An In Depth Review of Ad Hoc Mobile Network & Cloud Security

Joshua Alcorn and Larry Brachfeld
College of Engineering and Applied Science
University of Colorado
Colorado Springs

Abstract - In this paper we will discuss research in defense of cyber-attack technologies on mobile ad hoc and cloud hosted networks. This shall include a review of new and unique attacks that are specific to mobile ad hoc and cloud hosted networks, as well as implementation of existing or theoretic attacks that are unique to mobile ad hoc and cloud hosted networks.

1. Introduction

Ad hoc mobile and cloud networks are an exciting new avenue in computing. Not only do they shatter the traditional walls of wired computing, but they also open the door for massive amount of computing power for individuals, industry, and academics. The new shared landscape of ad hoc computing does not come without its issues and concerns. Chief among them is security. Pushing vast amount of data and processing outside and inviting countless unknown users into our networks is filled with the potential for disaster. This paper provides a review of these concerns first, by discussing the technologies themselves, then categorizing risks, addressing potential attacks, discussing commercial solutions, and finally identifying future research topics.

1.1 Description of Mobile Ad hoc networks.

In order to conduct a review of mobile ad hoc networks, first we must lay the groundwork with a solid foundation in what comprises a mobile ad hoc network. An ad-hoc network is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. The mobile nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure. They form an arbitrary topology, where the routers are free to move randomly and arrange themselves as required [8, 14].

Each node or mobile device is equipped with a transmitter and receiver. They are said to be purpose-specific, autonomous and dynamic. This compares greatly with fixed wireless networks, as there is no master slave relationship that exists in a mobile ad-hoc network. Nodes rely on each other to established communication, thus each node acts as a router. Therefore, in a mobile ad-hoc network, a packet can travel from a source to a destination either directly, or through some set of intermediate packet forwarding nodes [8].

Historically speaking, ad hoc networks date back to the 1970s. They were developed by the Department of Defense, to comply with a new mobile military framework. The aim was to rapidly deploy a robust, mobile and reactive network, under any circumstances. These networks then proved useful in commercial and industrial fields, first aid operations and exploration missions. Ad hoc networks, also called peer-to-peer networks, still have a long way to go in order to be fully functional and commercial, as it has its defects such as security and routing which we will discuss further [8].

1.2 Description of Cloud Hosted Networks. The similarities between ad hoc cloud computing and mobile ad hoc networks are described in detail below.

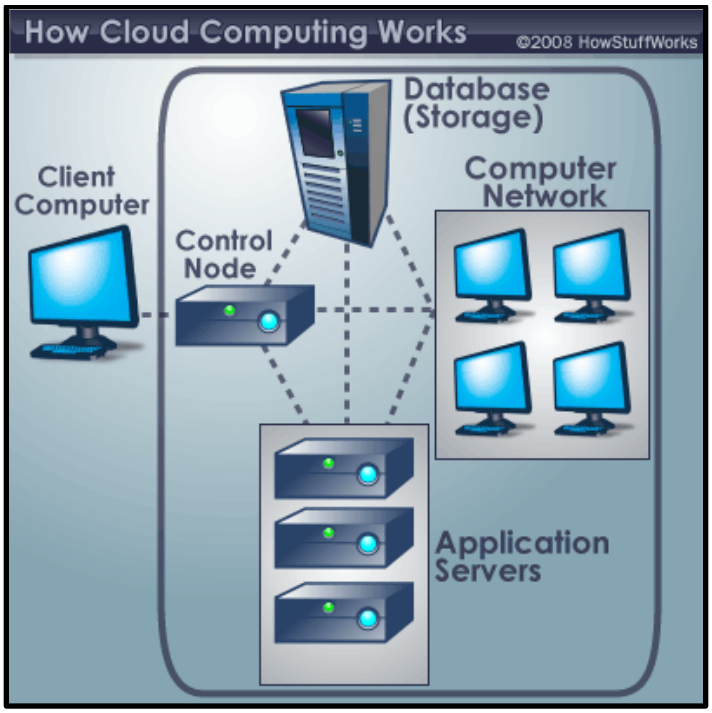

Figure 1. Overview of Cloud Computing [9].

A few major takeaways from cloud computing are [9]:

- Cloud computing systems generally have a front end, which is what the user sees, and a back end, which does all the work.

- Cloud computing shares some similarities with an older model of computing called timesharing. A timesharing computer system connects multiple users to a single computer processor through dumb terminals, which have a keyboard and monitor, but leave the computing to the central machine.

- While cloud computing promises to offload tasks like data storage and processing power, the model raises questions about data accessibility and security

- The three primary services models are [10]:

    - Infrastructure as a Service (IaaS): In this most basic cloud service model, cloud providers offer computers – as physical or more often as virtual machines – raw (block) storage, firewalls, load balancers, and networks. IaaS providers supply these resources on demand from their large pools installed in data centers.
    - Platform as a Service (PaaS): In PaaS the cloud providers deliver a computing platform and/or solution stack typically including operating system, programming language execution environment, database, and web server.

Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers.

- Software as a Service (SaaS): In SaaS the cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. What makes a cloud application different from other applications is its elasticity.

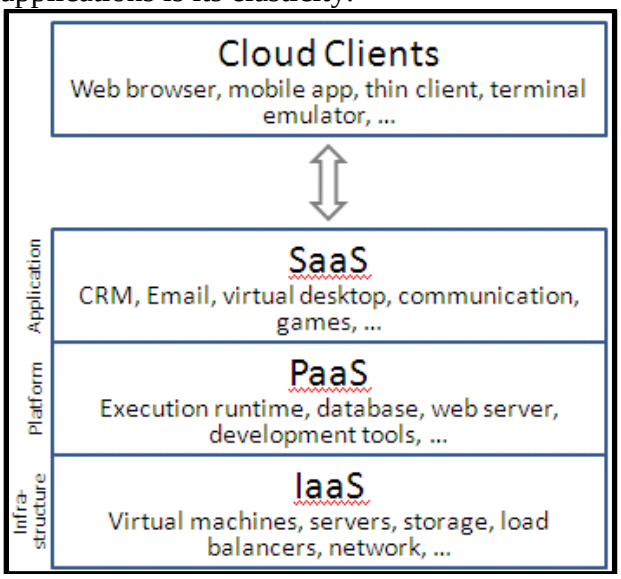

Figure 2. Layers of Cloud Computing [10].

1.3 Discussion of Mobile Network and Cloud Security Concerns. The very characteristics which make ad hoc networks so valuable and appealing are what cause its limitations. Attacks from both external and internal nodes can easily affect the stability of the ad hoc mobile and cloud networks. The degree of the influence depends largely on the active level of the malicious nodes. The time to recover the services relies on the detection of the mistakes or errors and responding policy. For example, an active bad relay node can cause multiple packet loss and may disable the remote connections. If this relay node can be identified quickly and select a different relay node, the attack would not be effective long. These concerns and more will be discussed in greater detail in the proceeding section [1].

2 Security Issues.

Because mobile ad hoc networks have many more vulnerabilities than a traditional wired network, security is much more of a challenge in the mobile ad hoc network environment. While a wireless network is more versatile than a wired one, it is also more vulnerable to attacks. This is due to the very nature of radio transmissions, which are made on the air.

On a wired network, an intruder would need to break into a machine of the network or to physically wiretap a cable. On a wireless network, an adversary is able to eavesdrop on all messages within the emission area, by operating in promiscuous mode and using a packet sniffer

(and possibly a directional antenna). There is a wide range of tools available to detect, monitor and penetrate an IEEE 802.11 network, such as AirSnort; a wireless LAN (WLAN) tool which cracks encryption keys on 802.11b WEP networks. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered and Ethereal; a GUI network protocol analyzer. It lets you interactively browse packet data from a live network or from a previously saved capture file. Hence, by simply being within radio range, the intruder has access to the network and can easily intercept transmitted data without the sender even knowing (for instance, imagine a laptop computer in a vehicle parked on the street eavesdropping on the communications inside a nearby building). As the intruder is potentially invisible, it can also record, alter, and then retransmit packets as they are emitted by the sender, even pretending that packets come from a legitimate party.

Furthermore, due to the limitations of the medium, communications can easily be perturbed; the intruder can perform this attack by keeping the medium busy sending its own messages, or just by jamming communications with noise.

Figure 3 describes how policies can be applied at both the user and service level and has mechanisms in place to ensure those policies remain in force wherever the information is replicated in the cloud environment.

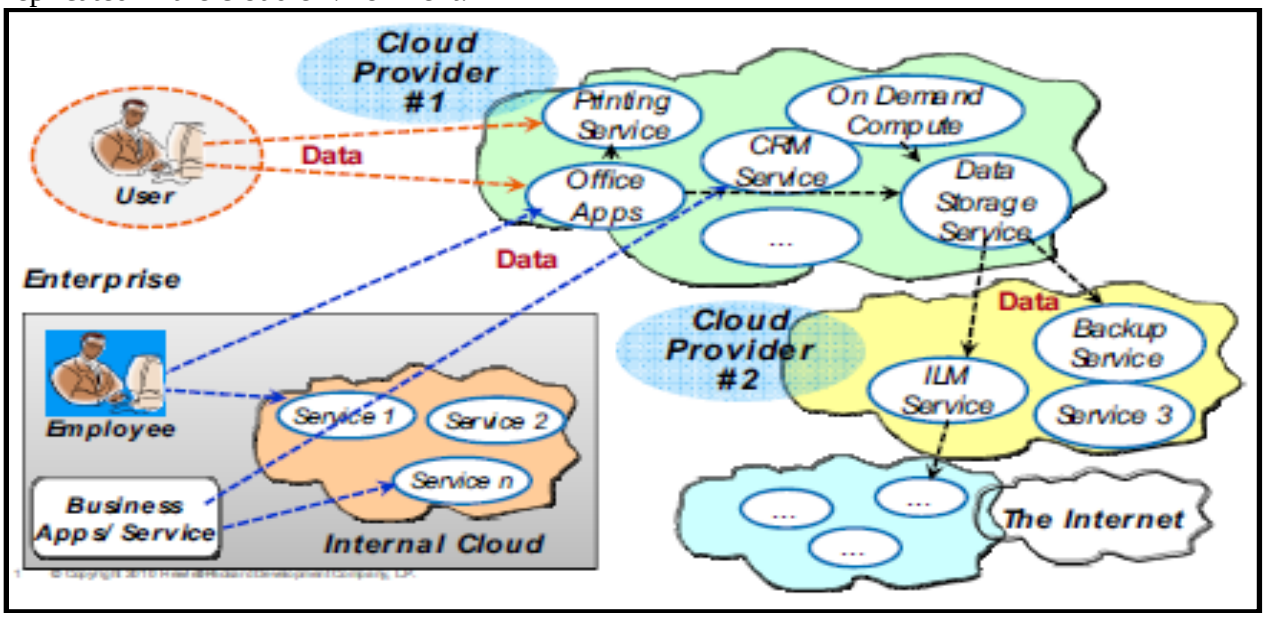

Figure 3. Cloud Computing Scenario.[1]

2.1 Access Issues. Moving data into a cloud offers great convenience to users since they do not have to care about the large capital investment in both the deployment and management of the hardware infrastructures. Clients would be able to access their applications and data from anywhere at any time. They could access the cloud computing system using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network. Corporations that rely on computers have to make sure they have the right software in place to achieve goals. Cloud computing systems give these organizations company-wide access to computer applications. The companies don't have to buy a set of

software or software licenses for every employee. Instead, the company could pay a metered fee to a cloud computing company for access on an as needed basis.[1]

Perhaps the biggest concerns about cloud computing are security and privacy. The idea of handing over important data to another company worries some people. Corporate executives might hesitate to take advantage of a cloud computing system because they can't keep their company's information under their own lock and key. The counterargument to this position is that the companies offering cloud computing services live and die by their reputations. It benefits these companies to have reliable security measures in place to control access. Otherwise, the service would lose all its clients. It's in their interest to employ the most advanced techniques to protect their clients' data.

Privacy is another matter. If a client can log in from any location to access data and applications, it's possible the client's privacy could be compromised. Cloud computing companies will need to find ways to protect client privacy. One way is to use user names and passwords. Another is to employ an authorization format where each user can access only the data and applications relevant to his or her job.

2.2 Physical Data Access. Customers allow cloud providers to have access to specific data based on agreed policies and by forcing interactions with interchangeable independent third parties called Trust Authorities. The access to data can be as tightly controlled as necessary, based on policy definitions, underlying encryption mechanisms supporting adherence of policies to the data and a related key management approach that allows sets of data attributes to be encrypted specifically based on the policy. Access to data is mediated by a Trust Authority that checks for compliance to policies in order to release decryption keys. By these means users can be provided with fine-grained control over access and usage of their data within the cloud, even in public cloud models. [4]

2.3 Availability Issues. To ensure high availability of services, data is replicated within virtualized and cloud infrastructures. As job functions and responsibilities change, so too do access control requirements. There is always a significant threat of user and application configuration errors; data can easily be exposed to those who should not have access to it. Insider threats also put sensitive information at risk to breach, manipulation, and theft.

2.4 Criteria for a Secure Ad-hoc Network. In the following, we briefly introduce the widely-used criteria to evaluate if the mobile ad hoc network is secure.

2.4.1. Availability. The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service. [4]

2.4.2. Integrity. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways:

- Malicious altering

- Accidental altering

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

2.4.3. Confidentiality. Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

2.4.4. Authenticity. Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

2.4.5. Nonrepudiation. Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

2.4.6. Authorization. Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

2.4.7. Anonymity. Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

3 Review of Ad Hoc and Cloud Hosted Networks Cyber-Attack Methods

Ad hoc networks are susceptible to a wide range of cyber-attacks; many of those issues were discussed above. The proceeding sections cover specific two attacks and some theoretical solutions.

3.1 Routing Layer Attacks. Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the ad hoc networks, attacks against routing are generally classified into two categories:

attacks on routing protocols and attacks on packet forwarding/delivery. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along predefined path [1].

A technique to protect against such an attack is the concept of a localized self-healing community. It is based on the observation that packets forwarding typically relies on more than one immediate neighbor to relay packets. Community-based security is focuses on node redundancy at each step of the packet forwarding process. The term self-healing refers to that as long as at least one "good" community node is forwarding, then the ad hoc network will continue to function.

3.2 Denial of Service Attacks. The final type of attack is denial of service (DoS), which is an attempt to make a computer or network resource unavailable to its intended users. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to exhaust the processing power of the target and make the services provided unavailable. Ad hoc networks by their very nature are less susceptible due to the distributed nature of the services. However, mobile ad hoc networks are more vulnerable than the wired networks because of they are prone to radio interference and the limited battery power. Admittedly ad hoc cloud networks do offer some advantages over both wired and mobile network in relation to DoS attacks [1].

In one of the newer DoS attacks, a rushing attack, the attacker exploits the duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group. Although there is no one simple solution to this attack, it has been proposed that a series of mechanisms working in concert will help defend against DoS as depicted in the figure below. Utilizing secure neighbor detection, secre route delegation and randomized route request forwarding, working together these protocols help prevent the duplication during route discovery. This will help fend off rushing attacks.

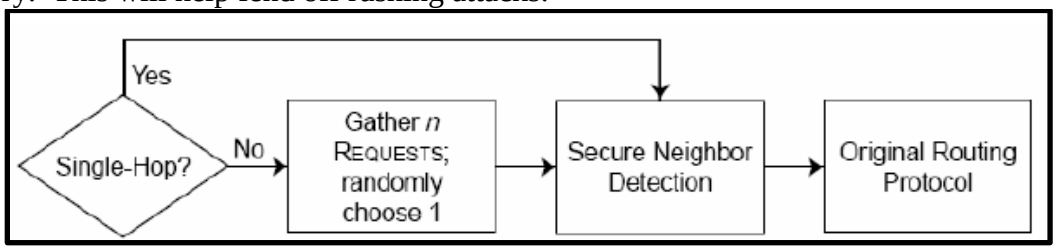

Figure 4. Combined Mechanism against Rushing Attacks [1].

4 Discussion of Specific Security Proposals

Because mobile ad hoc networks have many more vulnerabilities than a traditional wired network, security is much more of a challenge in the mobile ad hoc network environment. On a wireless network, an adversary is able to eavesdrop on all messages within the emission area, by operating in promiscuous mode and using a packet sniffer. Furthermore, due to the limitations of the medium, communications can easily be perturbed; the intruder can perform this attack by keeping the medium busy sending its own messages, or just by jamming communications with noise. We discuss several security proposals to help mitigate the vulnerabilities and mobile ad hoc and cloud networks.

4.1 CloudSEC Discussion (CloudSEC: A Cloud Architecture for Composing Collaborative Security Services). CloudSEC proposes a new architecture for composing collaborative security-related services in clouds, such as correlated intrusion analysis, anti-spam, anti-DDOS, automated malware detection and containment. CloudSEC is modeled as a dynamic peer-to-peer overlay hierarchy with three types of top-down architectural components. Based on this architecture, both data distribution and task scheduling overlays can be simultaneously implemented in a loosely coupled fashion, which can efficiently retrieve data resources from heterogeneous network security facilities, and harness distributed collection of computational resources to process data-intensive tasks. [5]

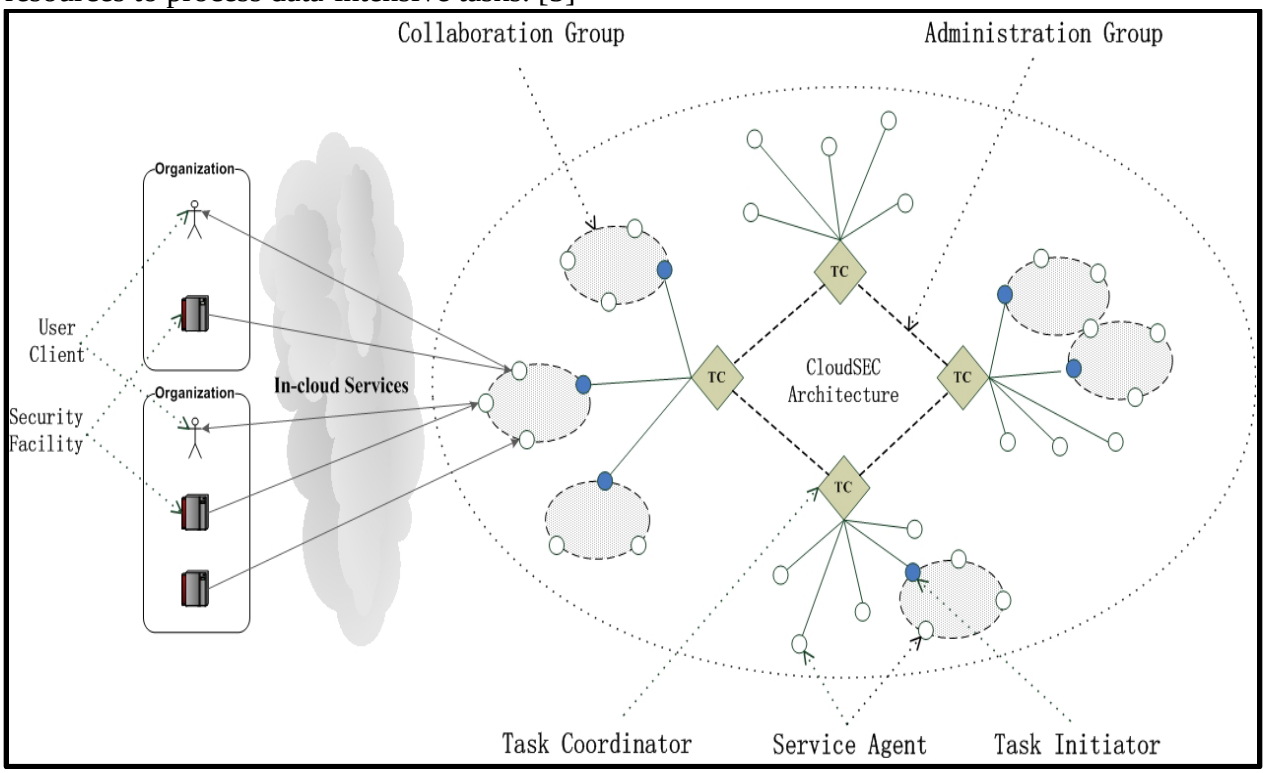

Figure 5. CloudSec Architecture. [5]

As depicted in Figure 5, A CloudSEC System is comprised of three sets of components: administration group, collaboration groups and peripheral entities. All communication between the nodes of administration group and collaboration group is encrypted. A description of each follows. [5]

1) Administration group. Administration Group is the kernel component of the CloudSEC architecture, which is an overlay organized by those peers called task coordinator. Each task coordinator is in charge of a dynamic administrative domain, which contains a collection of autonomous security agents. Task coordinators are responsible for making security policy decisions, managing collaboration tasks as well as distributing analytical results across multiple administrative domains.

2) Collaboration groups. Each collaboration group is organized to compose a certain security service by carrying out a collaborative task. CloudSEC harnesses the distributed nature of cloud

computing to enable dynamic and strategic organizing of overlay networks in proximity to the service users. Therefore, collaboration groups are the vital components of CloudSEC's "Providing Services on Demand" characteristic. The first security agent joining a collaboration group is called task initiator, which is the direct correspondent between the collaboration group and its task coordinator. It obtains collaborative tasks and instructions from task coordinator, and in turn reports back task status and final results. In this way, collaboration groups are preserving hierarchical attributes toward the administration group, such that every security agent has the potential to efficiently route all messages within the entire CloudSEC architecture, simply through the forwarding mechanism of task coordinators.

3) Peripheral entities. Peripheral entity is a functionality abstraction summarizing all service contributors and users. These nodes don't implement the CloudSEC protocol, and have no access authority to any architectural overlay. Rather, these nodes could install various heterogeneous security facilities and client software, and simply supply and consume data resources through a combination of push and pull mechanism. Extensions to provide support for CloudSEC would be implemented as plug-ins for these systems.

4.2 **Encryption and Management of Data in the Cloud.** The main idea behind end-to-end policy based encryption to provide accountability within the cloud is customers allow cloud service providers to have access to specific data based on agree upon policies and ensure compliance by using Trusted Agents and PKI infrastructure as shown in Figure 6.

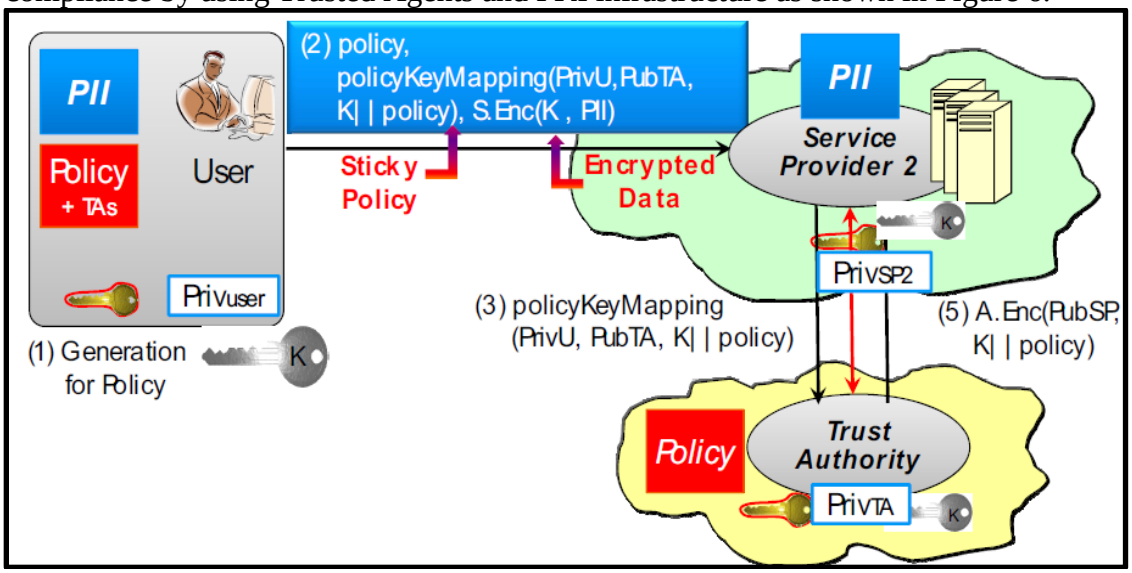

Figure 6. PKI Infrastructure adapted to the Cloud. [4]

4.3 Trend Micro and VMWare SecureCLoud Approach. Trend Micro SecureCloud provides data protection and encryption key management for public cloud, private cloud, hybrid cloud, and community cloud environments. The Data is encrypted on a VM before being written to any storage device and is only decrypted when it is read back. The proprietary key management system ensures that encryption keys are only released into safe cloud environments via identity and integrity checks. [6]

When the virtual machine image boots up, it uses the Runtime Agent to provide its credentials to

SecureCloud and request an encryption key along with the appropriate information to connect to data storage. For example, a virtual machine image could be required to report items like malware pattern file version, last full scan, network services, and location of the instance to SecureCloud during the request. This identifying information helps to ensure that the instance meets security and environmental criteria set by the administrator in order to run certain applications. Data is only decrypted within the virtual machine; this ensures that data at rest within or traversing the cloud infrastructure remains encrypted at all times. SecureCloud generates and manages your encryption keys. Further, the virtual machine image does not store encryption keys when the image is not in use. SecureCloud also provides other management capabilities such as reporting and audit functions. This is depicted in Figure 7. [6]

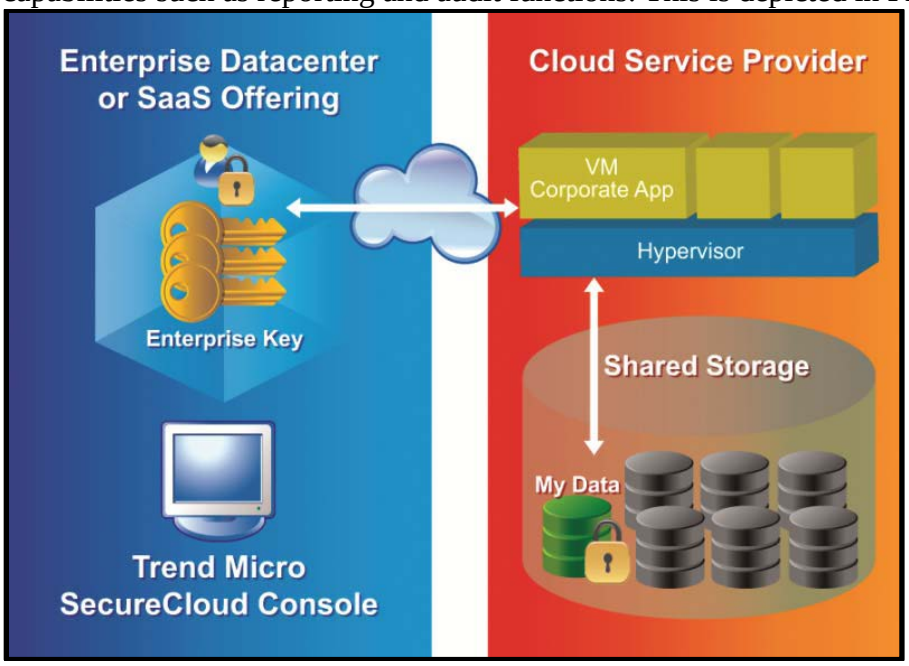

Figure 7. Management and Generation of Encryption Keys. [6]

The basic components of SecureCloud are the Runtime Agent, Management Server, and the VMWARE Vcloud API. Each is briefly discussed below:

RUNTIME AGENT

The SecureCloud Runtime Agent is the software module that is installed with your virtual machine image in your cloud service provider's environment. The SecureCloud Runtime Agent provides integrity checking functionality such as IP address and location and uses Advanced Encryption Standard (AES) as the encryption standard to encrypt the volume using VM-Level encryption. The Configuration Tool resides in your Cloud Service Provider's environment as part of the Runtime Agent. After product installation, you can launch the Configuration Tool from the installation wizard. If you decline to run the Configuration Tool at this time, you can launch it later. The Configuration Tool configures the following:

- Cloud service provider and virtualization plugin
- Cloud service provider's credentials
- SecureCloud account ID
- Web Service API URL
- Device information for the running machine instance

• Device encryption

MANAGEMENT SERVER

Trend Micro SecureCloud is offered in multiple delivery models, you can either use the hosted services delivered by Trend Micro, or deploy your own SecureCloud Management Server on-premise within your own datacenters. Trend Micro hosted services provide the SecureCloud Management Server with multitenant capability. The Management Server hosts the key approval process, log collection, and reporting. The SecureCloud Web console is the Graphical User Interface (GUI) front end to the Management Server. Your interaction with the SecureCloud Web console is based on role-based administration and privilege levels. The Management Server allows for multiple users, having varying user roles. [6]

VMWARE VCLOUD API

The vCloud API is the primary way for customers, partners, and ISVs such as Trend Micro to integrate with the vCloud Director product. delivered by Trend Micro, or deploy your own SecureCloud Management Server on-premise within your own datacenters. Trend Micro hosted services provide the SecureCloud Management Server with multitenant capability. The Management Server hosts the key approval process, log collection, and reporting.The SecureCloud Web console is the Graphical User Interface (GUI) front end to the Management Server. Your interaction with the SecureCloud Web console is based on role-based administration and privilege levels. The Management Server allows for multiple users, having varying user roles. The vCloud API is used by SecureCloud to determine the identity of a machine image in the vCloud environment. The vCloud API is also used by SecureCloud to learn what data storage devices in the vCloud environment are available for encryption. The SecureCloud Runtime Agent uses the vCloud API to learn the identity and integrity of the vCloud machine image. This information is retrieved from the vCloud API and sent to the Management Server where the user can either grant or deny an encryption key to the requesting machine image, based on the identity and integrity credentials of the vCloud machine image. [6]

The vCloud API in an extremely important element of SecureCloud; it is utilized by the SecureCloud Runtime Agent configuration tool to gather information about what data storage devices in the vCloud environment are available for encryption, as these products and technologies evolve this will only increase. The VCloud API is depicted in Figure 8. [6]

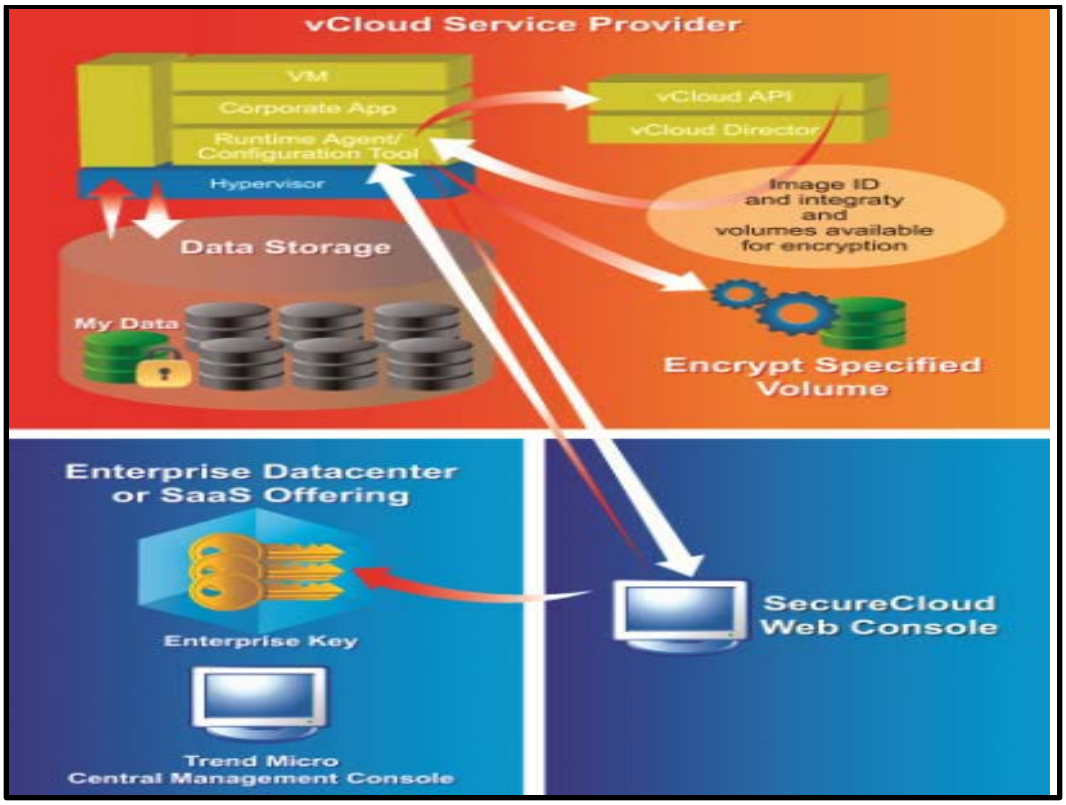

Figure 8. VCloud API [6]

Many of the risks that plague traditional computing are still prevalent in cloud computing. Cloud computing increases these risks because additional steps must be taken to ensure data protected. Instead of the customary security approach where external layered perimeters strategies are employed to protect sensitive data; Cloud computing requires a different approach. An inside-out approach, where the data is protected no matter where it is accessed from or replicated to as well as where the data is secured no matter where exists in the cloud. Using solutions from Trend Micro and VMware enterprises can rest assured that access to their data is controlled from multiple levels through user access control principles provided by vCloud Director and virtual machine access control principles provided by SecureCloud. [6]

5 Future Research

The field of ad hoc mobile and cloud computing is an exciting and emerging new area of computing and computing security. Three areas we have identified for continued research and development are:

- Collaborative Mobile Environment Security
- Better Network Map Utilization
- Jurisdiction & Provider Integrity.

5.1 Collaborative Mobile Environment. To this point there has been a fair amount of research with regard to potential for collaboration between mobile devices, particularly within a commercial organization. It has been stated that mobile devices (laptops, cell phone, tablets, etc.) have an average 24 hour usage rate of 25%. Researchers identified this area as an

untapped sensor network in need of partitioning [13]. The figure below depicts one such proposed partition algorithm developed at the University of Colorado.

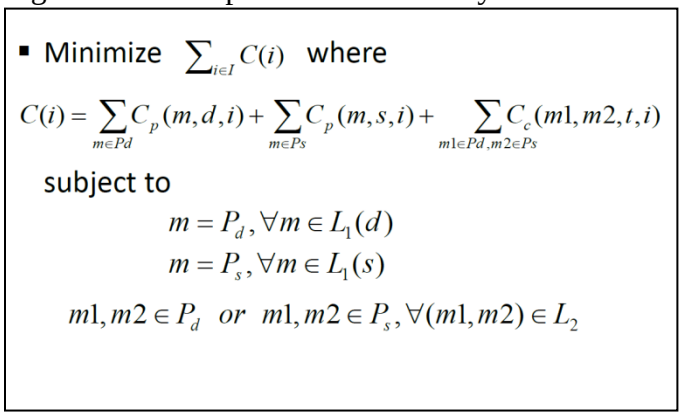

Figure 9. A potential partitioning algorithm [13].

To date, there has been little discussion as to the security concerns in partitioning work across an ad hoc network. The same applies for cloud networks. What are the potential risks to sharing the workload? What impact will a man-in-middle or replay have on this process?

5.2 Better Network Map Utilization. There are many existing network mapping tools to include: Intermapper, WhatsUpGold, OpManagerPro, and even embedded tools within Amazon EC2. These tools focus primarily upon real-time mapping, general network security, and traffic analysis. What is missing from the ad hoc network realm is the ability to harness the vast computing power of ad hoc networks through task assignment. We touched on this above when discussing partitioning, but in order to do such a task the network tools to determine usage and send tasks must be established. During the establishment of these protocols security should be the key concern. Beyond the issues listed above, an ad hoc network would be vulnerable to available fake or spoofed nodes. The network could assign tasks that would never be completed. Furthermore, the attacker could create enough spoofed nodes, that it might be able to determine the complete task [11].

5.3 Jurisdiction and Provider Integrity. The final topic for future research as users push the limits of ad hoc mobile networks and cloud computing is jurisdiction and provider integrity. Larger providers like Amazon and Microsoft have addressed some of these legal issues. However for smaller providers and an independent company, concerns of who owns the data is of key concern. What happens if the provider goes out of business? Can a competitor buy your data via bankruptcy? If you push processing outside of your country's borders, then where is legal jurisdiction determined? As users attempt to push mobile and cloud computing closer to their customers and maximize computing power, it is likely these legal questions will have to be answered in either prior security planning or in a court of law [12].

6 Conclusion

Many of the risks that plague traditional computing are still prevalent in ad hoc mobile and cloud computing. Ad hoc computing increases these risks because additional steps must be taken to ensure data and networks are protected. Instead of the customary security approach where external layered perimeters strategies are employed to protect sensitive data; ad hoc computing

requires a different approach. An inside-out approach, where the data is protected no matter where it is accessed from or replicated to as well as where the data is secured no matter where it exists. Several emerging new commercial solutions, from the likes of Trend Micro and VMware Enterprises, can help assure users that access to their data is controlled from multiple levels through user access control principles. Although future research into the shared computing is necessary, tools like PKI Encryption, CloudSec, vCloud Director and virtual machine access control principles provided by SecureCloud provide the architecture for composing collaborative security-related services in ad hoc mobile and cloud networks such as correlated intrusion analysis, anti-spam, anti-DoS, automated malware detection, and containment. The continued study of collaborative computing, legal ramification, and security is necessary to prevent potential attackers from exploiting this vast new computing realm.

References:

1. W. Li and A. Joshi, *Security Issues in Mobile Ad Hoc Networks*, 2007.

2. C. Alcaraz, I. Agudo, D. Nunez, and J. Lopes. *Managing Incidents in Smart Grids a la Cloud*, 2007.

3. Siani Pearson and Azzedine Benameur, *Privacy, Security and Trust Issues Arising from Cloud Computing*, Internet: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5708519, [April, 2012].

4. Siani Pearson, Marco Casassa Mont, Liqun Chen, and Archie Reed, *End-to-End Policy based Encryption and Management of Data in the Cloud,* Internet: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06133227, [April, 2012].

5. Jia Xu, Jia Yan, Liang He, Purui Su, and Dengguo Fend, *CloudSEC: A Cloud Architecture for Composing Collaborative Security Services*, Internet: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05708520, [April, 2012].

6. "Trend Micro SecureCloud." Internet: http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_effective-end-to-end-cloud-security.pdf, [April, 2012].

7. "Security Schemes for the OLSR Protocol for Ad Hoc Networks." Internet: http://perso.crans.org/raffo/papers/phdthesis/thesisch3.html, [April, 2012].

8. "Ad Hoc Networks." Internet: http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group11/index.html, [April, 2012].

9. "Cloud Computing." Internet: http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm, [April, 2012].

10. "Cloud Computing." Internet: http://en.wikipedia.org/wiki/Cloud_computing, [April, 2012].

11. "Schneier on Security." Internet: http://www.schneier.com/blog/archives/2009/06/cloud_computing.html, [April, 2012].

12. Prepared by the Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, December 2009.

13. "Mobile and Cloud Computing." Internet: http://www.cs.colorado.edu/~rhan/MCS/, [April, 2012].

14. P. Nie. *Security in Ad Hoc Network*, 2006.