International Journal of Computer Science and Engineering Communications
Volume.4, Issue.4 (2016): Page.1435-1444
www.scientistlink.com/ijcsec

DDTA- DDoS Defense Techniques and Attributes to Integrate Smart Grid and Cloud

S.Ezhilarasi,
Assistant Professor,
Department of Computer Science and Engineering,
Roever Engineering College,Perambalur, India.
Email: ezhilarasise@gmail.com

Abstract—Smart Grid (SG) constitutes business and operational challenges for utility companies and energy suppliers and those are easily met by Cloud Computing (CC). From the distributed property of CC and SG it is unable to be avoided that the two methodologies will become integrated. Here I discuss about the opportunities and risks that CC gives to utility companies and energy suppliers, and consider what inseparable elements of CC may be capable of improving Distributed Denial of Service (DDoS) defense for SG. A prolonged literature survey is executed to identify which DDoS defense methods can be raised by CC and used to defend the SG. I propose that, when risks are suitably mitigated, the deployment of CC is known to be overall advantage, where its inseparable elements can be combined to make the SG highly secure and help in mitigation of a crippling DDoS attack.

Keywords—Smart Grid, Cloud Computing, Cyber Security, DDoS attack, DDTA

I. INTRODUCTION

The smart grid (SG) is an electric grid which has overlay of a communication grid to achieve high visibility that is able to improve its resilience and efficiency and also easy integration of surrogate energy sources at micro level [1]. The SG is used to link together our homes, vehicles, electronic devices, and businesses into a large, intelligent network [2]. Methodologies such as Smart Home technology, SCADA, corporate networks, the Advanced Metering Infrastructure (AMI) and other Industrial Control Systems (ICS) will all communicate with one another to distribute, monitor and control electricity [3]. A fully realized SG will influence these methodologies maximize the reliability of energy distribution and generation, decentralize energy generation [4].

Cloud Computing (CC) is advised as a possible solution for the energy industry to store and process the data that is aggregated by the AMI [5]. CC is a cost efficient computing solution that has several advantages involving, but not limited to, reliability, scalability, device location independence replication and security [4]. Considering the enactment of CC by utility companies and energy suppliers I explore how specific elements of CC could be influenced to actively secure the SG against one of the most disastrous types of cyber-attacks, known as distributed denial-of-service attack (DDoS).

As a fault-finding infrastructure, the SG must be functional under all circumstances [6]. The complexity and diversity of the automation systems and communication networks make the SG susceptible to cyber-attacks like DDoS [6]. Maligned efforts to disturb communication between SG elements could result in many negative effects such as loss of service, delays and physical damage [7], [8]. New approaches are being made to secure the SG data and infrastructure against malicious intent [9], and given how sensitive and detailed this type of data can be [10], countermeasures to secure privacy of paramount concern [8].DDoS attacks are carried out with the intention of suspending or interrupting the communication capacity [11], [12] of any service or networked device by draining the bandwidth or memory of the targeted device [7]. They have been identified as an important concern to the SG [13] since the level of technical ability needed to handle them is low and they are easy to apply. The number of DDoS attacks have increased, and their asperity has increased, excelling traffic volumes of 100Gbps [14]. There are many DDoS defense techniques that, when connected with a quick defensive reaction [15] and easily scalable computing resources, can be efficient at mitigating the asperity of attacks. I explain about the elements of CC that could be used to improve these methods in the fact of a DDoS attack on SG. Based on an elongated survey of the literature, I propose that CC may be influenced to improve DDoS defense for the SG and its aiding infrastructure. The paper is developed such as to describe the CC opportunities and challenges for SG and describe the main benefits and potential risks of integrating CC into SG, describe how a DDoS could be carried out against the SG and how CC can improve existing DDoS defense techniques.

II. SMART GRID

The smart grid is described as an electricity network that is able to intelligently combine the actions of all users linked to it consumers, generators and those that do both – in order to effectively deliver secure, economic and sustainable electricity supplies ".A Smart Grid is a intricate infrastructure consist of seven main domains as given in Fig.1.

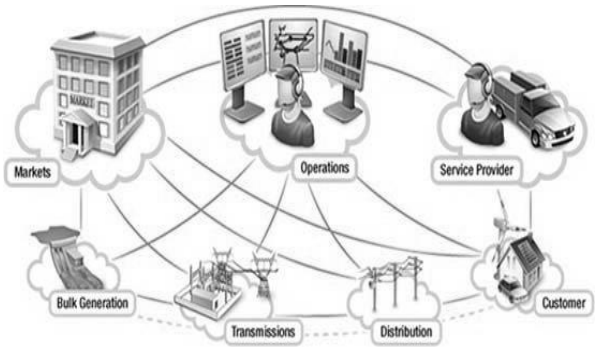

Fig1. Smart Grid

Bulk generation is the first step in the electricity supply to customers. *Markets.* The information management supplies information base for the optimization and analysis. *Service providers.* The actors accomplish a number of functions that support the business processes *Operations.* The typical applications carried out within the Operations domain *Transmission* is the large transport of electricity from sources to destination through multiple stations *Distribution.* This domain is electrically connected with the customer and transmission system. *Customers* are granted to regulate their generation, energy usage and storage. The smart grid systems suggest meaningful benefits for society: information availability and greater efficiencies can provide greener energy generation and it is cheaper, less loss in transmission and energy storage, better recovery and fault isolation

A. Interactions between SG and CC

Data centers, with storage capacities and massive computation, are key attributes of the cloud computing. Data centers have a great impact on the electric grid by enhancing the load at their locations. In order to decrease their greater energy utilization and with the cooling complications that datacenters have, cloud servers determined to use some creative approaches of housing their centers functions. Interactions between SG and CC are shown in Fig.2.

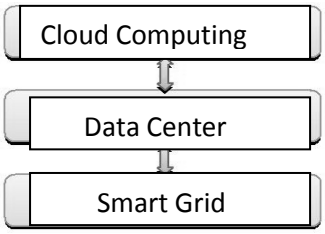

Fig 2 . The interactions between cloud computing, data centers, smart grid

The Smart grid application in the cloud is shown in fig.3

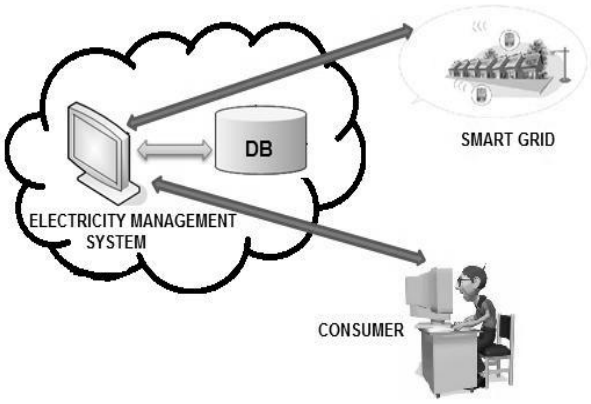

Fig 3. Electricity management in smart homes.

III. CLOUD COMPUTING THREATS AND OPPORTUNITIES FOR SMART GRID

Energy suppliers will have to compete with a major shift away from a model of consolidated electricity generation at huge nuclear power plants or fossil fuel burning , to one where generation will appear in smaller, widely-scattered pockets of renewable energy sources [16]. Linked with the improved communication among customers, energy suppliers, and utility companies the SG is capable of reacting to shifts in electricity claim in real-time. The SG is a overlay of a communication grid over the power grid where operational sensor data and fine grain usage data is combined from the grid and prepared to increase resilience, reliability and operational efficiency. As a result of this new example, energy suppliers are granted with various new challenges [12], such as how to compromise with an excessive amount of data composed from advanced metering technology, how to track number of scattered sources of energy generation, and the relevant security and privacy issues for each [17].

There are basic risks related with the integration of CC into the SG, because CC was not really made for high-assertion applications where security and consistency of data has been the primary responsibility [18]. In the fact of a communications interruption or system failure , Cloud Service Providers (CSPs) need to assure that data integrity is preserved and lost data is rectifiable. Issues with the latency of CC services and applications, such as degree of latency and variability need to be mitigated [19]. CSPs have to determine the location of data in the cloud while establishing data segmentation, encryption and granular access control are imposed [20]. Active auditing controls and security measures have to be determined in service level agreements to establish confidentiality, data reliability and auditing capabilities are maintained [4]. Most essentially, CC confide on the Internet, a technology that is naturally unreliable and prone to corruption activity [6]. If CC is to be used for SG it will be needed to accomplish higher levels of reliability and security within the present Internet infrastructure.
Integrating CC into SG is a realistic business model for energy suppliers to grapple with the processing capabilities and storage prescribed of a fully realized SG [19], [21], [22]. CC offers utility companies and energy suppliers events, such as: functioning their services at a lower cost by taking leverage of economies of scale; real-time reaction for demand management and control signals; automation services that are accessible as a service; faster implementation of disaster recovery and security distributions through virtualization [23]; and scalable resources that can adjust to changes in demand. Most basically, CC provides utility companies and energy suppliers the capability to outsource resource intensive tasks to the cloud [5].

These merits connected with a hybrid deployment, mixing private cloud and community cloud, could accomplish high privacy and security standards for SG [24], [4]. Further, the deployment of CC provide utility companies and energy suppliers approach to computing resources that could head to enhanced or new services, the development of operating efficiencies and new business models. Given this, it is sensible to consider how some of the basic elements of CC can reduce the crippling impact of a DDoS attack made adjacent to a fully realized SG. There are various basic CC attributes that make it appropriate for the SG..

First, CC supports a highly frisky system that can quickly adjust to changes in processing needs or data storage. As an impact, new features or further services are achieved by utility companies or energy suppliers can be made without disturbing existing services [4]. Second, with a robust network, the impacts of natural calamities can be reduced by shifting networking and processing needs to other unaffected locations of fully realized SG [3]. Backing up entire sets of data or spreading out portions of data in many locations raise the capability of the system to recoup from disturbing events [3]. Third, even though geographically varied, the CC would act as a centralized processing infrastructure acquiring greater utilization than distinctive energy suppliers performing their own data processing [19]. The flexibility of computing resources would assist customers accord with unexpected growth in data load. When data load levels recoil to normal, the additional computing power will be retired [22]. Fourth, critical CC systems can be deployed to self-heal, has the ability to diagnose, detect and react to software disruptions or infrastructure [25]. Self-healing systems have the capability to react to operational disruptions or environmental in real-time, greatly reducing or eliminating the need for human intervention. Fifth, when maintenance is needed on cyber-physical systems, virtualization would grant for the SG systems to perform without service interruptions when [26] applying secure configurations, installing new patches or performing security upgrades. Making use of virtual machines (VMs) on SG systems evolve into less risky on account of the installation of special software is not needed to perform computations or run applications. Table I summarizes the potential benefits of integrating CC into SG.

TABLE.I. BENEFITS OF INTEGRATING CC INTO SG

Cc Attribute	Potential Benefit
Agility and redundancy	Adapt to fluctuations , Low storage costs
Device and location independence	Resilience, Low operation costs, Location geographic independence
Real time response and elastic performance	Energy demand fluctuation response, electricity distribution/delivery
Self-healing	Robustness and endurance of SG
Virtualization and automation services	Faster response time, disaster recovery, deployment of security implementations

IV. ENHANCEMENT OF DDOS DEFENSE TECHNIQUES BY CLOUD COMPUTING

The complexity and physical size of the SG increases its susceptibility to DDoS attacks. An attack could be done against several the grid components, involving but not limited to, networking devices, smart meters, communication links, infrastructure control systems and energy supplier servers [2]. A DDoS attack across a portion of the SG infrastructure would disturb the communications network causing disturbance in remote or automated services, electricity distribution and delivery or energy usage forecasting [2]. This could head to wide-scale blackouts, leak of customer data and the devastation of the cyber-physical infrastructure [12]. Further, there are legal and financial implications for energy suppliers in the fact that customer data is stolen, lost or if billing data is falsified [12].

DDoS attacks can likely influence every layer of the OSI model, but the reduction of large scale DDoS attacks occur over layers 3, 4 and 7. My analysis targets on attacks carried out over layer 4 and 7, because of their recent increase in popularity and complication at defending and reducing their
effects. A DDoS attack commencing from malware affected SG devices that is performed over these layers could have major impacts to the processes of the SG [6]. Fig. 4 shows how a DDoS attack could be performed over SG through malware affected smart appliances over the OSI application layer, intending industrial control systems and corporate networks of utility companies or energy suppliers.

There are various techniques to secure against DDoS attacks [27], but my study is limited to the DDoS defense techniques that can be increased by utilizing the basic elements of CC. Assuming that CC is a fully unified component of SG, to the extent that CC is not just for utilizing data storage, but also virtualizing software for energy suppliers, data processing, consumers, utility companies, industrial control systems and integrating corporate networks. [28] classifies DDoS defense techniques into four different types i) attack prevention, ii) attack detection, iii) attack source identification, and iv) attack reaction.

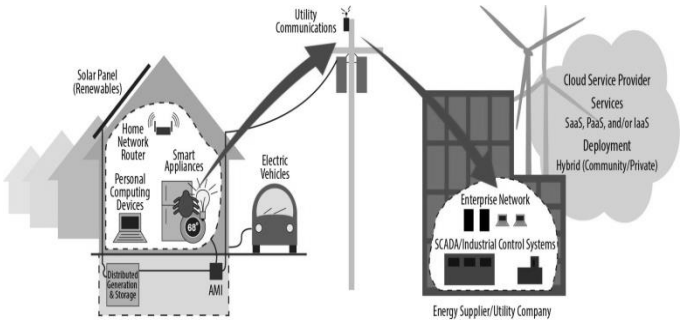

Fig 4. DDoS Attack over Application Layer from Malware Infected SG Connected Device

A. Attack Prevention Defense Mechanisms

Attack prevention methods try to stop DDoS attacks before they can reach their goal, generally through the use of different packet filtering techniques [11], [29]. Methods such as router-based packet filtering and ingress/egress filtering are efficient for small scale attacks, but in widely distributed, large DDoS attacks, they are limited even when if source of

the attack is well-known [28]. While the capability of filtering techniques is questionable, particularly for OSI layer 7 attacks, utility companies and energy suppliers could utilize honeypots and honeynets to achieve intelligence of possible DDoS attacks. Honeypots are systems composed with less security to trick would-be attackers to point them as a substitute of the actual system [30]. Honeypots could take leverage of CCs capability to duplicate services and virtualize servers [31]. Classically, high-interaction honeypots have been costly to manage, particularly when virtualization is not available. The development of an array of honeypots with various configurations, to identify susceptibilities from malware, replication vectors, and databases could be cheaply achieved, be limited resource intensive, and be rebuilt faster if compromised. In combination with a robust network intrusion detection system (IDS), honeypots can be actively dispersed across VMs to reduce computational overload, and play a vital role in a related DDoS defense strategy [31], [26].

B. Attack Detection

Detection techniques need to be capable of identifying attacks in real time as well as post event. Detection of DoS attacks is generally based on network data analysis such as connection requests, packet headers, etc to identify anomalies in traffic patterns and traffic imbalance rates [32]. The detection system must be capable of differentiating between malicious traffic and legitimate, keeping false positives results less so that legitimate users are not getting affected. Further, these methods must have short detection time and good system coverage[33]. Further, if authentication methods for SG attached devices are negotiated, attack source detection methods may establish very useful at identifying malicious activity [16].

DoS Attack Specific Detection

DoS-Attack-Specific Detection is used to identify attacks that accomplish the Transmission Control Protocol (TCP) across OSI layer 4. DoS Attack Specific detection techniques try to detect when incoming traffic is not reciprocal to outgoing traffic, the traffic is unstable statistically, or the attack flow does not have occasionally behavior [34]. The detection techniques has less success against DDoS attacks [28], on account of each compromised host can firmly mimic a legitimate user as it is not necessary to manage the traffic pattern of a single host. considering that the basic features of the attack are able to be identified early, elastic computing resources could harden SYN flood defense techniques [35], and critically be used to influence an intentional rise in attack strength. The geographic difference of cloud resources could be an advantage, using data from both first-mile and last-mile routers all over a CSPs network to indicate the attack source and support ingress or egress filtering. This, connected with redundant resources capable of performing packet state analysis, would reduce the amount of time required to shut out illegitimate traffic [36].

Anomaly-Based Detection

Anomaly-Based Detection targets at identifying distortion in traffic patterns on OSI application layer that do not match normal traffic patterns aggregated from training data. This detection approach has less success against DDoS attacks because of the perceived legitimacy and size of BOTNETs. Anomalies are not identified when traffic seems to adhere to normal traffic patterns. This method may only be efficient if distortions can be identified regarding the percentage of new IP addresses or geographical location of IP addresses seen by the victim [28]. Traditional data from across geographic difference CSP resources may create anomaly detection methods more efficient by giving a more robust dataset for analysis. The elastic performance and frisky capabilities of CC may provide more resilient mitigation algorithms, such as an adjustable system for identifying XML and HTTP application layer attacks [37], and SOTA [38] to reduce DX-DoS and X-DoS attacks.

C. Attack Source Identification

This method tries to identify where DDoS attacks are emerging from. These methods are more dependent on the Internet router infrastructure, and on account of DDoS attacks emerge from various geographical locations, different traceback methods are not efficient against DDoS attacks. The hash-based IP traceback technique is worth mentioning as it has been shown to be efficient against DDoS attacks, with some caveats [39]. The network topology capabilities offered by CC and SG [13] may provide new attack source identification methods that succeed where classical traceback methods have fallen less [29]. For hash-based IP Traceback to be efficient, it requires a wide geographic dissemination of recent traceback routers and a great amount of computing overhead to determine packet data, particularly over large amount of time [39]. Considering that CSPs have more distribution of traceback routers all over their network, and that cloud

resources are dispersed geographically, IP Traceback could be leveraged of the redundant and frisky resources present in CC. The redundant and frisky computational capabilities could be leveraged for packet filtering methods working in combination with other DDoS defense mechanisms [40] to maintain SG services, and accomplish data analysis from traceback routers on the CSP network to support ingress and egress filtering.

D. Attack Reaction

These methods try to eliminate or reduce the impact of a DDoS attack. For the future SG, this is an essential feature to protect the SG from being fully paralyzed by an attack [3]. Techniques involve but are not limited to duplicating network resources, filtering out bad traffic or transactions to reduce the abuse of computational resources or designating costs to certain processes. CC provides several opportunities to increase these capabilities, enhancing their endurance and capacity.

History-based IP filtering (HIP)

HIP is a technique where routers grant incoming packets when they are checked against a pre-populated IP address database [41]. This protection technique is deemed meaningless if devices with a valid purpose on the SG are negotiated and actually used as part of a BOTNET [42]. HIP filtering defense could influence the geographic dispersion, elastic performance and agility of CC, but more detail would be required about how CSPs would implement the checking process for IPs to know when and how this would be a benefit.

Load balancing

This method is done when there is a necessity to rise the available server operations for critical systems to secure them from shutting down in the impact of a DDoS attack [42]. Load balancing has the ability to make use of computational resources over distributed networks [43], readily making use of basic abilities of CC, such as redundancy and agility, elastic performance and real-time response, and automation services and virtualization [43]. There are threats to overcome, such as the latency, cost of the distributed computational load, and computational bottlenecks, but if correctly implemented, the merits of load balancing could be used by CSPs to reduce the impact of a DDoS attack done against the SG.

Selective pushback

This method ties to separate the data stream adjacent to the DDoS attack source by identifying the source of the attack and dispatching the location data to all upstream routers [33]. When attack traffic is legitimately distributed, or the attack origin IP is spoofed, events of filtering attack traffic become crucial [28]. Regardless of the exact method used to observe packets legitimacy and network congestion, the target of the pushback method is to separate the bad traffic as adjacent to the source of the attack as possible. CC would be developed indirectly, likely with IP Traceback and DoS Attack Specific Detection, taking advantage of geographic diversity, agility and elastic performance to increase the capability of push-back methods such as the cooperative pushback technique given by [33].

Source-end reaction

Source-end reaction methods, like D-WARD, attempt to catalog data flow statistics by uniformly monitoring the two-way traffic between the rest of the Internet and source network. Statistics are accumulated such as the ratio of out-traffic and in-traffic, and total number of connections per destination. The system regularly compares aggregated data against legitimate flow data models for each and every type of traffic that the source network receives, and if a disparity occurs, traffic is either rate-limited or filtered. Barring privacy issues, the frisky CC could be influenced with automation services and virtualization to catalog the traffic between SG infrastructure, utility companies, CSP resources and infrastructure control networks, providing a robust dataset that could be used to secure the SG infrastructure. Further, the elastic performance of CC could be influenced quickly and efficiently compare new data and historical to identify distortions and create a quicker attack responses.

Event logs

Determination of traffic data tries to detect forensic information in event logs that can detect the particular patterns and features of a DDoS attack [41]. This type of defense only works if a DDoS against the system has happened, data was able to be accumulated and analyzed, and defense techniques have been made to throttle or separate future attack traffic [42]. Event logs from server logs, firewalls, and honeypots would be examined to determine the elements of future DDoS attacks [41]. CC attributes such as real-time response, agility, elastic performance, automation services and virtualization could be used to increase the capacities of event log analysis, in extension to applying configuration updates to honeypots and automating security patches to firewalls based off of investigation results.

Fault Tolerance

Fault Tolerance methods considers that it is not possible to stop or prevent DDoS attacks fully, and rather focus on reducing the effects of attacks so the damaged network can remain operational. The technique is based on duplicating network services and varying the points of access to the network. In the impact of an attack, the crowdedness caused by attack traffic will not take down all of the damaged network. Related to that of fault tolerance, load balancing methods could influence CC attributes, such as redundancy and agility, elastic performance and real-time response, and automation services and virtualization to duplicate services and keep the SG network responsive for normal traffic.

Resource Pricing

Resource Pricing is a mitigation mechanism that makes use of a payment protocol and distributed gateway architecture to establish a dynamically changing computational burden or cost for initiating various types of network services. This method favors users who behave well, and segregates against users who abuse system resources, by separating services into pricing tiers to refrain malicious users from flooding the system with false requests to pursuit price manipulation. The high elastic performance and agility inherent in CC would mitigate the computational burden of Resource Pricing methods. As the demand of selecting prices to users grows, the computational demand would be easily reduced by the capability of CSPs to add further computing resources. Cost levels could easily be designated to put users into a cost hierarchy, and virtualization capacities could be used to duplicate network resources and infrastructure capacities, separating users paying various cost levels into different processing areas. Unauthorized traffic would be sectioned off from the normal traffic, mitigating the effect of an attack, and if necessary, be geographically independent.

E. Other Approaches to Consider

Even before CC was appropriately branded as such, it was contended that isolated defense techniques fail to offer performance guarantees over DDoS attacks. This would need a paradigm shift, where systems acting in seclusion would rather act as a distributed infrastructure of non-stratified, specific defense nodes linking with each other to accomplish an overall level of improved defense against DDoS attacks. Distributed control architectures, like ENERGOS project, introduces a multi-layered system of intelligent nodes that comprises enough operational information to process difficult tasks if there is a stratified breakdown of communication. The caveat of this method needs the opportunity of advanced processing capacities and a networked architecture robust enough to aid big data streams.

Table II summarizes the DDoS defense techniques that can be increased by make use of the CC attributes to defend SG over DDoS attacks.

TABLE II. Defense Techniques & Cc Attributes

DDoS Attacks	Defense Technique	CC Attributes
SYN Flood (TCP), Smurf Attack, PDF GET, HTTP GET, HTTP POST	Honeypots	AR, SH, V
SYN Flood, Smurf Attack	DoS-Attack-Specific Detection	AR, DLI, RREP
PDF GET, HTTP GET, HTTP POST	Anomaly-Based Detection	AR, DLI, RREP
SYN Flood, Smurf Attack; PDF GET,	Hash-Based IP Traceback	AR, DLI

HTTP GET, HTTP POST		
SYN Flood, Smurf Attack; PDF GET, HTTP GET, HTTP POST	HIP Filtering	AR, DLI, RREP
	Load Balancing	AR, RREP
	Selective Pushback	AR, DLI, RREP
	Source-End Reaction	AR, RREP
	Analysis of Traffic Data	AR, RREP, SH, V
	Fault Tolerance	AR, DLI, RREP, SH, V
	Resource Pricing	AR, DLI, RREP, V

AR: Agility & Redundancy, SH: Self-healing, V: Virtualization, DLI: Device & Location Independence, RREP: Real-time Response & Elastic Performance

The comparative analysis with the application and without application of DDoS Defense Techniques and Attributes (DDTA) in Smart Grid is shown in Table.III

TABLE III. Comparative Analysis

	w/o DDTA in SG	**w/ DDTA in SG**
Scalability, Reliability	less	high
Replication	less	high
Device location independence	less	high
Diversity , complexity	vulnerable	No
Delays, loss of service, physical damage	occur	Does'nt occur
Communication capability	suspended	increased
Memory & bandwidth	saturated	Does'nt
Disaster recovery	slow	faster
Security, Confidentiality	less	high

IV. Conclusion

As modernizations to our personal devices, electric vehicles, automated homes continue to bridge the gap between physical and cyber the CC and SG will eventually become associated, if not integrated with one another. The conception of SG technology has presented utility companies and energy suppliers with threats that CC could readily meet, but not without reducing different CCs outstanding issues. Carelessness in the development of CC explanations for SG applications may provide an environment that is highly prone to cyber-attacks like DDoS. Unless isolated communications network is laid on top of the electrical grid [6], the hazards of a DDoS attack from those with pernicious intent, whether for financial benefit or to horrify our society remains a very real feasibility with serious consequences. The fault-finding nature of the SG means that a real defense result needs to be deployed to secure against DDoS attacks. Victims of DDoS attack requires an easily scalable technique that can quickly add further resources to defend over DDoS attacks. CC gives the capability of distributing this computational burden against a large pool of resources to recoup for a rapid raise in computational needs. Influencing the basic elements of the CC to help secure DDoS attacks may not be a constant solution, but it may be readily available solution to this need. While the integration of SG and CC is inevitable, the characteristics of CC can be influenced to improve defense against DDoS attacks.

References

[1] S. Goel, S. F. Bush, and D. Bakken, IEEE Vision for Smart Grid Communications: 2030 and Beyond. IEEE, 2013.

[2] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," Proceedings of the IEEE, vol. 100, no. 1, pp. 195–209, 2012.

[3] R. E. Brown, "Impact of smart grid on distribution system design," in
Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE. IEEE, 2008, pp. 1–4.

[4] M. Yigit, V. C. Gungor, and S. Baktir, "Cloud computing for smart grid applications," Computer Networks, vol. 70, pp. 312–329, 2014.

[5] X. Fang, D. Yang, and G. Xue, "Evolving smart grid information management cloudward: A cloud optimization perspective," Smart Grid, IEEE Transactions on, vol. 4, no. 1, pp. 111–119, 2013.

[6] S. Goel, "Anonymity vs. security: The right balance for the smart grid,"
Communications of the Association for Information Systems, vol. 36, no. 1, p. 2, 2015.

[7] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," Smart Grid, IEEE Transactions on, vol. 2, no. 4, pp. 782–795, 2011.

[8] J. Liu, Y. Xiao, S. Li, W. Liang, and C. Chen, "Cyber security and privacy issues in smart grids," Communications Surveys & Tutorials, IEEE, vol. 14, no. 4, pp. 981–997, 2012.

[9] A. Wokutch, "The role of non-utility service providers in smart grid development: Should they be regulated, and if so, who can regulate them?" Journal of Telecommunications and High Technology Law, vol. 9, p. 531, 2011.

[10] S. Iyer, "Cyber security for smart grid, cryptography, and privacy,"
International Journal of Digital Multimedia Broadcasting, vol. 2011, 2011.

[11] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, pp. 39–53, 2004.

[12] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," Computer Networks, vol. 57, no. 5, pp. 1344–1371, 2013.

[13] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," Smart Grid, IEEE Transactions on, vol. 4, no. 2, pp. 847–855, 2013.

[14] T. Karnwal, T. Sivakumar, and G. Aghila, "A comber approach to protect cloud computing against xml ddos and http ddos attack," in
Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on. IEEE, 2012, pp. 1–5.

[15] A. G. Tartakovsky, B. L. Rozovskii, R. B. Blazek, and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods," Signal Processing, IEEE Transactions on, vol. 54, no. 9, pp. 3372–3382, 2006.

[16] Z. M. Fadlullah, M. M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," Network, IEEE, vol. 25, no. 5, pp. 50–55, 2011.

[17] S. Goel, Y. Hong, V. Papakonstantinou, and D. Kloza, "Smart grid security," SpringerBriefs in Cybersecurity, 2015.

[18] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on. IEEE, 2009, pp. 44–51.

[19] E. Brynjolfsson, P. Hofmann, and J. Jordan, "Cloud computing and electricity: beyond the utility model," Communications of the ACM, vol. 53, no. 5, pp. 32–34, 2010.

[20] M. T. Khorshed, A. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Future Generation computer systems, vol. 28, no. 6, pp. 833–851, 2012.

[21] L. Zheng, S. Chen, Y. Hu, and J. He, "Applications of cloud computing in the smart grid," in Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011 2nd International Conference on. IEEE, 2011, pp. 203–206.

[22] D. S. Markovic, D. Zivkovic, I. Branovic, R. Popovic, and D. Cvetkovic, "Smart power grid and cloud computing," Renewable and Sustainable Energy Reviews, vol. 24, pp. 566–577, 2013.

[23] G. C. Wilshusen, Information Security: Federal Guidance Needed to
Address Control Issues with Implementing Cloud Computing. DIANE Publishing, 2010.

[24] F. Luo, Z. Y. Dong, Y. Chen, Y. Xu, K. Meng, and K. P. Wong, "Hybrid cloud computing platform: the next generation it backbone for smart grid," in Power and Energy Society General Meeting. IEEE, 2012, pp. 1–7.

[25] Y. Dai, Y. Xiang, and G. Zhang, "Self-healing and hybrid diagnosis in cloud computing," in Cloud computing. Springer, 2009, pp. 45–56.

[26] A. Bakshi and B. Yogesh, "Securing cloud from ddos attacks using intrusion detection system in virtual machine," in Communication Soft-ware and Networks, 2010. ICCSN'10. Second International Conference on. IEEE, 2010, pp. 260–264.

[27] M. Darwish, A. Ouda, and L. F. Capretz, "Cloud-based ddos attacks and defenses," in Information Society (i-Society), 2013 International Conference on. IEEE, 2013, pp. 67–71.

[28] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the dos and ddos problems," ACM Computing Surveys (CSUR), vol. 39, no. 1, p. 3, 2007.

[29] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed dos attack prevention in power-law internets," in ACM SIGCOMM Computer Communication Review, vol. 31, no. 4. ACM, 2001, pp. 15–26.

[30] L. Spitzner, Honeypots: tracking hackers. Addison-Wesley Reading, 2003, vol. 1.

[31] S. Biedermann, M. Mink, and S. Katzenbeisser, "Fast dynamic extracted honeypots in cloud computing," in Proceedings of the 2012 ACM Workshop on Cloud computing security workshop. ACM, 2012, pp. 13–18.

[32] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," Internet Computing, IEEE, vol. 10, no. 1, pp. 82–89, 2006.

[33] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and
S. Shenker, "Controlling high bandwidth aggregates in the network,"
ACM SIGCOMM Computer Communication Review, vol. 32, no. 3, pp. 62–73, 2002.

[34] T. M. Gil and M. Poletto, "Multops: a data-structure for bandwidth attack detection," in USENIX Security Symposium, 2001.

[35] S. R. Ghanti and G. Naik, "Protection of server from syn flood attack," Journal Impact Factor, vol. 5, no. 11, pp. 37–46, 2014.

[36] K. Choi, X. Chen, S. Li, M. Kim, K. Chae, and J. Na, "Intrusion detection of nsm based dos attacks using data mining in smart grid," Energies, vol. 5, no. 10, pp. 4091–4109, 2012.

[37] T. Vissers, T. S. Somasundaram, L. Pieters, K. Govindarajan, and
P. Hellinckx, "Ddos defense system for web services in a cloud environment," Future Generation Computer Systems, vol. 37, pp. 37–45, 2014.

[38] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against http-dos and xml-dos attacks," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1097–1107, 2011.

[39] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio,
S. T. Kent, and W. T. Strayer, "Hash-based ip traceback," in ACM SIGCOMM Computer Communication Review, vol. 31, no. 4. ACM, 2001, pp. 3–14.

[40] M. Sung and J. Xu, "Ip traceback-based intelligent packet filtering: a novel technique for defending against internet ddos attacks," Parallel and Distributed Systems, IEEE Transactions on, vol. 14, no. 9, pp. 861– 872, 2003.

[41] A. Mitrokotsa and C. Douligeris, "Denial-of-service attacks," Network Security: Current Status and Future Directions, pp. 117–134, 2007.

[42] C. Douligeris and A. Mitrokotsa, "Ddos attacks and defense mecha-nisms: classification and state-of-the-art," Computer Networks, vol. 44, no. 5, pp. 643–666, 2004.

[43] M. Randles, D. Lamb, and A. Taleb-Bendiab, "A comparative study into distributed load balancing algorithms for cloud computing," in Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on. IEEE, 2010, pp. 551– 556.