AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Enhancing the Security of Smart Grid Resources in Cloud Environment

[1]Dr. P. Anbalagan Assistant Professor, [2]J. B. Shriram, [3]Teaching Fellow, S. Ragha Ranjani P.G Student

[1]*Department of Electrical and Electronics Engineering, BIT Campus, Anna University, Tiruchirappalli 620024*
[2]*Department of Computer Science and Engineering, BIT Campus, Anna University, Tiruchirappalli 620024*
[3]*M.E Mobile and Pervasive Computing, BIT Campus, Anna University, Tiruchirappalli 620024*

Address For Correspondence:
Dr. P. Anbalagan Assistant Professor, Department of Electrical and Electronics Engineering, BIT Campus, Anna University, Tiruchirappalli 620024
E-mail: anbutau@gmail.com

ARTICLE INFO

Article history:
Received 26 April 2016
Accepted 21 July 2016
Published 30 July 2016

Keywords:
smart grid, cloud computing, datacenter, electricity generation

ABSTRACT

Cloud computing is a term that delivers host services and sharing computing resources over the internet. Cloud data centers are powerful computing system which acquire huge amount of electrical energy. The consumption of energy can be effectively managed by smart grid. Smart grid monitors on electricity distribution. It is generally launch to be used on electricity network level which is in the form of power plants. Smart grid spans three different domains- generation system, transmission side and distribution side. Generation system consists of traditional power plant generation. Transmission side is responsible for delivering electricity to the distribution side. Computational requirements for Smart Grid applications can be met by utilizing the Cloud Computing. Implementing cloud industries, with smart grids two-way communications and advanced sensors, will improve the efficiency, reliability and safety of power delivery to cloud data centers. This paper proposes cloud computing technology because of its low cost, flexible and fast response time, has the functionality needed to provide the security for large scale smart grid application.

INTRODUCTION

Driven by the new emerging technologies and the increasing pressure of the global warming, the conception of “smart grid” was proposed in the last few years. These features make the future grid to be a complex cyber-physical system and impose some significant requirements on the information infrastructure of the next-generation power grid, including fast reaction to disturbances and faults, wide area data management, high-performance computing and real-time analysis, and data security. This centralized information infrastructure cannot satisfy the information requirements of the future grid. The first limitation is that the control center can hardly manage the mass data generated by future grid due to its storage bottleneck. For instance, in the future grid a phase measurement unit (PMU) generates 50 or 60 phasor measurements per second. Such big data cannot be fully transmitted to the control center due to the bandwidth limit. It can be expected that even a small number of PMU will generate a large amount of data and reach the bandwidth bottleneck. Even the bandwidth can be upgraded to serve the peak-rate data transmission (obviously this is not a cost-efficient solution), the storage capacity limitation of the control center restricts the storing of the big data centrally. Therefore, to effectively aggregate the wide area distributed data, a decentralized, platform-centric infrastructure is desired. With the exploration of the big data, the computing power consumption of the future grid will become a big challenge for the centralized information infrastructure.

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient

To Cite This Article: Dr. P. Anbalagan Assistant Professor, J. B. Shriram, Teaching Fellow, S. Ragha Ranjani P.G Student., Enhancing the Security of Smart Grid Resources in Cloud Environment. ***Aust. J. Basic & Appl. Sci.,*** *10(12): 224-230, 2016*

computing by centralizing storage, memory, processing and bandwidth. Cloud computing is a comprehensive solution that delivers IT as a service. The flexibility of cloud computing is a function of the allocation of resources on demand. Before cloud computing, websites and server-based applications were executed on a specific system. Cloud computing is broken down into three segments application, storage and connectivity.

Cloud computing is a large scale distributed computing paradigm that is driven by economies of scale in which a pool of abstracted, virtualized ,dynamically scalable, managed computing power, storage, platforms and services are delivered on demand to customers over the internet. Cloud computing is the offspring of distributed and grid computing. It is nothing but a specialized form of distributed and grid computing which varies in terms of infrastructure services, deployment and geographic dispersion. The advantages of cloud computing includes the following as reduced costs, easy maintenance, re-provisioning of resources and increased profits.tha aim is to increase productivity of resource management over Dynamic Resource Scheduler (DRS). The cloud has evolved in two broad perspectives – to rent the infrastructure in cloud, or to rent any specific service in the cloud, where the former one deals with the hardware and software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers.

Smart Grid (SG) is an electrical grid that uses information and communication technologies to gather and act on information.SG system provide more electricity to meet rising demand, increased reliability and quality of power supplies, increased energy efficiency be able to integrate low carbon energy sources into power networks. SG is conceptualized as a combination of electrical network and communication infrastructure. With the integration of information and communication technology, modern smart grid is capable of providing electricity to the end users in an increasingly efficient manner. Implementation of SG will change the way of power utilization in cloud computing environment. Any smart grid infrastructure should support real-time, two-way communication between utilities and consumers, and should allow software systems at both the producer and consumer ends to control and manage the power usage. Grid is a service for sharing computer power and data storage capacity over the internet. The primary attributes are Computer resources are not administered centrally; Open standards are used; Nontrivial QOS is achieved. Power grid was considered within the context control, ecology, human cognition, glassy dynamics, information theory and microphysics of cloud. With grid optimization we can find the perfect balance between Reliability, Availability, Efficiency and Cost. It ranges from generation to transmission and from distribution to end user. A smart grid can be considered as a cyber-physical system that connects physical electricity systems and cyber-infrastructure, with the integration of the Internet. This service can communicate with the consumer appliances and also provide the backbone for utilities to assimilate content and control operations.

II. Related works:

Hybrid Cloud Computing Platform: The Next Generation It Backbone For Smart Grid:

The prospective of applying cloud computing technologies in the development of smart grid. Firstly, the conceptions of cloud computing are introduced, and then a hybrid cloud computing platform for smart grid is designed. After that, the distinguished characteristics of the proposed platform are explained in detail, following with the introduction of some potential power system applications. Advanced Metering Infrastructure algorithm is used. Finally, some notable state-of-the-art products that can be used to build the proposed platform are introduced**.** Long distance transmission systems are the main disadvantage.

Cloud-Based Demand Response For Smart Grid: Architecture And Distributed Algorithms:

Cloud-based demand response (CDR), a novel demand response architecture for fast response times in large scale deployments. The proposed architecture is in contrast to master/slave based demand response where the participants directly interact with the utility using host address-centric communication. CDR leverages data-centric communication, publisher/subscriber and topic-based group communication to make demand response secure, scalable and reliable. cloud-based demand response (CDR) algorithm is used. To the utility, CDR appears to be a black box function call that takes an input from the utility, e.g., power deficit and gives an output to the utility, e.g., power reduction per customer and the corresponding price incentive. Using this implementation framework, we propose two market-based distributed algorithms (bisection and Illinois methods). The proposed algorithms exhibit at least exponentially fast convergence with O(1) iteration as the number of customers grows and outperform prior work of the dual gradient method in terms of convergence speed while keeping the same messaging overhead. power imbalance is the limitation.

Cloud Computing And Grid Computing 360-Degree Compared:

Cloud Computing has become another buzzword after Web 2.0. However, there are dozens of different definitions for Cloud Computing and there seems to be no consensus on what a Cloud is. On the other hand, Cloud Computing is not a completely new concept; it has intricate connection to the relatively new but thirteen-year established Grid Computing paradigm, and other relevant technologies such as utility computing, cluster computing, and distributed systems in general. This paper strives to compare and contrast Cloud Computing

with Grid Computing from various angles and give insights into the essential characteristics of both. The problems are mostly the same in Clouds and Grids. Java and C implementations of WSRF is the algorithm used.

Analysis Of Key-Exchange Protocols And Their Use For Building Secure Channels:

The analysis of key-exchange protocols that combines previous definitional approaches and results in a definition of security that enjoys some important analytical benefits: (i) any key-exchange protocol that satisfies the security definition can be composed with symmetric encryption and authentication functions to provide provably secure communication channels (as defined here); and (ii) the definition allows for simple modular proofs of security: one can design and prove security of key-exchange protocols in an idealized model where the communication links are perfectly authenticated, and then translate them using general tools to obtain security in the realistic setting of adversary-controlled links. Exemplify the usability of results by applying them to obtain the proof of two classes of key-exchange protocols, Diffe-Hellman and key-transport, authenticated via symmetric or asymmetric techniques. The limitation is the Perfect forward secrecy. Simulation-based and indistinguishability-based algorithm is used.

An Optimized Algorithm For Task Scheduling Based On Activity Based Costing In Cloud Computing:

Large scale data processing is increasingly common in Cloud Computing systems. In these systems, files are split into many small blocks and all blocks are replicated over several servers. High priority queue algorithm is used. To process files efficiently, each job is divided into many tasks and each task is allocated to a server to deal with a file block because network bandwidth is a scarce resource. In Cloud Computing, traditional way for task scheduling cannot measure the cost of cloud resources accurately by reason that each of the tasks on cloud systems is totally different between each other. There may be no relationship between the overhead application base and the way that different tasks cause overhead costs of resources in cloud systems. Poor cost control is the disadvantage. The traditional way for task scheduling cannot meet the cloud market well enough. An optimized algorithm for task scheduling based on ABC (Activity Based Costing) in Cloud Computing reduces the total time required to schedule the task.

III. Proposed System:

Smart grids have recently been adopted in electronic grid replacing traditional power grids. One of the reasons is that compared to traditional power grids, smart grids bring significant improvement in the efficiency, reliability, economics, and substantiality of electricity services. Power Grid is an electrical supply distribution network that carries electricity from a power plant to the user. The control center can hardly manage the mass data generated by future grid due to its storage bottleneck. For that in the future grid a phase measurement unit (PMU) is used, because it generates 50 or 60 phasor measurements per second. Cloud center develops a cloud-based collaborative direct load control framework, because big data cannot be fully transmitted to the control center due to the bandwidth limit. Providing information security for smart grids is very important since much of the information in smart grids is sensitive and needs to be strictly protected. Information leakage in smart grids can lead to vulnerabilities that affect not only individuals but also the whole nation because leaked information can be used to launch attacks to both individuals and the whole smart (power) grids at the national level. By employing cloud computing in smart grids, This not only address the issue of large information management but also provide a high energy and cost saving platform.

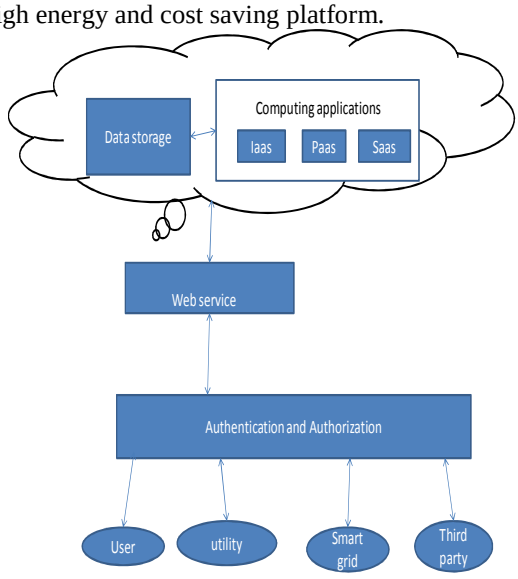


Fig. 1: System Architecture

It is because 1) the framework can scale very fast to deal with changes in the amount of processing information and 2) it can provide a high utilization of computing resources. Smart grid put Information and Communication Technology (ICT) into electricity generation, delivery and consumption, making systems cleaner, safer and more reliable and efficient.

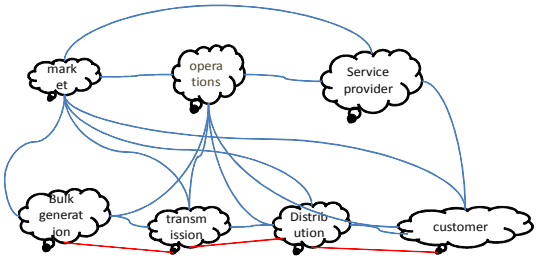


Fig. 2: Conceptual model of SG

Advantage:

- Reduce the workload
- Providing more accuracy
- Resource Provisioning is properly allocated
-

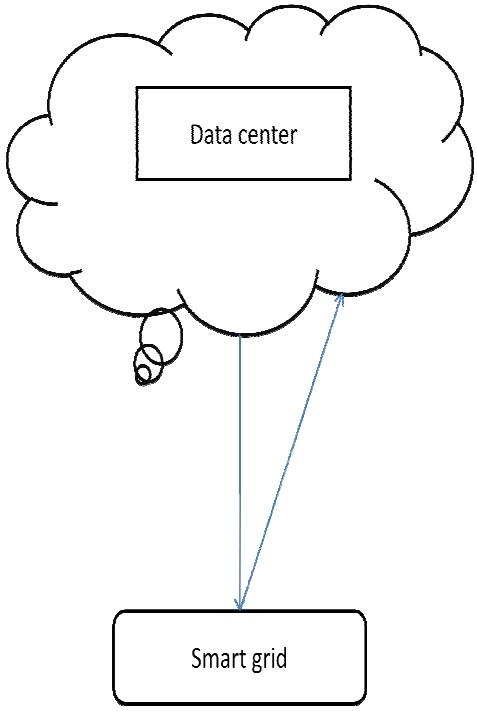


Fig. 3: Interaction Between Cloud Datacenter and Smart Grid

IV.Security Issues In Smart Grid:

A.Ddos Attack:

Distributed Denial of Service (DDOS) attack is a major threat for cloud computing environment. It makes the system unavailable to the legitimate users and adversely affects the availability requirement of the cloud computing. DDOS attack, in which an array of zombies, slaves, agents controlled by an attacker or bot-master are used against some target(s) to cause denial of service. This attack blocks the legitimate access to the servers, exhaust their resources such as network bandwidth, computing power and even lead to great financial losses. DDOS attack becames a major threat for cloud environment. Significant problem of DDOS attacks is that they are difficult to detect. DDOS is distributed, large scale coordinated attempt of flooding the network with large

amount of packets which becomes difficult for victim network to handle and hence the victim sever becomes unable to provide the services to its legitimate user.

B.Defense Methods Against Ddos Attack:

To address this problem a model is proposed based on hop count filtering (HCF) and confidence based filtering (CBF) methods.

Hop Count Filtering (Hcf) Method:

Hop Count (HC) is defined as the number of hops a packet traverses as it moves from the sender to the receiver. HC is not usually sent in the IP packet but is rather inferred from the IP Time-to-Live Field (TTL). The main function of IP TTL field is to prevent packets from looping forever. Usually, initial TTL values are operating system dependent and are limited to few possibilities. Guessing the initial TTL set by the OS is possible without explicitly knowing what the OS is. It can even be used to prevent Distributed Denial of Service attacks.

Three steps to Hop-Count computation and filtering of spoofed packets

Step1: Calculate the initial TTL of the packet which has reached the destination by extracting the final TTL of the packet from the IP header of the connection packet.

Step 2: The hop-count value can be calculated by subtracting the final TTL and the initial TTL value of the packet extracted given Hop-count = Initial TTL – Final TTL.

Step 3: IP2HC table is used to index between the source IP address and the corresponding hop-count value which is maintained in the cloud server. The rules are written in the cloud server to identify the spoofed packets from the legitimate ones. The SYN=0 represents the SYN filed is not set and if 1, it is clear that is set.

2.Confidence Based Filtering (Cbf) Method:

A Confidence-Based Filtering method, named CBF, is investigated for cloud computing environment, in this paper. This method is deployed by two periods, i.e. non-attack period and attack period. More specially, legitimate packets are collected in the non-attack period, for extracting attribute pairs to generate a nominal profile. With the nominal profile, the CBF method is promoted by calculating the score of a particular packet in the attack period, to determine whether to discard it or not. In this method, creating a normal profile according attribute pairs inside the TCP and IP header. This method included discarding threshold which always compared with a CBF score for using at the attack period time. Because it is not based on attack severity the performance of this method is better than packet score. The CBF score for the packet is given by:

$$\text{CBF score} = \sum_{I=1}^{n} (\text{confidencevalue} * \text{weightofattribute}) / \text{Total weight}$$

a) Non-Attack Period:

Step 1: In the non-attack period, the main target is to generate nominal profile. For incoming packets, this method firstly extracts the required attribute value pairs from them.

Step 2: To calculate the number of appearances of these value pairs will be counted and their confidence values calculated. Then these confidence values are used to update nominal profile.

b) Attack Period:

Step 1: In the attack period, most packets are not legitimate, so CBF will stop generating nominal profile. Like in the non-attack period, extracting the attribute value pairs from the incoming packets is the first step. With these value pairs, our method searches nominal profile for their confidence values in legitimate flows. Then CBF score, the filtering criterion, is calculated using weighted average of the confidence of the attribute value pairs in it.

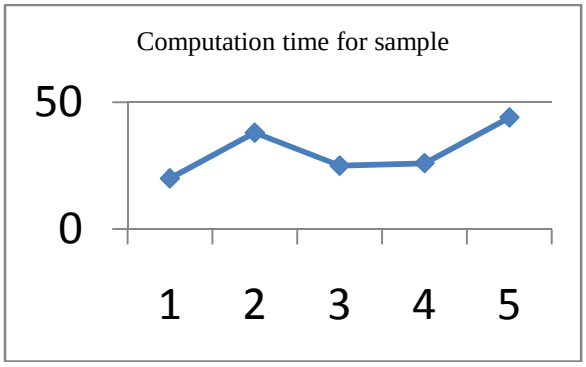
Step 2: After a packet discarding strategy is selected, CBF will judge the legitimacy of the packet based on CBF legitimate packets, and decide to let it pass or not.

V. Experimental results:

The experimental results are shown in the table for computation time. The sample inputs are taken as a arrival rate ‘A’ and various results has been analyzed.

Table I: Sample Inputs

Sample	Sample input (arrival rate in packet/sec)	Computation time(in ms)
1	1000	20
2	2000	38
3	4000	25
4	6000	26
5	8000	44



Discussion:

In this paper, Clouds and Grids share a lot of commonality in their vision, architecture and technology, but they also differ in various aspects such as security, programming model, business model, compute model, data model, applications, and abstractions. In building this distributed "Cloud" or "Grid", we will need to support on-demand provisioning and configuration of integrated "virtual systems" providing the precise capabilities needed by an end-user In order to reduce the total power consumption by cloud computing environments, this paper first has identified the need of the collaboration among servers, communication network and power network.

Conclusion:

The use of cloud computing environment in smart grid is one of the useful techniques to overcome the issues related to traditional power grid management. Neither the energy nor the computing grid will look like electric power grid. Thus, the integration of cloud computing in smart grid is envisioned to be useful for evolving smart grid architecture in terms of computing, power management and security.

REFERENCES

Bitzer, B. and E. Gebretsadik, 2013. "Cloud computing framework for smart grid applications," in *Proc. Power Eng. Conf.*, Dublin, Ireland, pp: 1-5.

Canetti, R. and H. Krawcyzk, 2001. ''Analysis of key-exchange protocols and their use for building secure channels," in advances in cryptology-EUROCRYPT (LNCS 2045). Berlin, Germany: springer-verlag, apr. pp: 453-474.

Cao, Q., Z. Wei and W. Gong, 2009. ''An optimized algorithm for task scheduling based on activity based costing in cloud computing," in proc. 3rd Int. conf. Bioinformat. Biomed. Eng., Beijing, China, pp: 1-3.

Dou, W., Q. Chen and J. Chen, 2013. "A confidence-based filtering method for DDoS attack defense in cloud environment," *Future Gener. Comput. Syst.*, 29(7): 1838-1850.

Foster, I *et al*., 2008. ''Cloud computing and grid computing 360-degree compared," in proc. Grid Comput. Environ. Workshop, Austin, TX, USA, pp: 1-10.

Gunjal, P. and S. Tamhankar, 2013. "Review of attack detection scheme for cyber physical security system," *Int. J. Comput. Sci. Mobile Comput.*, 2(12): 401-405.

Kim, H., Y. Kim, K. Yang, and M. Thottan, 2011. "Cloud-based demand response for smart grid: Architecture and distributed algorithms," in Proc. Int. Conf. Smart Grid Commun., Brussels, Belgium, pp: 398-403.

Lo, C., C. Huang and J. Ku, 2010 "A cooperative intrusion detection system framework for cloud computing networks," in *Proc. 39th Int. Conf. Parallel Process. Workshops*, San Diego, CA, USA, pp: 280-284.

Luo, F. *et al*., 2012. "Hybrid cloud computing platform: The next generation IT backbone for smart grid," in Proc. IEEE PES Gen. Meeting, San Diego, CA, USA, pp: 1-7.

Mohsenian-Rad, A. and A. Leon-Garcia, 2010 "Coordination of cloud computing and smart power grids," in *Proc. 1st Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, pp: 368-372.

Nagata, T. and H. Sasaki, 2002. "A multi-agent approach to power system restoration," *IEEE Trans. Power Syst.*, 17(2): 457-462.

Pibernik, R., Y. Zhang, F. Kerschbaum and A. Schropfer, 2011. "Secure collaborative supply chain planning and inverse optimization—The JELS model," *Eur. J. Oper. Res.*, 208(1): 75-85.

Rusitschka, S., K. Eger and C. Gerdes, 2010. "Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain," in *Proc. 1st Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, pp: 483-488.

Suresh, K. and K. Prasad, 2012. "Security issues and security algorithms in cloud computing," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 2(10): 110-114.

Thomas, C., T. Cui and F. Franchetti, 2013. "Privacy preserving smart metering system based retail level electricity market," in *Proc. Power Energy Soc. Gen. Meeting*, Vancouver, BC, Canada, pp: 1-5.