www.ijiarec.com

/*0

ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Mitigating Security Challenges for Insider Attacker on Fog Devices

[1]Sam Immanuvel.P, [2]Shankara Perumal.A, [3]Shiddharth.C,[4]Parvathi.M
[1-3] UG Students, [4]Associate Professor
Department of CSE, Nandha Engineering College

***Abstract*— Cloud computing related insider threats are often listed as a serious concern by security researchers, but to date this threat has not been thoroughly explored. We believe the fundamental nature of current insider threats will remain relatively unchanged in a cloud environment, but the paradigm does reveal new exploit possibilities. Fog Computing is a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users. In this article, we elaborate the motivation and advantages of Fog computing, and analyze its applications in a series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined networks. Security and privacy issues are further disclosed according to current Fog computing paradigm.. We investigate the stealthy features of this attack by examining its CPU and memory consumption on Fog device.**

***Keywords*—Fog Computing, Cloud Computing, Internet of Things, Software Defined Networks.**

I. INTRODUCTION

Organizations continue to embrace the advantages of flexibility, scalability, and management provided by cloud computing platforms and services, and often consider security one of their top concerns in cloud environments. One of the most serious challenges, not only to cloud computing, but to data security in general, is the insider threat - a threat well known to security professionals.

The open application environment encourages more developers to bring their own applications and connectivity interfaces at the edge of the network. we first answer the questions of what the Fog computing is and what are the differences between Fog and Cloud.

In Fog computing, services can be hosted at end devices such as set-top-boxes or access points. The infrastructure of this new distributed computing allows applications to run as close as possible to sensed actionable and massive data, coming out of people, processes and thing. Such Fog computing concept, actually a Cloud computing close to the 'ground', creates automated response that drives the value.

Both Cloud and Fog provide data, computation, storage and application services to end-users. However, Fog can be distinguished from Cloud by its proximity to end-users, the dense geographical distribution and its support for mobility.WeadoptasimplethreelevelhierarchyasinFigure1.In this framework, each smart thing is attached to one of Fog devices. Fog devices could be interconnected and each of them is linked to the Cloud.

In this article, we take a close look at the Fog computing paradigm. The goal of this research is to investigate Fog computing advantages for services in several domains, such as Smart Grid, wireless sensor networks, Internet of Things (IOT) and software defined networks (SDNs). We examine the state- of-the-art and disclose some general issues in Fog computing including security, privacy, trust, and service migration among Fog devices and between Fog and Cloud. We finally conclude this article with discussion of future work.

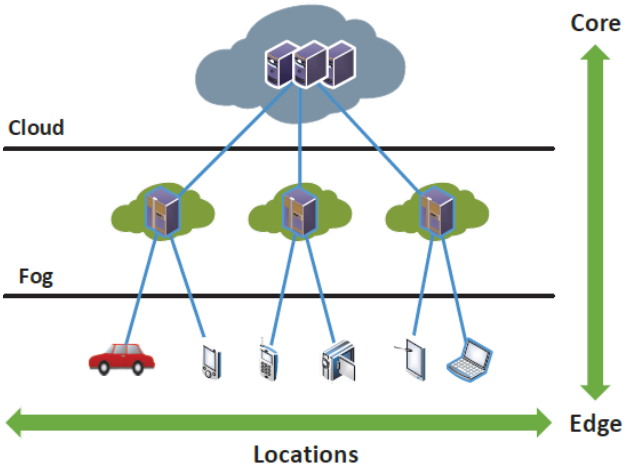


Fig 1. Fog between Edge and Cloud

II. WHY DO WE NEEDFOG?

In the past few years, Cloud computing has provided many opportunities for enterprises by offering their customers a range of computing services. Current "pay-as-you-go" Cloud

computing model becomes an efficient alternative to owning and managing private data centre for customers facing Web applications and batch processing. Cloud computing frees the enterprises and their end users from the specification of many details, such as storage resources, computation limitation and network communication cost. However, this bliss becomes

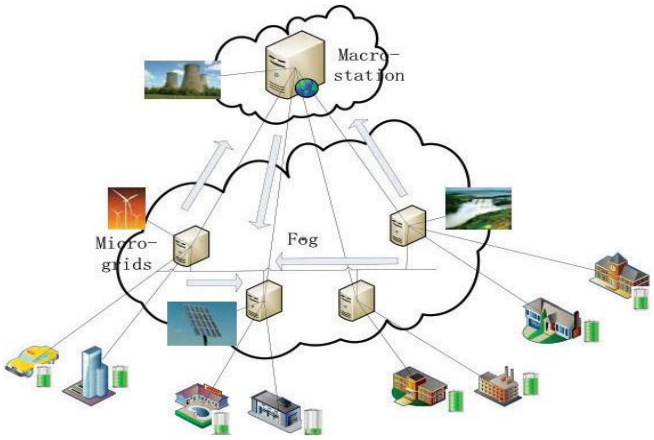


Fig. 2. Fog computing in smart grid.

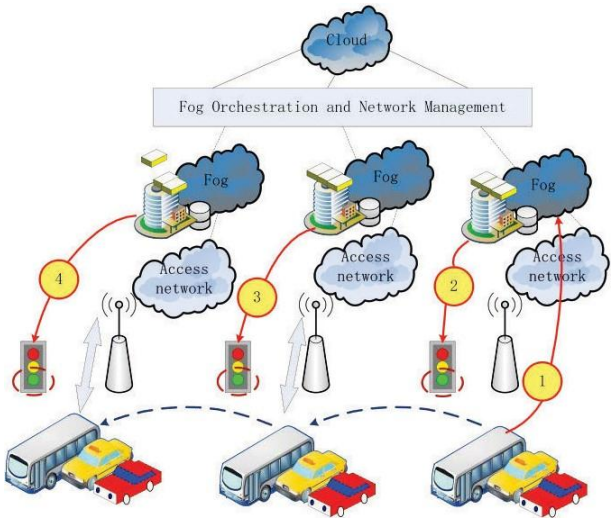


Fig. 3. Fog computing in smart traffic lights and connected vehicles.

a problem for latency-sensitive applications, which require nodes in the vicinity to meet their delay requirements [2]. When techniques and devices of IoT are getting more involved in people's life, current Cloud computing paradigm can hardly satisfy their requirements of mobility support, location awareness and lowlatency.

Fog computing is proposed to address the above problem [1]. As Fog computing is implemented at the edge of the network, it provides low latency, location awareness, and improves quality-of-services (QoS) for streaming and real time applications. Typical examples include industrial automation, transportation, and networks of sensors and actuators. Moreover, this new infrastructure supports heterogeneity as Fog devices include end-user devices, access points, edge routers and switches. The Fog paradigm is well positioned for real time big data analytics, supports densely distributed data collection points, and provides advantages in entertainment,
advertising,personalcomputingandotherapplications.

III. WHAT CAN WE DO WITHFOG?

We elaborate on the role of Fog computing in the following six motivating scenarios. The advantages of Fog computing satisfy the requirements of applications in these scenarios.

Smart Grid: Energy load balancing applications may run on network edge devices, such as smart meters and micro-grids [4]. Based on energy demand, availability and the lowest price, these devices automatically switch to alternative energies like solar and wind. As shown in Figure 2, Fog collectors at the edge process the data generated by grid sensors and devices, and issue control commands to the actuators [2]. They also filter the data to be consumed locally, and send the rest to the higher tiers for visualization, real-time reports and transactional analytics. Fog supports ephemeral storage at the lowest tier to semi-permanent storage at the highest tier. Global coverage is provided by the Cloud with business intelligence analytics.

Smart Traffic Lights and Connected Vehicles: Video camera that senses an ambulance flashing lights can automatically change street lights to open lanes for the vehicle to pass through traffic. Smart street lights interact locally with sensors and detect presence of pedestrian and bikers, and measure the distance and speed of approaching vehicles. As shown in Figure 3, intelligent lighting turns on once a sensor identifies movement and switches off as traffic passes.

Neighboring smart lights serving as Fog devices coordinate to create green traffic wave and send warning signals to approaching vehicles [2]. Wireless access points like WiFi, 3G, road-side units and smart traffic lights are deployed along the roads. Vehicles-to- Vehicle, vehicle to access points, and access points to access points interactions enrich the application of this scenario.

Wireless Sensor and Actuator Networks: Traditional wire- less sensor networks fall short in applications that go beyond sensing and tracking, but require actuators to exert physical actions like opening, closing or even carrying sensors. In this scenario, actuators serving as Fog devices can control the measurement process itself, the stability and the oscillatory behaviors by creating a closed-loop system. For example, in the scenario of self-maintaining trains, sensor monitoring on a train's ball-bearing can detect heat levels, allowing applications to send an automatic alert to the train operator to stop the train at next station for emergency maintenance and avoid potential derailment. In lifesaving air vents scenario, sensors on vents monitor air conditions flowing in and out of mines and automatically change air-flow if conditions become

dangerous to miners.

Decentralized Smart Building Control: The applications of this scenario are facilitated by wireless sensors deployed to measure temperature, humidity, or levels of various gases in the building atmosphere. In this case, information can be exchanged among all sensors in a floor, and their readings can be combined to form reliable measurements. Sensors will use distributed decision making and activation at Fog devices to react to data. The system components may then work together to lower the temperature, inject fresh air or open windows. Air conditioners can remove moisture from the air or increase the humidity. Sensors can also trace and react to movements (e.g, by turning light on or off). Fog devices could be assigned at each floor and could collaborate on higher level of actuation. With Fog computing applied in this scenario, smart buildings can maintain their fabric, external and internal environments toconserveenergy,waterandotherresources.

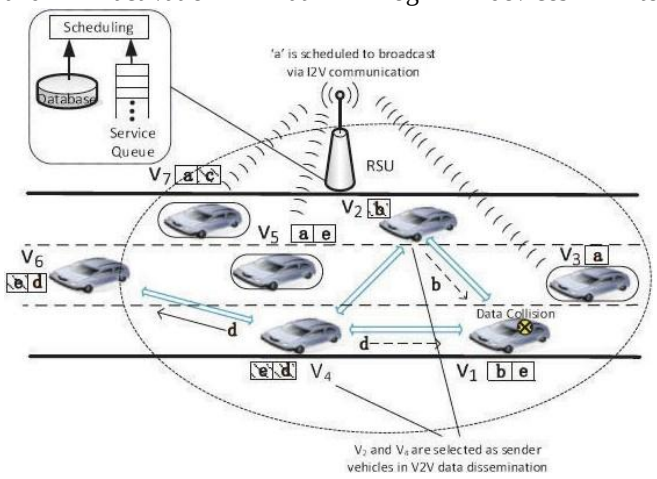


Fig. 4. Fog computing in SDN in vehicular networks [6].

IoT and Cyber-physical systems (CPSs): Fog computing based systems are becoming an important class of IoT and CPSs. Based on the traditional information carriers including Internet and telecommunication network, IoT is a network that can interconnect ordinary physical objects with identified addresses [5]. CPSs feature a tight combination of the system's computational and physical elements. CPSs also coordinate the integration of computer and information centric physical and engineered systems. IoT and CPSs promise to transform our world with new relationships between computer-based control and communication systems, engineered systems and physical reality. Fog computing in this scenario is built on the concepts of embedded systems in which software programs and computers are embedded in devices for reasons other than computation alone. Examples of the devices include toys, cars, medical devices and machinery. The goal is to integrate the abstractions and precision of software and networking with the dynamics, uncertainty and noise in the physical environment. Using the emerging knowledge, principles and methods of CPSs, we will be able to develop new generations of intelligent medical devices and systems, 'smart' highways, buildings, factories, agricultural and roboticsystems.

Software Defined Networks (SDN): As shown in Figure 4, Fog computing framework can be applied to implementthe SDN concept for vehicular networks. SDN is an emergent computing and networking paradigm, and became one of the most popular topics in IT industry [7]. It separates control and data communication layers. Control is done at a centralized server, and nodes follow communication path decided by the server. The centralized server may need distributed implementation. SDN concept was studied in WLAN, wireless sensor and mesh networks, but they do not involve multi-hop wireless communication, multi-hop routing. Moreover, there is no communication between peers in this scenario. SDN concept together with Fog computing will resolve the main issues in vehicular networks, intermittent connectivity, collisions and high packet loss rate, by augmenting vehicle- to-vehicle with vehicle-to-infrastructure communications and centralized control. SDN concept for vehicular networks is first proposed in[6].

IV.THREE TYPES OF CLOUD-RELATED INSIDER THREATS

We consider the cloud-related insider threat from three different perspectives: the rogue cloud provider administrator, the employee in the victim organization that exploits cloud weaknesses for unauthorized access, and the insider who uses cloud resources to carry out attacks against the company's local IT infrastructure.

A. Rogue Administrator

Let us first consider the type of insider described by CSA [2] - the rogue administrator employed by a cloud provider. This cloud-related insider is the most commonly addressed by researchers. An attack often posited by this insider is theft of sensitive information, resulting in loss of data confidentiality and/or integrity. The insider described by this threat may be motivated financially, a common motivator for theft of intellectual property or fraud.

Different Types of Rogue Administrators: It is important to note that the threat of rogue administrators is layered differently for a cloud architecture than a standard enterprise environment. There are at least four levels of administrators to consider in the cloud:

- Hosting Company Administrators
- Virtual Image Administrators
- System Administrators
- Application Administrators

B. ExploitWeaknessesIntroducedbyUseoftheCloud

A second type of cloud-related insider threat, often

overlooked by security researchers, is the insider within the organization who exploits vulnerabilities exposed by the use of cloud services to gain unauthorized accessto organization systems and/or data. This may be malicious or accidental, and is sometimes enabled by differences in security policies or access control models between cloud-based and local systems. This threat may also be successful because direct administrative control of systems and data can difficult for an organization to effect quickly. This type of insider is most likely looking to gain access to sensitive information to sell (fraud) or use for future employment opportunities (theft of intellectual property), and the cloud may provide the easiest way to compromise security measures with the least chance of detection.

C. C.UsingtheCloudtoConductNefariousActivity

A third type of cloud-related insider is one who usescloud services to carry out an attack on his own employer. This is similar to the previous type of insider, who targets systems or data in the cloud. In contrast, the third type of insideruses the cloud as the tool to carry out the attack on systems or data targeted that are not necessarily associated with cloud- based systems.

V.SECURING AGAINST CLOUD-RELATED INSIDERS

Security of cloud computing is a popular research topic,and insider threats in the cloud is no exception. Unfortunately, as cloud computing is primarily a collection of previously existing technologies used in a new way, many solutions to cloud security concerns are merely repackaged solutions to other problems. Though responsibilities may differ, there are few fundamental differences between a rogueadministrator at the cloud provider and a rogue administrator within the customer organization; both insiders have root access to systems and data, and both may employ similar types of attacks to steal information. However, architecture differences and trust issues between organizations and cloud providers does present the need for specialized approaches to insider security in the cloud.

A. Protecting Against RogueAdministrators

The remediation listed in CSA's document is quite applicable to the rogue administrator :

- Enforce strict supply chain management and conduct a comprehensive supplierassessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance re- porting.
- Determine security breach notificationprocesses.

A. Protecting Against CloudExploits

Protecting against the insider who uses weaknesses exposed through use of cloud services is also challenging, but can be addressed via diligence and planning in implementing, transitioning to, and maintaining cloud services. Enforcing fundamental security controls such as separation of duties, least privilege, consistent auditing, data loss prevention, etc., on cloud-hosted systems is important.

Additionally, organizations should have agreements and policies in place with cloud providers to handle cloud-based security incidents. A plan for incident response, including offline credential verification, is essential for a timely and efficient reaction to an attack in progress. System administrators within the organization should be familiar with configuration tools for their cloud-based systems, including procedures for quickly changing access controls or even disabling cloud-based services if necessary.

B. ProtectingAgainstThoseUsingtheCloudAgainstYou

Detecting insiders who use cloud-based services to carry out attacks on local resources can be challenging, particularly if an organization permits internal access to theseservices, such as web-based email accounts. Data loss prevention tools and techniques can be effective in detecting sensitive data being sent via email or uploaded to cloud- based storage. Limiting employee access to external re- sources via network or host-based controls (i.e. firewalls, proxies, etc.) is another option for some organizations.

VI.SECURITY AND PRIVACY IN FOGCOMPUTING

Security and privacy issues were not studied in the context of fog computing. There are security solutions for Cloud computing.However, they may not suit for Fog computing because Fog devices work at the edge of networks. The working surroundings of Fog devices will face with many threats which do not exist in well managed Cloud. In this section, we discuss the security andprivacyissuesinFogComputing.

A. SecurityIssues

Themainsecurityissuesareauthenticationatdifferentlevelsofgateways aswellas(incaseofsmartgrids)atthesmart meters installed in the consumer's home.EachsmartmeterandsmartappliancehasanIP address. A malicioususercaneithertamperwithitsownsmartmeter,reportfalse readings,orspoofIPaddresses. There are some solutionsfor the authentication problem. The work[26] elaboratedpublickeyinfrastructure(PKI)basedsolutionswhichinvolvemulticast authentication. Some authenticationtechniquesusingDiffie-Hellmankeyexchangehavebeendiscussedin[27].Smartmetersencryptthedataandsendtothe Fogdevice,suchasahome-areanetwork(HAN)gateway.HANthendecryptsthedata,aggregatestheresultsandthenpassesthemforward.Intrusion detection techniques can also be appliedinFogcomputing[28].Intrusioninsmartgridscanbedetectedusing either a signature-based method in whichthepatternsofbehaviorareobservedandcheckedagainstanalreadyexisting database of possible misbehaviors.methodin

whichan observed behavior is compared withexpectedbehaviortocheckifthere is a deviation. Thework [29]
developsanalgorithmthatmonitorspowerflowresultsanddetect sanomaliesintheinputvaluesthatcouldhavebeenmodified byattacks.Thealgorithmdetectsintrusionbyusingprincipalcom ponentanalysistoseparatepowerflowvariabilityinto
regular and irregular subspaces.

B. *An Example: Man-in-the-MiddleAttack*

Man-in-the-middle attack has potential to become a typical attack in Fog computing. In this subsection, we take man- in-the-middle attack as an example to expose the security problems in Fog computing. In this attack, gateways servingas Fog devices may be compromised or replaced by fake ones [30]. Examples are KFC or Star Bar customers connecting to malicious access points which provide deceptive SSID as public legitimate ones. Private communication of victims will behijackedoncetheattackerstakethecontrolofgateways.

1) Environment Settings of Stealth Test: Man-in-the-middle attack can be very stealthy in Fog computing paradigm. This type of attack will consume only a small amount of resources in Fog devices, such as negligible CPU utilization and memory consumption. Therefore, traditional anomaly detection methods can hardly expose man-in-the-middle attack without noticeable features of this attack collected from the Fog.Two steps are needed to realize the man-in-the-middle attack for the stealth test. First, we need to compromise the gateway, and second, we insert malicious code into the compromised system. For susceptible gateways, we can either refresh the ROM of a normal gateway or place a fake active point in

Fig. 5. The hijacked communication in Fog (e.g. from phone toPC).

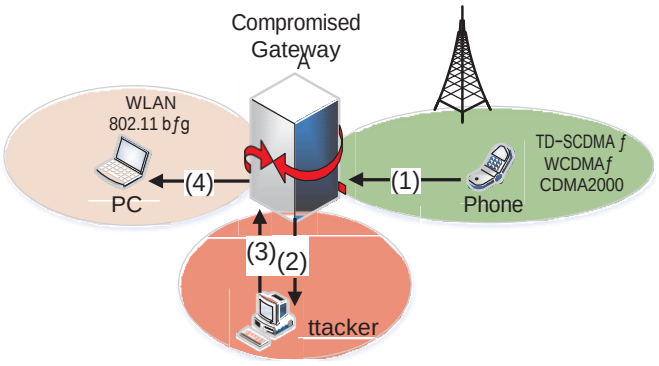
2) Work Flow of Man-in-the-Middle Attack: The communication between 3G and WLAN needs a gateway to translate the data of different protocols into the suitable formats. Therefore, all the communication data will firstly arrive at thegateway
and then be forwarded to other receivers.

In our experiment, the man-in-the-middle attack is divided into four steps. We illustrate the hijacked communication from 3G to WLAN in Figure 7. In the first two steps, the embedded hook process of the gateway redirects the data received from the 3G user to the attacker. The attacker replays or modifies the data of the communication at his or her own computer, and then send the data back to the gateway. In the final step, the gateway forwards the data from the attacker to the WLAN user. In fact, the communication from the WLAN user will also be redirected to the attacker at first, and then be forwarded by the hook in the gateway to the 3G user. We can see clearly from Figure 5 that the attacker can monitor and modify the data sent from the 3G user to the WLAN user in the 'middle' of thecommunication.

3) Results of Stealth Test: Traditional anomaly detection techniques rely on the deviation of current communication from the features of normal communication. These features include memory consumption, CPU utilization, bandwidth usage, etc. Therefore, to study the stealth of man-in-the- middle attack, we examine the memory consumption and the CPU utilization of gateway during the attack. If man-in-the- middle attack does not greatly change the features of the communication, it can be proofed to be a stealthy attack. For simplicity, we assume the attacker will only replay the data at hisorherowncomputerbutwillnotmodifythedata.

C. *PrivacyIssues*

In smart grids, privacy issues deal with hiding details, such as what appliance was used at what time, while allowing correct summary information for accurate charging. R. Lu et al. described an efficient and privacy-preserving aggregation scheme for smart grid communications [33]. It uses a super-increasing sequence to structure multi-dimensional data and encrypt the structured data by the homomorphic cryptogram technique. A homomorphic function takes as input the encrypted data from the smart meters and produces an encryption of the aggregated result. The Fog device cannot decrypt the readings from the smart meter and tamper with them. This ensures the privacy of the data collected by smart meters, but does not guarantee that the Fog device transmits the correct report to the other gateways. For data communications from user to smart grid operation center, data aggregation is performed directly on cipher-text at local gateways without decryption, and the aggregation result of the original data can



be obtained at the operation center [33]. Authentication cost isreducedbyabatchverificationtechnique.

VII.CONCLUSIONS

Insider threats are a persistent and increasing problem. Cloud computing services provide a resource for organizations to improve business efficiency, but also expose new possibilities for insider attacks. Fortunately, it appears that few, if any, rogue administrator attacks have been successful within cloud service providers, but insiders continue to abuse organizational trust in other ways, such as

using cloud services to carry out attacks. Organizations should be aware of vulnerabilities exposed by the use of cloud services and mindful of the availability of cloud services to employees within the organization.

We investigate Fog computing advantages for services in several domains. Based on the work of this paper, some innovations in compute and storage may be inspired in the future to handle data intensive services based ontheinterplaybetweenFogandCloud.

VIII.REFERENCES

[1] F. Bonomi, "Connected vehicles, the internet of things, and fog computing,"in*TheEighthACMInternationalWorkshoponVehicularInter- Networking (VANET)*, Las Vegas, USA,2011.

[2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, ser. MCC'12. ACM, 2012, pp.13–16.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A.Konwinski,
G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr 2010.

[4] C. Wei, Z. Fadlullah, N. Kato, and I. Stojmenovic, "On optimally reducing power loss in micro-grids with power storage devices," *IEEE JournalofSelectedAreasinCommunications*,2014toappear.

[5] L.Atzori,A.Iera,andG.Morabito,"Theinternetofthings :Asurvey,"
Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[6] K. Liu, J. Ng, V. Lee, S. Son, and I. Stojmenovic, "Cooperative data dissemination in hybrid vehicular networks: Vanet as a softwaredefined network," *Submitted for publication*,2014.

[7] K.Kirkpatrick,"Software-definednetworking,"*Commun.ACM*,vol.56, no.9,pp.16–19,Sep.2013.

[8] Cisco, "Cisco delivers vision of fog computing to accelerate value from billions of connected devices," Cisco, Tech. Rep., Jan.2014.

[9] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B.Kold- ehofe, "Opportunistic spatio-temporal event processing for mobile situ- ation awareness," in *Proceedings of the 7th ACM International Confer- ence on Distributed Event-based Systems*, ser. DEBS'13. ACM, 2013, pp.195–206.

[10] H. Madsen, G. Albeanu, B. Burtschy, and F.Popentiu-Vladicescu, "Reliability in the utility computing era: Towards reliable fog comput- ing," in *Systems, Signals and Image Processing (IWSSIP), 2013 20th InternationalConferenceon*,July2013,pp.43–46.

[11] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B.Kold- ehofe, "Mobile fog: A programming model for large-scale applications ontheinternetofthings,"in*ProceedingsoftheSecondACMSIGCOMM Workshop on Mobile Cloud Computing*, ser. MCC'13. ACM, 2013, pp. 15–20.

[12] .B. Ottenwalder, B. Koldehofe, K. Rothermel, and U. Ramachandran, "Migcep: Operator migration for mobility driven distributed complex eventprocessing,"in*Proceedingsofthe7thACMInternationalConfer- ence on Distributed Event-based Systems*, ser. DEBS'13. ACM, 2013, pp.183–194.

[13] J. Zhu, D. Chan, M. Prabhu, P. Natarajan, H. Hu, and F. Bonomi, "Improving web sites performance using edge servers in fog computing architecture," in *Service Oriented System Engineering (SOSE), 2013 IEEE7thInternationalSymposiumon*,March2013,pp.320–323.

[14] BETaaS,"Buildingtheenvironmentforthethingsasaservice,"BETaaS, Tech. Rep., Nov.2012.

[15] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A stackelberg game approach," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 120– 132, March2013.

[16] D. Korzhyk, V. Conitzer, and R. Parr, "Solving stackelberg games with uncertain observability," in *The 10th International Conference on Autonomous Agents and Multiagent Systems - Volume 3*, ser. AAMAS '11, 2011, pp.1013–1020.

[17] Z.Fadlullah,D.Quan,N.Kato,andI.Stojmenovic,"Gtes: Anoptimized game-theoretic demand-side management scheme for smart grid," *SystemsJournal,IEEE*,vol.8,no.2,pp.588–597,June2014.

[18] T. Luo, H.-P. Tan, and T. Quek, "Sensor openflow: Enabling software- defined wireless sensor networks," *Communications Letters, IEEE*, vol. 16, no. 11, pp. 1896–1899,Nov. 2012.

[19] Y. Daraghmi, C.-W. Yi, and I. Stojmenovic, "Forwarding methods in datadisseminationandroutingprotocolsforvehicularadhocnetworks," *Network,IEEE*,vol.27,no.6,pp.74–79,November2013.

[20] B. Zhou, J. Cao, X. Zeng, and H. Wu, "Adaptive traffic light control in wireless sensor network-based intelligent transportation system," in *Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd*, Sept 2010, pp.1–5.

[21] B. Zhou, J. Cao, and H. Wu, "Adaptive traffic light control of multiple intersections in wsn-based its," in *Vehicular Technology Conference (VTCSpring),2011IEEE73rd*,May2011,pp.1–5.

[22] C. Li and S. Shimamoto, "An open traffic light control model for reducing vehicles co2 emissions based on etc vehicles," *Vehicular Technology,IEEETransactionson*,vol.61,no.1,pp.97–110,Jan2012.

[23] W. Wang and Z. Lu, "Survey cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[24] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "Grs: The

green, relia- bility, and security of emerging machine to machine communications," *CommunicationsMagazine,IEEE*,vol.49,no.4,pp.28–35,April2011.

[25] Y. W. Law, M. Palaniswami, G. Kounga, and A. Lo, "Wake: Key managementschemeforwide-areameasurementsystemsinsmartgrid," *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 34–41, January 2013.

[26] Z. Fadlullah, M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, andY. Noza- ki, "Toward intelligent machine-to-machine communications in smart grid,"*CommunicationsMagazine,IEEE*,vol.49,no.4,pp.60–65,April 2011.

[27] C.Modi,D.Patel,B.Borisaniya,H.Patel,A.Patel,andM. Rajarajan,"A survey of intrusion detection techniques in cloud," *Journal of Network andComputerApplications*,vol.36,no.1,pp.42–57,2013.

[28] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusiondetection in power system operations," *Power Systems, IEEE Transactions on*, vol.28,no.2,pp.1052–1062,May2013.

[29] L. Zhang, W. Jia, S. Wen, and D. Yao,"A man-in-the-middle attack on 3g-wlan interworking," in *Communications and Mobile Computing (CMC),InternationalConferenceon*,vol.1,April2010,pp.121–125.

[30] Broadcom bcm 5354. [Online]. Available: http://www.broadcom.com/ products/Wireless-LAN/802.11-Wireless-LAN-Solutions/BCM5354

[31] Wikipedia. (2014) Hooking, what is hooking? [Online]. Available: http://en.wikipedia.org/wiki/Hooking

[32] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid com- munications," *Parallel and Distributed Systems, IEEE Transactions on*, vol.23,no.9,pp.1621–1631,Sept2012.