Using Features of Cloud Computing to Defend Smart Grid against DDoS Attacks

Anthony Califano, Ersin Dincelli, and Sanjay Goel
University at Albany, State University of New York
Albany, New York
Email: {acalifano, edincelli, goel}@albany.edu

***Abstract*—Smart Grid (SG) poses operational and business challenges for energy suppliers and utility companies that are readily met by Cloud Computing (CC). Given the distributed nature of SG and CC it is inevitable that the two technologies will become integrated. In this paper we discuss the risks and opportunities that CC presents to energy suppliers and utility companies, and consider what inherent attributes of CC may be able to be leveraged to improve Distributed Denial of Service (DDoS) defense for SG. An extended literature review is performed to determine which DDoS defense techniques can be enhanced by CC and utilized to defend the SG. We propose that, when risks are properly mitigated, the deployment of CC can be seen as an overall benefit, where its inherent attributes can be harnessed to make the SG more secure and help mitigate the threat of a crippling DDoS attack.**

Keywords*—*Smart Grid, Cloud Computing, DDoS, Cyber Security, DDoS Defense, Critical Infrastructure

I. Introduction

The smart grid (SG) is an overlay of a communication grid over the electric grid to gain greater visibility that can be leveraged to improve its efficiency and resilience as well as to ease integration of alternate energy sources at a micro level [1]. The SG will link together our homes, electronic devices, vehicles, and businesses into a giant, intelligent network [2]. Technologies such as Smart Home technology, the Advanced Metering Infrastructure (AMI), corporate networks, SCADA, and other Industrial Control Systems (ICS) will all communicate with one another to control, distribute and monitor electricity [3]. A fully realized SG will leverage these technologies and decentralize energy generation, maximizing the efficiency and reliability of energy generation and distribution [4].

Cloud Computing (CC) is suggested as a viable solution for the energy industry to process and store the data that is collected by the AMI [5]. CC is a cost effective computing solution that has many benefits including, but not limited to, scalability, reliability, replication, device location independence and security [4]. Considering the adoption of CC by energy suppliers and utility companies, we explore how specific attributes of CC could be leveraged to proactively protect the SG against one of the most devastating types of cyber-attacks, the distributed denial-of-service attack (DDoS).

As a critical infrastructure, the SG must remain functional under all circumstances [6]. The diversity and complexity of the communication networks and automation systems make the SG vulnerable to cyber-attacks such as DDoS [6]. Maligned efforts to disrupt communication between SG components could result in major negative effects such as delays, loss of service and even physical damage [7], [8]. New strategies are being developed to help protect the SG infrastructure and data against malicious intent [9], and given how detailed and sensitive this type of data can be [10], countermeasures to protect security and privacy are of paramount concern [8].

DDoS attacks are performed with the intention of interrupting or suspending the communication capability [11], [12] of any networked device or service by saturating the memory or bandwidth of the targeted device [7]. They have been recognized as a significant concern to the SG [13] as the level of technical prowess needed to conduct them is low and they are easy to implement. In fact, the number of DDoS attacks has begun to rise, and their severity has increased, exceeding traffic volumes of 100Gbps [14].

There are multiple DDoS defense techniques that, when coupled with a quick defensive response [15] and easily scalable computing resources, can be effective at mitigating the severity of attacks. We discuss the attributes of CC that could be used to enhance these techniques in the event of a DDoS attack on the SG. Based on an extended review of the literature, we propose that CC may be leveraged to enhance DDoS defense for the SG and its supporting infrastructure.

The paper is organized as follows: section two will describe the CC challenges and opportunities for SG and present the main potential risks and benefits of integrating CC into SG, section three will discuss how a DDoS could be performed against the SG and how CC can enhance existing DDoS defense techniques, section four presents concluding remarks.

II. Cloud Computing Challenges and Opportunities for Smart Grid

Energy suppliers will have to contend with a fundamental shift away from a model of centralized electricity generation at large fossil fuel burning or nuclear power plants, to one where generation will occur in smaller, widely-distributed pockets of renewable energy sources [16]. Combined with the enhanced communication between customers, utility companies, and energy suppliers, the SG will be able to react to shifts in electricity demand in real-time. The SG is a superposition of a communication grid over the power grid where fine grain usage data and operational sensor data is collected from across the grid and processed to improve operational efficiency, resilience, and reliability. As a result of this new paradigm, energy suppliers are presented with many new challenges [12], such as how to deal with an exorbitant amount of data collected from advanced metering technology, how to track many distributed sources of energy generation, and the related privacy and security issues for each [17].

There are inherent risks associated with the integration of CC into the SG, because CC was not originally designed for high-assurance applications where consistency and security of data has been the primary concern [18]. In the event of a system failure or communications interruption, Cloud Service Providers (CSPs) need to ensure that data integrity is maintained and lost data is recoverable. Issues with the latency of CC applications and services, such as variability and degree of latency need to be mitigated [19]. CSPs need to define the location of data in the cloud while ensuring encryption, data segmentation, and granular access control are enforced [20]. Strong security measures and auditing controls need to be defined in service level agreements to ensure data reliability, confidentiality, and auditing capabilities are preserved [4]. Most importantly, CC relies on the Internet, a technology that is inherently unreliable and prone to nefarious activity [6]. If CC is to be used for SG it may be necessary to achieve greater levels of security and reliability within the current Internet infrastructure.

Integrating CC into SG is a sensible business model for energy suppliers to grapple with the storage and processing capabilities required of a fully realized SG [19], [21], [22]. CC offers energy suppliers and utility companies opportunities, such as: operating their services at a lower cost by taking advantage of economies of scale; automation services that are available as a service; real-time response for control signals and demand management; faster deployment of disaster recovery and security implementations through virtualization [23]; and scalable resources that can adapt to fluctuations in demand. Most importantly, CC provides energy suppliers and utility companies the ability to outsource resource intensive tasks to the cloud [5].

These benefits coupled with a hybrid deployment, mixing community and private CC, could achieve strong security and privacy standards for SG [24], [4]. Additionally, the deployment of CC would give energy suppliers and utility companies access to computing resources that could lead to new or enhanced services, the creation of new business models, and operating efficiencies. Given this, it is prudent to consider how some of the inherent attributes of CC can help mitigate the crippling effects of a DDoS attack made against a fully realized SG. There are several inherent CC attributes that make it suitable for the SG..

First, CC provides a highly agile system that can quickly adapt to fluctuations in data storage or processing needs. As a result, additional services or new features implemented by energy suppliers or utility companies can be deployed without disrupting existing services [4]. Second, with a robust network, the effects of a natural disasters can be mitigated by shifting processing and networking needs to other unaffected portions of fully realized SG [3]. Spreading out portions of data or backing up entire sets of data in multiple locations increase the ability of the system to recover from disruptive events [3]. Third, even though geographically diverse, the CC would act as a centralized processing infrastructure gaining higher utilization than individual energy suppliers doing their own data processing [19]. The elasticity of computing resources would help customers deal with unexpected increases in data load. When data load levels return to normal, the extra computing power can be retired [22]. Fourth, critical CC systems can be designed to self-heal, having the capability to detect, diagnose, and react to infrastructure or software disruptions [25]. Systems that are self-healing have the ability to respond to environmental or operational disruptions in real-time, eliminating or greatly reducing the need for human intervention. Fifth, when maintenance is required on cyber-physical systems, virtualization would allow for the SG systems to operate without service interruptions when [26] installing new patches, applying secure configurations, or performing security upgrades. Utilizing virtual machines (VMs) on SG systems becomes less risky because the installation of special software is not required to run applications or perform computations. Table I summarizes the potential risks and benefits of integrating CC into SG.

TABLE I. MAIN POTENTIAL RISKS AND BENEFITS OF INTEGRATING CLOUD COMPUTING INTO SMART GRID

CC Attribute	Potential Risk	Potential Benefit
Agility & redundancy	Lack of efficiency in ability to scale up and down to match the demand. Costs associated with latency.	Ability to adapt to fluctuations and resource intensive tasks. Low storage costs due to economies of scale.
Device & location independence	Consistency of the data: Connectivity, latency and performance issues.	Resilience. Low operation costs. Location / geographic independence.
Real-time response & elastic performance	Consistency of the data: latency, performance, and data auditing issues, billing errors.	Quick response to fluctuations in energy demand ensuring proper electricity distribution/delivery.
Self-healing	Causes of errors / malfunctions may remain unknown. Self-repair may lead to system inefficiencies or data inaccuracy.	Would greatly enhance the robustness and endurance of SG systems.
Virtualization & automation services	Data security: Hypervisor and VM vulnerabilities and potential misconfigurations.	Faster response time, disaster recovery, and deployment of security implementations.

III. How Cloud Computing Can Enhance Existing DDoS Defense Techniques

The physical size and complexity of the SG increases its vulnerability to DDoS attacks. An attack could be performed against many of the grid components, including but not limited to, smart meters, networking devices, communication links, energy supplier servers, and infrastructure control systems [2]. A DDoS attack against a portion of the SG infrastructure would disrupt the communications network causing disruption in automated or remote services, energy usage forecasting, or electricity delivery and distribution [2]. This could lead to a leak of customer data, wide-scale blackouts, and the destruction of the cyber-physical infrastructure [12]. Additionally, there are financial and legal implications for energy suppliers in the event that customer data is lost, stolen, or if billing data is falsified [12].

DDoS attacks can possibly affect every layer of the OSI model, but the mitigation of large scale DDoS attacks occur over layers 3, 4 and 7. Our discussion focuses on attacks performed over layer 4 and 7, because of their recent rise in popularity and difficulty at defending and mitigating their

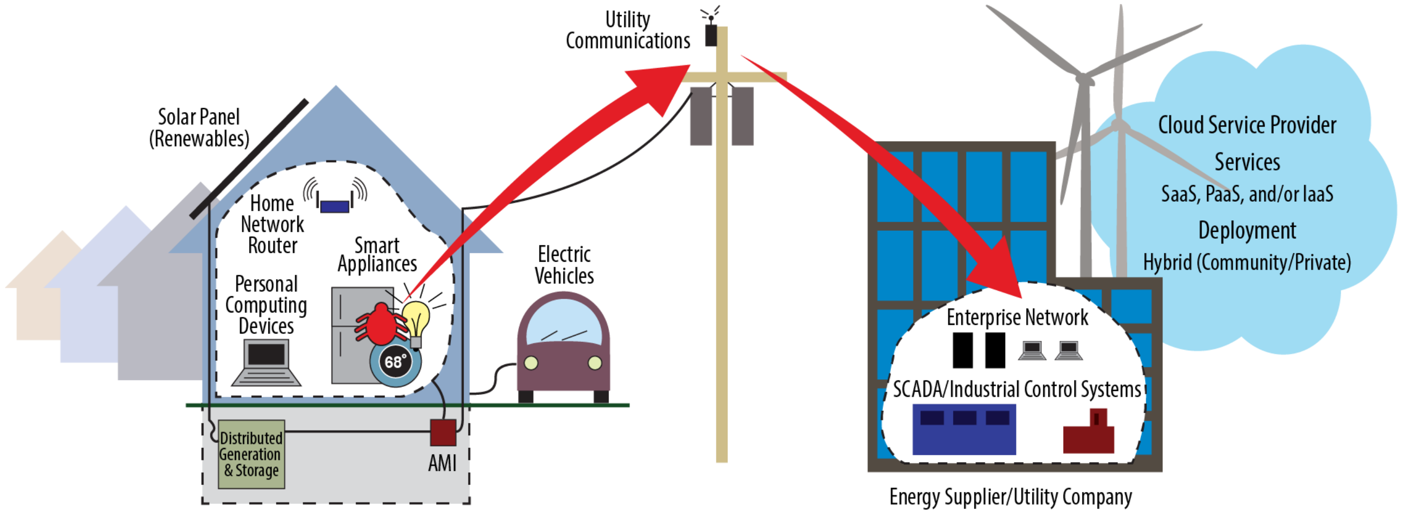

Fig. 1. DDoS Attack Risk over OSI Layer 7 from Malware Infected SG Connected Devicee

effects. A DDoS attack originating from malware infected SG devices that is executed over these layers could have major impacts to the operations of the SG [6]. Figure 1 illustrates how a DDoS attack could be executed over SG through malware infected smart appliances over the OSI layer 7 (application layer), targeting the corporate networks and industrial control systems of energy suppliers or utility companies.

There are many different techniques to defend against DDoS attacks [27], but our analysis is limited to the DDoS defense techniques that can be enhanced by utilizing the inherent attributes of CC. We are also assuming that CC is a fully integrated component of SG, to the extent that CC is not just being used for data storage, but also data processing, virtualizing software for energy suppliers, utility companies, consumers, and integrating corporate networks and industrial control systems. [28] categorizes DDoS defense techniques into four types: 1) attack prevention, 2) attack detection, 3) attack source identification, and 4) attack reaction.

A. Attack Prevention Defense Mechanisms

Attack prevention mechanisms attempt to stop DDoS attacks before they can reach their target, mostly through the use of a variety of packet filtering techniques [11], [29]. Methods such as ingress/egress filtering and router-based packet filtering are effective for small scale attacks, but in large, widely distributed DDoS attacks, they are ineffective even when the source of the attack is known [28]. While the effectiveness of filtering techniques is questionable, especially for OSI layer 7 attacks, energy suppliers and utility companies could utilize honeypots and honeynets to gain intelligence of potential DDoS attacks. Honeypots are systems configured with limited security to trick would-be attackers to target them instead of the actual system [30]. Honeypots could take advantage of CCs ability to virtualize servers and duplicate services [31]. Traditionally, high-interaction honeypots have been expensive to maintain, especially when virtualization is unavailable. The creation of an array of honeypots with different configurations, to detect vulnerabilities from malware, replication vectors, and databases could be implemented cheaply, be less resource intensive, and be restored more quickly if compromised. In conjunction with a robust network intrusion detection system (IDS), honeypots could be actively distributed across VMs to mitigate computational overload, and play an integral role in a coordinated DDoS defense strategy [31], [26].

B. Attack Detection

Attack detection techniques need to be able to detect attacks in real time as well as post incident. Identification of DoS attacks is primarily based on network data analysis (e.g. connection requests, packet headers, etc.) to detect anomalies in traffic patterns and imbalances in traffic rates [32]. The detection system must be able to differentiate between legitimate and malicious traffic, keeping false positives results low so that legitimate users are not affected. In addition, these methods should have good system coverage and a short detection time [33]. Additionally, if authentication schemes for SG attached devices are compromised, attack source identification schemes may prove very useful at detecting malicious activity [16].

DoS-Attack-Specific Detection is used to detect attacks that exploit the Transmission Control Protocol (TCP) over OSI layer 4 (e.g., SYN Flooding). DoS-Attack-Specific detection methods attempt to identify when incoming traffic is not proportional to outgoing traffic, the traffic is statistically unstable, or the attack flow does not have periodic behavior [34]. These types of detection techniques have had limited success against DDoS attacks [28], because each compromised host can closely mimic a legitimate user since there is no need to manipulate the traffic pattern of a single host. Assuming that the inherent features of the attack are able to be detected early, elastic computing resources could strengthen SYN flood defense mechanisms [35], and theoretically be used to instigate an intentional increase in attack strength. The geographic diversity of cloud resources could be leveraged, using data from both first-mile and last-mile routers throughout a CSPs network to pinpoint the attack source and aid ingress or egress filtering. This, coupled with redundant resources able to perform packet state analysis, would decrease the amount of time needed to shut out illegitimate traffic [36].

Anomaly-Based Detection aims at detecting irregularities in traffic patterns on OSI layer 7 that do not match normal traffic patterns collected from training data. This detection method has seen limited success against DDoS attacks because of the size and perceived legitimacy of BOTNETs. Anomalies are not detected when traffic seems to comply with normal traffic patterns. This technique may only be effective if irregularities can be detected regarding the geographical location of IP addresses or percentage of new IP addresses seen by the victim [28]. Historical data from across geographic diverse CSP resources may make anomaly detection techniques more effective by providing a more robust dataset for analysis. The agile and elastic performance capabilities of CC may enable more resilient mitigation algorithms, such as an adaptive system for detecting XML and HTTP application layer attacks [37], and SOTA [38] to further mitigate X-DoS and DX-DoS attacks.

C. Attack Source Identification

Attack source identification attempts to locate where DDoS attacks are originating from. These techniques are highly dependent on the Internet router infrastructure, and because DDoS attacks originate from different geographical locations, many Traceback schemes are not effective against DDoS attacks. The hash-based IP traceback method is worth mentioning as it has been shown to be effective against DDoS attacks, with some caveats [39]. The network topology possibilities offered by SG and CC [13] may enable new attack source identification schemes that succeed where traditional traceback schemes have fallen short [29]. For hash-based IP Traceback to be effective, there needs to be a wide geographic distribution of modern traceback routers and an abundance of computing overhead to analyze packet data, especially over long periods of time [39]. Assuming that CSPs have a large distribution of traceback routers throughout their network, and that cloud resources are spread out geographically, IP Traceback could take advantage of the agile and redundant resources available in CC. The agile and redundant computational capabilities could be leveraged for packet filtering techniques working in conjunction with other DDoS defense mechanisms [40] to sustain SG services, and perform data analysis from traceback routers on the CSP network to aid ingress and egress filtering.

D. Attack Reaction

Attack reaction techniques attempt to mitigate or eliminate the effects of a DDoS attack. For the future SG, this is a necessary feature to prevent the SG from being completely paralyzed by an attack [3]. Methods include but are not limited to filtering out bad traffic, duplicating network resources, or even assigning costs to certain processes or transactions to limit the abuse of computational resources. CC offers many opportunities to enhance these capabilities, increasing their capacity and endurance.

History-based IP filtering (HIP) is a mechanism where routers allow incoming packets when they are verified against a pre-populated IP address database [41]. This defensive method is deemed meaningless if devices with a legitimate purpose on the SG are compromised and being used as part of a BOTNET [42]. HIP filtering defense could leverage the geographic diversity, agility, and elastic performance of CC, but more detail would be needed about how CSPs would implement the verification process for IPs to know how and when this would be a benefit.

Load balancing is implemented when there is a need to increase the available server functions for critical systems to prevent them from shutting down in the event of a DDoS attack [42]. Load balancing has the capability to utilize computational resources across distributed networks [43], readily utilizing inherent abilities of CC, such as agility and redundancy, real-time response and elastic performance, and virtualization and automation services [43], [44]. There are challenges to overcome, such as the cost of the distributed computational load [45], latency, and computational bottlenecks [46], but if properly implemented, the benefits of load balancing could be used by CSPs to help mitigate the effects of a DDoS attack made against the SG.

Selective pushback attempts to filter the data stream close to the DDoS attack source by determining the source of the attack and sending the location data to all upstream routers [33]. When attack traffic is normally distributed, or the attack origin IP is spoofed, attempts of filtering attack traffic become difficult [28]. Regardless of the exact technique used to monitor network congestion and packets legitimacy, the goal of the pushback method is to filter the bad traffic as close to the source of the attack as possible. CC would be deployed indirectly, much like with DoS-Attack-Specific Detection and IP Traceback, taking advantage of agility, geographic diversity, and elastic performance to enhance the effectiveness of pushback schemes such as the cooperative pushback mechanism proposed by [33].

Source-end reaction schemes, such as D-WARD, attempt to catalog data flow statistics by constantly monitoring the two-way traffic between the source network and the rest of the Internet [47]. Statistics are collected such as the ratio of in-traffic and out-traffic, and number of connections per destination. The system periodically compares collected data against normal flow data models for each type of traffic that the source network receives, and if a mismatch occurs, traffic is either filtered or rate-limited [47]. Barring privacy issues, the agility of CC could be leveraged with virtualization and automation services to catalog the traffic between SG infrastructure, CSP resources, utility companies, and infrastructure control networks, creating a robust dataset that could be used to protect the SG infrastructure. Additionally, the elastic performance of CC could be leveraged to quickly and efficiently compare historical and new data to detect irregularities and generate a quicker attack responses.

Analysis of traffic data attempts to identify forensic information in event logs that can identify the specific features and patterns of a DDoS attack [41]. This form of defense only works if a DDoS against the system has occurred, data was able to be collected and analyzed, and defense mechanisms have been created to filter or throttle future attack traffic [42]. Event logs from firewalls, server logs, and honeypots would be analyzed to determine the attributes of future DDoS attacks [41]. CC attributes such as agility, real-time response and elastic performance, and virtualization and automation services could be used to enhance the capabilities of event log analysis, in addition to automating security patches to firewalls and applying configuration updates to honeypots based off of analysis results.

TABLE II. DEFENSE TECHNIQUES AND BENEFICIAL CLOUD COMPUTING ATTRIBUTES

Type of Defense	Type of Attack	Defense Technique	Beneficial CC Attributes*
Attack Prevention	SYN Flood (TCP), Smurf Attack, PDF GET, HTTP GET, HTTP POST	Honeypots	AR, SH, V
Attack Detection	SYN Flood, Smurf Attack	DoS-Attack-Specific Detection	AR, DLI, RPP
	PDF GET, HTTP GET, HTTP POST	Anomaly-Based Detection	AR, DLI, RPP
Attack Source Identification	SYN Flood, Smurf Attack; PDF GET, HTTP GET, HTTP POST	Hash-Based IP Traceback	AR, DLI
Attack Reaction	SYN Flood, Smurf Attack; PDF GET, HTTP GET, HTTP POST	HIP Filtering	AR, DLI, RPP
		Load Balancing	AR, RPP
		Selective Pushback	AR, DLI, RPP
		Source-End Reaction	AR, RPP
		Analysis of Traffic Data	AR, RPP, SH, V
		Fault Tolerance	AR, DLI, RPP, SH, V
		Resource Pricing	AR, DLI, RPP, V

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

Fault Tolerance methods assume that it is impossible to prevent or stop DDoS attacks completely, and rather focus on mitigating the effects of attacks so the affected network can remain operational. The methodology is based on duplicating network services and diversifying points of access to the network. In the event of an attack, the congestion caused by attack traffic will not take down all of the affected network. Similar to that of load balancing, fault tolerance methods could leverage CC attributes, such as agility and redundancy, real-time response and elastic performance, and virtualization and automation services to duplicate services and keep the SG network responsive for legitimate traffic.

Resource Pricing is a mitigation approach that utilizes a distributed gateway architecture and payment protocol to establish a dynamically changing cost, or computational burden, for initiating different types of network services [48]. This technique favors users who behave well, and discriminates against users who abuse system resources, by partitioning services into pricing tiers to avoid malicious users from flooding the system with fake requests to attempt price manipulation. The high agility and elastic performance inherent in CC would alleviate the computational burden of Resource Pricing techniques [49]. As the demand of assigning prices to users grows, the computational demand would be easily mitigated by the ability of CSPs to add additional computing resources. Cost levels could easily be assigned to put users into a cost hierarchy, and virtualization capabilities could be used to duplicate network resources and infrastructure capabilities, partitioning users paying different cost levels into separate processing areas. Illegitimate traffic would be sectioned off from the legitimate traffic, reducing the impact of an attack, and if needed, be geographically independent.

Table II summarizes the DDoS defense techniques that can be enhanced by utilizing the CC attributes to defend SG against DDoS attacks.

E. Other Approaches to Consider

Even before CC was aptly branded as such, it was argued that isolated defense mechanisms fail to offer performance guarantees against DDoS attacks [50]. This would require a paradigm shift, where systems acting in isolation would instead act as a distributed framework of non-hierarchal, specialized defense nodes connecting to one another to achieve an overall level of better defense against DDoS attacks. Distributed control architectures, such as the ENERGOS project [51], proposes a multi-layered system of intelligent nodes that contain enough operational information to carry on complex tasks if there is a hierarchal breakdown of communication. The caveat of this approach is that it requires the availability of advanced processing capabilities and a networked infrastructure robust enough to support large data streams.

IV. CONCLUSION

As innovations to our personal devices, automated homes, and electric vehicles continue to close the gap between cyber and physical, the SG and CC will eventually become connected, if not integrated with one another. The proliferation of SG technology has presented energy suppliers and utility companies with challenges that CC could readily meet, but not without mitigating many of CCs outstanding issues. Carelessness in the deployment of CC solutions for SG applications may result in an environment that is more prone to cyber-attacks such as DDoS. Unless a separate communications network is layered on top of the electrical grid [6], the dangers of a DDoS attack from those with malicious intent, whether for financial gain or to terrorize our society remains a very real possibility with severe consequences. The critical nature of the SG means that a real defense solution needs to be developed to protect against DDoS attacks. Victims of DDoS attacks need an easily scalable approach that can quickly add additional resources to defend against DDoS attacks. CC provides the ability to distribute this computational burden across a large pool of resources to compensate for a rapid increase in computational needs. Leveraging the inherent attributes of the CC to help defend against DDoS attacks may not be a permanent solution, but it may be the most readily available answer to this need. While the integration of CC and SG is inevitable, the features of CC can be leveraged to improved 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 Software 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 mechanisms: 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.

[44] S. Begum and C. Prashanth, "Review of load balancing in cloud computing." *International Journal of Computer Science Issues (IJCSI)*, vol. 10, no. 1, 2013.

[45] A. Khiyaita, M. Zbakh, H. El Bakkali, and D. El Kettani, "Load balancing cloud computing: state of art," in *Network Security and Systems (JNS2), 2012 National Days of*. IEEE, 2012, pp. 106–109.

[46] J. Hu, J. Gu, G. Sun, and T. Zhao, "A scheduling strategy on load balancing of virtual machine resources in cloud computing environment," in *Parallel Architectures, Algorithms and Programming (PAAP), 2010 Third International Symposium on*. IEEE, 2010, pp. 89–96.

[47] J. Mirkovic, G. Prier, and P. Reiher, "Attacking ddos at the source," in *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*. IEEE, 2002, pp. 312–321.

[48] R. J. Gibbens and F. P. Kelly, "Resource pricing and the evolution of congestion control," *Automatica*, vol. 35, no. 12, pp. 1969–1985, 1999.

[49] M. Mihailescu and Y. M. Teo, "Dynamic resource pricing on federated clouds," in *Cluster, Cloud and Grid Computing (CCGrid), 2010 10th IEEE/ACM International Conference on*. IEEE, 2010, pp. 513–517.

[50] J. Mirkovic, M. Robinson, and P. Reiher, "Alliance formation for ddos defense," in *Proceedings of the 2003 workshop on New security paradigms*. ACM, 2003, pp. 11–18.

[51] Y. K. Penya, J. C. Nieves, A. Espinoza, C. E. Borges, A. Peña, and M. Ortega, "Distributed semantic architecture for smart grids," *Energies*, vol. 5, no. 11, pp. 4824–4843, 2012.