International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.1, No.3, August 2012, pp. 90~115
ISSN: 2089-3337

Conceptualizing a Secure Wireless Cloud

Tyson Brooks*, Jerry Robinson*, Lee McKnight*
* School of Information Studies (iSchool), Syracuse University

Article Info

Article history:

Received June 20th, 2012
Revised July 10th, 2012
Accepted July 28th, 2012

Keyword:

Cloud computing
Wireless grids
Wireless networks
Wireless grid security
Cloud computing security

ABSTRACT

The interest in cloud computing by organizations has driven a core desire to become more effective and efficient with information technology (IT). Cloud computing enables organizations to utilize instantly provisioned scalable IT resources on a pay-per-use basis. The wireless grid provides a new model for heterogeneous devices to share physical and virtual resources within an ad-hoc environment with no dedicated server needed to manage the network. Both of these technologies provide new opportunities to provide innovative architectures but also have a number of security related issues that concern many potential users. Despite the potential benefits, each integration of a cloud computing and a wireless grid architecture raise even more concerns related to information security than each architecture alone. As a new paradigm for organizational strategic initiatives, these are the issues which prevent cloud computing and wireless grid solutions from becoming the prevalent integration for an operational system. This article will identify a wireless cloud architecture and identify potential vulnerabilities and threats to a wireless cloud solution. We also identify the beginnings of a promising wireless grid security architecture, which focuses on a wireless cloud authentication, authorization and access control process.

Corresponding Author:

Tyson Brooks, PMP
School of Information Studies (iSchool),
Syracuse University,
Email: ttbrooks@syr.edu

1. INTRODUCTION

Computer networks and telecommunications backbones have made distributing computing power essential in the majority of industries and homes worldwide. The financial industry conducts trillions of dollars in transactions each day using current networking and distributed computing technology; and governments around the world maintain information on networks and in distributed databases. Each of these examples represents ways that telecommunications and network technologies are used to efficiently conduct daily operations. However, there is a downside. The information that is stored in and passed along global networks is exposed to malicious attempts to intercept it without proper authorization [10]. IT systems should be designed to minimize network vulnerabilities and protect the information contained within them [26].

Cloud computing represents the long-held dream of computing as a utility. It has the potential to transform a large part of the IT industry, making software even more attractive as a service through leveraging a data center's shared resources and shaping the way IT hardware is designed and purchased [3, 4]. Cloud computing is being touted as a new paradigm in computing, which will obviate an organization's need to build, manage, and fund internal data centers and complex IT infrastructures. Cloud computing infrastructures enable companies to cut costs by outsourcing computations, on-demand [64]. Many people in the IT industry are interested in advancing cloud computing and it is envisioned by many as the next generation architecture of IT enterprises [33, 36].

Many organizations are beginning to see the potential in cloud computing solutions but may not be aware of the wireless grid and its potential integration with cloud computing for critical systems. However,

organizations considering this integrated solution must carefully consider their specific needs, the security risks, and whether or not cloud computing will deliver value. Wireless grids provide the dynamic sharing of physical and virtual resources among heterogeneous devices [44]. A new wireless cloud option should be examined from a security perspective for potential business and technical benefits as it relates specifically to organizational IT assets.

This article discusses the implications of developing a wireless cloud and the potential security risks. We will identify a wireless cloud architecture, potential vulnerabilities and threats to a wireless cloud solution, and propose the beginnings of a wireless grid security architecture, which focuses on an authentication, authorization and access control process.

2. CLOUD COMPUTING

"Cloud" computing is a relatively recent term and builds on decades of research in virtualization, distributed computing, utility computing, and more recently networking, web and software services [4, 32]. A definition of cloud computing is:

> *"…a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*[1]

As displayed in Figure 1, cloud computing has emerged as a new computing paradigm that arrays massive numbers of computers in centralized data centers to deliver web-based applications, application platforms, and services via a utility model [25, 59]. Mell and Grance [46] describe the four deployment models identified by the National Institute of Standards and Technology (NIST) for cloud services as the following: (1) *private cloud* - the cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise; (2) *community cloud* - the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise; (3) *public cloud* - the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services and (4) *hybrid cloud* - the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

There are a number of service offerings and implementation models within the cloud computing umbrella. These models, as displayed in Table 1, can be grouped into the following three categories: Infrastructure-as-a-Service (IaaS), which offers the ability to lease services such as storage or computing resources (e.g. Amazon Simple Storage Service[2] and Elastic Compute Cloud[3]) [14], Platform-as-a-Service (PaaS), which provides the ability to lease an application development environment (e.g. Microsoft Azure Services Platform[4]) and Software as a Service (SaaS), which offers network accessible applications (e.g. Google docs[5]. These models provide distinct resources to the user/customer ranging from general infrastructure services provided by IaaS vendors to targeted customizable applications provided by SaaS vendors [69].

[1] http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf
[2] Amazon Simple Storage Service: http://aws.amazon.com/s3/
[3] Amazon Elastic Compute Cloud: http://aws.amazon.com/ec2/
[4] Microsoft Windows Azure: www.microsoft.com/windowsazure
[5] Google Docs: https:// docs.google.com

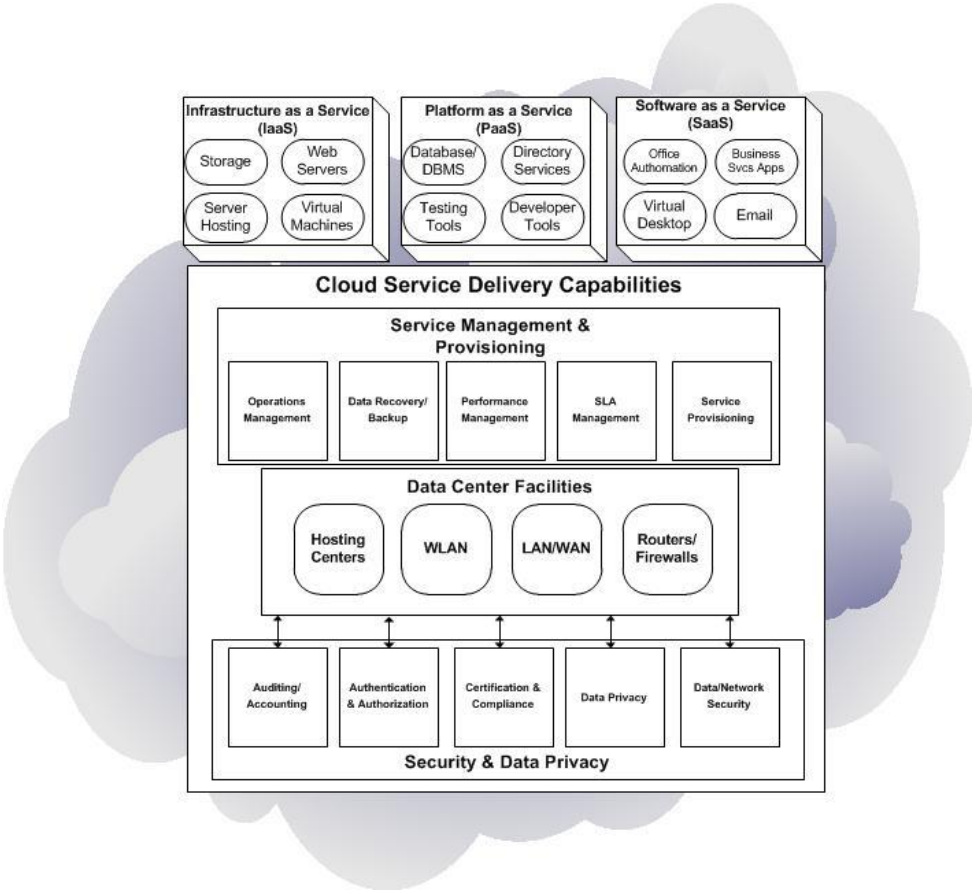

Figure 1. The Cloud Computing Framework

Table 1. Cloud Delivery Models

Delivery Model	Definition
Infrastructure as a Service (IaaS)	Includes the foundational elements, such as storage, operating system instances, network, and identity management upon which development platforms and application can be layered; the capability provided to the consumer is to rent processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications [14, 69].
Platform as a Service (PaaS)	Cloud systems can offer an additional abstraction level: instead of supplying a virtualized infrastructure, they can provide the software platform where systems run on. The sizing of the hardware resources demanded by the execution of the services is made in a transparent manner [14, 69].
Software as a Service (SaaS)	Builds upon PaaS to offer complete applications customizable by the user to a limited degree and utilizing a security model developed by the provider; services of potential interest to a wide variety of users hosted in Cloud systems, which is an alter native to locally run applications. An example of this is the online alternatives of typical office applications, such as word processors, Google Docs, etc. [14, 69].

Instead of buying and maintaining costly servers, the IAAS cloud computing model for example, allows one to dynamically and remotely control processing, memory, data storage, and network bandwidth from pools of these resources, providing the ability to specify and deploy computing capacity on demand [34, 37, 39]. If there is a need to scale up to accommodate sudden demand the necessary resources can be provisioned by the customer using a web browser. These same services are provided to multiple external

customers (multi-tenancy), leveraging the shared resources of large data centers to achieve economies of scale and reduce the cost of the service [60]. Multi-tenancy enables sharing of resources (and costs) among a large pool of users, provides reliability by way of multiple redundant sites, which makes it suitable for business continuity and disaster recovery. Clouds are advertised as a cheap alternative to supercomputers and specialized clusters. The cloud platform is much more reliable than grid platforms and it is more scalable [52]. The IAAS in cloud computing relies on large collections of commoditized computing resources provisioned via hypervisors.

Although cloud computing is in its early stages and its definitions vary greatly, the technologies used for the cloud include grid computing, utility computing, and virtualization technologies. Grid computing is a form of distributed, parallel computing whereby processes are split up to leverage the available computing power of multiple central processing units (CPU) acting in concert [23]. Utility computing allows users to purchase computing capacity, such as CPU, storage, and bandwidth, from an IT service provider and to be billed based on actual consumption [3]. Virtualization technologies are virtual servers and virtual private networks and they provide the ability to quickly reconfigure available resources on demand and provide the necessary security assurance, such as increased security protocols to protect against threats from the cloud environment and the data transported within the cloud [7].

Among the substantial challenges that hinder the widespread adoption of cloud computing are the security and privacy concerns of data in the cloud. Security has emerged as arguably the most significant barrier to faster and more widespread adoption of cloud computing [11]. Although cloud computing offers the benefits of moving computing resources to a cloud computing environment to take advantage of flexibility and cost savings, data confidentiality and integrity controls for the cloud need to be applied to limit exposure to unauthorized users [28]. Moving information assets to a cloud computing environment can reduce the costs of information management and storage but cloud-based systems are open to security threats and loss of control of data [64]. The cloud computing service deployment and architecture (e.g. private, community, public or hybrid) chosen must fit the security and privacy needs of the organization adopting this type of environment [15, 39, 46].

3. WIRELESS GRIDS

Treglia et al. [68] define wireless grids as ad-hoc dynamic sharing of physical and virtual resources among heterogeneous devices, content and users. As the future of distributed computing, wireless grids (see Figure 2) will enable resource sharing among dynamic groups or social networks with individual profiles that are assigned a specific status relative to similar objects and resources with no dedicated server needed to manage the network [45]. Grid computing involves the aggregation of network connected computers to form a distributed system for coordinated problem solving and resource sharing [16, 17, 57]. McKnight et al. [44] can be credited with describing wireless grid infrastructures along three dimensions: the physical layer, the networking infrastructure, and the middleware. Recent literature from Li et al. [42] and Ahuja and Myers [2] identify wireless grids as three distinct architectures: (1) wireless senor grid, (2) mobile wireless and (3) fixed wireless. McKnight et al. [44] provide a classification of the wireless grid which differs from a typical wired network such as the: (1) applications aggregating information from the range of input/output interfaces found in nomadic devices, (2) applications leveraging the locations and contexts in which the devices exist and, (3) applications leveraging the mesh network capabilities of groups of nomadic devices.

The wireless grid extends grid resources to wireless devices of varying sizes and capabilities such as sensors, mobile phones, laptops, special instruments, and edge devices [1]. These devices might be statically located, mobile, or nomadic, shifting across institutional boundaries and connected to the grid via nearby devices such as desktops [45]. Resources can be searched, found, viewed, and manipulated remotely from any other grid-enabled device or service and devices on the wireless grid network can serve as both servers and clients. Agarwal [1] identifies these grids as an augmentation of a wired grid that facilitates the exchange of information and the interaction between heterogeneous wireless devices. These grids will enable shared resources among dynamic groups or social networks of computing and communication devices and are composed of objects and resources with individual profiles that are assigned a specific status relative to similar objects and resources [45]. Wireless grids can take ubiquitous computing to the next level by providing seamless wireless extensions to the wired grid. The architecture for these types of grids are of importance because they can be deployed to provide autonomous nodes that communicate with each other in a decentralized manner and how each node of the network connects others with wireless links, and acts as both a host and a router in sending and receiving data.

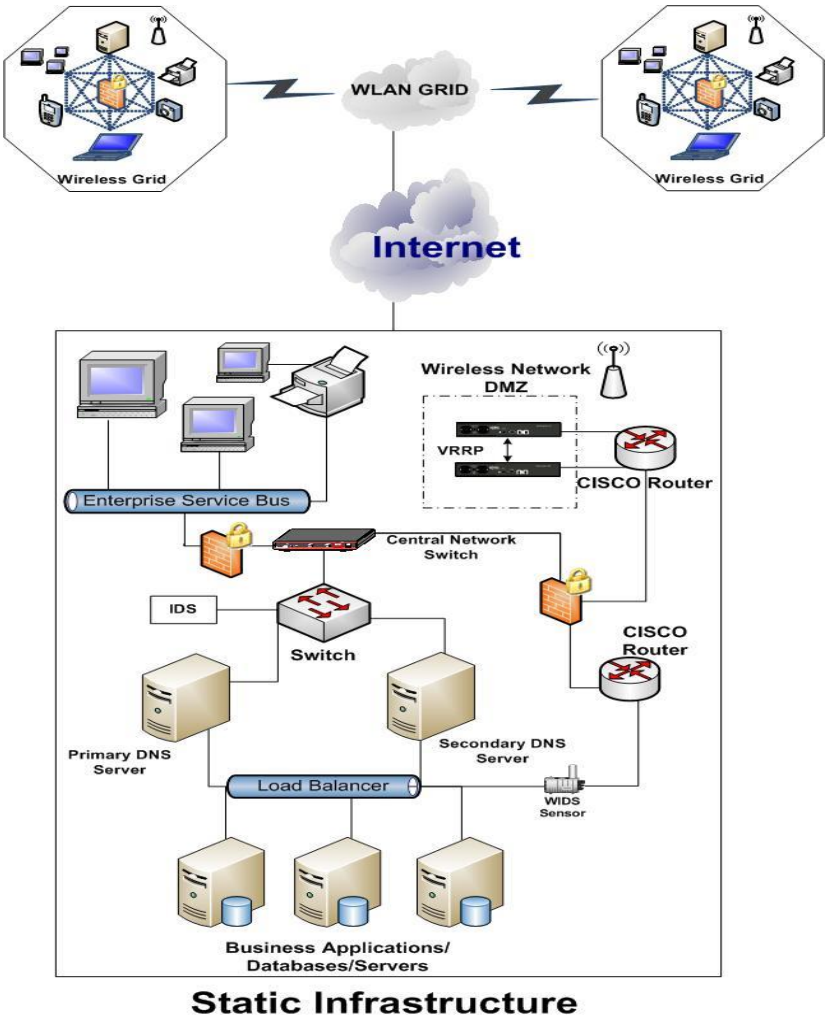

Figure 2. Wireless Grid

Grid computing and grid topologies have been extended into the wireless implementations and have been used to facilitate the exchange of information between heterogeneous wireless devices [1, 42]. Wireless grids can take distributed computing to the next level by providing seamless wireless extensions to the wired grid. Wireless grid computing consists of autonomous nodes that communicate with each other in a decentralized manner. Each individual node of the network connects with other nodes via wireless links and acts as both a host and a router.

One major issue with wireless grids is information security [1]. Integrating wireless grids with an existing information system (e.g. cloud computing) or traditional wired network raises new challenges in terms of routing, aggregating and querying data from multiple sources on wirelessly connected heterogeneous devices. As with all wireless information, the communication devices in the grid communicate and pass information over standard radio frequencies which can be easily tapped [42]. Even if the wireless grid utilizes a firewall and proxy system that filters out any potentially malicious network packets or web content, data can still leak outside of the grid. The wireless grid will generally be more vulnerable to malicious and accidental threats than their wired counterparts. A defined security architecture must be a mandatory component of the wireless grid if this inherent vulnerability is to be properly addressed.

Security architecture and security analysis of communication protocols for mobile wireless networks must also be taken into consideration [48, 61]. Security is always an issue with mobile wireless devices since wireless transmission is susceptible to a wide range of attacks [57]. Because of the inherent nature of the wireless connection, protecting information is difficult. The diversity of the link quality, the potential unreliability of the end-devices, the power constraints of the mobile device, and the enforcement of security and privacy policies all present major challenges in the wireless grid environment [1]. The Wireless Grid Innovation Testbed (WiGiT) at Syracuse University is one organization researching a deeper understanding

of wireless grid security, application, device, network, user and market behavior through academic, trade and popular publications [68].

Most existing wireless security typically includes some form of security mechanisms (e.g. wired equivalent privacy [WEP]) that provides security on an access point-by-access point basis [22]. As wireless grid technology continues to grow, the grid will become increasingly heterogeneous, requiring data to transit across various trusted wireless networks. For this reason users will come to demand more robust end-to-end security services. In order to make integrations more feasible, such as wireless grid and cloud computing services, grid services will have to be complemented by the addition of security services. This could potentially lead into the development of a new wireless cloud architecture.

4. THE WIRELESS CLOUD

Under emerging wireless grid architectures, however, such network-based security models are far from adequate. These new systems will be about net-centric information sharing and collaborating business functionality which will become service-enabled and exposed to external wireless clients via standard web services type protocols. These wireless clients, which themselves may be applications, will dynamically discover services and make real time use of their code and data. Their services will be inherently location independent, not necessarily bound to a physical location, which can change over time as services are relocated or for fail-over reasons. Since wireless grid clients and service providers may belong to different physical networks or even different service providers, these networks and/or organizations may be governed by entirely different security policies.

Therefore, in a wireless cloud environment, organizations will need to shift their focus from perimeter-based security models to a service-level view of security. Emphasis should be placed on network identities, trust, and authorization of both users and applications rather than on ownership and control. The architectural model of a wireless cloud computing environment is identified in Figure 3. Li et al. [39] identified the wireless cloud as a natural extension of the wireless grid. It provides seamless access to the internet, networked devices and computing capabilities. The wireless cloud is a kind of next-generation wireless grid and as an emerging technology, there is very little in the literature about it [38].

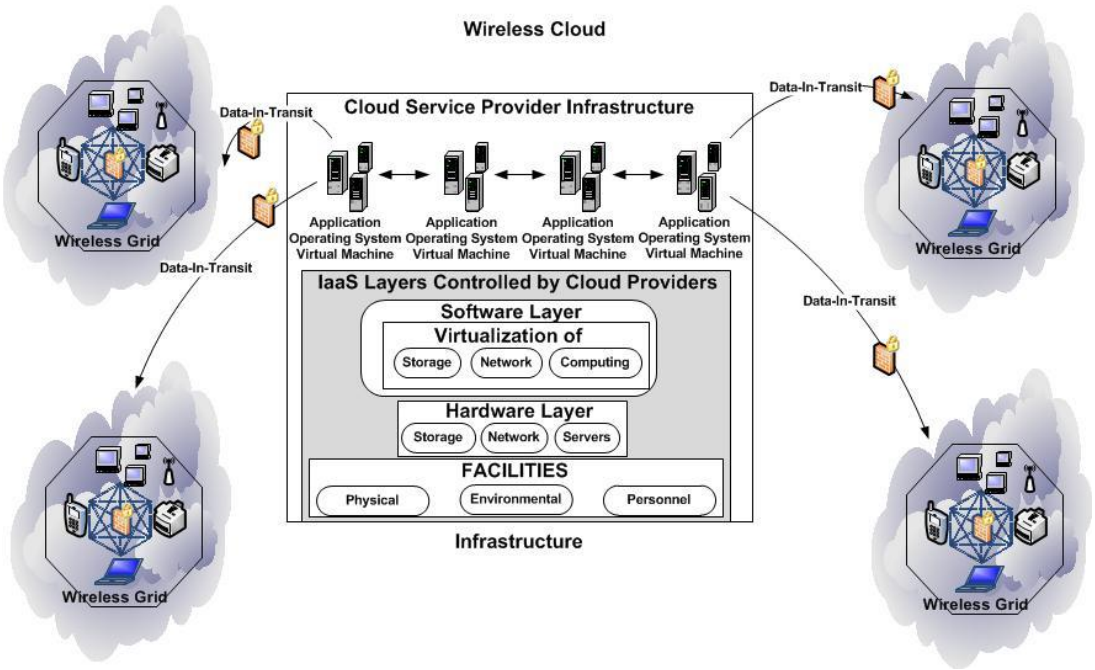

Figure 3. The Wireless Cloud

Combining cloud computing and the wireless grid will create a new form of distributed computing. Through loosely-coupled computers acting in concert to perform large tasks wirelessly, the packaging of computing resources, such as computation and storage, will provide a future architecture capable of a grid-utility like model. The wireless cloud's device and location independence enables the wireless grid to access the cloud systems regardless of device location or what device they are using. System performance could be monitored and managed for consistency but may be affected by insufficient bandwidth or high network load.

Since scalability changes system configuration to meet changing user demands, the wireless cloud could operate without having to engineer for peak loads which may result in lower operational costs.

This conceptual model also emphasizes the importance of architecting for the cloud versus simply deploying system components to the cloud to ensure that business requirements are met. Typical software and systems that are not designed to take advantage of the scalability and parallelism of the cloud will likely not achieve the full benefit that is provided by a cloud computing environment. Wireless cloud security may improve due to added security-focused resources but currently there are some concerns about possible loss of control over sensitive data. The data residing in the wireless cloud has to be managed on all security devices. The enforcement of security policies must take place to ensure the network has the latest protection against threats. The solution must also provide end-to-end visibility to validate and audit security effectiveness and monitor security events.

As cloud and wireless technology advances, the wireless cloud architecture could progress from a distributed, decentralized architecture with a lot of data in "thin" access points (APs) to a centralized architecture using "thick" APs with data located in wireless switches. When considering the risks associated with a wireless cloud architecture, the most fundamental element that must be considered is how the wireless cloud environment affects the trust model. In thinking about this question, first consider a traditional computing model where applications reside on client machines, servers, or mainframes that are owned and controlled by the enterprise. In this environment it is possible to levy a host of countermeasures to mitigate the security risks that exist in the IT world. Those countermeasures include firewalls, data encryption, antivirus solutions, tight access permissions, virtual or physical separation of networks, and more. Coupled with those technical countermeasures are the use of trusted network administrators, application developers and internal processes. Now consider what happens when the applications move to a wireless cloud in which the business model is typically driven by the provision of common service to a wide variety of customers. At this point, the security of those applications and their data are largely a function of the skill, willingness, diligence, and ability of the wireless provider to protect the data and provide reliable service.

Due to this issue of the movement of the trust model from customer to provider, the wireless cloud represents a significant challenge from an information security perspective. While the specific concerns will vary somewhat depending upon the implementation of a wireless cloud solution, the question remains as to just how far does the trust model extend? Certainly vulnerabilities and threats must be identified in dealing with this type of solution, where security may be a shared responsibility and where the final installation of a blend of network elements, operation system and tools will have to provide an operational solution.

5. VULNERABILITIES AND THREATS TO THE WIRELESS CLOUD

As data flows in the wireless cloud, data confidentiality and integrity controls need to be applied to limit exposure to unauthorized users. The knowledge of information security threats are quite useful to system administrators, testers, and information assurance professionals, who need to understand how an information system might be attacked. The intention of a threat is to exploit a vulnerability of a weakness in an information system. In any risk assessment, threats must first be identified. CNSS Instruction 4009 [13] defines a threat as 'any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial-of-service (DoS) attack'.

Unlike a wired network, the wireless cloud is not limited by physical space. This potentially opens up the network to attack from rogue users who spy on wireless transmissions or gain unauthorized access to the network from the inside or outside [26]. Traditional thieves, hackers, high-tech criminals, government sponsored organizations, viruses and other types of malicious code are the typical causes for security concerns on wireless networks [73]. The targets for attacks are the files stored on hard drives and other media, data and voice communications transferred between the remote clients and the internal networks, or the remote system, since it is used to gain access to the main network.

Vulnerabilities exist in wireless networks that are interconnected with any other system. The entire network becomes more vulnerable because when one part of the system is compromised, the rest of the network can be affected as well. Unprotected wireless communications equipment is also vulnerable to vandalism and terrorism that may cause large-scale communications outages [73]. The scale of any attack against any wireless network depends on the type of network, the security precautions of the network, the location of the network and the ability of the adversary that desires that information.

All the vulnerabilities that exist in a conventional wired network will apply to the wireless cloud. Malicious entities may gain unauthorized access to a given computer network through wireless connections, bypassing any firewall protections and may steal the identity of legitimate users and masquerade them on internal networks [72]. These entities may be able to violate the privacy of legitimate users by tracking their

movements or using third party, untrusted wireless network services to gain access to network resources. Malicious code or viruses may corrupt data on a wireless device and subsequently be introduced to a wired network connection. While it is more difficult and potentially more important to secure wireless communications, the issues, threats and the respective required services to adequately respond to these threats are mostly the same for wired and wireless technologies.

Managing security threats and vulnerabilities in information system assets are two fundamental challenges for organizations [51]. Security engineers can reduce the risks associated with systems by identifying threats, and making design or procedural changes in a system to reduce its vulnerability to those threats. This article identifies potential threats to a wireless cloud environment that can be used as a starting point to secure a wireless cloud architecture. While this list is not all inclusive, it will likely be expanded as industry experience with wireless clouds grows, technologies evolve, and the ingenuity of attackers seeks new ways to achieve their ends.

The knowledge of threats are quite useful to system administrators, testers, and information assurance professionals, who need to understand how an information system might be attacked. The intention of a threat is to exploit a vulnerability of a weakness in an information system. In any risk assessment, threats must first be identified. For example, researchers such as Welch and Lathrop [70] and Yang et al. [71] have identified some of the following threats against the IEEE 802.11 WEP, the standard for wireless networking, as follows:

- *Traffic Analysis*- a simple technique whereby the attacker determines the load on the communication medium by the number and size of packets being transmitted, the source and destination of the packets and the type of packets.
- *Passive Eavesdropping*- the attacker passively monitors the wireless session and the payload. If the payload is encrypted, this includes breaking the encryption to read the plaintext.
- *Active Eavesdropping*- involves the attacker injecting data into the communication to help decipher the payload and then the attacker not only listens to the wireless connection, but also actively injects messages into the communication medium in order to assist them in determining the contents of messages.
- *Unauthorized Access*- not directed at any individual user or set of users on the wireless local area network (WLAN). Once an attacker has access to the network, additional attacks can then be launched or free network use is provided.
- *Man-in-the-middle*- used to read private data from a session or to modify the packets thus violating the integrity of a session.
- *Session High-Jacking*- an attack against the integrity of a session; the attacker takes an authorized and authenticated session away from its proper owner.
- *Replay*- used to gain access to the network with the authorizations of the target, but the actual session or sessions that are attacked are not altered or interfered with in anyway.

While many of the attacks referenced above are common across wireless environments, the highly distributed and collaborative nature of the wireless cloud will have to take on increased security protocols to protect against threats from the wireless grid environment, the cloud environment and the data transported from the cloud to the grid (see Figure 4, Wireless Cloud Threat Model). While threats focus on specific attacks to computing environments, the model below takes into consideration that threats should consider the skill of the attacker, their propensity to actually launch an attack, their concern for risk of detection or attribution and the likelihood of success. The assumption is that the most highly skilled, motivated hackers would attack organizations that implement a wireless cloud within its environment.

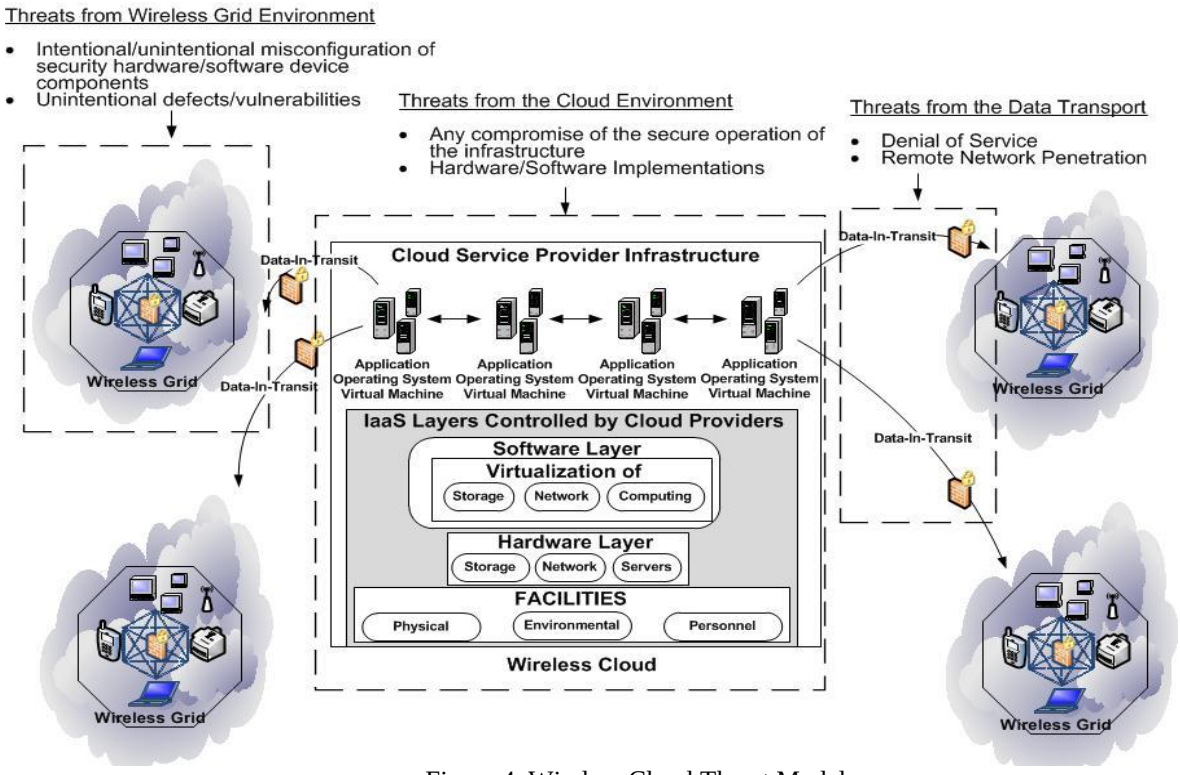

Figure 4. Wireless Cloud Threat Model

Threats from the wireless grid environment covers those conditions involved in the actual use of operational wireless grid devices. Since each wireless grid location being connected to a cloud environment may be different, the worst case environment would have to be considered from a risk assessment viewpoint. These conditions of use introduce the threat of people who have authorized access that may intentionally or unintentionally misuse, misconfigure, or bypass the security functions within the wireless grid. Threats related to people getting unauthorized, direct physical or logical access to the wireless grid devices security functions and any tampering or misconfiguration might occur as a result of a threat to this environment. This also includes those threats related to someone stealing or substituting hardware or software devices that provide security functions within the wireless grid.

Threats that arise from vendor's supply chain of wireless grid devices for an organization may cause security concerns to the wireless cloud architecture. The supply chain security challenges posed by the threat of attacks have significant implications for enterprises and their suppliers [9]. The whole process of implementing, maintaining, upgrading and patching hardware and software for wireless grid devices could introduce threats. Threats from the wireless grid hardware/software device supply chain include any related to having an adversary intentionally modify, bypass or weaken the security functions during development, production, distribution, maintenance, shipping and warehousing/storage of these entities. Since such functions are not perfect in their implementation, there is also the threat from unintentional defect in the device hardware or software or in the overall wireless grid security architecture in which they exist.

Threats to a cloud computing environment are also of concern. There are multiple attack vectors within the software architecture of a cloud including virtualization software, web browsers, security software, and client / server operating systems [40]. Attacks could also be launched against major cloud services, such as Amazon Web Services (AWS) and Google Apps, potentially affecting thousands of cloud consumers. Web services could be targeted through exploitation of vulnerabilities inherent in extensible markup language (XML), simple object access protocol (SOAP), and web services description language (WSDL). The provider and consumer security services, such as anti-virus and personal firewall applications, could be compromised. Attacks against web browsers can compromise communications between the consumer and the cloud provider and could allow attackers to intercept data (e.g. passwords, encryption keys, files); redirect web browsers to compromised sites; and prevent the web browser from functioning properly, thus inhibiting Internet communications.

One of the most critical and yet difficult challenges is ensuring continuous availability of wireless cloud resources. Protection of the critical infrastructure components, such as routers, gateways, and domain name system (DNS) servers, and the communications pathways between cloud provider and consumer, are

key to maintaining resource availability and the integrity and confidentiality of data transmitted across these channels. Threats that impact communications can be either malicious, such as DoS attacks, aimed at wireless connections or devices, provider, consumer, or network resources; authentication and encryption infrastructure components; or inadvertent outages to include technical failures, power outages, Internet congestion, and natural disasters. Blacklisting of internet protocol (IP) addresses used by cloud consumers or cloud providers could also be a serious problem. Perceived inappropriate behavior by cloud consumers, which originate from within a cloud provider data center, may cause the IP set utilized by the provider to be blacklisted by internet service provider's (ISP) and other cloud vendors. Whether the actions were inadvertent or malicious, the blacklisting of providers IP's would impact not only consumers from accessing cloud services, but could be financially devastating to a cloud provider.

Physical security deals with access to computing facilities, infrastructure, and personnel that support the cloud provider, consumer, and communication pathways in between. While physical security is not unique to cloud computing, the shared resource environment of a wireless cloud architecture increases the potential to access data and computing resources of other organizations. A physical security breach within the cloud provider data center allows intruders potential unauthorized access to the data of hundreds or thousands of users spanning various organizations [3]. Likewise, unauthorized access to computing assets at a consumer's facility may provide access into the cloud provider environment, allowing the attacker to inject malware into the infrastructure of the provider. Cloud provider administrators and maintenance personnel have physical access to the shared resources within the cloud (i.e. hardware, power, network, storage, firewalls).

Threats from the data transport from the cloud to a wireless grid environment must also be taken into consideration. Confidentiality and integrity of data must be protected at all times [58], whether that data is 'at-rest' or 'in-transit'. The wireless cloud must provide protection against unauthorized alteration of messages and documents during data transit. This is especially important in a wireless cloud environment as cloud consumers will be accessing data, applications, and services across the great expanse of the Internet, increasing the exposure of sensitive data to interception, modification, and injection attacks. Protection of data within the boundaries of a wireless cloud environment is equally important as public clouds are environments where computing resources are shared among potentially thousands of different users and must be protected from the prying eyes of other cloud users. It's also important to protect the underlying communication (transport) as well as messages and documents that are carried over the transport so they cannot be made available to unauthorized parties.

Typical threats to data-at-rest within the wireless cloud could include the inadvertent or malicious alteration or deletion of data and files, data theft, and DoS attacks that prevent access to data, applications, and services. Inadvertent alteration or deletion of data and files is often due to improperly configured access controls versus malicious attacks perpetrated by hackers. Data-in-transit is susceptible to interception (e.g. man-in-the-middle attacks), injection, and modification, all of which pose serious risks to the confidentiality and integrity of the data. Data may be extracted without detection from improperly configured devices. Improperly protected end-user machines (i.e. at work or home) could spread malware to a virtual machine (VM), and in turn spread to other users as they connect to the VM. As wireless cloud users connect to resources distributed across multiple VM's, malware may also spread. To reduce the potential spread of malware from unauthorized or personal devices, organizational security policies must address whether security services, such as anti-virus and personal firewall applications, will be extended to protect home personal computers (PC), Internet-enabled phones, or only allow users to connect to cloud resources with company-provided computing resources.

Much like an outside hacker, an insider with authorized access to a wireless cloud system could execute various attacks to gain unauthorized access to other systems or deny service to users of these others systems and even manipulate files that facilitate the provision of services on virtual/remote machines. Insider abuse, when both malicious and accidental insider misuse of internal systems occurs, poses the most serious threat for wireless clouds. While organizations have to deal with insider threats today, the concentration of information and processing into wireless clouds will magnify the potential impact of insider abuse. Wireless clouds will be particularly threatened by malware for two reasons: (1) the homogeneous structure, rich interconnections, and large scale of a cloud raises the possibility of initial malware injection and can offer malware easy avenues for propagation, and (2) the concentration of value in a cloud offers potential attackers, both insiders and external adversaries, a high-value target for tailored, specialized malware.

Wireless cloud data owners will have to worry about two potential threats: accidental leakage of information outside the security enclave, and negative impacts to the integrity or availability of their information from the introduction of malicious code or DoS attacks. Wireless clouds will store and process information from various sources (e.g. clouds, devices, etc.), offer access to many different users, and connect to a wide variety of external systems. This increases the threat of cross-domain leakage of

information. Therefore, wireless clouds will not have the luxury of keeping 'customers' completely segregated, but will have to provide controlled sharing. These sharing mechanisms will pose the greatest threat for leakage. As such, there must be securing mechanisms for addressing threats for securing wireless cloud environments.

6. SECURING THE WIRELESS CLOUD

Any communications network is subject to becoming the target of exploitation by individuals or groups outside of the authorized group of intended users. Traditionally, only the communications of governments and large corporations were regularly subject to such targeting. The military and diplomatic communications of governments were targeted for national secrets, while corporate communications were targeted for technology and trade secrets. Exploiting government and corporate communications networks required a large expenditure of resources. The exploitation of communications is conducted to gain access to data flowing over a network, disrupting the flow of data on the network and to parasitically seize the network's resources (i.e. to use a network free of charge). There is an additional reason for exploiting a communications network; however, it is used to a much lesser extent – disinformation. Disinformation can be injected into a communications network in order to mislead and to cause confusion and doubt and can give a political, military, or economic advantage to the exploiter [66].

The first and foremost goal of the new wireless cloud security architecture is to ensure services can be invoked and managed in a secure fashion. As with just about every critical distributed system, there is a set of key security requirements that will need to be met which include authentication and authorization, confidentiality, data integrity, availability, non-repudiation, security policy exchange, intrusion detection, protection, and secure logging, manageability and accountability [6, 16, 18, 41]. For the wireless cloud, additional security measures will have to be implemented to ensure the cryptography (e.g. confidentiality, data integrity, entity authentication, and data origin authentication and availability) of all information that is acquired, process and transmitted due to the nature of its architecture [43]. The integration must ensure that security boundaries and security tools are designed and positioned to complement each other and interoperate as appropriate. These include:

- *Interoperability*: the cornerstone of the wireless cloud architecture and must be preserved to the maximum extent by the security architecture. Major security integration points in the architecture – such as those between cloud computing service providers and wireless grid clients, between service providers and the security infrastructure, and between security infrastructures in different trust domains – must have stable, consistent interfaces based on widely adopted industry and government standards, which enables each domain or organization to implement its own market-driven solution while maintaining effective interoperability.
- *Tailored security policy constraints*: in a traditional security domain, resources and services are often protected by a uniform set of security rules that are not granular enough to meet specific application needs. Because customer who may access a resource may or may not be from the organization's local domain, different "strengths" of authentication and access control may be required. Consequently, security policies need to be expressive and flexible enough to be tailored according to both service providers' and wireless grid policy attributes.
- *"At-Rest" data security*: focusing primarily on securing "in-transit" data, such as XML messages and resource access, security measures also need to be in place to protect data "at rest", which include but not limited to protection of storage of credentials (private keys, etc.), protection of security infrastructure components, such as policy stores, and security logs.

Organizations must ensure the quality of data being processed and distributed with respect to defense of the network at a level that is useful to the end user. The wireless cloud will have to provide the nature of each transaction, to include the data standard, the content of the data, and the performance attributes of the data. Appropriate components must ensure that each of these parameters remain constant for data being relayed to wireless cloud activities, as well as meeting the performance standards defined within the wireless cloud. Data transported through the wireless cloud network must have a constant and reliable level of integrity, must not be undermined while passing through the network, and must maintain quality of the data if latency occurs. For information that is processed or created for an external user, it must be guaranteed that the quality and timeliness of the data remain useful in the analysis and combat of threats to the network.

Because of the threat of exploitation, the wireless cloud will have to be protected by a well-defined security architecture. A security architecture encompasses IT security and data privacy requirements as well as solutions within the context of an over-arching enterprise architecture [5]. The wireless cloud model is one in which organizations will have less control over their security architecture than in traditional networks and

at the same time are required to share IT infrastructure with other entities. This dynamic causes certain key challenges to rise in prominence in which the security architecture components for the wireless cloud must have an extensive security architecture in place. One such framework that could potentially address the wireless cloud security approach to creating secure, integrated and interoperable grid services based on a set of security abstractions that unify formerly dissimilar technologies is the Grid Security Model [18, 49] as depicted in Figure 5.

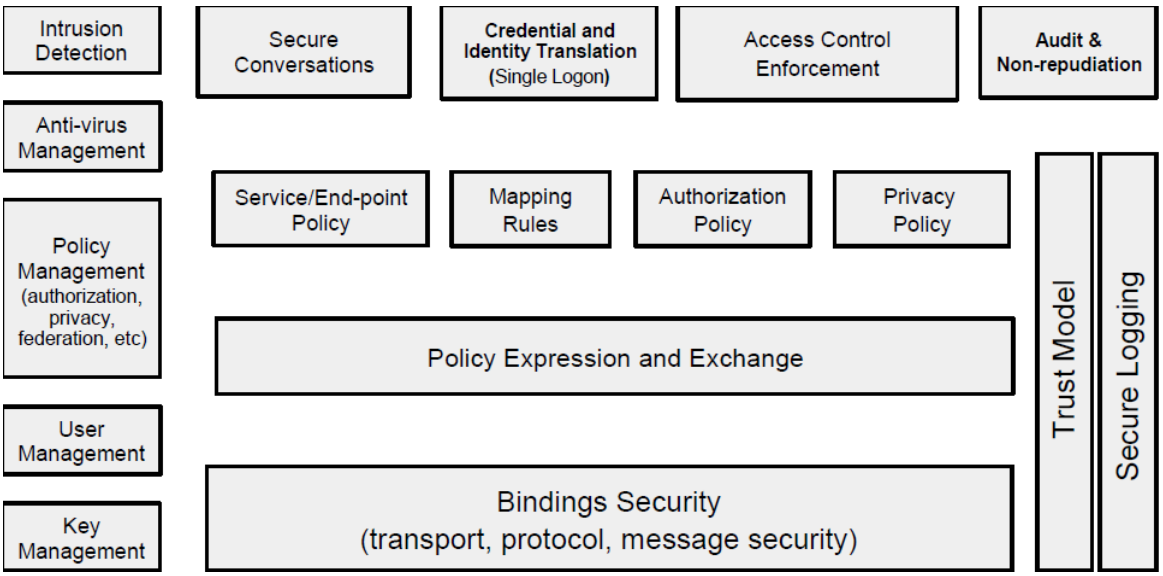

Figure 5. Grid Security Model
(Source: The Open Grid Services Architecture, Version 1.5)

A security framework ensures that basic security practices are implemented across an organization by integrating industry security best practices at multiple levels of the enterprise: information infrastructure design; software, hardware, and service procurement; application development; and training. This emerging Grid Security Model appears to offer an inherently practical framework in which to build and manage wireless cloud systems to meet security requirements [19]. For the purposes of this article, the authors are only addressing the authorization (including authentication) processes of this particular model.

7. AUTHENTICATION

One of the most important security controls of any IT system is the authorization, authentication and access of the system [31]. Policies are one aspect of information which influences the behavior of objects within systems. To achieve both sharing of information and protection of information in a wireless cloud environment, it is necessary that common authorization and authentication policies and mechanisms be used. Whereas authorization is the process of giving user's access rights to computer resources based on their permissions and privileges [5], authentication is the verification of the identity or other attributes claimed by or assumed of an entity (user, process or device) or verifying the source and integrity of data. The wireless cloud's authorization policy has to address the processes of ascertaining authorizations prior to allowing performance of an action such as viewing or accessing information through authentication. Ideally, the authorization policy mechanism will have to provide interoperable authorization capabilities among cloud providers.

Cloud service providers will require that wireless grid organizations have authorization/authentication policies and contracts in place before granting them access to specified data. Different authentication mechanism standards should be leveraged, supported, configurable and pluggable depending on service-specific requirements (e.g. eXtensible Access Control Markup Language [XACML] Authorization Model, Security Assertion Markup Language [SAML], Globus Toolkit [GT] 5.03 [35, 50, 67]. Control access to cloud services based on authorization policies (i.e., who can access a service, under what conditions) may be attached to each service. Different access control models may be used, such as mandatory access control [53], discretionary [63], or role based models [62]. The authorization implementation should also be extensible to allow for service-specific customizations (i.e. specific financial information for financial institutions). Ideally, the authorization policies will have to be provided by the cloud computing provider and

the organizations using a wireless grid. This level is necessary, as additional structures must be put in place to have interoperable authorization capabilities among multiple enterprises (i.e., shared community space). Without procedures and methods in place to ensure that sharing takes place without ignoring appropriate protection of the information, collaboration is not possible.

A fully realized secure wireless cloud systems architecture will be highly dependent on a decentralized identity management and authentication architecture able to offload authentication. Authentication systems not only need to manage user identity certificates but also device-to-device certificates. Users utilize these certificates to authenticate to the policy enforcement point, while the devices utilize these certificates to authenticate each other and negotiate encrypted tunnels. Because of the lack of maturity of endpoint policy enforcement systems that can self-scan and automatically assure compliance as part of the authentication process, assurances of a secured endpoint remains the arena of hardened configurations and aggressive compliance scanning and remediation. For this reason, initial implementation of this wireless cloud solution should focus on systems where internet connectivity and the use of high efficient equipment can reasonably be restricted.

Authentication /authorization collectively generates, assigns and manages identities and places those identities into credentials (i.e. X.509 certificates) [54]. Thus, authentication mechanisms are required so that the identity of individuals and services can be established, and service providers must implement authorization mechanisms to enforce policy over how each service can be used [49]. Authentication uses identities in the system and manages security-related attributes such as role in the system. Figure 6 provides a generic Wireless Cloud Authentication, Authorization and Access Control Process.

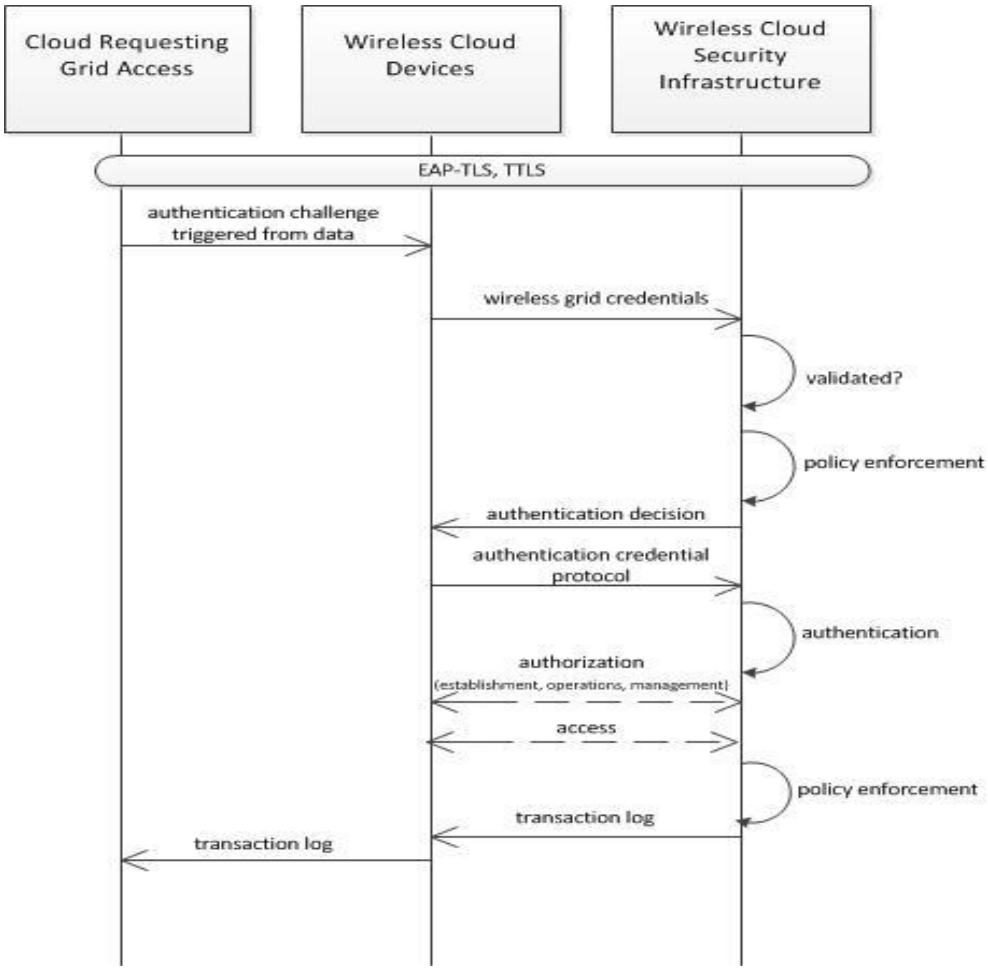

Figure 6. Wireless Cloud Authentication, Authorization and Access Control Process

Authentication requires that the user (e.g. cloud computing system) prove its identity. As data is received from the cloud to the wireless grid, a challenge/response mechanism is used as a method of identification. Authentication should be two-way, so once wireless grid credentials have been accepted and

validated; policy enforcement must be enforced in order to render an authentication decision. This lets the system know that it is communicating with a valid user. By having the system authenticate to the user, it is less likely that an unauthorized third party will be able to pose as a system by inserting itself into the link between the user and the valid system (i.e. man-in-the-middle).

Wireless grid authentication should be based on wireless network authentication mechanisms [21]. Authentication for wireless grids must involve strong encryption to prevent eavesdropping, and must involve mutual authentication to ensure that sensitive information is transmitted only over legitimate networks. The wireless grid must also have strong authentication standards to meet the challenges for strict encryption and authentication requirements. Strict encryption and authentication requirements are met by IEEE 802.11-based wireless local area networks (LAN) through the implementation of the IEEE 802.1x standard. This standard specifies the use of the extensible authentication protocol (EAP) directly over a link layer protocol [24].

EAP is essentially a transport protocol that can be used by a variety of different authentication types, known as EAP methods. EAP was standardized by the Internet Engineering Task Force (IETF) in March 1999 [8]. Among the EAP methods developed specifically for wireless networks are a family of methods based on public key certificates and the transport layer security (TLS) protocol. These are extensible authentication protocol transport layer security (EAP-TLS) and the extensible authentication protocol tunneled transport layer security (EAP-TTLS).

EAP-TLS uses the TLS public key certificate authentication mechanism within EAP to provide mutual authentication of client to server and server to client [20]. With EAP-TLS, both the client and the server must be assigned a digital certificate signed by a certificate authority (CA) that they both trust. The EAP-TLS key system uses dynamic wired equivalent privacy (WEP) or temporal key integrity protocol (TKIP) keys. EAP-TLS uses a TLS handshake as the basis for mutual authentication [20]. EAP-TTLS has been implemented in some remote authentication dial-in user service (RADIUS) server and supplicant software designed for use in 802.11 WLAN networks. In EAP-TLS, a TLS handshake is used to mutually authenticate a client and server [12]. EAP-TTLS extends this authentication negotiation by using the secure connection established by the TLS handshake to exchange additional information between client and server. In EAP-TTLS, the TLS handshake may be mutual, or it may be one-way, in which only the server is authenticated to the client. The secure connection established by the handshake may then be used to allow the server to authenticate the client using existing, widely-deployed authentication infrastructures such as RADIUS [12].

8. AUTHORIZATION

After the user has proven who they present themselves to be, the next step is to provide authorization. Authorization is the granting of access to network resources and services, and entails restricting internal resources from users; it also determines access control [12]. In order to provide a complete authentication function in the wireless cloud system, three categories of an authorization sub-function have to be implemented: establishment, operations and management. The first process is the establishment function; that is, those related to successfully initiating the function and getting it running correctly. The second is the operations functions, which are the ones that the authorization function performs to carry out its business purpose. The third category is the maintenance function, which deals with keeping the authorization operating properly.

8.1. Establishment Functions

The authorization process for the wireless cloud has to be pre-provisioned with necessary values and information so that it can execute and deliver results. Figure 7 provides the Establishment Functions for the Wireless Cloud Authorization process.

The first step in the authorization process is to establish the pattern of the data being received. Once received, the provision identity (ID) credential process identifies the identity credential (e.g. PKI certificate) for its own use, so that it can be identified and authenticated itself in the system. This may come from a wireless identity management and/or credential management function. The protection mechanism has to protect the information it handles, both in-transit and at-rest. This might include cryptographic key material with which to encrypt and decrypt data. Trust anchors, with which to validate messages and signatures, have algorithms and signature key material to provide integrity.

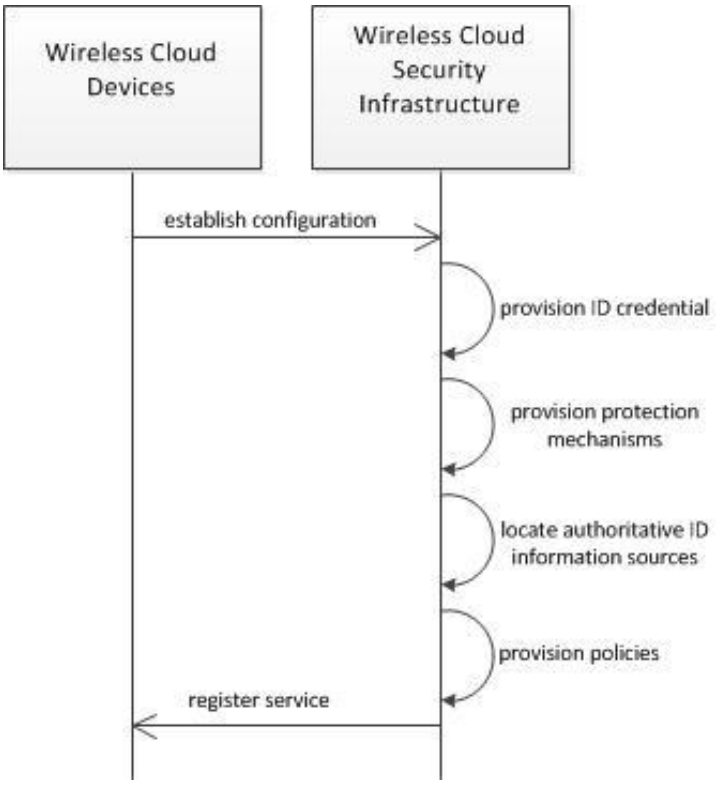

Figure 7. Establishment Process

Next, the locate authoritative ID information sources discovers the location within the system of enterprise services with which function has to interact. In addition, this sub-function discovers the location of all authoritative sources with which the authentication function has to interact including the identification of specific types of content for each source and the materials necessary to validate that the source of transactions with each of these authoritative sources can be validated. The provision policies sub-function downloads any digital policy updates and installs and updates those policy updates. Finally, the register service makes the authorization function discoverable across the system. This should be the last establishment sub-function to be executed.

8.2. Operations Functions

Once the authorization function is established in a wireless cloud system, it can carry out its processing purpose. Figure 8 provides the Operations Functions for the Wireless Cloud Authentication process. Once data is received, processing input messages come into the authorization function requesting a particular service (e.g. authorization of an entity, authorization of the source of the message, etc.). The first step is always for arriving messages to be processed to ensure that the message integrity is validated; that the message can be correctly decrypted if it is encrypted; that the message source can be authorized, if required and that the message source is authorized to send such a message. If all tests pass, the message is passed to the main authorization function. A request to authorize an entity in the system will contain a claimed identity, and an authorization value showing that the entity is claimed identity. Depending on the system used, the authorization value will be a string signed or encrypted with the private key, to prove possession of the private key.

Next, maintain the authorization status will track whether entities are currently authorized in the system. When an entity is authorized, this sub-function enters a record in the authorization repository. Policies dictate the parameters of the authorization (e.g. it is valid for 24 hours before re-authorization is required; it automatically expires after 10 minutes, etc.). This sub-function keeps a registry of all current and recently-expired authorizations and can tell other functions when a new authorization is required. Validating data integrity determines whether any of the data contained in the message has been changed. Possible mechanisms that can be used include cyclic redundancy checks, hashed message authentication checks, and digital signatures.

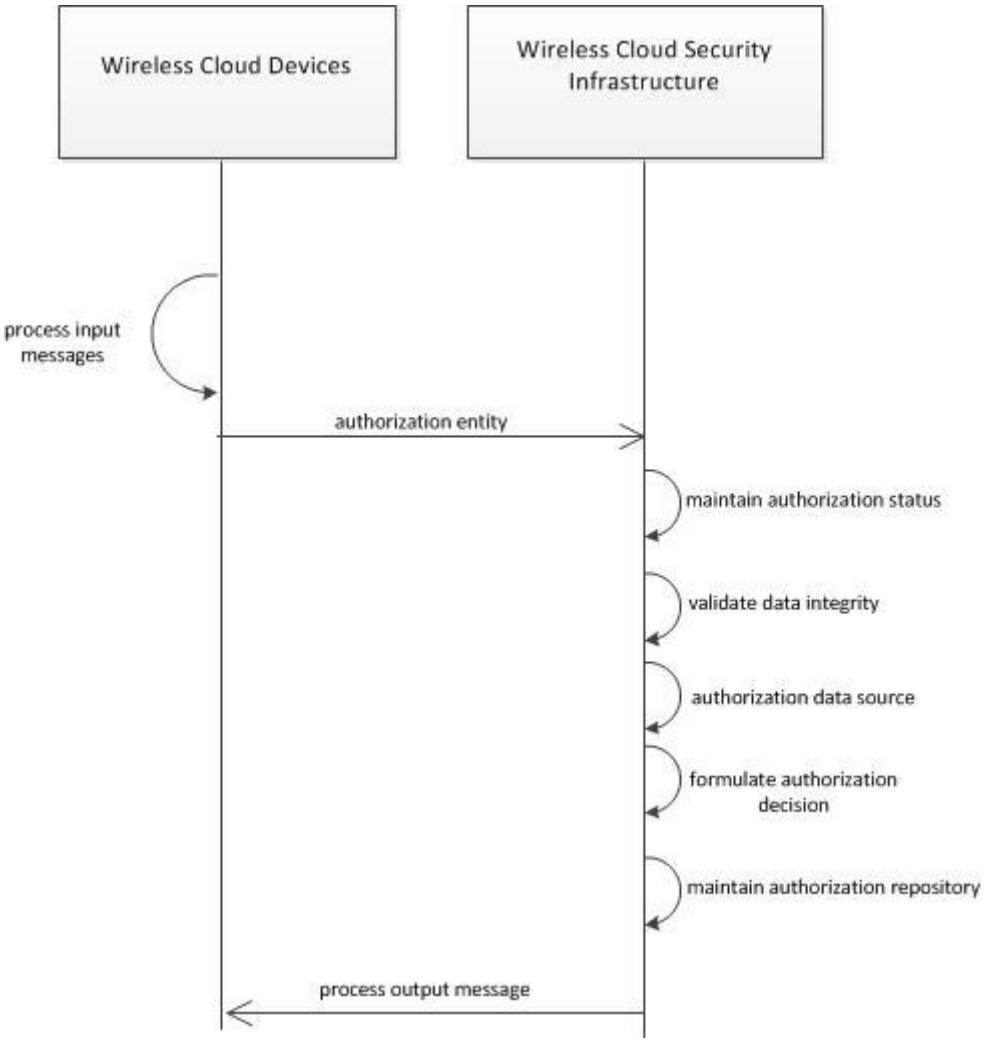

Figure 8. Operations Process

Authorization data source will require two steps to perform a source of authorization: (1) validating the integrity of the data to ensure it has not changed and (2) authorizing the entity that is the purported source of data. Calculating the assurance level calculates an assurance value for an entity authorization and passes it back to the requestor. Authorization decisions can be stronger or weaker based on a number of factors, including the type of authorization (e.g. two-factor authorization should be stronger than single-factor authorization), protection provided to the authorization channel (e.g. whether it is possible that an attacker copied a reusable authorization value, or injected a false value into the channel) and protection provided to the authorization database (e.g. whether it is possible that an attacker removed the true authorization value from the database and replaced it with a false one).

Finally, formulating the authorization decision takes the responses from the other sub-function and creates a response message that can be sent to the requestor. Maintaining the authorization repository needs a local repository for its own use, to store its policies, authorization decisions and current authorization values. The process output message is responsible for determining the destination of a message and protecting it according to policy (e.g. encryption, integrity protection, digital signature).

8.3. Management Functions

Management functions are performed concurrently with operations functions. Management functions are those concerned with the health and functioning of the authorization function, rather than performing the purpose of the authorization function. Figure 9 provides the Maintenance Functions for the Wireless Cloud Authorization process.

As with procedures messages, all management messages must be processed to decrypt them if necessary and to determine their integrity source and the source's authorization. When a condition is detected that is not considered a normal condition, an exception is deemed to have occurred. In this case, the authorization function's maintenance must report the exception condition (e.g. system administer); determine

the appropriate options (e.g. rebooting the system, restarting a process); and take action to restore the authorization function to normal operations.

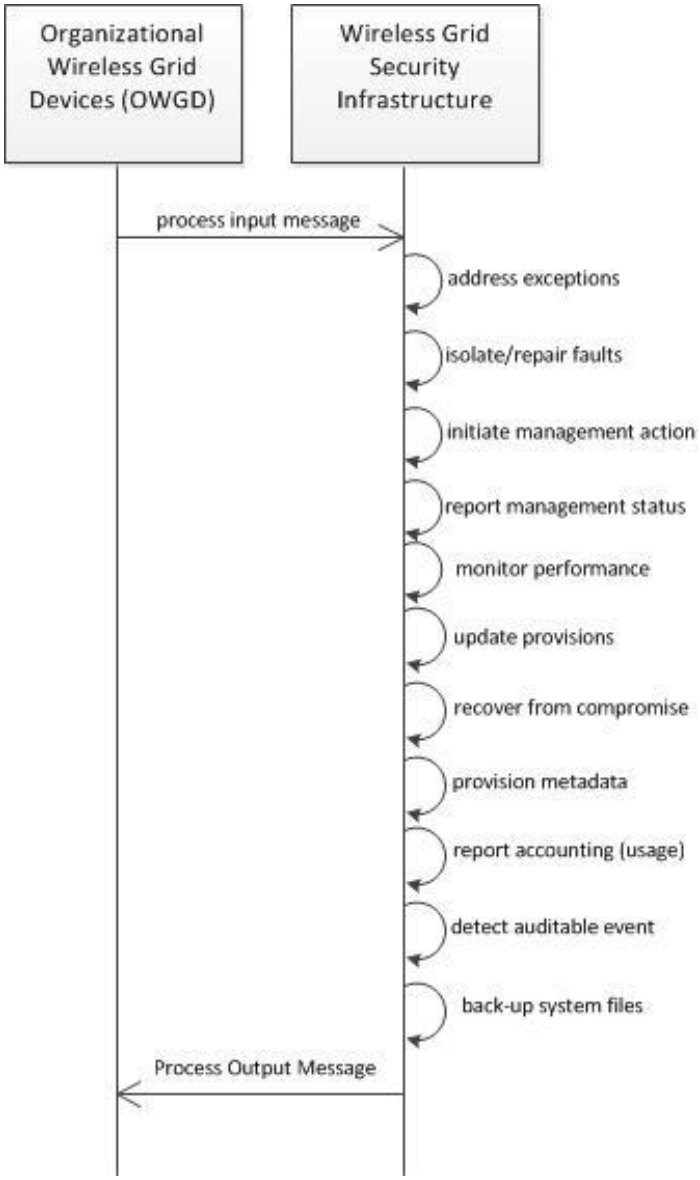

Figure 9. Management Functions

Authorization's fault process must include provisions to identify malfunctions or failures of the function mechanisms and resources (e.g. transport) upon which the function relies, and initiate an appropriate means of remedying the situation while ensuring ongoing operations during the failure. The remedy may be initiating a repair action, activation of, or cutover to some space or stand-by capability, or some combination. When a fault has occurred, or performance has degraded below some acceptable level, a management action, whether automated or human-in-the-loop, must be started to address the issue.

In response to requests, the report management status can report on usage, detected faults, performance anomalies, management action status, provision status, incident status, response status and other values. Monitoring performance monitors key performance indicators as specified in policies and reports or takes other action when performance degradation occurs, regardless of the cause. Updating provisions is responsible for reporting the status of and updating when necessary any of a number of key values, including policies, configuration items, key materials, etc.

The recover from compromise sub-function responds to the determination that a compromise to the system has occurred or suspicion that one has occurred. It includes capabilities to determine the impact of the

compromise, identification of options for mitigating the effect of the compromise and selection and execution of the mitigation response option. The provision metadata function initiates the discovery of metadata schemas required to assign valid discovery and metadata values from messages generated by the authorization function.

The report accounting (usage) sub-function maintains usage logs indicating when the authorization function is on-line and available as well as parameters and statistics about transactions. Examples of these parameters include the number of request transactions, specific requester and transaction requests, time of transaction occurrence, and the amount of time required before a response is initiated. The detect auditable event sub-function identifies the occurrence of events that specified by an audit policy. Upon detection, this function will generate an audit log event record, which it will protect and archive internally. Based on another input of digital policy, it will report the audit records. Finally, the back-up systems files create and archive all information necessary to reconstitute or re-initialize the operation status of the authorization function. Just as for operational messages, processing output messages is responsible for determining the destination of a message and protecting it according to policy (e.g. encryption, integrity protection, digitally signing it).

9. ACCESS CONTROL

Wireless cloud access control deals with the processes and procedures to verify that an authenticated and authorized cloud computing/wireless grid system entity is assigned to a role (e.g. retrieve data, process data, store data, etc.). The system entity must have the authorizations needed to use or access a system resource and decide whether to permit access to information or execution of an operation based on wireless cloud security policy and the operational context of the entity. The system should only permit pre-selected entities which have access based upon a wireless cloud access control list (WCACL). A WCACL[6] is operated and maintained by applications or data repositories to provide security management capabilities for wireless cloud access control activities.

A critical feature of any access control mechanism is recording of transactions (processes accomplished) and events (unexpected occurrences) for subsequent audit or other analysis by a system or security management activities [29, 48, 56]. Systems implementing access control decisions points must incorporate logging of transactions and events [62]. Systems implementing access control decision points must ensure the integrity of their transaction and event logs both in storage and in transmission [27]. Depending upon the log content, confidentially protection may also be required for storage and transmission. Figure 10 displays the Wireless Grid Access Control process:

Once an authenticated and authorized system entity invokes a session[7], the system entity selects a wireless cloud point-of-service (e.g. sensor network) to contact based on what task they wish to accomplish. The entity's identifier (e.g. PKI certificate, etc.) is securely passed to the point-of-service. The identifier enables where the entity is physically located, the associated risk to information and any security policy constraints or mandates associated with the location. To obtain system entity roles (and the authorizations associated with those roles) the wireless cloud point-of-service forwards via a secure path the entity's identity to the wireless cloud security infrastructure.

Using the passed entity identity, the wireless cloud security infrastructure looks up the roles (and associated authorizations) the entity has been assigned to for this particular process and returns, by secure means, the entity's roles (and associated authorizations) to the point-of-service. The wireless cloud security infrastructure caches the session parameters (entity identity, roles involved, etc.) for the duration of the functional session.

[6] The WCACL list would possibly include a list of authorized entities like system usernames and passwords, provide integrity protection for this information and may provide confidentiality protection for this information depending upon the function of the system.

[7] A session refers to the series of interactions between the entity and the point-of-service, plus all actions within the enterprise resulting from the entity's invocation of the particular point-of-service. The session ends when the entity receives their requested products or services and then terminates interaction with the particular point-of-service.

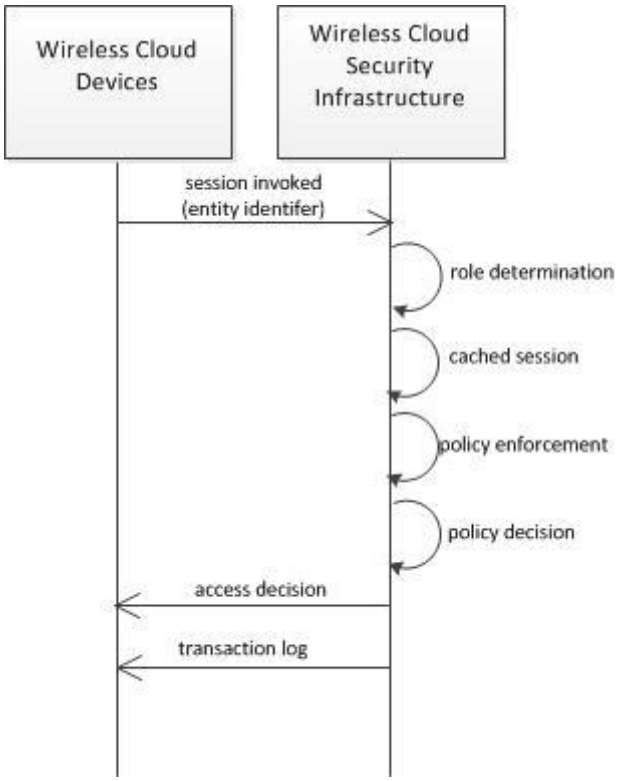

Figure 10. Access Control

Simultaneously, the wireless cloud policy enforcement cross checks this entity identity against the cache of other active sessions the same entity has underway to ensure the entity is not invoking mutually exclusive roles or triggering other policy concerns. If the additional role would cause a violation of security policy, notification is sent to the wireless cloud point-of-service handling the offending role. In turn, the functional portal caches the entity's role (and authorizations) for the duration of the session and securely forwards the system entity's role-based authorizations when initiating interaction with any additional organizational capabilities (e.g. applications, query services, data brokers, etc.). All requests forwarded to these capabilities are within the entity's role-based authorizations and restricts all information flowing back to the system entity within the entity's role-based authorizations. The system then notifies the wireless cloud security infrastructure upon completion or termination of the entity's session with the wireless cloud point-of-service and logs all of the transactions for subsequent policy compliance audit or other analysis.

In some cases, authentication, authorization and access control could be accomplished solely by a wireless point-of-service at the interface, allowing a system entity access only to those capabilities specifically authorized by the entity's role. In other cases, a combination of authentication, authorization and access control points might be needed with multiple information brokers tailoring repository queries to ensure only role allowable responses. An information broker interface, followed by an application review of the aggregated information and an operational system check by the wireless cloud, will initiate the information retrievals and forward the results through the wireless point-of-service to the entity.

To summarize, creating a wireless cloud must ensure adequate protection for information, systems and sources. There must be flexibility in both the location and nature of the wireless cloud authentication, authorization and access control decisions. To these ends, the wireless cloud may have to accommodate these decisions at many locations as well as at the interfaces between the receiving organization and external parties or other enterprises.

10. RECOMMENDATIONS

The wireless cloud system, applications or services must include a defined set of authentication, authorization and access control options appropriate for all possible use cases and sufficiently robust enough to ensure security policy compliance in a combined cloud computing/wireless grid environment. Alternative approaches must be considered and evaluated during system design rather than pre- or post-deployment. In some cases the best option will be for the wireless cloud system itself to make all authentication, authorization and access control decisions. In other cases, the wireless cloud will need to rely on other

systems or the information enterprise infrastructure for some or all of the required authentication, authorization and access control processes.

Regarding the security issues addressed in this article, the following section provides some key wireless cloud architecture recommendations that will help to make the wireless cloud a more trusted computing platform.

10.1 Identity and Access Management Policies

Identity and access management (IAM) policies, contracts, and mechanisms must guide the process for determining which devices (and their respective users) in the wireless grid have the ability to access applications and/or data residing in the wireless cloud. Identity provisioning enables cloud service providers to securely on-board and off-board cloud users in a timely manner [65]. Setting up a robust identity provisioning platform will facilitate access management and control while enabling quick responses to requests for service access and termination. The authentication schema chosen must work across all cloud services, mesh with the customer's IAM schema for non-cloud services, and work on all devices connected to the wireless cloud.

Cloud customers will have the responsibly for creating, following, and maintaining IAM practices, policies, and procedures. The action or inaction of any one user of the wireless cloud in this key area has implications for all users. Extending IAM to the cloud takes careful planning and consideration of the user's current and future internal IAM platform. Cloud providers and wireless cloud architects must form partnerships to establish IAM policies, procedures, and contracts that will support the interoperable use of cloud services across organizations within the wireless grid. Such support is needed at the SaaS, PaaS, and IaaS service model levels. Assisting customer with IAM planning is likely to send a message to potential customers and current skeptics that providers are focused on security and privacy and are willing to play a part in protecting the services they provide against unauthorized access. Wireless cloud architects and cloud provider collaborations could potentially lead to the establishment of authoritative guidance on issues, such as IAM, as it relates to both the wireless cloud and cloud computing in general which would also lead to greater trust in this computing paradigm.

10.2 Encryption, Key Management and Cryptographic Inclusion

Some of the biggest fears that potential customers have related to cloud computing are data malicious alteration or deletion of data and files, data theft, and data loss and interception by unintended parties. In multi-tenant virtualized cloud environments, where data is managed by a third party, there is always a need to protect confidential data. In a wireless environment, the information that is communicated and passed between network nodes travels across standard radio frequencies that are vulnerable to being tapped by unintended third parties. Authentication and encryption has to work together to prevent eavesdropping as data moves across wireless networks and to make sure that sensitive information is transmitted across a legitimate network. In addition to protecting data already in the wireless cloud, customers need assurance that their credit card numbers, passwords, individual user identity, and cloud service identity information will remain secure while traveling over the Internet and between the grid and the cloud, or sitting at-rest on devices connected to the grid. Encryption and key management will be implemented by wireless cloud architects using the technologies and standards described earlier.

Cryptography uses mathematics to code and decode digital information, transactions, and digital computations [30]. By implementing cryptography in the cloud, providers can protect grid wireless organizations from malicious co-tenants and exploitable processes in the cloud by scrambling data so that it cannot be understood by unintended parties. Providers should offer encryption tools to IaaS customers that allow them to both encrypt data before sending it to the cloud for storage and decrypt data once it is retrieved from storage and back on the customer's premises. PaaS offerings should include standard tools to protect data at-rest and/or in memory. SaaS customers should be told upfront that the provider alone has the ability to encrypt data at-rest in the cloud [65].

Encryption service and support should be offered at the SaaS level to wireless cloud users without having to ask for it. In addition, cloud providers should do everything possible to support robust key management schemes where key stores are secure and keys in storage, in transit, and in backup cannot be intercepted or stolen by unintended parties. Key stores inside the cloud should be managed in such a way that access to individual keys is limited to the entities that legitimately need them. Also, the roles of entities that use keys should be kept separate from the roles of entities that store them. Along with key storage policies, cloud service providers should have strong key generation and destruction policies as well as secure key backup and recovery capabilities.

It is undeniable that data security vulnerabilities are magnified when wireless grids are layered on top of cloud services and a robust solution to deal with these vulnerabilities is needed. However, making

sure that data is of no use to unintended parties goes a long way in mollifying the impact of a data breach in the wireless cloud if it does occur. Until the cloud industry is able to come up with standards and end-to-end technology solutions that protect data at-rest, in-use, and in-transit, wireless cloud architects and cloud providers should work together to build and maintain robust key management and encryption policies and practices.

10.3 Provenance

Increased data and service transparency in the cloud is another impediment to widespread cloud adoption. Many potential customers are reluctant to utilize the cloud because of the downside of rapid service provisioning: the inability of cloud providers to provide detailed information about data (e.g. movement, geographical storage location, multi-tenant/co-location information, etc.), which wireless cloud administrators will need in order to meet certain audit requirements. Provenance is a first step in that direction. Provenance is metadata that describes the origins of a digital object [47]. Service providers can use provenance to detect access patterns and unusual behavior as well as to improve offerings. Wireless cloud administrators and users can utilize provenance to keep track of data, comply with audit standards/requirements, and to search through data even when it is encrypted. Commercial cloud providers, such as Amazon, Microsoft, and Nirvanix, provide some ability for customers to create, store, and retrieve provenance metadata from their own host devices. However, these providers are unable to automatically generate and store provenance data [47]. The responsibility for doing so belongs to the user of the cloud services. In order to make use of the provenance, wireless cloud organizations must subscribe to the cloud providers database service so that provenance information generated by devices connected to the cloud can be stored. The organization can then use either client software or a software application built on top of the provider's database service to search through provenance data.

Provenance in the cloud is still under research and currently has some limitations. Unresolved questions related to the use of provenance include how to prevent users from providing false provenance, how to protect provenance from forgery or destruction, how to ensure data provenance consistency with the object it describes, and how to properly retain provenance (e.g., when the data object it describes no longer exists or is connected to unrelated objects [47]. As researchers, cloud providers, and consumers of cloud services work together to answer these questions the true potential of provenance is still unknown. The wireless cloud stands as a new use case for cloud computing and may introduce new issues related to the use of provenance in a distributed wireless environment. Wireless cloud architects should join the discussions around provenance and the potential benefits and challenges of using it in the wireless cloud.

10.4 Addressing Privacy During the Development/Selection of Wireless Cloud Services

As it stands, many see privacy as more of an afterthought than forethought in the minds of cloud providers and software developers that design cloud services. For some major commercial providers, such as Google, cloud computing started out as a way to leverage and monetize excess capacity in data centers. In doing so these providers paid less attention to privacy and security and more attention to producing a marketable service offering when the cloud computing paradigm first developed. Currently, researchers such as Pearson [55], are pointing out the fallacy in that approach by saying that privacy should be taken into account during the development stage of new offerings.

According to Pearson [55], cloud service developers have a responsibility to follow design and development practices that avoid basic design and implementation flaws that can later lead to privacy violations. These practices include the following: (1) designing services that keep the amount of personal information sent to and stored in the cloud to a minimum; (2) giving users maximum control over who and under what circumstances personal data in the cloud can be accessed, managed, and changed; (3) providing a means for providers to make certain that personal data is being handled according to user specifications; and (4) providing feedback to customers and users on how personal data is being used and protected. Wireless cloud architects must serve as liaisons between cloud service providers and wireless grid organizations when it comes to privacy, particularly when the wireless cloud is being developed.

The privacy measures embedded in the wireless cloud should be seamless, complementary, and comprehensive. Wireless cloud architects must be sure to design interfaces between the provider and the grid environments that monitor the movement of data from and to the cloud as well as make use of any information the provider can or will one day be able to give concerning the use and protection of personal/confidential data in the cloud. Also, when choosing services from a cloud service provider wireless grid organizations should discuss privacy expectations with service providers. Rather than assume that data privacy is guaranteed by the service provider the organization must be diligent about understanding what the provider is and is not responsible for and what can be done by the adopting organization to ensure the privacy of wireless cloud user data.

11. CONCLUSION

This article discussed the implications for developing a wireless cloud and potential security threats from this architectural construct. It identified some of the academic literature around cloud computing and wireless grids, reviewed a conceptual model of a wireless cloud architecture, identified potential vulnerabilities in the wireless cloud, identified a proposed security solution for the wireless cloud and briefly discussed authorization policy issues and developed a generic authentication/authorization process pertaining to its security architecture. The use of a cloud computing and wireless grid integration for creating the wireless cloud should only exist in the context of clear business values and technical fit, including adherence to defined security and privacy standards.

The move to a wireless cloud architecture could potentially meet the business needs and service expectations of business users. This new platform could one day become a cost-effective solution, leading to a positive return on investment (ROI) for organizations. As part of an organizations transition to a wireless cloud environment, it will be important that organizations evaluate the potential cost-effectiveness to ensure that their IT funds are used wisely and to comply with management requirements. The positive ROI will likely be derived from reduced operational costs resulting from shared infrastructure and resources (e.g., hardware and software costs, staff resource costs, etc). This aspect of the wireless cloud solution will require further research. Critical to the success of transitioning to a wireless cloud is the requirement for cloud providers to ensure the continuum of data protection for their customers. Cloud providers must investigate new data-protection mechanisms to secure data privacy, resource security, and content copyrights [14]. Wireless cloud customers will face unique challenges not only in satisfying security imperatives, but also privacy imperatives. Privacy in the wireless cloud considers the individual's contractual and statutory rights to control his or her own information, including decisions about submitting, using, disclosing, and protecting the data.

Wireless cloud customers must realize that using a wireless cloud will change how they define their system security boundaries. For example, how can they know that the integrity and confidentiality of their data is sufficiently protected? Data protection mechanisms need to be re-evaluated in the customer's own security strategy and the wireless cloud provider's architecture, to ensure that adequate self-protection of data (i.e., building protection into the data itself using cryptographic techniques), event and violation auditing and logging, disclosure/non-disclosure policies and reporting, etc., are all included. Cloud customers must understand that their data protection needs will need to be addressed at the information security level to ensure their cloud-based data processing, storage, and transmission systems and applications operate as effectively and efficiently as do their counterparts in traditional computing environments. This is especially true for ensuring the continuity of critical processes and operations.

Despite the challenges a wireless cloud introduces, none of the security requirements identified within this article are entirely new. Further research on wireless cloud security will help reduce risks, but it must be combined with security architecture, policy, governance, risk management, and risk mitigation. Successful, secure migration to a wireless cloud will require understanding cloud and wireless grid technologies and evolving government policies to adopt a comprehensive transition methodology and more collaboration between the cloud providers, wireless grid experts, community partners, and wireless networking security experts.

Critical to the success of a wireless cloud will be the ability to explore the possibly of a cloud computing and wireless grid integration. Future research areas around leveraging this type of architecture include addressing the following:

- How does threat exposure change when using a wireless cloud?
- How are the security responsibilities divided between cloud providers and wireless grid developers?
- What properties of a wireless cloud cause major security challenges?
- What properties of a wireless cloud result in major security advantages?
- What are the security controls I should expect to see in a wireless cloud?

For confidence in a wireless cloud implementation, the need to have sufficient visibility to see who was doing what and how across the infrastructure is paramount. This means the use of governance, or the ability to monitor, manage, and control, all aspects of the architecture, including the ability to trace issues with security down to the sources of the problems. Understanding that a wireless cloud architecture creates risks and requires a rethinking–but not reinvention–of security controls and architecture. However, with some forethought and planning, a wireless cloud computing-based system can be just as secure, if not more secure, as a traditional wired system.

ACKNOWLEDGEMENTS

The development of the Wireless Grid Innovation Testbed (WiGiT) is primarily funded by the support of the National Science Foundation (NSF) Partnership for Innovation (PFI) program grants NSF #0227879 (2002-2006) and continued under NSF # 0917973 (2009-2011).

REFERENCES

[1] A. Agarwal, *et al*., "Wireless Grids: Approaches, Architectures and Technical Challenges," *Working Paper, Massachusetts Institute of Technology (MIT), Sloan School of Management*, 2004.
[2] S. Ahuja and J. Myers, "A Survey on Wireless Grid Computing," *Journal of Supercomputing*, vol. 37(1), pp. 3-21, 2006.
[3] M. Armbrust, *et al*., "Above the Clouds: a Berkeley View of Cloud Computing," *Technical Report No. UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley*, vol. 28, 2009.
[4] F. Aymerich, *et al*., "An Approach to a Cloud Computing Network," In *Proceedings of the First International Conference on the Applications of Digital Information and Web Technologies*, 2008, pp. 113–118.
[5] S. Bernard and S. Ho, "Enterprise Architecture as Context and Method for Designing and Implementing Information Security and Data Privacy Controls in Government Agencies," in *Saha, P. (Ed.), Advances in Government Enterprise Architecture*, 2008, pp. 340-370.
[6] M. Bishop, "Computer Security," *Art and Science*, Addison-Wesley, Boston, 2003.
[7] R. Buyya, *et al*., "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," *Future Generation Computer Systems*, vol. 25(6), pp. 599–616, 2009.
[8] S. Bradner, "The Internet Engineering Task Force," In *Chris DiBona, Sam Ockman and Mark Stone, eds., Open Sources: Voices from the Open Source Revolution*, O'Reilly, 1999, pp. 47- 52.
[9] D. Closs and E. McGarrell, "Enhancing Security Throughout the Supply Chain. Michigan," *Michigan State University, IBM Center for Business of Government*, pp. 1-52, 2004.
[10] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," *IEEE Computer*, vol. 36(10), pp. 103–105, 2003.
[11] Y. Chen, *et al*., "What's New About Cloud Computing Security?" *Technical Report No. UCB/EECS*-2010-5, *Electrical Engineering and Computer Sciences, University of California at Berkeley*, vol. 20, 2010.
[12] J. Chen and Y. Wang, "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience," *IEEE Communications Magazine*, vol. 43 (12), pp. 26 – 32, 2005.
[13] CNSS Instruction 4009, "National Information Assurance Glossary," Committee on National Security Systems, 2003, accessed June 15, 2011, from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.
[14] M. Dikaiakos, *et al*., "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," *IEEE Internet Computing*, vol. 13(5), pp. 10–13, 2009.
[15] J. Ekanayake, *et al*., "High Performance Parallel Computing with Clouds and Cloud Technologies," in *Cloud Computing and Software Services: Theory and Techniques*, CRC Press (Taylor and Francis). 2010.
[16] I. Foster, "What is the Grid? A Three Point Checklist," *GRIDToday*, vol. 1(6), 2002.
[17] I. Foster, *et al*., "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," *International Journal of Supercomputer Applications*, vol. 15(3), pp. 200-222, 2001.
[18] I. Foster, *et al*., "The Open Grid Services Architecture, Version 1.5," *Global Grid Forum*, 2006, accessed June 15, 2011, from http://www.ggf.org/documents/GFD.80.pdf.
[19] I. Foster, *et al*., "The Physiology of the Grid," in *Berman, F., Hey, A. and Fox, G. (eds.), Grid Computing - Making the Global Infrastructure a Reality*, John Wiley and Sons, pp. 217-249, 2003.
[20] P. Funk and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)," RFC 5281, *Internet Engineering Task Force*, 2008.
[21] M. Gaynor, *et al*., "Integrating Wireless Sensor Networks with the Grid," *IEEE Internet Computing*, vol. 8(4), pp. 32–39, 2004.
[22] L. Hendrickson and V. Piotrowski, "Wireless Security: From WEP to 802.11i," *Midwest Instruction and Computing Symposium*, 2004, accessed June 15, 2011, from http://portal.acm.org/.
[23] C. Hoffa, *et al*., "On the Use of Cloud Computing for Scientific Workflows," in *ESCIENCE '08: Proceedings of the 2008 Fourth IEEE International Conference on eScience, IEEE Computer Society*, 2008, pp. 640–645.

[24] Institute of Electrical and Electronics Engineers, Inc. (IEEE), "Standard 802.11 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE, Inc*., 2009, access June 15, 2011, from http://www.ieee.org/index.html.
[25] P. Jaeger, *et al*., "Cloud Computing and Information Policy: Computing in a Policy Cloud?" *Journal of Information Technology & Politics*, vol. 5(3), pp. 269-283, 2008.
[26] S. Jajodia, *et al*., "Topological Analysis of Network Attack Vulnerability," in *Managing Cyber Threats: Issues, Approaches and Challenges*, V. Kumar, J. Srivastava, A. Lazarevic (eds.), Kluwer Academic Publisher, Kluwer Academic Publisher, Chapter 5, 2003, pp. 248–266.
[27] S. Jajodia, *et al*., "A Unified Framework for Enforcing Multiple Access Control Policies," in *SIGMOD Record (ACM Special Interest Group on Management of Data)*, vol. 26(2), 1997, pp. 474–485.
[28] M. Jensen, *et al*., "On Technical Security Issues in Cloud Computing," in *IEEE International Conference on Cloud Computing (CLOUD-II 2009)*, 2009, pp. 109- 116.
[29] H. Johnson, *et al*., "SOLA: A One-Bit Identity Authentication Protocol for Access Control in IEEE 802.11," in *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'02)*, vol. 1, 2002, pp. 768- 772.
[30] J. Katz and Y. Lindell, "Introduction to Modern Cryptography," *Cryptography and Network Security*, Chapman & Hall/CRC, Boca Raton, FL, 2008.
[31] D. Kotz and K. Baek, "A Survey of WPA and 802.11i RSN Authentication Protocols," *Technical Report No. TR2004-524, Computer Science Department, Dartmouth College*, 2004.
[32] K. Keahey, *et al*., "Science Clouds: Early Experiences in Cloud Computing for Scientific Applications," in *Proceedings of the First Workshop on Cloud Computing and its Applications (CCA2008)*, 2008.
[33] A. Khajeh-Hosseini, *et al*., "Research Challenges for Enterprise Cloud Computing," in *Proceedings of the First ACM Symposium on Cloud Computing (SOCC 2010)*, 2010.
[34] M. Klems, *et al*., "Do Clouds Compute? Framework for Estimating the Value of Cloud Computing," in *Weinhardt, C., Luckner, S. & Stößer, J. (eds.) Lecture Notes in Business Information Processing*, vol. 22, 2009, pp. 110 – 123.
[35] B. Lang, *et al*., "A Multipolicy Authorization Framework for Grid Security," in *Proceedings of the Fifth IEEE Symposium on Network Computing and Application*, pp. 269-272, 2006.
[36] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time? *Computer*, vol. 42(1), pp. 15–20, 2009.
[37] A. Lenk, *et al*., "What's Inside the Cloud? An Architectural Map of the Cloud Landscape," in *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, IEEE Computer Society, 2009, pp. 23–31.
[38] G. Li, *et al*., "A Survey on Wireless Grids and Clouds," in *Proceedings of the Eighth IEEE International Conference on Grid and Cooperative Computing*, 2009, pp.261- 267.
[39] H. Lim, *et al*., "Automated Control in Cloud Computing: Challenges and Opportunities," in *Proceedings of the First workshop on Automated Control for Datacenters and Clouds (ACDC '09)*, 2009, pp. 13-18.
[40] H. Lohr, *et al.*, "Enhancing Grid Security Using Trusted Virtualization," in *Autonomic and Trusted Computing, Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 2007, pp. 372–384.
[41] Q. Ma and J. Pearson, "ISO 17799: Best Practices in Information Security Management?" *Communications of the Association for Information Systems*, vol. 15(32), pp. 577-591, 2005.
[42] S. Manvi and M.Birje, "A Review on Wireless Grid Computing," *International Journal of Computer and Electrical Engineering*, vol. 2(3), pp. 469-474, 2010.
[43] A. Menesez, *et al*., "Handbook of Applied Cryptography", *CRC Press*, 1997.
[44] L. McKnight, *et al*., "Wireless Grids: Distributed Resource Sharing by Mobile, Nomadic, and Fixed Devices," *IEEE Internet Computing*, vol. 8(4), pp. 24–31, 2004.
[45] L. McKnight, *et al*., "Wireless Grids: Assessing a New Technology for a User Perspective," in *Designing Ubiquitous Information Environments: Socio-Technical Issues and Challenges*, 2005, pp. 169–181.
[46] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology, Information Technology Laboratory*, Version 15, 2009.
[47] K. Muniswamy-Reddy and M. Seltzer, "Provenance as First Class Cloud Data," *ACM SIGOPS Operating Systems Review*, vol. 43(4), pp. 11-16, 2010.
[48] S. Nanz and C. Hankin, "A Framework for Security Analysis of Mobile Wireless Networks," *Theoretical Computer Science*, vol. 367 (1-2), pp. 203-227, 2006.
[49] N. Nagaratnam, *et al*., "The Security Architecture for Open Grid Services," Open Grid Service Architecture Security Working Group (OGSA-SEC-WG), 2002, accessed June 15, 2011, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.5693&rep=rep1&type=pdf.

[50] M. Naedele, "Standards for XML and Web Services Security," *Computer*, vol. 36 (4), pp. 96-98, 2003.
[51] C. Onwubiko and A. Lenaghan, "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises," in *Proceedings of the 2007 IEEE International Conference on Intelligence and Security Informatics*, 2007, pp. 244-249.
[52] S. Ostermann, *et al*., "A Performance Analysis of EC2 Cloud Computing Services for Scientific Computing," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 34 (4), 2010, pp. 115-131.
[53] J. Park and R. Sandhu, *et al*., "Towards Usage Control Models: Beyond Traditional Access Control," in *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies (SACMAT'02)*, 2002, pp.57–64.
[54] J. Park and R. Sandhu, *et al*., "Smart Certificates: Extending X.509 for Secure Attribute Services," in *Proceedings of the of 22nd National Information Systems Security Conference (NISSC)*, 1999, pp. 337-348.
[55] S. Pearson, "Taking Account of Privacy When Designing Cloud Computing Services," in *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009, pp. 44-52.
[56] A. Perrig, *et al*., "Security in Wireless Sensor Networks," *Communication of the ACM*, vol. 47(6), pp. 53–57, 2004.
[57] T. Phan, *et al*., "Integrating Wireless Devices into the Computational Grid," in *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MOBICOM 2002)*, 2002, pp. 271–278.
[58] A. Raghunathan, *et al*. "Securing Wireless Data: System Architecture Challenges," In *Proceedings of the 15th International Symposium on System Synthesis (ISSS 2002)*, 2002, pp. 195-200.
[59] B. Rimal, *et al*., "A Taxonomy and Survey of Cloud Computing Systems," in *Proceedings of the Fifth International Joint Conference on INC, IMS and IDC*, 2009, pp. 44–51.
[60] B. Rochwerger, *et al*., "The Reservoir Model and Architecture for Open Federated Cloud Computing," *IBM Systems Journal*, vol. 53(4), pp. 4:1- 4:11, 2009.
[61] D. Rosado, *et al*., "Analysis of Secure Mobile Grid Systems: A Systematic Approach," *Information and Software Technology*, vol. 52, pp. 517– 536, 2010.
[62] R. Sandhu, *et al*., "Role-Based Access Control Models," *IEEE Computer*, vol. 29(2), pp. 38–47, 1996.
[63] R. Sandhu and Q. Munawer, "How to do Discretionary Access Control Using Roles," in *Proceedings of the Third ACM Workshop on Role-Based Access Control (RBAC '98)*, 1998, pp. 47–54.
[64] N. Santos, *et al*., "Towards Trusted Cloud Computing," in *Proceedings of the 2009 conference on Hot Topics in Cloud Computing (HotCloud 2009)*, vol. 3, 2009.
[65] G. Brunette and R. Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," *Cloud Security Alliance*, pp. 1-76, 2009.
[66] A. Snyder, "Warriors of Disinformation: American Propaganda, Soviet Lies, and the Winning of the Cold War," *Arcade Publishing*, 1995.
[67] The Global Alliance, "Globus ToolkitVersion 5.0.3," 2011, accessed June 15, 2011, from http://www.globus.org/toolkit/.
[68] J. Treglia, *et al*., "Collaboration in a Wireless Grid Innovation Testbed by Virtual Consortium," in *Networks for Grid Applications. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, vol. 25, 2010, pp. 139 – 146.
[69] L. Vaquero, *et al*., "A Break in the Clouds: Towards a Cloud Definition," *SIGCOMM Computer Communications Review*, vol. 39(1), pp. 50-55, 2008.
[70] D. Welch and S. Lathrop, "Wireless Security Threat Taxonomy," in *Proceedings of the IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*, 2003, pp. 76-83.
[71] H. Yang, *et al*., "Security in Mobile Ad Hoc Networks: Challenge and Solutions," *IEEE Wireless Communications*, vol. (11)1, pp. 38-47, 2004.
[72] P. Yau and C. Mitchell, "Security Vulnerabilities in Ad Hoc Networks," in *Proceedings of the Seventh International Symposium on Communication Theory and Applications (ISCTA'03)* ,2003, pp. 99–104. 2003.
[73] S. Yi, *et al*., "Security-Aware Ad-Hoc Routing for Wireless Networks," in *Proceedings of the Second ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '01)*, 2001, pp. 299 – 302.

BIOGRAPHY OF AUTHORS

Tyson Brooks, PMP, works for the U.S. Department of Defense (DoD) and has more than 17 years of professional experience in the design, development and production of a broad range of information systems/technology products and services for the federal government. His expertise includes work in the areas of enterprise architecture, cybersecurity, business process modeling, project management, systems analysis and design, systems engineering and requirements analysis. Mr. Brooks is pursuing his Doctorate in Information Management and holds a master's degree in Information and Telecommunications Systems from Johns Hopkins University; a master's degree in Business Administration from Thomas More College; and a bachelor's degree in Business Administration/Management from Kentucky State University. Mr. Brooks also received his Certificate of Advanced Study (CAS) in Information Security Management (ISM) from Syracuse University; a Certification in Enterprise Architecture (CEA) from Carnegie Mellon University's Institute for Software Research International (ISRI); and a Project Management Professional (PMP) certification from the Project Management Institute (PMI).

Jerry Robinson is a third year PhD student in the Syracuse University School of Information Studies. He received his B.A. in Business Administration from Morehouse College and his M.S. in Information Management from Syracuse University. His research interests include universal design and neo-institutional theory. Specifically, he plans to explore the social, theoretical, and historical underpinnings of universal design, the interpretation and application of universal design principles by designers, and the implications of universal design as a practice for persons with disabilities (PWDs).

Lee W.McKnight is Kauffman Professor of Entrepreneurship and Innovation and an Associate Professor in the iSchool (The School of Information Studies), Syracuse University; Founder and Member of the Board of Directors of Wireless Grids Corporation; as well as a Founding Member of the Board of Directors of Summerhill Biomass Systems. Lee is Principal Investigator of the National Science Foundation Partnerships for Innovation Wireless Grids Innovation Testbed (WiGiT) project, is recipient of the 2011 TACNY Award for Technology Project of Year, and is the inventor of edgeware, a new class of software for creating ad hoc overlay network applications, known as wiglets. Lee's research focuses on virtual markets and wireless grids, the global information economy, national and international technology policy, and Internet governance and policy. He was an Associate Professor and Director of the Edward R. Murrow Center at the Fletcher School of Law and Diplomacy, Tufts University; Principal Research Associate and Lecturer at MIT, and Founder of the Internet Telephony Consortium, also at MIT. McKnight received a Ph.D. in 1989 from MIT; an M.A. from the School of Advanced International Studies, Johns Hopkins University in 1981; and a B.A. magna cum laude from Tufts University in 1978.