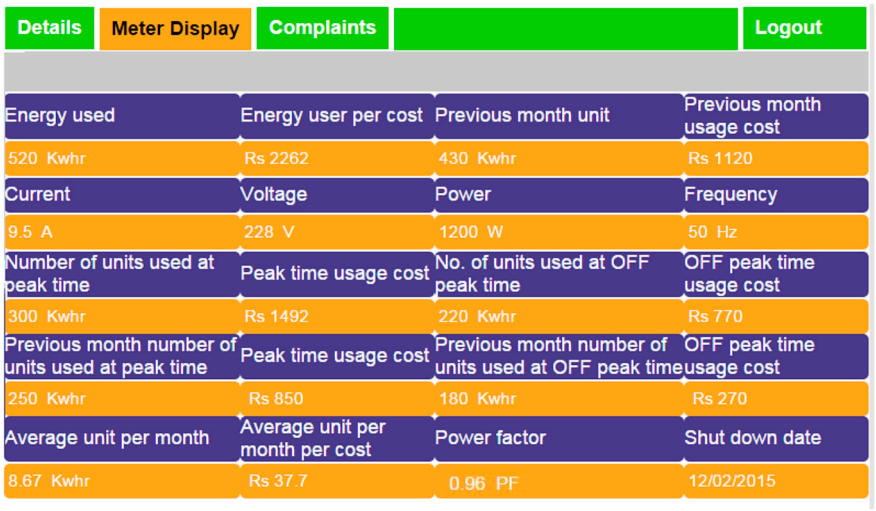

Figure 2. Snapshot of the smart meter display.

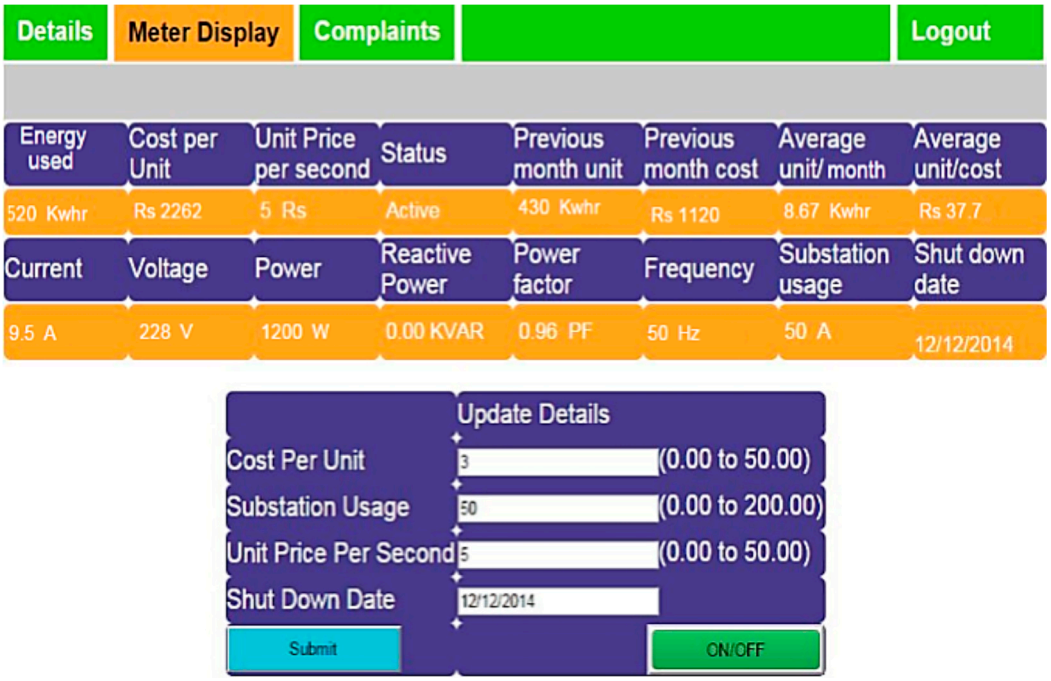

Figure 3. Snapshot of the power station interface.

Table 2. Comparative of completeness ratio results.

Completeness Ratio				
Laxity (S)	**EDF**	**SAREG**	**SARDIG**	**Location-Based**
100	0.79	0.82	0.83	0.89
200	0.80	0.81	0.85	0.90
300	0.83	0.85	0.87	0.91
400	0.84	0.86	0.89	0.92
500	0.85	0.87	0.91	0.93

The proposed solution has been implemented is Hadoop, which is a cloud computing platform integrated with the proposed solution to evaluate the proposed methodology. Three different clouds are created, with each one is running at various locations and on three service providers, which are running at N locations. The proposed solution is hardwired with the electric meter, and wireless communication is enabled to access the cloud service. Another web interface is specially designed for users to use and complete the payment procedures. To evaluate the performance of the proposed solution, Availability Ratio, Completeness Ratio, Security Value, Overall Performance Ratio, measures were the metrics examined. Availability is the ratio of total requests submitted and total requests handled. Completeness is the ratio between total submitted requests and the number of requests processed successfully. The security level is measured by total requests generated and completed. Overall performance is the ratio of the total number of requests submitted and the number of jobs completed in a particular time-frame.

The performance of the proposed method is compared with three well-known scheduling methods of the grid environment, namely Earlier Deadline First (EDF) [29] algorithms, Security-Aware scheduling strategy for Real-time applications on Clusters (SAREC) [30] and the Security of Real-Time Data-Intensive Applications on Grids (SARDIG) [31]. Table 2 shows the simulation results of the completeness ratio for the four algorithms. The completeness ratio is computed using different deadline bases or latency time (from 100 to 500 s). The proposed algorithm shows a better completeness ratio than the other algorithms as the deadline base or latency increases. Table 2 shows that the proposed

method has a higher ratio, which raised from 0.85 to 0.93, which demonstrates its efficiency in providing guaranteed service.

Table 3 shows the service availability ratio of four different algorithms, and it shows that the proposed method provides more service availability than other methods. Table 4 shows the simulation results of the security value for the four algorithms. The security value is computed using the total number of requests submitted and several requests fulfilled per number of users present in the network.

Table 3. Shows the comparison results of serviceability.

Availability Ratio %				
No. of Users	**EDF**	**SAREG**	**SARDIG**	**Location-Based**
1 million	72	82	89	98.7
2 million	69	79	85	97.6
3 million	67	75	81	96.6
5 million	63	72	77	95.8
10 million	59	69	72	95.1

Table 4. Shows the comparison results of the security level.

Security Level Value				
No. of Users	**EDF**	**SAREG**	**SARDIG**	**Location-Based**
1million	0.89	0.92	0.95	0.99
2 million	0.83	0.85	0.90	0.96
3 million	0.77	0.79	0.86	0.93
4 million	0.61	0.72	0.82	0.91
5 million	0.55	0.65	0.77	0.89

Figure 4 shows the time complexity of different methods to access the service where the service and data are available at various locations of the region. The time complexity is Φ (N $\times$ M), where N—is the number of locations where the service is available, and M—is the number of service providers available. The overall time complexity is computed as follows:

$$\text{Time complexity } Tc = N \times \text{Log } (M)$$

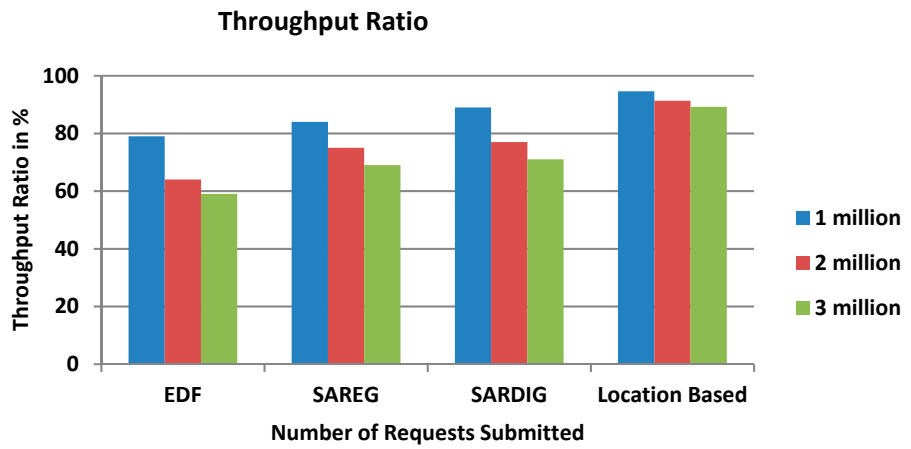

Figure 4. The time complexity of different approaches.

Figure 4 shows that the proposed method produces more efficient results compared to the other algorithms.

5. Conclusions

In this paper, we have proposed a user-aware power regulatory model with a location-based service selection approach for smart grids. The model provides functionality for smart meters to update the user details to the cloud as well be displayed on a smart meter display. Depending on the recommendations from the smart meter display, the users can change their usage patterns. As per the design, the proposed model manages the power supply to all its connecting units and a location-based service selection for secure and reliable access for the cloud services in a smart grid. It maintains a list of trustworthy users with different authentication mechanisms. For a registered internal user, it provides role-based access and user access restriction is provided based on their frequency of access. A malicious intruder or an unauthorized user is restricted from accessing the system through various hash-based signature verification mechanisms that ensure that the cloud is secure. Further, the access session duration is limited to prevent the system from being affected by flooding attacks. The experimental results show that the proposed model obtains higher performance in terms of high throughput and quality of assurance than other existing methods. The next step to introduce a secure and trusted solution is the requirement that needs to be focused on and to be addressed by the cloud-computing infrastructure.

Author Contributions: All authors have involved in this research activities for the final presentation of the work as a comprehensive research current article.

Funding: No source of funding for this research activities.

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

References

1. Sivapragash, C.; Thilaga, S.R.; Kumar, S.S. Advance Cloud Computing in Smart Power Grid. In Proceedings of the IET Chennai 3rd International on Sustainable Energy and Intelligent Systems (SEISCON 2012), Tiruchengode, India, 27–29 December 2012; pp. 356–361.
2. Rathi, A.; Parmar, N. Secure Cloud Data Computing with Third Party Auditor Control. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Bubaneswar, Odisha, India, 14–15 November 2014; pp. 145–152.
3. Liu, X.; Golab, L.; Golab, W.; Ilyas, I.F.; Jin, S. Smart meter data analytics: Systems, algorithms, and benchmarking. *ACM Trans. Database Syst.* **2017**, *42*, 2. [CrossRef]
4. Mohammad, R. AMI Smart Meter Big Data Analytics for Time Series of Electricity Consumption. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1771–1776.
5. Kee, K.K.; Shahab, S.M.F.; Loh, C.J. Design and development of an innovative smart metering system with GUI-based NTL detection platform. In Proceedings of the 4th IET International Conference on Clean Energy and Technology Conference, Kuala Lumpur, Malaysia, 14–15 November 2016.
6. Alahakoon, D.; Yu, X. Advanced analytics for harnessing the power of smart meter big data. In Proceedings of the 2013 IEEE International Workshop on Intelligent Energy Systems (IWIES), Vienna, Austria, 14 November 2013; pp. 40–45.
7. Sankar, L.; Rajagopalan, S.R.; Mohajer, S. Smart meter privacy: A theoretical framework. *IEEE Trans. Smart Grid* **2013**, *4*, 837–846. [CrossRef]
8. Prasad, S.; Avinash, S.B. Smart meter data analytics using OpenTSDB and Hadoop. In Proceedings of the 2013 IEEE on Innovative Smart Grid Technologies-Asia (ISGT Asia), Bangalore, India, 10–13 November 2013; pp. 1–6.
9. Larumbe, F.; Sanso, B. A Tabu Search Algorithm for the Location of Data Centers and Software Components in Green Cloud Computing Networks. *IEEE Trans. Cloud Comput.* **2013**, *1*, 22–35. [CrossRef]
10. Amokrane, A.; Zhani, M.F.; Langar, R.; Boutaba, R.; Pujolle, G. Greenhead: Virtual Data Center Embedding across Distributed Infrastructures. *IEEE Trans. Cloud Comput.* **2013**, *1*, 36–49. [CrossRef]

11. Malik, S.U.; Khan, S.U.; Srinivasan, S.K. Modeling and Analysis of State-of-the-art VM-based Cloud Management Platforms. *IEEE Trans. Cloud Comput.* **2013**, *1*, 1. [CrossRef]
12. Bilal, K.; Manzano, M.; Khan, S.U.; Calle, E.; Li, K.; Zomaya, A.Y. On the Characterization of the Structural Robustness of Data Center Networks. *IEEE Trans. Cloud Comput.* **2013**, *1*, 1. [CrossRef]
13. Lei, X.; Liao, X.; Huang, T.; Li, H.; Hu, C. Outsourcing Large Matrix Inversion Computation to A Public Cloud. *IEEE Trans. Cloud Comput.* **2013**, *1*, 1. [CrossRef]
14. Kesavan, M. Practical Compute Capacity Management for Virtualized Data Centers. *IEEE Trans. Cloud Comput.* **2013**, *1*, 1. [CrossRef]
15. Lin, J.W.; Chen, C.H.; Chang, J.M. QoS-Aware Data Replication for Data-Intensive Applications in Cloud Computing Systems. *IEEE Trans. Cloud Comput.* **2013**, *1*, 1. [CrossRef]
16. Doyle, J. Stratus: Load Balancing the Cloud for Carbon Emissions Control. *IEEE Trans. Cloud Comput.* **2013**, *1*, 1. [CrossRef]
17. Simmhan, Y.; Aman, S.; Cao, B.; Giakkoupis, M.; Kumbhare, A.; Zhou, Q.; Paul, D.; Fern, C.; Sharma, A.; Prasanna, V.K. *An Informatics Approach to Demand Response Optimization in Smart Grids*; Report; Computer Science Department, University of California: Los Angeles, CA, USA, 2013.
18. Zen, Z.D. Cloud computing based on trusted computing platform. In Proceedings of the International Conference on Intelligent Computation Technology and Automation, Changsha, China, 11–12 May 2010.
19. Ma, C.Y.T. Scalable Solutions of Markov Games for Smart-Grid Infrastructure Protection. *IEEE Trans. Smart Grid* **2013**, *4*, 47–55. [CrossRef]
20. Kassakian, J.G.; Schmalensee, R.; Desgroseilliers, G.; Heidel, T.D.; Afridi, K.; Farid, A.M.; Grochow, J.M.; Hogan, W.W.; Jacoby, H.D.; Kirtley, J.L.; et al. *The Future of the Electric Grid: An Interdisciplinary MIT Study*; Massachusetts Institute of Technology: Cambridge, MA, USA, 2011.
21. Crossley, D. *The Role of Advanced Metering and Load Control in Supporting Electricity Networks*; Tech. Rep. No 5 Task XV, International Energy Agency Demand Side Management Programme; Energy Futures Australia PTY LTD: Brisbane, Australia, 2008.
22. Mathieu, J.L.; Callaway, D.S.; Kiliccote, S. Examining uncertainty in demand response baseline models and variability in automated responses to dynamic pricing. In Proceedings of the 50th IEEE Conference on Decision and Control (CDC), Orlando, FL, USA, 12–15 December 2011; pp. 4332–4339.
23. Roozbehani, M.; Dahleh, M.; Mitter, S. On the stability of wholesale electricity markets under real-time pricing. In Proceedings of the 49th IEEE Conference on Decision and Control (CDC), Atlanta, GA, USA, 15–17 December 2010; pp. 1911–1918.
24. Ustun, T.S. Fault current coefficient and time delay assignment for micro grid protection system with central protection unit. *IEEE Trans. Power Syst.* **2013**, *28*, 598–606. [CrossRef]
25. Ziari, S. Optimal distribution network reinforcement considering load growth, line loss, and reliability. *IEEE Trans. Power Syst.* **2013**, *28*, 587–597. [CrossRef]
26. Shao, S.H. Development of physical-based demand response-enabled residential load models. *IEEE Trans. Power Syst.* **2013**, *28*, 607–614. [CrossRef]
27. Lianordi, B. An approach for real time voltage stability margin control via reactive power reserve sensitivities. *IEEE Trans. Power Syst.* **2013**, *28*, 615–625. [CrossRef]
28. Shaaban, M.F. DG allocation for benefit maximization in distribution networks. *IEEE Trans. Power Syst.* **2013**, *28*, 639–649. [CrossRef]
29. Stankovic, J.A.; Spuri, M.; Ramamritham, K.; Buttazzo, G.C. *Deadline Scheduling for Real-Time Systems: EDF and Related Algorithms*; Kluwer: Dordrecht, The Netherlands, 1998.
30. Xie, T.; Qin, X.; Sung, A. SAREC: A security-aware scheduling strategy for real-time applications on clusters. In Proceedings of the 34th International Conference on Parallel Processing, Oslo, Norway, 14–17 June 2005.
31. Islam, M.R.; Hasan, M.T.; Ashaduzzaman, G.M. An architecture and a dynamic scheduling algorithm of grid for providing security for real-time data-intensive applications. *Int. J. Netw. Manag.* **2011**, *21*, 402–413. [CrossRef]