An Investigative Analysis Into Security in the Clouds and the Impact of Virtualization on the Security Architecture

Bassam S Farroha, Deborah L Farroha
US Department of Defense
Ft Meade, MD
farroha@ieee.org, bassam.s.farroha@ugov.gov, deborah.l.farroha@ugov.gov

ABSTRACT

The new trend to increasing efficiency in Information Systems (IS) investments is to migrate data processing and storage to external service-centers and vendors that provide a commodity computing platforms that are called Cloud Computing. The approach advocates minimizing the local capabilities to utilize thin clients while providing data manipulation and/or storage services by the service provider over time-shared resources. The concept is not new, however the implementation approach presents a strategic shift in the way organizations provision and manage their IT resources. The systems that process and fuse such data would have to be capable of classifying the resulting information and clearing the computing resources prior to allowing new application to be executed. Processing various levels of sensitive information and fusing results might require the development of a multi-level security system that can send the output to a protected network and systems in order not to have data spill or contaminated resources. The paper discusses these security requirements and potential impact on the cloud architecture. Additionally, the paper discusses the unexpected advantages of the cloud framework providing a sophisticated environment for information sharing and data mining. Finally, the paper introduces emerging issues that need to be addressed including providence, data tagging, and governance.

1.0 INTRODUCTION

Cloud computing is conceptualized as utilizing common resources (software, platform, and infrastructure) as a service over an Intra-net or inter-net to provide dynamically scalable computing infrastructure, for data storage and/or processing. Ideally, identities are checked at login and access is granted and reconfirmed periodically and when new requests take place and the access is authorized to a level commensurate with the attributes and the prevailing digital policy in effect. All communications and data are encrypted with appropriate keys that are capable of protecting the data based on its location and the sensitivity of that data. Meta-data should be extensively utilized to tag all aspects of data that allow potential users to understand the data reliability as well as authorize access.

1.1 Cloud Essential Characteristics

The 21st century Information Technology (IT) transformation is fueled by the need for more processing power, more data, and better access, all of which lead us to work on developing a more connected environment. However we also have to face a shortage of resources (e.g., financial and manpower) that have adverse impacts on our environment. [5] Cloud computing is a concept that promises to address this situation in part with *On-Demand Self-Service,* where the services and infrastructure are always available and ready to support the needs of users, but not dedicated when not being used. *Resource Pooling* is implemented to ensure that resources are not left idle while other subscribers are facing shortage in processing or storage capacities. The new concept allows for *Rapid Elasticity* of resource allocation to overcome the problems associated with having to provision dedicated capacity needed only to support operations during peak performance times. Figure 1 shows the projected growth path of computing infrastructure [12].

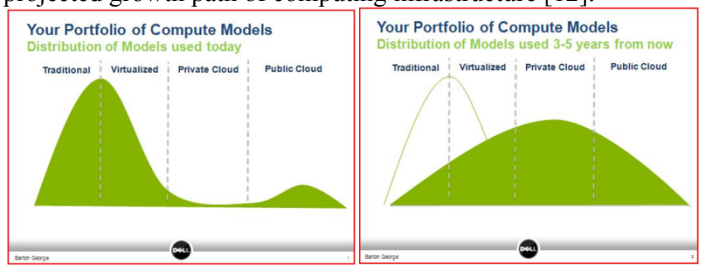

Figure 1 Capacity Allocation Options

With Cloud architecture, users get *broad network access* to any part of their data and can process their data in a *location-independent fashion*. This means that a user can login from a remote location, start a session that requires data manipulation and search functions, (with all the processing being performed within the cloud), and then receives the results through the remote link. The implication here is the capability to ensure that each user is authenticated and their access level is verified based on ID credentials and their associated hard and soft attributes.

1.2 Security Issues

The currently accepted model for the Enterprise Security Management (ESM) is best presented in the form of ten capabilities that need to be applied to provision and manage enterprise IA functions that protect assets including data and information systems. The ESM Framework provides the architecture, design, and guidance for implementation of ESM within an enterprise.

While cloud computing has enormous potential to be a game changer for businesses around the world as the backend of the enterprise, there are still a number of major issues that need to be resolved before the cloud approach can live up to the huge amount of hype it has gotten thus far.

First and foremost is security. For the individual corporation, they are handing over their most protected corporate data to essentially an outsourced storage provider, or relying on another party's server processing or software for their business applications. With Cloud computing, your data could literally be stored on the same server as that of our competitors or adversaries. Rather than having direct or even indirect control over your data, it is at the mercy of your provider. The decision of putting critical data on a server that you don't physically control turns traditional security paradigms on their head.

Traditional Secure Access Control for sensitive information is done through first identifying the person or entity that is requesting the information by means of authentication. The second step is to review the current policies that govern the data, and the requestor and the locations where that data is allowed to be shared. Finally, we look at the specified data and examine all the attributes that are available including such information as source, sensitivity, and location to determine based on the meta data if that information is sharable with the requesting entity. The current approaches to access control vary, and include such methods like Policy Based Access Control (PBAC) and Attribute Based Access Control (ABAC) [2]. The goal is to

build access control that is dynamic and adaptive to allows the system to have built-in intelligence to comply with current policy, investigate the requesting entity's identity and location and deliver data based on the current threat level, while logging that activity and marking the metadata. The new model for access control is Risk Adaptive Access Control (RAdAC), which is presented in Figure 2.

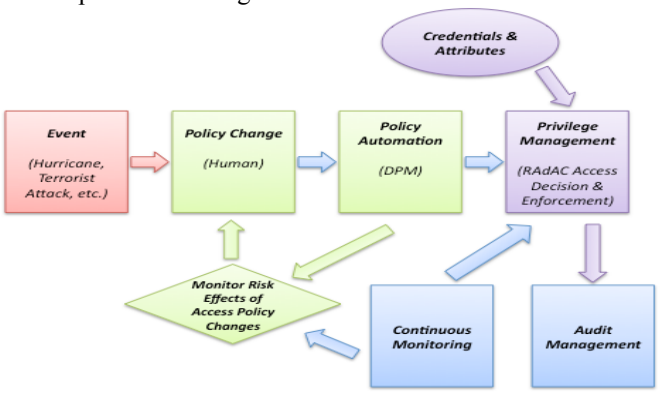

Figure 2 RAdAC Model Process Flow

When asking top CEOs about Cloud adoption, Security concerns are probably one of the major reasons why the latest numbers show that over half of all enterprises have cloud in their plans, but only 2 percent are actually implementing it.[8] Therefore, in order for us to reap the overwhelming advantages of converting to cloud based IT we need to quickly embrace security, adopt common standards, and provide APIs to researchers and vendors so become intrinsic to cloud service offerings.

2.0 CLOUD MODELS AND ARCHITECTURES

A second major area that needs to be sufficiently addressed by cloud providers is *portability*. Practically every cloud provider today operates differently, making it difficult to move data from one provider to another. We need to move beyond proprietary implementations and data silos, to a committed set of public providers that use standard protocols and services to open competition and eliminate vendor lock-in. Another major issue is *reliability*. We need to guarantee a measurable quality of service (QoS), complying with service level agreements (SLA), and suitable controls on latency. There is a real dependency on the public Internet to provide services to commercial and government customers; a commodity that was build to deliver a best-effort information transfer capability primarily for researchers.

2.1 The Cloud Concept

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of several essential characteristics, three service models, and four deployment models. The essential characteristics include On-demand self-service, Rapid elasticity, Measured Service, Resource pooling [4].

2.2 The Migration Path

We have been moving towards service based computing where applications, servers and data elements are placed on a common service bus with access granted to qualified sources. This approach has been accelerated by the need to increase the processing power beyond the currently available processing speeds due to approaching the physical limitation on hardware speeds. This first approach to overcoming this limitation was to add more processing cores to each processor to increase the overall system throughput by utilizing the onboard bus with multiple cores. The next was to add specialized processors that are optimized for specific functions. They were connected through the Mission Service Bus (MSB) and had load balancing and distribution functions to ensure a higher efficiency. At the same time the IT community has been gaining additional expertise and confidence with very large datacenters, and have developed advanced algorithms for massive storage and search techniques. The recent economic downturn, energy costs skyrocketing, and the culture shift towards building capabilities that are more environmentally friendly led to concentrating on developing pooled resources with higher utilization and efficiency.

2.3 Enhancing the Model

The SOA model was originally developed to allow corporate entities to build centralized and specialized computing services that can be shared within the enterprise to deliver uniform services to all subscribing communities. The model grew to a new trend in architectures that allowed multiple entities to share common services over a common services bus. The value was apparent where standing up a service for a new customer would have been as simple as subscribing to the service, and search and discovery were simplified by enabling the process by providing metadata and allowing comprehensive searches through available and authorized resources. Security was to be more comprehensive because it would be applied equally to all components, and all patches and policy updates would be remotely administered to all connected resources.

2.4 Essential Cloud Technologies

2.4.1 Hadoop File Systems

Hadoop was originally inspired by Google's MapReduce and Google File System. It is a top-level Apache project being built and used by a variety of individuals and global organizations. The Apache Hadoop is a software framework that supports data-intensive distributed applications available under a free license. The product is organized in clusters that enable applications to work with thousands of nodes and petabytes of data. The typical Hadoop cluster includes a single master and multiple slave nodes. The master node consists of a jobtracker, tasktracker, namenode, and datanode. Each slave node consists of a datanode and tasktracker. The reference to Hadoop Distributed File System (HDFS) refers to a distributed, portable and scalable filesystem written in Java for the Hadoop framework, which was architected to handle very large files [9]; however the HDFS does not provide High Availability. The filesystem uses the TCP/IP layer for communication. This is because the filesystem requires one unique server, the name node. This is a single point of failure for the HDFS installation. If the name node goes down, the filesystem is offline. When it comes back up, the name node must replay all outstanding operations. The HDFS stores large files; with an ideal file size being a multiple of 64 MB [9], across multiple machines. HDFC achieves the advertized reliability by replicating data across multiple hosts, instead of the traditional RAID architecture. It is recommended that data is stored on at least three nodes: two on the same rack, and one on a different rack. Data nodes are designed to coordinate with each other on rebalance data, moving copies around, and to keeping the replication of data high.

2.4.2 Distributed File Systems

The traditional definition of distributed file system or network file system is any file system that allows access to files from

multiple hosts sharing via a network or a common services bus. This makes it possible for multiple users on multiple machines to share files and storage resources. It is essential that client nodes do not have direct access to the protected information but interact over the network using common protocols. This makes it possible to restrict access to the file system based on access methods running on both the servers and the clients. In contrast, in a shared disk file system all nodes have equal access to the block storage where the file system is located. On these systems the access control must reside on the client. Distributed file systems may include facilities for transparent replication and fault tolerance.

2.4.3 Map Reduce Search

The term MapReduce refers to a programming model for processing and generating large data sets. Consumers specify a Map function that processes specific pairs of key and value to generate a set of intermediate key/value pairs, and a Reduce function that merges all intermediate values associated with the same intermediate key. Many real world tasks are expressible in this model. [5] This approach is a departure from standard programming methods where new programs written in this functional style are inherently parallel, executing on a large cluster of low-end commodity machines. The operating system needs to accommodate input partitioning, scheduling, failures, and managing inter-machine communications. These enhancements of infrastructure capabilities allow basic users to utilize the resources of a large distributed system. The general implementation of this technique implements MapReduce on a large cluster of commodity machines. The product is a highly scalable architecture processing many terabytes of data on thousands of machines. [5] MapReduce is a highly effective and efficient tool for large-scale fault-tolerant data analysis. MapReduce also provides fine-grain fault tolerance for large jobs; failure in the middle of a multi-hour execution does not require restarting the job from scratch.

3.0 SECURITY and PRIVACY

While cloud computing is not a revolutionary technology, it does present unique security challenges based on the outsourced, multi-tenant nature of the services being provided. The earlier definitions of clouds show multiple models and architectures under varying authorities. Traditionally physical security has been the first line of defense for both commercial and military systems. The cloud environment essentially removes that layer of protection for either data storage, data processing or both. The demise of physical isolation necessitates increased logical protection to compensate for the lost security. Commercial cloud service providers will guarantee the availability of their systems via redundancy and some physical protection; however, organizations using these services have to trust the provider's processes of screening of their employees to protect the valuable data from insider threats of theft, destruction, and manipulation.

Logical security is accomplished through encryption of data a rest and on the move, and by developing robust methods of access and identity management. Furthermore, users need to be guaranteed real-time access to the vendor's audits and continuous monitoring outputs. Even though the vendor would have a custom virtual environment for each individual customer, there is still a need to make sure that the vendor applies very strict secure configuration controls that ensures the adoption of the latest malware detection and correction products. This will ensure that we don't get a virus epidemic that can destroy all data on the cloud.

When considering securing the cloud, we should first consider the goal of the new architecture. If we are seeking virtualization of processors to enable a centralized, general purpose processing of multi organizations' computing functions to be efficiently accomplished, then we need to consider many intermediate steps to secure the end-to-end operations. First we need to make sure that virtual machines are malware free. The system has to start with a Clean Load at the inception of each new processing load. Second is that we have to ensure a clean wipe of memory between tasks and between user loads. It would no longer be sufficient to only remove the addressing space and ignore the data. Additionally, cross memory access should be prohibited in the architecture.

The second type of application to cloud processing is massive storage, searches, and retrieval processes. The mere fact that many users will be storing their sensitive information on the same infrastructure creates a new paradigm for the security architecture. We can certainly encrypt data in a storage device, but here we need to encrypt data in transit and while being stored in processor memory. Data stewards need to either catalog their data and keep a local copy of references to determine which data needs to be recalled to search for content, or must simply bring back large blocks of data each time they need to access information. Access control also gets more complicated when we have multiple levels of security, but the initial concept used in a single classification level environment is still the same, as shown in Figure 3.

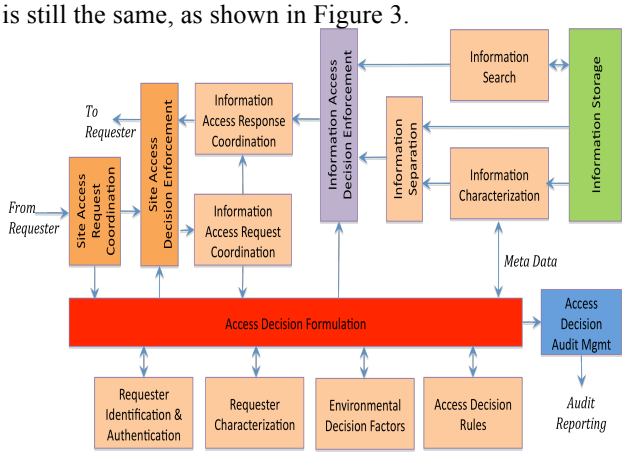

Figure 3 Access Control in a Single Classification Level Environment

Finally, there is a need for Security-Enabled Hardware where the hardware will have specific signatures that are known to authorized users and is traceable to allow encryption/decryption approaches that cannot be penetrated. This becomes more relevant in a virtualized environment where processes are not tied to specific or attributable processors. As we move forward with implementing cloud security, we first have to overcome the migration issues of converting our current stovepipe infrastructure into an interconnected environment with measurable trust levels between elements. We then need to apply digital policy [11] homogeneously and allow the smart structures to selectively exercise the applicable policy components based on identities, environment and available attributes. Figure 4 shows the interaction between a digital policy management engine and the enterprise security services components.

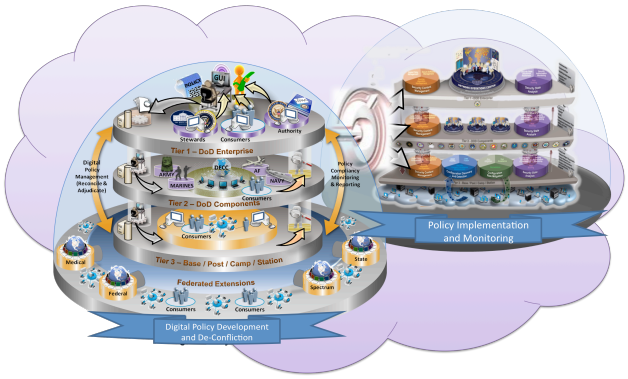

Figure 4 Managing Digital Policies in a Cloud Environment

The continuous focus on low hanging fruit only approach will surely prevent us from getting where we need to be for better protection of data in security-engineered/evaluated systems. The short sightedness might bring quick wins for the near-term, but will leave us totally vulnerable to sophisticated attacks. This will have worse consequences as time goes by and we grow more dependent on the new environment. The question that keeps being asked is: "Can highly sensitive data and applications be supported in cloud processing?" The answer is that it depends on how sensitive the data is, and who has access to that cloud.

3.1 Virtualization

This is one of the most common types of cloud being developed to increase accessibility and allow users to consolidate security resources to protect the common data. This can be implemented as Private or Public cloud. However this model turns the prevailing security approach on its head and weakens the physical security element. The competitor or adversary would only need to subscribe to the same service to get physical access to the data. Consequently, this raises the need for a better access and encryption techniques to add logical security to replace traditional physical protection.

The second part of the storage dilemma is the Search and Discovery of the stored data. Since data is encrypted, searching it requires either bringing it back, decryption, and searching or the development of search tables that are stored locally to pinpoint the data to be retrieved.

The server virtualization approach of cloud computing encompasses multi users per hardware to achieve multi missions. The approach capitalizes on sharing commodity resources between subscribing organization to achieve higher efficiency and have access to additional resources when needed. The servers are made available over the network with common software loads and capability to process data in parallel. The security of such an environment is essential, especially to prevent unauthorized monitoring and the possibility of infection with malware. One of the best approaches to utilize such an environment is to start with a clean copy of the virtual environment every time there is a log in. The virtual environment will be available for the session duration and then terminated after the data is safely stored and the keys are secured. When the same user or others request service, a new session is initiated with a new virtual machine that is hosted over one of the commodity resources. It is essential to start with a strong user authentication at log in, and then entry into the environment. Based on the identity of the user, the current threat environment, and the attributes of the data and users, access is granted to select data sets. The issues associated with Cross Domain and Multi-Security domain exists in these environments and must be dealt with to eliminate security breaches.

3.2 Multi Level Security

Sanitization is a problem area for MLS systems. Systems that implement MLS restrictions, like those defined by the Bell-La Padula model, only allow sharing when it does not obviously violate security restrictions. Users with lower clearances can easily share their work with users holding higher clearances, but not vice-versa. There is no efficient, reliable mechanism by which a Top Secret user can edit a Top Secret file, remove all Top Secret information, and then deliver it to users with Secret or lower clearances. In practice, MLS systems circumvent this problem via privileged functions that allow a trustworthy user to bypass the MLS mechanism and change a file's security classification. However, the technique is not reliable.

Bypass is problematic when introduced as a means to treat a system high object as if it were MLS trusted. A common example is to extract data from a secret system high object to be sent to an unclassified destination, citing some property of the data as trusted evidence that it is 'really' unclassified (e.g. 'strict' format). A system high system cannot be trusted to preserve any trusted evidence, and the result is that an overt data path is opened with no logical way to securely mediate it. Bypass can be risky because, unlike narrow bandwidth covert channels that are difficult to exploit, bypass can present a large, easily exploitable overt leak in the system. Bypass often arises out of failure to use trusted operating environments to maintain continuous separation of security domains all the way back to their origin. When that origin lies outside the system boundary, it may not be possible to validate the trusted separation to the origin. In that case, the risk of bypass can be unavoidable if the flow truly is essential.

3.3 Access Control

Granting access is determined by many factors including establishing a positive identity of the requester. Establishing the positive true identity follows different processes depending on the sensitivity of information and sophistication of the provider. This can be as simple as a user having physical access to the enterprise, by virtue of being allowed entry to a physically controlled facility. Logical identity can be established by issuing a User Name and Password to each entity, where the user name is issued to identify the user, and the password provides a means to verify that the entity asserting the identity is authenticated as being on a list of authorized user name/password pairings. The availability of public key cryptography has given rise to the issuance of PKI certificates as identity credentials. Here, each entity is assigned a globally unique digital identifier, which is embedded in an identity credential that includes that identifier, some certificate management and a public key that can be used by a relying party to authenticate the user, all bound by a digital signature of an authorized source. Use of biometrics for humans that can be validated against an authoritative source for the biometric data that is captured prior to or during a session.

3.4 Meta-Data and Smart Labeling in Multi Tenancy

Trusted Meta-Data is an essential requirement in a multi tenant environment where multiple independent users share common IT resources for their computing needs. Crypto-binding meta data to the data guarantees that the data is trustworthy and that is has not been modified by third parties. However, when modification and updates are part of the mission, the utilization of smart data becomes necessary where the meta data will be updated by the system with proper labeling to identify the entity,

and time of modification. The smart data concept investigates the possibility of including all the identity of recipient of data to ensure that decisions are made based on full knowledge of who has access to the information. In a multi-tenant environment that is controlled by a service provider, we need to determine which elements of information need to be made "visible" to which group of users. The visibility protocols controls technical, operational, and legal processes that allow the users to access user, monitoring and audit data In a leased IT environment, there is a need for verifiable transparency to access system security information and confirm claims of incidents, responses, and verify that nothing else took place that was not reported.

3.5 Network Exposures and Dependencies

Since we are reducing the customary Border protection techniques when choosing to utilize public or private clouds, then we need to change our defenses from perimeter focus to an internal approach that offers more robust protection. The approach amplifies our greater dependency on network resilience to ensure the continued operations of systems and the success of the organization's mission

Similar to an internal enterprise, adversaries will attempt to attack from internal and external locations, however, in our new environment, that line between the two types of attack is blurred. Attacks will occur at both storage and processing resources as well as on the infrastructure, and data in transit. When dealing with Legacy System Access that was built to utilize single factor authentication, we are used to having a specific level of sensitivity for the information and the systems hosting that information.

The cloud subscriber has to take part of the responsibility for security obligations that are needed to develop a data segmentation capability by adhering to stricter data labeling/marking guidelines and standards. The next generation of privileged access to the data should be based on higher confidence algorithms and attributes. When new data is encrypted, the keys should be in the customer's control and stored locally to prevent unauthorized access. Moreover, the key generation and management process should be driven by some *trusted* third party. When the service provider supports multi-tenant audit logging, data stewards need to be immediately informed of all access to their sensitive data and provided a smart method to track that use. Dynamic, real-time, continuous monitoring is key to preventing large data compromises, and should be a requirement where sensitive data is stored. The customer should be getting a direct feed of that monitoring application to ensure the status of their data.

3.6 Information Sharing

As we move more and more into the information sharing age, cross-domain information transfer becomes more important. The first part of this is an analysis that centers on the entity we need to protect. The cyber-security of assets has to identify the components and boundaries of the domain it intends to protect. This can be a system, a system of systems or an enterprise. More precisely, the boundaries and interfaces have to be well defined to develop and execute a cyber-security plan. The Department of Defense has identified the Global Information Grid (GIG) as their enterprise and is working on solidifying its boundaries. As sensitive information is often encrypted, signals intelligence often involves the use of cryptanalysis. However, traffic analysis—the study of who is signaling whom and in what quantity—can often produce valuable information, even when the messages themselves cannot be decrypted.

The GIG is composed of multiple security domains and carries the information end-to-end in different ways, depending on the security of the information as well as the security provided by the data link. When higher sensitivity data is transmitted over a lower classification path, another encryption mechanism is employed to offer the additional protection. The system of systems controlling the security of the data and links can determine, based on a priori knowledge, the type of encryption needed to enable the transaction. The DoD has been working with industry and academia to develop a more flexible Access Control model where a trusted automation would grant access to authenticated users through an approved process. Figure 5 illustrates an interoperable ABAC process with Policy Decision Points (PDP) and Policy Enforcement Points (PEP) for the Defense Military Data Center and the Global Force Management Data Initiative.[7]

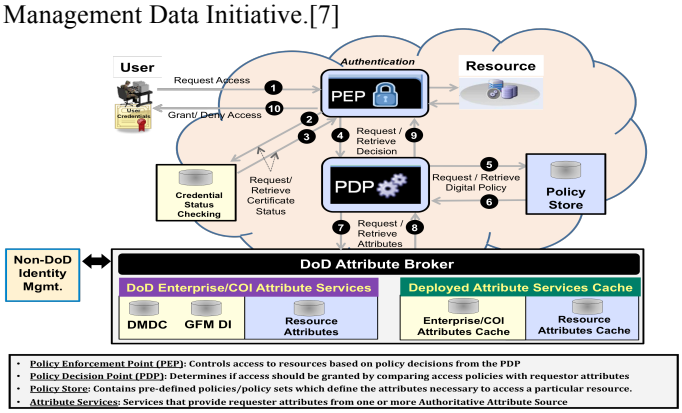

Figure 5 Deploying ABAC in the Clouds [7]

4.0 IMPLEMENTATION CONCERNS

4.1 Types of Attack

The ways our adversaries and competitors can invade or attack our IT resources have grown and changed, challenging the new technologies being utilized to host and process information. We have seen an exponential increase in the number, type, and intensity of attacks. Some common types of attacks include:

- *Malicious Code:* This is transmitted to the victim's site through Attachments, Piggybacking, Internet Worms, Web Browser Exploits, Hacking, and Affiliate Marketing.
- *Theft of Data:* This is done through hacking, identity theft, access manipulation, and other methods.
- *Infiltration:* This includes social and technical infiltration of the information systems and the personnel managing these important assets. The adversary agents get access through physical or logical access holes in the security and steal, destroy and manipulate information.
- *Man In The Middle:* This type of attack involves intercepting data while in process or in transmission between source and destination. The attacker ether steals, destroy or changes the data to harm the competitor.
- *Denial of Service (DOS):* This type of attack usually consists of the concerted efforts of a person or persons to prevent the information source services from functioning efficiently or at all, by temporarily or indefinitely flooding the servers with requests beyond their ability to respond.

When migrating to a cloud infrastructure, these systems and services will be exposed to many new players, which increases the number of possible attackers, and since the users don't have

access to security information, the provider has to be more vigilant to detect trends that diverge from the aggregated customer utilization trends, in addition to monitoring each user's data individually and reporting on unexpected activities. More types of security attacks are described in the reference [11]

4.2 Mobility

Mobility and cloud computing are two of the most sought about technologies in this decade. The promise of lowered IT costs and flexibility to manage information remotely and on the move has given this trend a huge advantage. When looking at a future with wideband wireless utilizing 4G and a cloud infrastructure, we are likely to see merging of telecom and IT budgets and emergence SaaS as the new IT delivery model for the home consumer market. Alternatively we could see a trend change to a network-based delivery of applications or an IaaS. There is also an opinion that a model can emerge where communications service providers, mobile operators and even ISPs, providing Everything as a Service (EaaS).

4.3 Compliance with Laws and Regulations

We need to ensure compliance with the laws and regulated data with respect to data location, access, and modification. There is also a need for legal and acquisition partnership in obtaining agreement of SLAs, and methods to observe and measure the provider's compliance. We need to know what can be shared, and where data originated and where it got modified so we can make the best decisions. Many organizations have strict laws the geographical boundaries where data can be handled and citizenship of operators which needs to be guaranteed.

4.4 ESM Services and Migration Approach

Referencing the ESM Components we introduced earlier, we can clearly conclude that the migration to a secure cloud would necessitate that these services not just be maintained, but strengthened to give subscribers an acceptable level of security[13]. Today, we can't legally place sensitive data on a system that has not been certified and accredited by an authorized agency. Since the role of Identity and Access management would be the gatekeeper to multi-organization data, we need to make sure that leaks are prevented and up-to-date policy and system protections are enforced. Key management in the Enterprise has to be handled by a trusted entity within the enterprise and a third party to manage the issuance and maintenance; when working in the Cloud, that function would have to be managed in a way that allows for storage of the key locally with the data owner, while allowing the encrypted data to reside in a common environment. Making the Access Control process dynamic within the clouds is fueled by the concept of RAdAC is being investigated to enable smart access capabilities to smart data. Dealing with sensitive data, especially when we have multiple levels of sensitivity and user clearances on the same hardware and fabric will also need reliable Meta-data plays which should be securely attached into the header of the data.

4.5 Future Considerations

Several issues need to be considered including:

- What is the service level agreement and what recourse do users have if the service provider lets him down?
- If an organization stores data into a cloud-based service, will the subscriber ever be able to get it back out again?
- What are the standards utilized by the provider? How is the service monitored? How are policies enforced?
- What cross-domain capabilities are provided to enable data sharing between organizations?
- How are data sets, processes, and identities protected within the environment?
- Is the concept of data portability even a consideration in the current implementation?
- The expanded view of Insider threats due to including the service provider employees as part of threat potential.

5.0 CONCLUSION

The common IT infrastructure suffers from persistent low utilization levels of the enterprise resources. Traditionally infrastructure is built to handle peak loads, which are occasional, and idle the rest of the time. Corporate cultures operate in a manner that creates inefficient workload density to the IT infrastructure; therefore we need to change the IT architecture model to a more efficient model that maps better to our business approach. Future IT spending is trending towards a pay-as-you-go model, where the vendors will have a transparent cost structure, and allow for optimized assignment of workloads within the available infrastructure. The actual day-to-day operation of a flexible infrastructure should employ a self-service, on-demand provisioning model, where users are allowed to log in from approved locations within a known security domain and are given the requested services and access to authorized data. For this model to work, it is essential to have a flexible and elastic scale-up-and-down model where additional resources are made available either on demand or automatically to satisfy a pre-agreed upon QoS in a Service Level Agreement.

6.0 REFERENCES

[1] Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Federal CIO Council, Draft version 0.9, November 2, 2010

[2] From ABAC to ZBAC: The Evolution of Access Control Models, Alan H. Karp, Harry Haury, M. Davis, HP Laboratories Feb 2009.

[3] Guidelines on Security and Privacy in Public Cloud Computing; Draft Special Publication 800-144; National Institute of standards and Technology; Wayne Jansen, Timothy Grance; January 2011

[4] Effectively and Securely Using the Cloud Computing Paradigm; Peter Mell, Tim Grance; NIST, Information Technology Laboratory; 10-7-2009

[5] MapReduce: Simplified Data Processing on Large Clusters; Jeffrey Dean, Sanjay Ghemawat; OSDI'04: Sixth Symposium on Operating System Design and Implementation, San Francisco, CA, 2004.

[7] OSD Organization Server Working Group Meeting, DoD Personnel and Readiness Information Management, June 7, 2006. https://www.mpm.osd.mil/documents/OSDOrgServer060706_WGBrief.pdf

[8] https://www.ceoupdate.com/

[9] Forum and Workshop II Artifacts; Track 3 "Cloud security" report, Ron Knode, National Institute of Standards and Technology, Information Technology Laboratory, November 2010

[10] A Novel Approach to Implementing Digital Policy Management as an Enabler for a Dynamic Secure Information Sharing in a Cloud Environment, Bassam S Farroha, Kristine R Essman, Deborah L Farroha, Andy Cohen, SPIE Defense & Security, Orlando, FL, 4/ 2011

[11] Enabling Net-Centricity through Cross Domain Information Sharing, B. Farroha, D. Farroha, M. Whitfield; IEEE International Systems Conference 2009, Vancouver, BC, Canada

[12] The Cloud Cometh, Barton George, enterpriseefficiency.com, April 2010

[13] An Adaptive Framework for Integrating Heterogeneous Enterprise SoS Security, Bassam S. Farroha, Deborah L. Farroha, INCOSE International Symposium 2011, Denver CO