ABSTRACT A PROTECTED WIRELESS CLOUD COMPUTING

Kinnera Veerababu
MCA, Saifabad PG College
Hyderabad
E-mail id: veeru.kinnera@gmail.com

P.V. Aparanjani Priyadarshini
Asst. Professor,
Dept. of Computer Science
SRAS College, Hyderabad

Jillepalli Jeeshitha
Asst. Professor,
Dept. of Computer Science
Anurag Group of Institutions Hyd.
E-mail id: jeeshitha.eng@gmail.com

ABSTRACT:

The interest in cloud computing by organizations has driven a core desire 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 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.

Keywords: *Cloud computing, wireless grid security, wireless cloud architecture.*

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. IT systems should be designed to minimize network vulnerabilities and protect the information contained within them.

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. 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. 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. 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. 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.

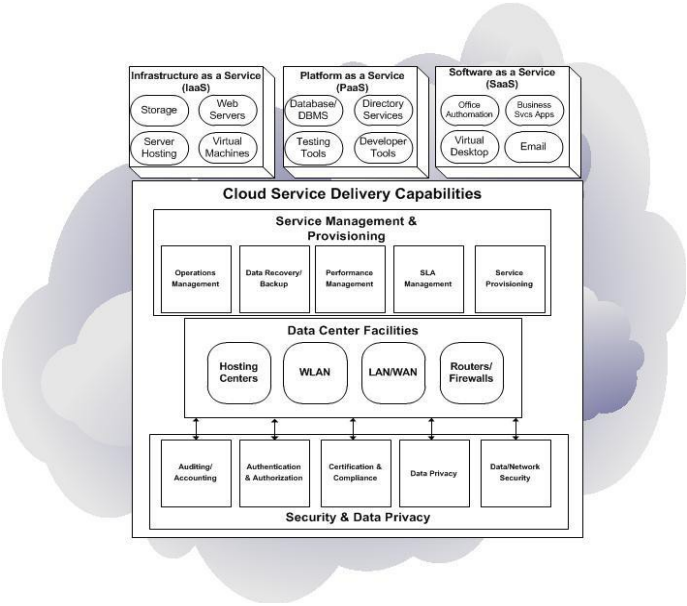
WHAT IS CLOUD COMPUTING? :

"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. 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."

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. Mell and Grance 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 Service2 and Elastic Compute Cloud3), Platform-as-a-Service (PaaS), which provides the ability to lease an application development environment (e.g. Microsoft Azure Services Platform4) and Software as a Service (SaaS), which offers network accessible applications (e.g. Google docs5. 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.



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.

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.

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.

WIRELESS GRIDS:

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 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. Grid computing involves the aggregation of network connected computers to form a distributed system for coordinated problem solving and resource sharing. McKnight can be credited with describing wireless grid infrastructures along three dimensions: the physical layer, the networking infrastructure, and the middleware. Recent literature from Li and Ahuja and Myers identify wireless grids as three distinct architectures: (1) wireless senor grid, (2) mobile wireless and (3) fixed wireless. McKnight 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 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 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.

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. 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. 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. 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.

- ***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.

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 networks 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.

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. 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. 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 organizations 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.

AUTHENTICATION:

One of the most important security controls of any IT system is the authorization, authentication and access of the system. 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 users access rights to computer resources based on their permissions and privileges, 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 clouds 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.

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 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 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. 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.

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?

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. Mc Garrell, "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., "Whats 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.