ISSN 2347 - 3983
Volume 10. No.4, April 2022
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter051042022.pdf
https://doi.org/10.30534/ijeter/2022/051042022

Case Study of Cloud Computing Security Issues and confidentiality Challenges

Najat Abohamra[1],SabriyaAlghennaiSalheen[2],Abdussalam Ali Ahmed[3]
[1]Computer DepartmentCollege of Electronics, Bani Walid, Libya.
[2]Department of Communications.College of Electronic Technology.Bani Walid, Libya.
[3]Mechanical and Industrial Engineering Department, Bani Waleed University, Bani Waleed/Libya
[1]Engnajat3@gmail.com,[2] Sabriya.Salheen97@gmail.com, [3]abdussalam.a.ahmed@gmail.com

Received Date:March 3, 2022 Accepted Date:March 22, 2022 Published Date:April 07, 2022

ABSTRACT

Cloud computing is a term, which involves virtualization, distributed computing, networking, software and web services. A cloud consists of several elements such as clients, data center and distributed servers. It includes fault tolerance, high availability, scalability, flexibility, reduced overhead for users, reduced cost of ownership, on demand services etc.Cloud Computing offers better computing through improved utilization and reduced administration and infrastructure costs. Cloud Computing is the sum of Software as a Service (SaaS) and Utility Computing. Cloud Computing is still at its infant stage and a very new technology. Therefore, most of the users are not very confident to adopt it.The main issue that faced the cloud computing is "security". In this paper, we try to find out what countermeasures best strengthen the confidentiality, integrity and availability (CIA) of the implementation of cloud computing within the DOD This will be done by analyzing threats and countermeasures within the context of the ten domains comprising the Certified Information System Security Professional (CISSP) Common Body of Knowledge (CBK). The ten domains include access control; telecommunications and network security; information security governance and risk management; application security; cryptography; security architecture and design; operations security; business continuity planning and disaster planning; legal regulations, compliance, and investigation; and physical security. The results will provide a comprehensive guide for any Department of DefenseDoD entity attempting to secure its cloud solution.

Key words: Cloud computing, Cloud Security, Cloud Security and Privacy, Department of Defense.

1. INTRODUCTION

Just as the Internet revolutionized and democratized access to information, the idea of cloud computing is the same for Information Technology (IT). Cloud is refactoring the IT landscape. Instead of uncrating computers and racking them in your server closet, the cloud allows for virtually downloading hardware and associated infrastructure. By abstracting IT infrastructure and services to be relatively transparent, the act of building a virtual data center is now Cloud Computing.There are several definitions that we can use to define the Cloud computing technology , but for this research , we defining Cloud computing as a virtual infrastructure which provides shared data and communication technology services, via an internet "cloud," for "multiple external users" through use of the Internet or "large-scale private networks[1]. Cloud computing make users able to access to services Information Technology (IT) services, (i.e., application, data storage) without requiring an understanding of the technology or even ownership of the infrastructure.For more simplify comprehensive of cloud computing, the example of an analogy to an electricity computing grid is useful. A power company maintains and owns the infrastructure, a distribution company disseminates the electricity, and the user only uses the resources without operational responsibilities. Likewise, a client's cloud computing access enables "shared resources, software, and information on-demand" on a fee-for-service basis.One of the attributes of cloud computing is elasticity of resources. This cloud capability allows users to increase and decrease their computing resources as the user needed. There is always an awareness of the baseline of computing resources, but it is not easy to predict the future needs, particularly when demands are invariably changing. Cloud computing can offer a means to provide IT resources on demand and address spikes in usage. Interest in the cloud is growing because cloud solutions provide users with access to supercomputer-like power at a fraction of the cost of buying such a solution outright. More importantly, these solutions can be acquired on demand; the network becomes the supercomputer in the cloud where users can buy what they need whenever they need it. Cloud computing identifies where scalable IT-enabled capabilities are delivered as a service to clients using Internet technologies.Cloud computing has generated significant interest in the marketplace and is forecasted for high growth[2],[3].

2. CLOUD COMPUTING

Cloud Computing Deployment Models:

There are four types of clouds:-

- Public (external).
- Private (internal).
- Community (a subset of public/private).
- Hybrid (combination of any two or more above)[1].

Cloud Computing Service Models:

There are three types of cloud service models: Infrastructure, Platform and Software as a Service. The software layer builds upon platform, while platform builds upon infrastructure.

a-Infrastructure as a Service (IaaS): With this model, a customer rents physical facilities, connectivity, and hardware to deploy customer software, operating systems and applications; specific IaaS vendors include "Amazon EC2, Go Grid, and FlexiScale." With IaaS, a customer is not required to manage/purchase servers and network infrastructure equipment, even though configuration management is still required. One disadvantage to IaaS is that bandwidth delays may occur with remote execution.

b-Platform as a Service (PaaS): This model enables a customer to rent a platform (hardware, storage, or virtual computers) to deploy itsown specifically created applications; applications are then supported by the provider. PaaS is middleware, which can include access/identity/authentication management; specific vendors of PaaS include "Force.com, Google, AppEngine and Coghead."59 One specific beneficial use of PaaS is the development of standardized software programs.

c-Software as a Service (SaaS): SaaS allows a customer to rent software applications provided over the Internet via a thin client/web browser (user does not own or control the infrastructure, servers, operating system, or storage); specific SaaS vendors include "Salesforce.com, GoogleApps, and Oracle on Demand"[1].

3. CLOUD SECURITY

Security is defined as Freedom from risk or dangers while information security is defined as save gardening or organization's data unauthorized access or modifications to ensure its availability confidentiality or integrity (CIA). The three principles are the main concerns when dealing with information security and each principle requires different security mechanisms to be able to be enforced. For Cloud Computing to be considered to be secure, these principles are what it has to live up to. The Committee on National Security Systems (2010) defines the three areas as:

Confidentiality - assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Integrity - in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Availability – timely, reliable access to date and information services for authorized users.

To enforce these principles, there are different mechanisms that can be applied. The mechanisms are retrieved from a blog called Continuity Disaster Recovery[2].

Confidentiality is sometimes referred to as privacy and to enforce it you can apply:

Access control - with access control you can control how and what information user can access. How could be by authentication through passwords and/or biometrics [3],[4].

Passwords - password is the basic authentication method and to make it even more secure it can be used alongside smart cards or biometrics.

Biometric - biometrics concerns the use of human physical characteristics for identification and authentication. It could be for example fingerprint scanning, retina scanning or face recognition[5].

Encryption - by encrypting information from plain text to be unreadable prevents unauthorized users to access information. Encryption is performed through a mathematical algorithm to alter the information.

Ethics - through policies employees can get the necessary guidance to know how to behave and prevent unethical use of for example an information system[6],[7].

To maintain the integrity of information we can use:

Configuration Management - this is how manage change when it comes to the information technology environment.

Configuration Audit - this mechanism controls that information that is altered is allowed to be performed. The auditing can be done by monitor log changes either manually or through an automated system [8].

Availability should always be ensured so the authorized users can access desired information whenever they want. To ensure that data is always kept available and safely stored.

The following points should be considered:

Data Backup Plan - to have a plan of how you backup your information is always important. It includes what information is being backed up and at which time interval. This depends on what type of business you run and how often information is altered[9].

Disaster Recovery Plan (DRP) - this includes the procedures for how a quick backup is performed with minimum impact on the business[6].

Business Continuity Plan or Business Resumption Design -this is a part of the DRP and documents of how a business gets back to normal after a disaster has struck[2].

The most important Security Risks of Cloud Computing

According to the report" top threats to cloud computing V1.0" by CSA we listed the most important risks of cloud computing below:

- When a customer requests that certain information should be deleted, copies of the information could still reside somewhere in the Cloud due to backups or some other redundant reason. The risk could be that this information is left unprotected on a hard-drive that is shared with some other company.
- If the service does not control the authentication and authorization properly by having weak control mechanisms, there is a risk that information can be affected by unauthorized change or deletion[7],[10].
- When not having control of who is using the Cloud, by for example providing the possibility to be anonymous when registering for a Cloud service, criminals could get the

possibility to exploit Clouds by applying malicious software that can give them access to information they should not have. This is mostly applicable to PaaS and IaaS where customers have the possibility to develop and run software[8],[11].

- If malicious software is executed in the Cloud, it could affect the integrity if the intent is to alter or delete information.
- A weak interface that for example transmit information in clear-text or allows anonymous access lead to that information can be easily acquired by unauthorized users.
- Interfaces needs to be secure so they can withstand malicious attacks that could compromise the availability of the service[6],[12].
- When a Cloud provider hires their Cloud employees, there are matters as hiring standards and practices, as well as how they grant their employees access to virtual and physical assets and if the employees are monitored in their work. If the Cloud provider does not consider these matters important, there could be a big risk that they hire someone that have a criminal intent such as someone that is involved in organized crime and wants to have access to confidential information[6],[13].
- If a Cloud provider has employed persons with a criminal intent, such as hackers or people involved in organized crime, because of poor hiring standards and practices, important information could be changed or deleted. The risk is even greater if there are no monitoring processes set up for the Cloud employees[9],[14].
- If a hypervisor that controls the virtualization of the infrastructure fails to control the levels of authorization of users in the Cloud, users could get an inappropriate level of control that could lead to alteration or deletion of information.

-Account or Service Hijacking, by using attacks such as phishing or exploitation of software, credentials could be acquired that can be used for getting access to sensitive information[10].

-If an unauthorized party gets hold of credentials by for example phishing, information runs a risk of being changed or deleted by that party[15].

-If an account gets hijacked, there is a risk that the service availability can get compromised.

-The need to encrypt information is very important when it comes to Cloud due to the use of the services through Internet. When running an IT infrastructure in house, the need to encrypt transmitted information is not as important as encrypting the hard-drives and databases. But by using a Cloud service, everything needs to be encrypted to ensure safety, both the transmitting and storing of information[11],[16].

- Information that is not encrypted when it is transmitted can easily be altered so the message that is received does not correspond to the original message [17].

Security Advantages of Cloud Computing

Security automation: The homogeneity of a cloud environment facilitates automation in auditing/testing/security/data retention, which increases the speed of request, change, release, configuration, compliance, capacity, and patch management[18].

Centralization of data: Centralization of data facilitates "patch[ing], Upgrade [ing], monitor[ing] and encrypt[ing]" data. It also decreases the area needed to collocate or provide physical security because the perimeter is smaller[12].

Mirroring assists in data recovery. Replicated content or redundancy, as well as multiple storage sites, provides an excellent source for both disaster recovery and business continuity controls.

Data provisions by zone: Zones create partitions that block information spillage. These provisions also can prevent reverberations during a denial of service attack[13],[19].

Encryption: "Encryption of data at rest and in transit" protects confidentiality of a user's data.

Buying security in bulk. Every type of security measure, (i.e., filtering, authentication, access control measures, federated identity management) when implemented on a larger scale, is cheaper, in that "the same amount of investment buys better protection"[14],[20].

Audit and forensic investigation: With IaaS, customers can create live virtual images, and image components, in order to conduct investigations.

Ubiquity or infinite availability of data: Cloud Computing provides dynamic resource availability and portability, which could prove useful for military operations if properly secured[15],[21].

Security Challenges With Cloud Computing

There are many security challenges with cloud computing. Some of the recognized challenges or risks include:

External reliance for securing data: Reliance on an external provider for security (physical, logical, personnel and security controls) can add risk to the CIA of customer data. An alarming 22 out of 24 major federal agencies reported being "concerned or very concerned" about general security risks with cloud computing. This dependence on an external provider could result in lost data or an inability to transfer data, and requires the customer to monitor and examine security controls. In a survey conducted by the U.S. Government Accountability Office (GAO), major agencies reported concerns about "ineffective or non-compliant service provider security controls," lack of security control in delegation to third parties, and lack of comprehensive security investigations when hiring provider personnel. a customer should obtain information about access[16],[22].

Scarce federal security guidance/procurement strategy: Comprehensive security guidance in the federal government is yet to be available. Even though the Federal CIO created a cloud computing executive steering group, guidance is pending. Also, NIST is still working on specific cloud standards for security guidance. In a report released July 1, 2010, the U.S. GAO recommended that the Office of Management and Budget, the General Services Administration, and the Department of Commerce develop a strategy for integrating security into the procurement process for cloud computing services[11],[23].

Regulation compliance of cloud providers. Traditional IT service providers are subject to audits and accreditation, therefore cloud providers should not be exempt.

Identity management problems: Improper identity management could compromise authentication or authorization to access data[5],[24].

Confusion with responsibilities: There are often confusion over responsibilities regarding incident response, response to

an audit finding or forensic investigation. Agencies voiced challenges with defining responsibilities and roles of vendor verses customer in cloud computing implementations[6],[25].

General cloud security issues: Some of these challenges include: knowing the physical location of data and the provider's adherence to local privacy laws; the inability to access proprietary security implementations for testing; lack of accountability with system administrators; isolation management of data and permissions in a multi-tenant environment (e.g., use of encryption); ensuring a storage controller or hypervisor does not present a single point of failure; DRP and continuity of operations (what happens to data in case of disaster, and how long does data restoration take?); properly using SLAs to securely implement an external cloud provider's services (e.g., investigative support despite logging collocation); and long-term viability (CIA of data despite cloud company going out of business or transferring service to another provider)[17],[20],[26].

Elasticity challenges: The dynamic nature of elasticity (through use of virtualization) brings unique security challenges:

Traversal vulnerability: The traversal vulnerability allows an individual to traverse from one VM to another if managed by the same hypervisor. This vulnerability requires protective administrative separation between customers. This is a major challenge to providers since the premise of their financial gains rests on "shared administrative management systems (i.e., hypervisors) across multiple virtual customer environments". (Note: solution is stringent/granular access controls)[18],[27].

Encryption: The traversal vulnerability could easily negate any front end encryption for data-at-rest within a virtual milieu. (Note: solution could entail research into a provider's means for encryption in a shared environment)[19],[28].

Configuration/change management: A problem with elasticity is enforcing strict and proper configuration/change management at the enforcing strict and proper configuration/change management at the PaaS/IaaS level. (Note: solution is stringent/granular access controls, i.e., which actions are allowed, as well as when and under what conditions these actions are taken; mechanisms for enforcing change policies are also needed)[7],[29].

Integrity within zones: The challenge of protecting integrity within different zones of test, development and production environments.

Management control: Control of management authorizations of expanding services [20],[30].

4. DEPARTMENT OF DEFENSE

A vital DoD (Department of Defense) interest is to protect its information systems to ensure the confidentiality, integrity and availability (CIA) of critical data at home and abroad. In order to protect DoD information infrastructures within the context of cloud computing, the tactics and insight of network security profession-nals on both threats and corresponding countermeasures provide invaluable references necessary for deterring malicious attacks from U.S. adversaries. The USA Administration is encouraging a push for agencies to implement cloud computing when operational efficiencies and financial benefits are evident. This push is accompanied with a requirement for cyber security[21],[31]. On May 29, 2009, President Obama named cyber security as a top economic and national security priority as a result of his 60-day review that called for securing information systems used by the government and the U.S. economy.The analysis of threats and countermeasures in each of the ten domains of the CISSP CBK will provide lessons learned to ensure a secure implementation of cloud computing within the DOD.Problems and possibilities Secretary of Defense Robert Gates stated the U.S. is "under cyber-attack virtually all the time, every day." The DoD reported spending over $100 million from September 2008 to March 2009 on repairs to damage resulting from cyber-attacks. In 2008, the DoD removed 1,500 computers from the Pentagon's unclassified network due to a cyber-attack, and in the fall of 2008 banned external removable media devices to prevent the spread of viruses. Brigadier General John A. Davis, commander of the Joint Task Force for Global Network Operations, after a cyberspace conference in Omaha, Nebraska, stated that investments are necessary up front on computer countermeasures rather than later for repairs DoD information security is so diverse that military services and components are challenged to focus their efforts. Sims and Gerber in their book "Transforming U.S. Intelligence," recommend the following areas be addressed:

- Decreasing the inherent vulnerabilities within our hardware and software. Increasing the difficulty of an adversary introducing vulnerabilities into our systems through life-cycle approaches[22],[32].
- Increasing our ability to deeply evaluate critical components-design for evaluation; increasing the cost and uncertainty to an adversary attempting to exploit our vulnerabilities[23],[33].
- Increasing the probability of detecting a component (hardware or software) behaving badly (violating a security requirement)[18],[34].
- Increasing the probability of attributing bad behavior to an adversary.
- Increasing the consequences to the attacker for bad behavior. With the DoD's latest implementation of cloud computing in the 2010, 2011 years, security remains a major concern. The Cloud Security Alliance (CSA), in consultation with thirty commercial security experts, published a report on the top security threats with cloud computing. [24],[35].

These threats included:

- Nefarious personnel working for cloud computing providers.
- Malicious attackers targeting providers.
- Lack of security in interfaces or application programming interfaces (APIs).
- Vulnerabilities in shared technology.
- Data loss or leakage.
- Service hijacking [25],[36],[37].

In April 2010, CSA published results from a survey on cyber security stating that seventy percent of 198 respondents from across the military and government are "concerned about [the] data security, privacy and integrity" of cloud computing. Also, during the latest Cloud Computing Summit in

Washington, D.C., May 2010, the main lesson was "caveat emptor," which means "buyers beware" in Latin. One of the main problems with cloud computing is that a customer, such as the DoD, places trust in the protection of data (for privacy and security) with an outside commercial vendor. Since data is on the cloud, the IT management team of the cloud controls the security and privacy settings [25]. Moreover, providers often work with third party venders, and it is difficult to guarantee how all these interweaved parties safeguard data.Whatcurrently in the DOD is four known implementations of cloud computing with many more starting up, these four implementations include:

a-Army Experience Center (AEC)

A successor to the Army Recruiting Information Support System, the AEC cloud solution is in pilot mode as a public/community cloud providing SaaS, as of 2008. The AEC uses Salesforce.com as a customer relationship management tool to track recruits by integrating email, Twitter, and Face book for dynamic social interactions. Cloud computing increased the speed of response times from recruiters[26],[38].

b-Rapid Access Computing Environment (RACE):

DISA began using RACE, a private/community DOD cloud providing PaaS, in 2008. Starting in October 2009, RACE offered DOD users a "self-service provision operating environment within the highly secured Defense Enterprise Computing Center's production environment." Users can customize and purchase test and computing platforms quickly and cheaply[39].

c-Forge.mil: Forge.mil is a private/community DOD cloud providing SaaS, and specifically used by DISA to create, test and deploy software and other systems. Forge.mil saves resources through "economies of scale, ubiquitous delivery, and cross collaboration." DISA uses a cloud provider platform from CollabNet, which services 5,000 users across 300 projects; this solution gloats $200 to $500,000 in savings per project, and an additional $15 million in "cost avoidance by utilizing an open source philosophy" of collaborative development and software reuse. Since forge.mil is an open source solution mixed with cloud computing, other benefits include version control, traceability shortened time-to-market, and collaboration. This solution is utilized by the Army, Navy, Air Force, Marine Corps, and the Joint Chiefs of Staff[11],[40].

Personnel Services Delivery Transformation (PSDT):

The Air Force Personnel Center (AFPC) implemented a private/community DoDSaaS solution, provided by Right Now, to increase efficiencies in customer service, "knowledge management and case tracking." With this SaaS solution, AFPC efficiently completed a manpower reduction initiative, which saved $4 million annually while increasing customer service/engagement by 70 percent.[36]SpecificDOD cloud computing security challenges:Many of the above challenges will apply to the DOD, but some security challenges are slightly unique. The DoD might experience cyber-attacks as a result of wartime missions, such as a tactical cloud solution which becomes subject to attack during a mission. The DoD uses many different classification levels, under different authorities, which may present challenges with "sanitization/purging of local storage, data labeling, privilege-based access control…, [and] tailoring common operating pictures" to these different levels of access or privilege. Finally, certification and accreditation is challenging in a provisioned infrastructure. While the DoD may have a few unique challenges, many of these might be similar to what commercial organizations face in protecting their sensitive data for financial/proprietary verses wartime incentives[26].

5- THE FUTUREOF CLOUD COMPUTING

According to an article in cloud computing journal which is published in November -23- 2012, in this article a variety of members of the cloud computing ecosystem from CIOs to independent consultants to marketers were asked for their top five predictions , we summery these predictions in points:Cloud computing will allow everybody to be a service provider. The infrastructure to do things is no longer a limiting factor. Focus will shift to application and business services[5],[41]. A new class of real time, personalized service providers will emerge and they will develop partnerships to exploit the advantages of big data, social media and mobility[27],[42].In Africa, the convergence of social, mobile and cloud will emerge as critical tools for governments to deliver services and drive economic growth. VMware will break the LAN barrier through partnerships and in house innovations around networking and make significant headway in infrastructure[7],[43]. Surging volume of externally originating data (e.g., social nets) will drive more companies to cloud-based analytics. Accelerating tablet use will create vast numbers of multi-device users who will prefer cloud-based tools like Google Docs.File-based models of collaboration will give way to cloud-based, conversational models like Chatter where file location is irrelevant[10],[44].Continued scarcity of IT skills - despite still-high general unemployment - will discourage complex 'private cloud' schemes.Developer talent will focus on HTML5, and other skill sets that improve cloud experience and weaken legacy preferences.VMware acquires one of the Software Defined Network (SDN) start-ups, creating the final distinction between traditional Data Center and "Cloud" (Private or SP/Public provided). They now provide all the tools (virtualization, security, and network, automation) to allow CloudOps groups to be created within Enterprise or Service Provider.Running a real IaaS cloud at scale is hard and takes a lot more than downloading some open source software and installing it on x86 servers. Cloud security stops being a blocker to cloud adoption: Enterprise security teams will reach a détente with IT and business users on guidelines for allowing at least a subset of applications and data to run in the cloud. 2014 reviews of app portfolios and facts on the ground will yield some agreement about moving forward with external clouds in addition to private ones[45].More Private Cloud – After spending the last few years toe-dipping in public cloud for point projects, enterprise users will start to utilize private cloud for mission critical and data-sensitive applications. Heavy virtualization users will start augmenting high-availability virtual infrastructure by creating private clouds to reap the benefits of resource pooling, self-service

and elasticity on top of their existing virtual infrastructure. The Rise of the Cloud Management Tools - Now that IT operations has the ability to easily spawn 1000s of servers in a cloud environment it only will illustrate the need for tools that can handle the dynamics of increased scale and rapid elasticity[46]. Management tools that are cloud aware and lend themselves to automation become critical. Look to solutions from Opscode, PuppetLabs and enStratus for these needs.Cloud Hosted Desktops – What's good for the server may be good for the desktop. With the success of Google Docs, DropBox and other mobile productivity tools it sets the stage for greater virtual desktop adoption. Look for more virtual desktop infrastructure (VDI) solutions paired with data-as-a-service allowing users to take their desktop computing everywhere (think iPad) without requiring a wholesale migration to thin client computing.The consumer convinces the enterprise that cloud is cool. Things like iCloud and Amazon's Cloud Drive help get your average consumer comfortable with cloud. Consumer acceptance goes a long way to convincing the enterprise that this model is worth investigating – and deploying to. "There might be something to this cloud thing after all…." This, of course, accelerates the adoption of cloud and causes a bunch of changes in the role of IT. It's all about orchestrating services – and its business cards, mission statements, and org charts change accordingly[21],[31]. Enterprises start to think about "split processing" – where you are and in the cloud. Pressure from mobile devices and the "split browser" idea from things like Amazon Silk lead people to consider doing heavyweight processing in locations other than where the user is interacting. It's a great model for working with that myriad of mobile devices that have limited processing power (and battery life) that IT is working feverishly to figure out how to support. Somehow.Using Big Data in the cloud becomes as common as, well, data. Given the rise of NoSQL databases and the ecosystem around Hadoop and related approaches, companies begin to understand that collecting and using massive amounts of data isn't so hard any more. The cloud makes processing all this information possible without having to build the infrastructure permanently in your data center. And it's pretty useful in making smart business choices.The industry moves on from the "how is the infrastructure built and operated?" conversation and thinks instead about what you can do with cloud. This may sound like wishful thinking, but the nuts and bolts of how to use cloud computing are starting to coalesce sufficiently that fewer discussions need to pick apart the ways to deliver IaaS and the like.The small, smart service provider's move up the stack (leave the commodity stuff to Amazon and Rackspace), finding niches for themselves in delivering new service capabilities [47],[48]. Finally, enterprises can have a more useful conversation not about how do we make this work, but about how they our business can benefit? The question now becomes: what new business can come from the cloud model?Applications become disposable. Enterprises will start to leverage the on- demand nature of cloud computing and take a page from the user experience of tablet and smart phone apps. The result: thinking about applications and their deployment less monolithically[21]. The cloud will help enterprises make smarter decisions about how to handle their processing needs, and give them a way to do on-demand app distribution to both customers and employees. This will open up new options for access, even to older legacy applications. Enterprises will also start to evolve applications into smaller functional chunks - like iPad or iPhone apps.Pure play infrastructure providers (think colocation and IaaShosters) will move further up the stack with pre-packaged rapid Private Cloud deployment platforms and services. Big data's growing ease of deployment and management enables IT to actually mine and analyze the data to make real time apps and business decisions. Data integration platforms expand their capability to pull data from across environments - powering growth to companies that leverage their new data and analytics wealth.Mobile will drive an exponential number of data portability and synchronization projects - further moving data off devices to the cloud.The PC remains to primary and most important cloud client. Even as tablets, smart phones, thin clients, zero clients, iOS, Mac OS, Android, and desktop virtualization all gain, they at most represent 20 percent of enterprise clients used for mission critical activities. Therefore the PC is the most important client device for cloud computing for the foreseeable future. Supporting that PC, however, has never been more complex and costly, especially as it asked to support more of "all of the above." Big Data gives way to Right Data. The means by which to acquire, store, manage and analyze "Big Data" is in place or soon will be for most enterprises. Some may even look more to cloud services to augment their Big Data activities. The next step, however, is to decide the Right Data to analyze, acquire, access, manage, join, and/or buy. Making wise choices about what data from where and at what cost will be a important strategic chose for enterprises in 2012. Now it's time for the hard choices on what data is worth, and what are proper investments in data, especially as part of a greater whole and integrated data lifecycle approach.Big Data meets the IT information morass. If IT as a Service has future, real-time insights into IT equipment and software in total - across all types of deployments and cloud hybrids - is essential. The architectures and approaches used for Big Data and Complex Event Processing (CEP) will now be brought to bear on the IT operations and systems management problem[15],[33].

6-FUTURE DOD USES OF CLOUD COMPUTING

Some proposed projects in the DoD include using cloud computing internally (private cloud) for "large-scale planning, execution and reporting of program test and evaluation" workflow processes within the U.S. Army. Other uses could include logistical procurement, and intelligence collection and distribution ("storage/processing of tactical Intelligence, Surveillance,Reconnaissance (ISR) feeds"). Cloud computing could integrate with any solution for collaboration or interoperability of many users (i.e., ISR). It could be used for data center/system management, system auditing, monitoring/reporting, deployable operations overseas (e.g., for battle space awareness to track personnel, missions, equipment; "simulation and visualization" for "mission planning and training"), and "cyber network defense." Other uses of cloud services could include social networking, "data tagging, researching and indexing," and tactical environmental applications. Further creative uses

could be deciphered by using an Open Crowd Taxonomy diagram that outlines service offerings by different companies (note: researcher is not advocating use of any particular provider)[27],[49].

Dod Component Opsec Program Manager

The DoD Component OPSEC program manager responsible for:

- Developing, communicating, and ensuring implementation of standards, policies, and procedures that supplement this Manual and meet specific needs of the DoD Component.
- Identifying necessary resources for the effective implementation of Component OPSEC programs.
- Advising the Head of the DoD Component in determining the program levels required for subcomponents as outlined in section 3 of this enclosure and in identifying which subcomponents require additional full- or part-time program managers and coordinators.
- Conducting program reviews to evaluate and assess the effectiveness and efficiency of the OPSEC program. OPSEC programs should be reviewed at least annually.
- Identifying and protecting critical information related to the CIP with appropriate OPSEC measures and advising supporting contractors of information protection requirements[21],[50].

In fulfilling this responsibility, program managers shall:

- Work with CIP planners to identify and protect, through the use of OPSEC measures, critical information related to CIP plans and programs and to integrate CIP into OPSEC assessments and surveys as needed.
- Assist CIP planners in promoting information sharing while safeguarding information that could harm DoD operations or that could jeopardize information-sharing agreements among stakeholders.
- The DoD Component OPSEC program manager shall participate in training and education reviews and shall work with the USD (I) and the IOSS in identifying DoD OPSEC requirements.

Opsec Process

The OPSEC process is a systematic method used to identify, control, and protect critical information. This appendix presents the five elements of the OPSEC process as steps. These steps may or may not be used in sequential order but all elements must be present to conduct OPSEC analysis.

Steps in the OPSE process:

- Identify Critical Information.
- Conduct a Threat Analysis.
- Conduct a Vulnerability Analysis.
- Apply OPSEC Countermeasures.

OPSEC Surveys

Surveys involve analyzing the activities associated with specific operations or programs to determine if there is adequate protection of critical information from adversary intelligence exploitation during the planning, preparation, execution, and post-execution phases of an operation or program. the depth and breadth of a survey depends on the degree of threat, the importance of the mission, and the harm that an adversary could inflict[30],[51].

Procedures

(1) The Heads of DoD Components may supplement this Manual and stipulate more detailed procedures for conducting OPSEC surveys [28].

a)An OPSEC survey shall be conducted every 3 years or when required by the commander or director. A survey seeks to reproduce the intelligence image in light of the known collection capabilities of potential adversaries which activities in their command require surveys and develop implementing guidance for conducting them.

b)The survey shall require that a team of experts look at an activity from an adversarial perspective to determine if critical information may be disclosed through normal operations and functions, to identify vulnerabilities, and to propose countermeasures to mitigate them[29],[52].

c)At the commander or director's discretion, the survey may focus on human intelligence (HUMINT), signals intelligence (SIGINT), measurement and signature intelligence (MASINT), open-source intelligence (OSINT), and/or geospatial intelligence(GEOINT) collection capabilities. These may include telecommunications monitoring, radio frequency monitoring, network and computer systems assessment, and open-source collection. Survey team members shall use collection techniques of known adversaries. Commanders and directors are encouraged to use existing OPSEC support capabilities to conduct surveys, if available[27],[53].

(2) DoD Component guidance for conducting OPSEC surveys shall include:

a)Procedures for scheduling surveys through OPSEC support capabilities or designated DOD activities capable of providing OPSEC support.

b)Procedures for a planning, preparation, execution, and post-execution phase.

c)Clearly defined rules of engagement for collection activities.

d)Required use of the analysis ratings criteria in the appendix to this enclosure who analyzing information[31],[54].

7-CONCLUSIONS

Depending on how you adopt the cloud model or how you deliver cloud based services, cloud computing will bring fundamental change. Adopting cloud computing as a model for IT allows organizations to transition away from more traditional device-centric models and toward information and services based ones.Cloud offers many benefits that go beyond leaner and more agile IT infrastructure. The cloud model allows greater scalability and the change from a capital-heavy model of IT spending toward an operating model that is subscription-based brings new opportunities for a broader set of users and tenants to place larger bets with lower risk. But there are clear trade-offs that involve control over data and applications, compliance with laws and regulations and even with security. The bottom line with cloud security is that when a cloud is implemented with appropriate security, and then there is no reason why cloud

security can't be equal to or exceed traditional IT implementations.The ten domains provide a credentialed standard of security to protect the CIA of cloud computing.The access control domain addressed countermeasures for frictionless registration, account hijacking, and authentication attacks such as strong or multi-factor authentication. Recommendations were provided for overarching identity and access management issues, specifically involving identity provisioning, authentication, federation, and authorization and user profile management. Lastly, generic countermeasures were discussed, such as integration of access control with the DoD common access card, SAML, WS-federation, and proactive auditing and monitoring.The telecommunication and network security domain addressed the relevant issues and countermeasures to cloud hacking and to DoS and VM attacks. Boundary protection is paramount both within and outside of the cloud, and the provider must ensure that provisions protect the CIA of a customer's data. Some of these measures include internal/external layered security controls such as IDS & IPS, as well as compartmentalization of virtual instances in order to protect dispersive system components.The security architecture and design domain dissected several important areas: establishing isolation management within shared technologies; designing architectures for meeting customer demands for service and availability; and certifying and accrediting systems before use, while leveraging federal solutions.The application security domain addressed exploitation and countermeasures to protect insecure interfaces. It provided methods on increasing security for PaaS, SaaS, and IaaS in the realm ofmessage communication, information handling, key management, SDLC, tools and services, metrics, economics, and inter-host communication.The cryptographic domain highlighted that traditional encryption processes can transfer to the cloud, while encouraging encryption in transit, at rest and for backup purpose; and noted the potential use of homomorphic encryption techniques to secure confidentiality in the future.
The security architecture and design domain discussed establishing isolation management within shared technologies; designing architectures for meeting service and availability demands; and certifying and accrediting systems and leveraging federal solutions.The OPSEC domain highlighted the importance of patching; logging, monitoring and audit; and personnel practices to protect against the malicious insider.The BCP and DRP domain addressed the importance of ensuring the availability of data that is needed for mission-related functions. BCPs and DRPs must be validated and exercised by the DoD and any third party provider.The legal regulation, compliance and investigation domain specifically addressed SLAs, blurred responsibilities between providers and customers, the need for incident handling processes, compliance with legal regulations, intellectual property and privacy, cloud employee monitoring and surveillance, and the need for cloud experts. It highlighted the significance of IT and legal personnel working together in formulation of the SLA or contract.The physical and environmental security domain identified threats and countermeasures in several areas: data location, audit transparency, facility/server room security, server isolation, data deletion, tempest and proper separation. Through use of the ten domains, the DoD can better mitigate threats that are inherent in this new cutting edge technology. By taking precautions with the new technology of cloud computing, the DoD can reap benefits in efficiency while ensuring the CIA of their data remains intact.

REFERENCES

1. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather and SubraKumaraswamy.
2. KSA Cloud First Policy, Ministry of Communications and Information Technology (MCIT),2019.https://www.mcit.gov.sa/sites/default/files/ksa_cloud_first_policy_en.pdf
3. Cloud First Policy Strategy and Guidelines – to establish the United Arab Emirates as Regional Data Hub, Public Consultation Document, Telecommunication Regulatory Authority (TRA), 2018.https://www.tra.gov.ae/userfiles/assets/QqQuIA0SR5C.pdf
4. Bahrain's Cloud First Policy, Information &GovernmentAuthority (iGA), 2017.http://www.nea.gov.bh/Attachments/iGA_Cloud-First_Policy_V1.0.pdf
5. Knies, Rob. "**Peering into Future of Cloud Computing**." Microsoft Research, February 24, 2009,at:http://research.microsoft.com/enus/news/features/ccf-022409.aspx (accessed October 23, 2010).
6. Krebs, Brian. "**Obama: Cyber security is a National Security Priority**." The Washington Post, May 29, 2009,at:http://voices.washingtonpost.com/securityfix/2009/05/obama_cybersecurity_is_a_ natio.html (accessed Jun 13, 2010).
7. Kubic, Chris. "**DoD Cloud Computing Security Challenges.**" Briefing by Chief Architect, Information Assurance Architecture and Systems Security Engineering Group, National Security Agency,at:http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008 12/cloudcomputing-IA-challenges_ISPAB-Dec2008_C-Kubic.pdf (November 6, 2010).
8. Kumar, Karthik, and Yung-Hsiang Lu. "**Cloud Computing for Mobile Users: Can Offloading Computation Save Energy**?" Computer, Vol. 44, No. 4 (April 2010).
9. Kundra, Vivek. "**Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft Version 0.96**." CIO Council, November2,2010,athttps://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf (accessed November 24, 2010).
10. "**Public Sector Cloud Computing Case Study: Army Experience Center**," CIO.gov, June 8, 2010, at:http://cio.gov/pages.cfm/page/Public-Sector-Cloud- Computing-Case-Study-Army-Experience-Center (accessed October 27, 2010).

11. "**State of Public Sector Cloud Computing.**" CIO.gov,May20,2010,at:http://www.cio.gov/pages.cfm/page/STate-of-Public-Sector-Cloud-Computing (accessed November 24, 2010).
12. Lentz, Robert F. "Statement before the U.S. House of Representatives Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities," May 5, 2009, at: http://armedservices.house.gov/pdfs/TUTC050509/Lentz_Testimony050509.pdf (accessed November 24, 2010).
13. Linthicum, David. "**Three Cloud Computing Mistakes You Can Avoid Today."**MISAsia, March 12,2010,at:http://misasia.com/cio_focus/technology/3-cloud-computingmistakes-you-can-avoid-today (accessed September 10, 2010).
14. "**Google removes cloud security barrier for the government.**" InfoWorld, July 28, 2010, at: http://www.infoworld.com/d/cloud-computing/google-removes-cloudsecurity-barrier-the-government-889 (accessed September 10, 2010).
15. Mell, Peter and Tim Grance, "**Effectively and Securely Using the Cloud Computing Paradigm**." National Institute for Standards and Technology, IT Laboratory,October7,2009,at:http://csrc.nist.gov/groups/SNS/cloud-computing/ (accessed September 10, 2010).
16. Messmer, Ellen. "**US military takes cloud computing to Afghanistan.**" Network World, September23,2010,at:http://www.networkworld.com/news/2010/092310-cloudcomputing-afghanistan.html?page=1 (accessed October1, 2010).
17. Michael, Bret, and George Dinolt. "Establishing Trust in Cloud Computing." Information Assurance (IA) Newsletter. Vol. 13, No. 2 (Spring 2010).
18. "**In Clouds Shall We Trust?"***IEEE*, Vol. 7, Issue 5 (Sept - Oct 2009). Microsoft, "Snapshot Full Strategic Report," at: http://download.101com.com/GIG/Custom/Microsoft/SnapCloudFinal.pdf (accessed September 1, 2010).
19. Mills, Elinor. "Pentagon Spends Over $100 million on Cyberattack Cleanup." CNET News, April 7, 2009, at: http://news.cnet.com/8301-1009_3-10214416-83.html (accessed May 17 , 2010).
20. "Twitter, Facebook Attack Targeted One User." Cnet News, August 6, 2009, at: http://news.cnet.com/8301-27080_3-10305200-245.html (accessed September 10, 2010).
21. National Institute for Standards and Technology Website, Computer Security Division: Computer Security Resource Center, May 11, 2009, at: http://csrc.nist.gov/groups/SNS/cloud-computing/ (accessed September 10, 2010).
22. Naxal Watch, "**U.S.: DoD Advances Cloud Computing Usage.**" Intellibriefs, January 12, 2010, at: http://intellibriefs.blogspot.com/2010/01/us-dod-advances-cloudcomputing-usage.html(accessed October 1, 2010).
23. Newton, Ben. "**Building Private and Community Clouds for the DoD**." Defense Systems, September 23,2010,at:http://defensesystems.com/Articles/2010/09/02/Industry-Perspective-Automating-the-Cloud.aspx?Page=2 (accessed October 1, 2010). Owens, Dustin. "**Securing Elasticity in the Cloud**." Association for Computing.
24. Machinery,May.6,2010,at:http://queue.acm.org/detail.cfm?id=1794516 (accessed September 10, 2010).
25. Paquette, Scott, and Paul T. Jaeger, and Susan C. Wilson. "**Identifying the security risks associated with governmental use of cloud computing**." Government Information Quarterly, Vol. 27, Issue 3 (July 2010).
26. Wilshusen, Gregory C. U.S. Government Accountability Office Report GAO-10-855T: Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing. July 1, 2010, at: http://www.gao.gov/new.items/d10513.pdf (accessed October 7, 2010).
27. Prince, Brian. "**IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering.**" E-Week.com, June 25, 2009, at: http://www.eweek.com/c/a/Security/IBM-Uncovers-Encryption-Scheme-That-Could-Improve-Cloud-Security-Spam-Filtering-135413/ (accessed November 24, 2010).
28. Hord. "(ISC)2 Website**." Information Systems Security Certification Consortium**", at: http://www.isc2.org/aboutus/default.aspx (accessed May 27, 2010).
29. Paul, Frederick. "Cloud Computing's Dirty Little Secret." Enterprise Efficiency, August 30, 2010, at: http://www.enterpriseefficiency.com/author.asp?section_id=898&doc_id=196259 (accessed October 2, 2010).
30. U.S. Computer Emergency Response Team, National Vulnerability Database. "*Vulnerability Summary for CVE-2009-3733,*" November 2, 2009, at: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3733 (accessed September 10, 2011).
31. Pelgrin, William F. "**Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter**." April 2010, at: http://www.msisac.org/awareness/news/2010-04.cfm (accessed July 26, 2010).
32. Perry, Christopher. "**Security for Cloud Computing**." Department of the Navy Chief Information Officer Website, May 18, 2010, at: http://www.doncio.navy.mil/ContentView.aspx?ID=1744 (accessed August 27, 2010).
33. Pettey, Christy, and Ben Tudor. "**Gartner Says Worldwide Cloud Services Market to Surpass $68B in 2010.**" Gartner Newsroom, June 22, 2010, at: http://www.gartner.com/it/page.jsp?id=1389313 (accessed October 23, 2010).

34. Pokharel, Manish, and Jong Sou Park. "**Cloud Computing: Future solution for e- Governance**." ACM International Conference Proceeding Series, Vol. 322, (New York: ACM, 2010).
35. Sims, Jennifer E., and Burton Gerber. *Transforming U.S. Intelligence.* Washington, D.C.: Georgetown University Press, 2005.
36. Sutter, John D. "**Twitter hack raises questions about 'cloud computing**.' *CNN.com*, July 16, 2009, at: http://www.cnn.com/2009/TECH/07/16/twitter.hack /index.html (accessed July 13, 2010).
37. Tipton, Harold F. Official (ISC)2 Guide to the CISSP *CBK*. Boca Raton: Taylor and Francis Group, LLC, 2011.
38. Traynor, Ben. "**More on Today's Gmail Issue."** The Official Gmail Blog. 9 September 2009, at: http://gmailblog.blogspot.com/2009/09/more-on-tod ays-gmailissue. html (accessed June 13, 2010).
39. Wald, Heather. "**Cloud Computing for the Federal Community."** Information Assurance Newsletter. Vol. 13, No. 2 (Spring 2010).
40. Yasin, Rutrel. "House panel questions cloud computing assumptions." Government Computer News, July 1, 2011, at:http://gcn.com/articles/2010/07/01/congressheari ngs on-cloud-computing.aspx (accessed September 10, 2010).
41. Zetter, Kim. "**Vulnerabilities Allow Attacker to Impersonate Any Website**." *Wired.com*, July 29, 2009,at.http://www.wired.com/threatlevel/2009/07/ kaminsky/ (accessed July 23, 2011).
42. Machinery,May6,2010,at:http://queue.acm.org/detai l.cfm?id=1794516 (accessed September 10, 2010).
43. Paquette, Scott, and Paul T. Jaeger, and Susan C. Wilson. "**Identifying the security risks associated with governmental use of cloud computing**." Government Information Quarterly, Vol. 27, Issue 3 (July 2010).
44. Paul, Frederick. "**Cloud Computing's Dirty Little Secret**." Enterprise Efficiency, August 30, 2010, at: http://www.enterpriseefficiency.com/author.asp?sec tion_id=898&doc_id=196259 (accessed October 2, 2010).
45. Pelgrin, William F. "**Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter**." April 2010, at: http://www.msisac.org/awareness/news/2010-04.cf m (accessed July 26, 2010).
46. Perry, Christopher. "**Security for Cloud Computin**g." Department of the Navy Chief Information Officer Website, May 18, 2010, at: http://www.doncio.navy.mil/ContentView.aspx?ID =1744 (accessed August 27, 2010).
47. Pettey, Christy, and Ben Tudor. "**Gartner Says Worldwide Cloud Services Market to Surpass $68B in 2010**." Gartner Newsroom, June 22, 2010, at: http://www.gartner.com/it/page.jsp?id=1389313 (accessed October 23, 2010).
48. Pokharel, Manish, and Jong Sou Park. "**Cloud Computing: Future solution for e- Governance**." ACM International Conference Proceeding Series, Vol. 322, (New York: ACM, 2010).
49. Prince, Brian. "IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering." E-Week.com, June 25, 2009, at: http://www.eweek.com/c/a/Security/IBM-Uncovers -Encryption-Scheme-That-Could-Improve-Cloud-Security-Spam-Filtering-135 413/ (accessed November 24, 2010).
50. Ramienski, Dorothy. "DoD IT experts open up about cloud deployment." Federal Executive Forum,November10,2009,at:http://www.federalnew sradio.com/index.php?nid=35&sid=1808816 (accessed August 11, 2011).
51. Rigby, Bill. "**An Interactive eBook: Cloud Computing.**" Computer World, July 15, 2010, at: http://www.networkworld.com/whitepapers/nww/pd f/eGuide_cloud_5brand_final .pdf (accessed July 15, 2010).
52. Sims, Jennifer E., and Burton Gerber. Transforming U.S. Intelligence. Washington, D.C.: Georgetown University Press, 2005.
53. Sutter, John D. "**Twitter hack raises questions about cloud computing**" CNN.com, July 16, 2009, at:http://www.cnn.com/2009/TECH/07/16/twitter.ha ck/index.html (accessed July 13, 2010).
54. Tipton, Harold F. Official (ISC)2 Guide to the CISSP CBK. Boca Raton: Taylor and Francis Group, LLC, 2011.