Poster Abstracts

NIST Cloud Computing Forum & Workshop IX
September 13-15, 2016

Table of Contents

Cloud Customer Architecture for Big Data & Analytics 2

Procuring and Assessing Trustworthy Evidences for Robust Forensic Cloud Environment 3

IoT Virtualization in Micro-Clouds 5

ExoGENi Testbed 6

Cloud Computing R&D Pathfinder Initiative 7

Accessibility, of, by and for the Cloud 8

Cloud Auditor - A Perspective from the NIST Cloud Computing Reference Architecture 9

Cloud Customer Architecture for Big Data & Analytics

Melvin Greer
Cloud Standards Customer Council -- Steering Committee
tracie@omg.org
USA

Abstract: Using analytics reveals patterns, trends and associations in data that help an organization understand the behavior of the people and systems that drive its operation. Big data technology increases the amount and variety of data that can be processed by analytics, providing a foundation for visualizations and insights that can significantly improve business operations.

Cloud Customer Architecture for Big Data and Analytics written by the Cloud Standards Customer Council considers how harnessing cloud architectures can further change the economics and development lifecycle of these capabilities. It describes vendor neutral best practices for hosting big data and analytics solutions using cloud computing. The paper describes the architectural elements and cloud components needed to build out big data and analytics solutions.

Speaker Bio:
Melvin Greer is Director of Data Science and Analytics at Intel Corporation. Mr. Greer uses his knowledge in graph analytics, machine learning and cognitive computing to accelerate transformation of data into a strategic asset for Federal Agencies and global enterprises. His systems and software engineering experience has resulted in patented inventions in Cloud Computing, Synthetic Biology and IoT Bio-sensors for edge analytics. He functions as a principal investigator in advanced research studies, including Nanotechnology, Additive Manufacturing and Gamification. He significantly advances the body of knowledge in basic research and critical, highly advanced engineering and scientific disciplines. Mr. Greer is a member of the American Association for the Advancement of Science (AAAS) and U.S. National Academy of Science, Engineering and Medicine.
Mr. Greer has been awarded the BEYA Technologist of the Year Award, which recognizes his outstanding technical contribution and technical products that have a broad impact and high value to society as a whole. Mr. Greer has been appointed Fellow of the National Cybersecurity Institute where he assists government, industry, military, and academic sectors meet the challenges in cyber security policy, technology and education.

In addition to his professional and investment roles, he is Founder and Managing Director of the Greer Institute for Leadership and Innovation, focused on research and deployment of a 21st Century Leadership Model. Mr. Greer is a member of the International Monetary Fund / World Bank, Bretton Woods Committee where he explores how deployment of enabling technologies relates to private sector development, commercial opportunities, global financial stability and social responsibility. Mr. Greer is a frequent speaker at conferences and universities and is an accomplished author; his fifth book “Practical Cloud Security and Industry View” is his most recently published book. As a popular educator and board member at a number of Historical Black Colleges and Universities, Greer is leading science, technology, mathematical and engineering (STEM) research initiatives, directly trying to shape a more diverse generation of up-and-coming technical talent.
Mr. Greer received his Bachelor of Science degree in Computer Information Systems and Technology and his Master of Science in Information Systems from American University, Wash. D.C. He also completed the Executive Leadership Program at the Cornell University, Johnson Graduate School.

Procuring and Assessing Trustworthy Evidences for Robust Forensic Cloud Environment

Avinash Thakur, Dr Arati Dixit
Department of Technology, Savitribai Phule Pune University, India
A-101, Anantshilp, Bavdhan Pune, India
avi.thakur19@gmail.com, adixit98@gmail.com

Abstract: With the inception of cloud computing, the intruders have also raised their bar in the shadow of cybercrime. Security reasons are restricting the wide adoption of cloud computing. Live forensics on the other hand deals with minimizing the impacts to the integrity of data while collecting continuous evidence from the computer system. There are a lot of researches that have focused on these two aspects, but only a few that have merged live forensics with cloud environment for detecting and decreasing Intrusions. With increasing attacks, several organizations have deployed a standard security structure over the cloud, which comprises of firewall, secure e-mail gateways, network intrusion detection system, ingress and egress filtration of data, cryptographic systems, steganography, etc. However, the regular monitoring of the data is the most crucial aspect in detecting the attack and building the defense against it as cloud is prone to such vulnerabilities due to the sheer number of resources attached to it. Live forensics tools and techniques are developed to diminish the criminal intrusions in cloud environment. Some of the common forensic tools are: EnCase, FTK, Wireshark for cross platform, DECAF, Cofee, X-ways. However, they are faced with certain challenges such as accurate time synchronization, logs challenges, data discovery, and evidence segregation without breaching the confidentiality of other users, information analysis and evidence reporting. A robust framework with enhanced forensic technique for collecting live evidence in the emerging paradigm of cloud technology becomes a necessity.

The proposed **Robust Forensic Cloud** framework will primarily focus on obtaining accurate logs & its synchronization for auditing the system. The live forensic framework can be utilized by the security administrator in cases of breaches and intrusions and gather live evidence. It will not only identify the threat but also assist in building efficient defending mechanism. With the precipitate growth of global cloud adoption in private and public sector cloud computing aura is becoming the new frontline for cybercrime. As the cloud paradigm emerges the need for carrying out the digital investigation has become inevitable. Cloud forensics is the appositeness of digital forensics in cloud computing as a subset of network forensics. A log, in a computing context is the automatically produced and time -stamped documentation of events relevant to a peculiar system. Every event on Cloud produces various forms of logs. The logs stored in the log files needs to be managed effectively to lead to both security and compliance. Log management is a decisive purpose of cloud forensics for the synchronized aligned and formatted form of logs retrieved from cloud, this form of log can be useful for the understanding purpose of investigators and can lead the investigation process to its edge. We propose the methodology, approach and proper manner of log monitoring, retrieval and will contribute in the forensic management of logs. For the wide adoption of Cloud Computing, There is a requirement for a Forensically empowered architecture which can not only handle the logs for forensic purpose but also be able to generate alerts, support forensic activities to law enforcement agencies & be able to provide forensically robust cloud environment. Forensic management of the logs is the only initial step in this direction. Therefore, procuring and assessing trustworthy evidences lead to a robust forensic cloud environment.

Speaker Bio:

Arati M. Dixit received a Ph.D. in Computer Engineering from Wayne State University, Detroit, MI, USA. She has also completed The Certificate in Scientific Computing Program from Wayne State University. She is an Alumni of IIT Bombay with M.Tech. in Computer Science and Engineering. She has done BE in Computer Engineering from University of Pune. Currently she is an Associate Professor at the Department of Technology, Savitribai Phule Pune University. She a visiting faculty and Research & Development associate at the Department of Computer Engineering, PVPIT, Bavdhan. She has been associated with the academic profession for last 16+ years. She has published more than 80 research papers in reputed refereed national/international conferences and journals. Her areas of interest are Cyber Security, Cyber Physical Systems, Soft Computing, and High Performance Computing. She has been associated with Ph.D. students at Defence Institute of Advanced Technology and Savitribai Phule Pune University. She has been a member of Board of Studies and Research Recommendation Committees with reputed Institutes/Universities. She is an executive council member of Association for Computing Machinery (ACM) India's ACM-W. ACM-W is ACM Council on Women in Computing. She is the Vice-Chairperson of ACM iSIGCSE(India Special Interest Group on Computer Science Education) as well as ACM Pune Professional Chapter. She is an ACM Senior Member and active ACM-W volunteer supporting and advocating full engagement of women in computing.

IoT Virtualization in Micro-Clouds

Charif Mahmoudi, Mehdi Tazi, Fabrice Mourlin
Paris-Est Créteil Val-de-Marne University, France
61 avenue du Général de Gaulle 94010 Créteil Cedex
charif.mahmoudi@lacl.fr, mtazi@octo.com, fabrice.mourlin@u-pec.fr

Abstract: The aim of this project is the virtualization of "things" to add cloud based functionalities to a constrained IoT device. Building smarter devices, the assembly of the existing ones is achieved by message exchanges in a micro-cloud. A device virtualization is featured by its input and output interfaces. The proposed assembly strategy relies on putting interfaces together and the definition of a richer component. This effort focuses on three main topics:

- Make connected objects highly available.
- Manage spatial distribution of composed connected objects.
- Handle and manage transactions on a collection of connected objects.

Speaker Bio:
Dr. Charif Mahmoudi received the MSc and PhD degrees in computer engineering from the University of Paris-EST (France) in 2009 and 2014, respectively. Since then, he has been a PostDoc at the National Institute of Standards and Technology. He participated as consultant then software architect to several successful telecommunication projects within France Telecom and Bouygues Telecom. His areas of research are on distributed systems, cloud-computing, mobile computing and internet of things.

ExoGENi Testbed

Yufeng Xin
RENCI, University of North Carolina
Europa Dr. 100, Chapel Hill, NC 27517
USA
yxin@renci.org

Abstract: ExoGENI testbed, part of GENI, is a distributed Cloud testbed that federates over twenty Cloud sites over the world. The core of the testbed system is an orchestration and automation software system for networked infrastructure as as service (NIaaS). The targeted NIaaS platform consists of a large number of geographically distributed Cloud sites interconnected with multi-domain networks. This testbed has been used to develop and experiment various applications in networking, scientific workflow, big data, and CPS.

Comments:
www.exogeni.net
www.renci.org

Speaker Bio:
Yufeng Xin is a senior scientist at RENCI, University of North Carolina at Chapel Hill. He is also an adjunct professor in the Computer Science Department, North Carolina State University. His research focuses on high-speed networks, cloud computing, wireless networks, and cyber physical systems. He obtained his PhD in Operations Research and Computer Science from North Carolina State University in 2002.

Cloud Computing R&D Pathfinder Initiative

Todd Eppich, Hillary Armstrong, Sophia Corwell
Sandie National Laboratories
PO Box 5800, MS0763 Albuquerque, NM 87185
USA
tgeppic@sandia.gov, hmarmst@sandia.gov, secorwe@sandia.gov

Abstract: Sandia National Laboratories (SNL) has launched an initiative to leverage cloud computing capabilities across the development spectrum throughout SNL. This includes a vision to provide cloud-based development environments at multiple security levels. The Sky Cloud Common Operating Environment (COE) standardized private cloud deployment for SNL. A series of infrastructure projects is underway to implement OpenStack-based private clouds providing Infrastructure as a Service (IaaS) to complex systems development projects in a variety of domains. The private clouds allow SNL to experiment with various cloud technologies before deploying to a public cloud. During initial experiments, SNL recognized the need for a framework to guide projects looking to develop cloud-based solutions. A small team was chartered to create an architecture model to guide cloud-based development activities. This team selected a Model Based Systems Engineering (MBSE) approach to create the Cloud Analytics Reference Mission Architecture (CARMA) model to satisfy the framework need. CARMA builds on the lessons learned from implementing the Sky COE, SNL-internal customer-driven Big Data projects, the NIST Big Data Interoperability Framework, and the NIST Cloud Computing Reference Architecture. The model is being used by cloud-based development efforts across SNL. It provides a way for the customer to fully define their platform, data, and security needs and examine potential architecture solutions with the engineering team.

Accessibility, of, by and for the Cloud

Robert Bohn, NIST
Jim Tobias, Inclusive Technologies
robert.bohn@nist.gov, tobias@inclusive.com

Abstract: The NIST Cloud Computing Program (NCCP) released a draft two-volume US Government (USG) Cloud Computing Standards and Technology Roadmap[1] in November 2011 for public comments; it was published in final form in October 2014. The USG Cloud Computing Technology Roadmap lists ten requirements and several Priority Action Plans that should be followed to fulfill the requirements. Requirement #7 is to "***Define unique government regulatory requirements and solutions.***"

Accessibility is a valid challenge for the USG. Cloud computing solutions that address and highlight accessibility offer a path forward for an agency to fulfill its mission and requirements by providing a larger number of potential solutions that USG ICT managers can use to be creative in the development of new services and solve their unique accessibility requirements. As work progresses in cloud computing, it is important to promote, incorporate and discuss applicable standards in accessibility for cloud computing services as a discipline for investigation.

In response to the interest in cloud and accessibility, the NCCP formed a new Public Working Group (PWG) on "Cloud Computing and Accessibility" (CCA-PWG). This poster addresses the topics facing cloud computing with respect to accessibility, standards and usage.

[1] US Government Cloud Computing Technology Roadmap Volume I: High-Priority Requirements to Further USG Agency Cloud Computing Adoption; and Volume II: Useful Information for Cloud Adopters, NIST SP 500-293, http://dx.doi.org/10.6028/NIST.SP.500-293

Cloud Auditor - A Perspective from the NIST Cloud Computing Reference Architecture

Robert Bohn, NIST
Steven Woodward, Cloud Perspectives
robert.bohn@nist.gov, steve@cloudperspectives.com

Abstract: The Cloud Auditor was first identified as an actor in the NIST Cloud Computing Reference Architecture (CC RA) (NIST SP 500-292 – Sept 2011). The NIST CC RA also identifies 4 other actors – Cloud Consumer, Cloud Provider, Cloud Broker, Cloud Carrier. The original CC RA focused heavily on the Cloud Provider role, but this work does a more thorough analysis of this actor. The Cloud Auditor plays many of the same roles as a conventional IT Auditor, but their responsibilities take on additional complexities since they have to do audits of the Cloud Customer and the Cloud Provider in order to complete their report. Security is a shared responsibility between Cloud Customer & Cloud Provider, which increases the complexity of tasks assigned to the Cloud Auditor. This poster describes some of the similarities and differences between an IT Auditor and a Cloud Auditor.