Cloud Service Security & Application Vulnerability

Acklyn Murray, Geremew Begna, Ebelechukwu Nwafor, Jeremy Blackstone, Wayne Patterson
Department of Systems and Computer Science
Howard University
Washington, DC, USA
wpatterson@howard.edu

***Abstract*— Cloud computing is one of today's most appealing technology areas due to its cost-efficiency and flexibility. However, despite significant interests, deploying cloud computing in an enterprise infrastructure offers significant security concerns. Successful implementation of cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats, vulnerabilities, and possible countermeasures. This paper discusses security concerns of the three cloud computing models namely "Software as a Service" (SaaS), Platform as a Service" (PaaS) and "Infrastructure as a Service" (IaaS). It also discusses Cloud-based Security Tools currently available today. Under the U.S. Federal Security Requirements for Cloud Security. The paper demonstrated the Federal Information Security Management Act (FISMA) and the Federal Risk and Authorization Management Program (FedRAMP). The paper also discusses Cloud Data Encryption, Homomorphic Encryption and Access Control (Identity Access Management). Finally, this paper talks about cloud applications focusing on select cloud applications. It also looks at some of the known vulnerability issues associated with the applications and also the future of cloud applications.**

Keywords— cloud computing, IaaS; SaaS, PaaS; cybersecurity Application Vulnerability, cryptography; access control, FISMA, Data Encryption

I. INTRODUCTION : CLOUD MODELS

Cloud computing is defined as " a collection of IT resources (servers, databases, and applications) which are available on an on-demand basis, provided by a service company, available through the internet, and provide resource pooling among multiple users." [1].

According to National Institute of Standards and Technology (NIST) one of the most accepted definition of cloud computing is " a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The cloud model is composed of five essential characteristics, three service models, and four deployment models [5]. The five essential characteristics of cloud models are:

On-demand self-service- a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider,

Broad network access.-Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). *Resource pooling*- the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth. *Rapid elasticity*-capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. *Measured service*-cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

There are three models of Cloud services commonly known as SPI, an acronym for the most common cloud computing service models, Software as a Service, Platform as a Service and Infrastructure as a Service. Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. Platform as a Service (PaaS) is a paradigm for delivering operating systems and associated services over the Internet without downloads or installation. Infrastructure as a Service (IaaS) involves outsourcing the equipment used to support operations, including storage, hardware, servers and networking components. Example Amazon's Elastic Compute Cloud (EC2) [5]

There are four cloud deployment models. These are Private cloud, in which cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units), Community cloud, in which the infrastructure is provisioned for exclusive use by a specific

978-1-4673-7300-5/15/$31.00 ©2015 IEEE

community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations), Public cloud, in which the cloud infrastructure is provisioned for open use by the general public , and Hybrid cloud, which is a composition of two or more distinct cloud infrastructures (private, community, or public). Despite significant interests, deploying cloud computing in an enterprise infrastructure brings significant security concerns [5]

II. Cloud Services & Vendors

Security Concerns of Cloud Computing

1. Services

Security remains a major concern for moving data to the cloud. Although data encryption provides protection, decisions need to be made regarding when, where, and how to encrypt data heading to cloud [4].

2. Model Security

To understand more about security concerns, we discussed security concerns of the three cloud computing models describing the common security issues that are posed by the cloud service delivery models. Namely, ‘‘Software as a Service’’ (SaaS), Platform as a Service’’ (PaaS) and ‘‘Infrastructure as a Service’’ (IaaS).

2.1. Security Issues in SaaS

In SaaS, the client has to depend on the provider for proper security measures. The provider must do the work to keep multiple users’ from seeing each other’s data. So it becomes difficult to the user to ensure that right security measures are in place and also difficult to get assurance that the application will be available when needed.

According to [2], the following key security elements should be carefully considered as an integral part of the SaaS application development and deployment process:

Data security- in the SaaS model, the enterprise data is stored outside the enterprise boundary. Network security-in a SaaS deployment model, sensitive data is obtained from the enterprises processed by the SaaS application and stored at the SaaS vendor end.

Data locality-in a SaaS model of a cloud environment, the consumer’ does not know where the data is getting stored.

Data integrity-Data integrity is one of the most critical elements in any system

Data segregation -Multi-tenancy is one of the major characteristics of cloud computing. In such a situation, data of various users will reside at the same location.

Data access -Data access issue is mainly related to security policies provided to the users while accessing the data.

Authentication and authorization- the software is hosted outside of the corporate firewall.

Data confidentiality issue- Cloud computing involves the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the internet or other connections.

Web application security- Data breaches, Vulnerability, Availability, Backup and Identity management and sign-on process- Identity management (IdM) or ID management are other concerns of SaaS.

2.2. Security issues in PaaS

In PaaS, the provider may offer functional control to the client to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider and the provider has to offer strong assurances that the data remains inaccessible between applications. PaaS is intended to enable developers to build their own applications on top of the platform. As a result it tends to be more extensible than SaaS, at the expense of customer-ready features. This tradeoff extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security [2].

2.3. Security issues in IaaS

IaaS is prone to various degrees of security issues based on the cloud deployment model through which it is being delivered. Public cloud poses the major risk where as private cloud seems to have lesser impact. Physical security of infrastructure and disaster management is of utmost importance if any damage is incurred to the infrastructure (either naturally or intentionally). Infrastructure not only pertains to the hardware, where data is processed and stored, but also the path where it is getting transmitted. In a typical cloud environment, data will be transmitted from source to destination through numerous number of third-party infrastructure devices [11].

3. Cloud-based Security Tools

Protecting your network is becoming more important than ever. Despite what the size of your network is, hackers want access to it. Now, with modern technologies like software-as-a-service, or security-as-a-service it’s easier than ever to implement security strategies for your company. According to [14, 15], here are some of the top security products that are available today:

SilverSky is a cloud-based security provider. It offers email, monitoring and protection, network protection, and helps your company become HIPPA (Health Insurance Portability and Accountability Act) and PCI (*Payment Card Industry*) compliant.

Vaultive encrypts any data leaving the network using AES Encryption system. It sits between your network and the Internet without needing any on premise hardware. The company helps people protect cloud-based services like Office 365 and Exchange.

DocTrackr is a security layer that works with file-sharing services such as Box and Microsoft SharePoint. Once you send a document out of your system, you typically have no control of it anymore. DocTrackr however, reinstates your control and lets you set user privileges for each person you share a document with. It also tracks the views on your document, and allows you to “unshare” the document if you

want.

Proofpoint focuses on the security of email with cloud-only services. It protects any incoming and outgoing data. While Proofpoint admits to storing your data, it promises that it does so only for the purpose of protecting against data loss, and that they do not have the keys to decrypt any of the information.

Centrify focuses on identity-management across many different devices and applications. It puts all of your employees and/or customers into one centrally controlled, secure, and monitored area. Centrify will protect your network through on premise software, or cloud applications.

There are also other security tools which are available today such as Qualys secures your devices and web apps, White Hat Security focus on protecting website from the ground up, including in the coding process; Okta_focuses purely on identity management knowing who is where and why.

4. U.S. Federal Security Requirements for Cloud Security

NIST marks top security requirements for U.S. Government Cloud Computing Technology to ensure that cloud service providers meet a baseline set of federal security requirements. The Cloud system has to meet not only U.S. government security needs, but also those of other customers sharing the environment.

4.1. FISMA

The Federal Information Security Management Act (FISMA) requires U.S. government agencies to implement and document programs to protect the confidentiality, integrity, and availability of IT systems. All U.S. Agencies must budget allocated funding to be in compliance. As the controlling Federal Law, enacted in 2002 as the E-Government Act, 116 Statue 2899 under 44 U.S.C. §3541[12] the scope and purpose of initiative is described as the National Institute of Standards and Technology (NIST) interpretation of "important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation" [5]

The requested trusted service models under the Act, invoke Saas, PaaS and IaaS with provisions. Deployment models may vary based on independent Agency requirements. Such "Deviations" are limited in coordination with independent agency stipulations.

4.2. FedRAMP

The Federal Risk and Authorization Management Program, or FedRAMP, has been a unified, Federal government program focused on vendor and multiple agency systems. FedRAMP has been established to provide a standard approach to cloud computing by Assessing and Authorizing particular vetted services and products. FedRAMP allows joint authorizations and continuous monitoring services for Government and Commercial cloud systems intended for multiple agency use. FedRAMP was structured to reduce duplication efforts, inconsistencies, and cost inefficiencies associated with the current modern noted security processes.

The Federal Risk and Authorization Management Program (FedRAMP) supports the U.S. government's objective to enable U.S. federal agencies to use managed service providers that enable cloud computing capabilities.

FedRAMP allows U.S. federal agencies to make use of CPs platforms and offerings. The FedRAMP program provides an avenue for CPs to obtain a provisional authorization after undergoing a third-party independent security assessment. By assessing security controls on candidate platforms and providing provisional authorizations on platforms that have acceptable FedRAMP Governance. FedRAMP is governed by a Joint Authorization Board (JAB) that consists of representatives from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD). FedRAMP provides a standardized approach to security assessments and ongoing assessments and authorizations (continuous monitoring) designed to save cost, time, and staff required to assess and authorize cloud services.

5. Cloud Security Vendors

The following Cloud Security Vendors that have Federal ties under the FedRAMP program. FedRAMP mandates secure transference to Cloud technologies in an allotted schedule. FedRAMP certifies both commercial and government cloud service providers.

5.1 Encase

A current vendor with much promise comes from the realm of digital forensics. EnCase is the shared technology, within a suite of digital investigations products, by Guidance Software. Software is packaged separately for forensic, cyber security, security analytics, and e-discovery use. The focus would be on cyber security, specifically under the function of cloud security, which is validated for Federal integration under the NIST Cybersecurity Framework for cybersecurity risk mitigation.

As an immediate rapid response countermeasure, EnCase Cybersecurity products collaborate with other vendors' software to ascertain threats and secure data under the SIEM platform, (Secure Information and Event Management). When leveraging these integrations, EnCase Cybersecurity provides security operation centers the validation and details required from affected hosts in close to real time to completely understand the nature and scope of any incident with a valid remediation. Known partner vendors manufacturers are HP ArcSight, IBM Q1 Labs, FireEye, SourceFire and others [20].

5.2 Splunk

Splunk is software tailored to capture then indexes with noted correlations, data in a searchable repository for post incident event alerts and reports. The products featured apply to application management, security and compliance by identifying data patterns, providing metrics, diagnosis of

problems and provides predictive intelligence specifically for cloud security.

Splunk offers both Splunk Storm and Hunk: Splunk Analytics for Hadoop, which supports accessing, searching, and reporting on external data sets located specifically in Splunk ' s proprietary Cloud product or Hadoop from a Splunk interface. Splunk is currently under review for full Federal Agency use [21].

III. SECURITY VULNERABILITIES

B. Cloud Applications & Vulnerabilities

1. Netflix

Netflix is an online video streaming application that allows for ubiquitous access of video content. Users have the option of choosing a wide array of videos which can be paused or resumed on any client device. Netflix is entirely run on public cloud. It is run on Amazon Web Services. In August 2008, Netflix experienced database corruption. This served as a motivation for migrating to the cloud. Netflix is regarded as one of the largest cloud service.

Netflix moved all of its corporate IT applications to SaaS cloud applications such as Evernote, OneLogin, Workday, and Box. They also built their own Platform as a Service cloud tools that help test the efficiency of the cloud service which makes developers more productive. In September 2006, as part of its effort to improve consumer movie recommendations, Netflix organized a competition in which it allowed contestants to develop a movie recommendation algorithm that better improves Netflix current movie recommendation by 10%. Anonymized data of about 480,000 consumers3. 3. containing movie ratings were released. This data was believed to be anonymized but according to two researchers at University of Texas, information from the dataset can be used to reveal information about the consumers. A law-suit was filed against Netflix based on releasing dataset of its consumer rating recommendations. It was discovered that attackers tried to exploit Netflix based on a vulnerability found in Silverlight [55], a plug-in similar to adobe flash developed by Microsoft. These cybercriminals use fake website advertisement to install malicious software on the host systems. Once a user clicks on the ad, it is redirected to the website containing malicious contents. This site infects the browser with malicious content.

2. LinkedIn

LinkedIn is a social networking site in which users connect with people whom they know and trust professionally [48]. Each user creates a profile page with their employment history and education and is able to form connections with other users who they have worked with, know professionally or have gone to school with. In 2012, LinkedIn faced a $5 million class-action lawsuit after a hacker posted over 6.5 million of its hashed passwords on a password cracking forum [49]. The lawsuit was filed because of an appalling lack of security measures which was revealed by reports of the site being infiltrated by a SQL injection attack. In response to this attack the company had the passwords of all accounts that were affected by the attack rendered invalid [50]. Next, they emailed the user of these accounts with instructions on how to reset their passwords as well as a debriefing of the situation.

LinkedIn's current security measures now include Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), email verification, and two-step verification [51]. CAPTCHA is used to keep users accounts safe from unauthorized access by making sure that a person and not a computer is accessing the account. CAPTCHA operates by creating an image containing random, slightly distorted numbers and letters that computers are not able to read but humans are able to read. Proper completion of the test verifies that a human user is attempting to access the account. Through email verification, LinkedIn monitors anomalous activity such as signing in from a country not associated with the user's profile and sends a verification email to the email address associated with the account to make sure that it is the real user performing the activity. Finally, two-step verification is a security method in which more than one form of verification is required in order to gain access to an account. This usually consists of requiring a password for the account and sending an SMS of a numeric code any time there is a sign in from an unfamiliar device. By requiring both something you know and "something you know" and "something you have", this process provides an extra layer to keep the account secure if the user's password is compromised due to using the same password for multiple sites, downloading software from the internet or clicking on links with malicious content in email an messages[52].

3. iCloud

iCloud is a cloud storage application developed by Apple Inc. It allows apple client systems (iphone, ipad, ipod etc.) to store and retrieve information on the cloud. It was launched in October, 12, 2011. It allows users to seamlessly access information on any client system by using their apple id. iCloud contains an auto sync feature whereby once a user saves information on the cloud, the content is automatically synced on all of their devices connected to the cloud system. For data to be saved on the cloud, application places the data in a location called cloud container. This serves as the local representation of the data on the client system. iCloud is a private cloud managed solely by Apple Inc.

According to Forbes.com, a group known as Hackappcom posted a proof of concept script information on how to effectively guess username and password information using the find my app API. This API allows for unlimited amounts of username and password queries. The script was made public at a talk given by Andrey Balenko and Alexy Troshichev titled iCloud Keychain and IOS 7 Data protection at the Russian DEFCON group. It is also believed that iCloud was the medium of attack for the cyber-attack in which hundreds of personal celebrity photos were leaked. Due to the data breach, iCloud now uses 2-factor authentication whereby its users are required to enter a password and another security

feature such as SMS verification to further authenticate their identity.

4. Dropbox

Dropbox is a cloud based storage application that allows seamless synchronization of files on multiple clients. It was developed in 2007[26]. It offers a secure way of storing information using 256-bit AES data encryption. The client application is available for Microsoft windows, Apple OS X and Linux operating system platforms. When a user makes a request to upload or download a file, files that are larger than 4MB are split into different chunks when sent from the client system to the server. Each chunk is identified by a SHA-256 hash value which is contained in the meta-data description of the file. Dropbox uses three major servers: The control and the data storage servers. The control server is managed directly by Dropbox Inc. This server is responsible for the exchange of authentication and metadata information while the storage server which is responsible for file upload/download is an Amazon Elastic Compute Cloud (EC2) and Simple Storage Service (S3). Dropbox architecture also contains a notification server which keeps a constant TCP connection with the client and notifies it of any change to the file performed at another client. Metadata information is stored in a database which runs on MySQL. All servers except the notification server use HTTPS to establish connections with the client. The application reduces the amount of information sent by using delta encoding while the data chunks are being transmitted. Each data chunk is compressed before it is sent to the data storage server. The client application also keeps a local database which contains meta-data information of files sent. Dropbox application offers users the ability to control the maximum upload and download speed. File synchronization starts with message exchange through the meta-data servers. This is succeeded by a send or retrieve operation which is sent to the data-storage servers. Once data has been successfully exchanged, the client system sends messages to the meta-data server to terminate the connection [26].

In 2011, Dropbox system was compromised. About a hundred usernames and passwords of Dropbox consumers were stolen. According to Dropbox, this was due to a compromised administrator account which contained email address of several users. Dropbox has since also required users to use two-factor authentication which ensures a more stringent data security. Also, in 2011, it was confirmed by Dropbox that a programming flaw was detected which allowed access to an account without requiring a password. Access was possible between 1:54PM PT and 5:46 PM. This was detected and immediately updated.

IV. Noted Vulnerability Examples

1.1 Google-Docs

Google Docs is a cloud based application that allows the use of a web processor over the internet. Documents are created, formatted and saved on Google's cloud server which is accessed through the internet [31]. Documents created on Google Cloud can be exported in various formats (ODF, HTML, PDF, RTF, Text, and Open Office XML). It allows multiple users to work on the same document concurrently. Each user can see changes made character by character. It is available as a web application, on chrome browser extensions as a chrome app and also on mobile applications (iPhone, android). Google Docs is a typical example of Software as a Service office suite which allows for the creation, modification, editing, and deletion of documents, spreadsheets and presentations. Documents created can be saved locally and are automatically saved on Googles servers.
Some of the previously known vulnerabilities that existed in Google Docs are as follows:
In 2009, a previously authorized party of a Google Doc could still maintain access to a document even when access has been revoked by the owner of the document. Images embedded in Google Doc are identified with an ID which is accessible by a URL [53]. Google Doc did not provide protection to images embedded in a document (e.g. a user might restrict access to a given document but the images contained in the document can still be visible to unauthorized parties).

1.2 DocuSign

DocuSign is an application that allows users to send and sign legally binding documents electronically [33]. To begin the process, the sender uploads a document to DocuSign, adds the names and email addresses of signers and other recipients. Afterwards, the recipient clicks on a link from any internet-enabled device and is given access and instructions to sign the document using an electronic signature. Once signed, both the sender and recipients have access to the signed document and are able to download and print them as necessary.

DocuSign operates using a cloud service known as digital transaction management (DTM) which is able to perform transactions on documents digitally [34]. DocuSign uses DTM as an end to end solution for its document signing and management process providing all components and resources needed to meet its requirements. First, users define the order in which steps are completed as well as the associated actions in order to prepare for transactions [35]. Next, each transaction is carried out using enterprise level security and authentication methods as a validation method for signer identity. Finally, each transaction is recorded digitally in the cloud for use in reporting and proof of compliance.

DocuSign boasts in its bank grade security features [36]. It operates with compliance to the xDTM standard, a list of requirements for platforms and companies to uphold in order to ensure consumer data is protected in an online environment [37]. DocuSign utilizes this standard to provide protection for digital transactions, full document encryption for the confidentiality of data, robust anti-tamper controls for the integrity of documents, redundant, geo-diverse data centers to back up critical documents and numerous authentication

options to validate the identity of users. However, on December 5, 2012 users reported a breach in DocuSign's customer-information database resulting in an email pretending to be from DocuSign containing Trojan malware [38]. The user claims that the only way a spammer could have received knowledge of their email address used for DocuSign is through a DocuSign security leak. A DocuSign representative argues that more than 85% of messages it receives with similar issues are from individuals who do not even have DocuSign accounts asserting that the DocuSign eSignature network has undergone investigation and appears to be secure. The representative goes further to say that the attacker most likely received the email address through some sort of phishing method and gives suggestions to protect against spam. The user remains skeptical contending that the unique single-use address created links the leak to DocuSign and challenges DocuSign to focus their investigation on the time period between the date he or she created the single-use address and the date of the malicious email.

1.3 EverNote

EverNote is a note-taking application that allows users create, store, search for and share documents synchronizing them to be accessed by any computer, web browser or mobile device [39]. The user may create a note that starts off as a blank document that serves as a notepad and files can be attached to it via drag and drop [40]. Once this is a complete text, attached documents and legible handwriting in photos can be searched for using keywords and users may click on an icon to open documents embedded in the notes. Additionally, these notes can be shared with an unlimited number of other users. Users can be given viewing and editing permissions. All information EverNote records is placed in cloud storage and allows for a monthly upload of 60 MB for the free version and 1 GB for the premium version.

On March 2, 2013 EverNote reported that it was able to identify and block a malicious attempt to break into secure data [41]. The attacker was able to gain access to usernames, email addresses and encrypted passwords but EverNote has since reset all user passwords and claims there is no evidence of leaked user data or payment information. On June 11, 2014 EverNote was subject to an immense distributed denial of service (DDoS) attack that interrupted the company's normal operations and prevented users from accessing and synchronizing their notes [42]. Perhaps in response to the latest attack, EverNote now uses an on-demand DDoS mitigation service [43]. To secure passwords it uses Password Based Key Derivation Function 2 (PBKDF2) rather than plaintext in storage. PBKDF2 is a method for creating encryption keys from a password. It operates by performing a pseudorandom function to generate a derived key which could be any length [45]. While it does not require for users to create strong passwords, it encourages them to do so using a password strength meter and limits failed login attempts based on accounts and IP-addresses to inhibit password guessing attacks. In addition to this EverNote uses two-factor authentication for all of its accounts based on a time-based-one-time password algorithm (TOTP). TOTP is a password that can only be used once and changes continuously based on time passed since a set point of time [46]. Furthermore, its web service uses OAuth in order to authenticate third party applications so they do not need to store the user's username or password on their device. Instead, OAuth directly connects the third party application to the user's account without giving the application the user's login credentials by returning an authentication token to the client. Finally, EverNote operates two data centers in the United States and transmits encrypted data between them with a dedicated network link not connected to the Internet.

1.4 Joukuu

Joukuu is a cloud service that allows users to manage their files from other cloud storage applications in one location [47]. Rather than having to keep track of the locations of their files from Box.net, Dropbox and Google Docs, Joukuu gives the user the ability to search, manage and edit files from the other three applications. While the free web app can run from any browser, the desktop app is for Windows users only. The paid Joukuu Plus version which is also a Window only desktop app adds a drag and drop capability and has a document sync service that synchronizes files based on how frequently they are used in order to save the amount of bandwidth used. Joukuu does not store any passwords or files on its servers so the security of the users' data is dependent on the security of Box.net, Dropbox and Google Docs and the encrypted connections they utilize [48]. So far, there has not been any known security issues associated with Joukuu.

V. Further Cloud Security

1. Cloud Data Encryption and Access Control

Recent research result shows cloud service security can be secure via data encryption and access control. Under this topic, we discuss types of Encryption system that is convenient for Cloud and the type of access controls. Encryption is required for sensitive and sensitive-enhanced data, both at rest and in transit, to meet security requirements. Sensitive and sensitive-Enhanced data must be encrypted using FIPS 140-2–validated encryption modules. Keys must be managed separately from data and require higher privileges. Encryption keys must be changed every two years for sensitive data and annually for sensitive-enhanced data, decrypting data with the old key and re-encrypting the data with the new key. Encryption requirements are as follows:

I. Encryption of data at rest-Encryption must be used for sensitive and sensitive-enhanced information stored or archived on fixed and removable devices and media.
II. Encryption of data in transit-Encryption of data in transit protects data, including usernames and passwords, from interception. This is especially important when using untrusted network environments

1.1 Homomorphic Encryption

Homomorphic Encryption systems are used to perform

operations on encrypted data without knowing the private key (without decryption). The client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data. They are ones where mathematical operations on the cipher text have regular effects on the plaintext. Among the Homomorphic encryption, there are operations that allow assessing on raw data; the Additive Homomorphic encryption adds the raw data, and the Multiplicative Homomorphic encryption multiplies the raw data.

A very simple demonstration of the mathematical consistency required: A user sends a request to add the numbers 1 and 2, which are encrypted to become the numbers 44 and 55, respectively. The server in the cloud processes the sum as 99, which is downloaded from the cloud and decrypted to the final answer.

Definition: An encryption is homomorphic, if: from Enc (a) and Enc (b) it is possible to compute Enc (f (a, b)), where f can be: +, ×, ⊕ and without using the private key.

Fully Homomorphic Encryption is a good basis to enhance the security measures of un-trusted cloud systems or applications that stores and manipulates sensitive data [18]. At a high-level, the essence of fully homomorphic encryption is simple: given ciphertexts that encrypt $\pi 1, \ldots, \pi t$. Fully homomorphic encryption should allow anyone (not just the key-holder) to output a ciphertext that encrypts $f(\pi 1 \ldots \pi t)$ for any desired function *f*, as long as that function can be efficiently computed. No information about $\pi 1 \ldots \pi t$ or $f(\pi 1, \ldots, \pi t)$, or any intermediate plaintext values, should leak; the inputs, output and Intermediate values are always encrypted [19].

This type of encryption method accepts encrypted inputs and then performs blind processing to satisfy the user query without being aware of its content, whereby the retrieved encrypted data can only be decrypted by the user who initiates the request. This allows clients to rely on the services offered by remote applications without risking their privacy.
In Fully homomorphic encryption, two operations are required to be considered it + and □.

1.2 Access Control (Identity Access Management)

Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT professionals today. While an enterprise may be able to leverage several cloud computing services without a good identity and access management strategy, in the long run extending an organization's identity services into the cloud is a necessary prerequisite for strategic use of on-demand computing services [13]. The major IAM functions that are essential for successful and effective management of identities in the cloud are Identity provisioning/ deprovisioning, Authentication & federation, Authorization & user profile management and Support for compliance.

Identity Provisioning: One of the major challenges for organizations adopting cloud computing services is the secure and timely management of on-boarding (provisioning) and off-boarding (deprovisioning) of users in the cloud. Further, enterprises that have invested in user management processes within an enterprise will seek to extend those processes to cloud services.

Authentication: When organizations utilize cloud services, authenticating users in a trustworthy and manageable manner is a vital requirement. Organizations must address authentication-related challenges such as credential management, strong authentication, delegated authentication, and managing trust across all types of cloud services.

Federation: In the cloud computing environment, Federated Identity Management plays a vital role in enabling organizations to authenticate their users of cloud services using the organization's chosen identity provider (IdP).

Authorization and User Profile Management: The requirements for user profiles and access control policy vary, depending on whether the user is acting on their own behalf (such as a consumer) or as a member of an organization (such as an employer, university, hospital, or other enterprise). The access control requirements in SPI environments include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way.

Compliance: For customers who rely on cloud services, it is important to understand how Identity Management can enable compliance with internal or regulatory requirements. Well-designed identity management can ensure that information about accounts, access grants, and segregation of duty enforcement at cloud providers, can all be pulled together to satisfy an enterprise's audit and compliance reporting requirements.

VI. Conclusion

Cloud computing model offers so many benefits yet it faces issues and criticism due to its non-stringent security enforcement. There should be stricter security policies put in place when dealing with cloud applications. Also, applications should enforce more layers of security such as 2 factor authentication to ensure that data is properly secured. Data at rest or in transit should be encrypted and signed to ensure confidentiality, integrity. Also, most business organizations should employ a hybrid cloud model since this ensures that personal information is managed internally on private clouds and not stored on public clouds. This helps to alleviate the risk of personal information being compromised.

References

[1]. S. Subashini, V. Kavitha (2011) A survey on security issues in service delivery models of cloud computing
[2]. The Next Wave Vol.20 No. 3 | 2014 https://www.nsa.gov/research/tnw/tnw203/articles/pdfs/tnw203_article5.pdf
[3]. Cloud Computing http://searchcloudcomputing.techtarget.com/tip/Breaking-down-the-three-stages-of-cloud-data-encryption
[4].] Mell, Peter, Grance, Timothy [2011] The NIST Definition of Cloud computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[5]. The 20 Coolest Cloud Security Vendors of the 2014 Cloud 100 http://www.crn.com/slide-shows/cloud/240165645/the-20-coolest-cloud-security-vendors-of-the-2014-cloud-100.htm/pgno/0/10

[6]. Top-Ten-SaaS-security-tools http://venturebeat.com/2014/01/30/top-ten-saas-security-tools/

[7]. How Secure Is Your Cloud Service Provider? http://www.forbes.com/sites/cdw/2014/09/17/how-secure-is-your-cloud-service-provider/

[8]. NIST http://csrc.nist.gov/groups/SMA/fisma/

[9]. Fed ramp http://cloud.cio.gov/fedramp

[10]. Ristenpart T, Tromer E, Shacham H, Savage S. Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, US (2009). Hey, you, get off of my cloud: exploring information leakage in third- party compute clouds. In: Proceedings of the CCS 2009, ACM Press, 2009

[11]. 116 Statue 2899 under 44 U.S.C. §3541 :FISMA" http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

[12]. Cloud Security Alliance (2010) Guidance for Identity & Access Management V2.1 https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf

[13]. Meghan Kelly (January 30, 2014 10:11 AM) -The top 10 cloud-based security tools to protect your network in a hurry. http://venturebeat.com/2014/01/30/top-ten-saas-security-tools/

[14]. TrustIT http://www.trustitllc.com/five-cloud-based-security-tools-that-will-protect-your-business-effortlessly/

[15]. Fujitsu Laboratories Ltd. "Fujitsu develops world's _1st homomorphic encryption technology that enables statistical Calculations and biometric authentication" [press release].Aug 2013. Available at http://www.fujitsu.com/global/about/resources/news/press-releases/2013/0828-01.html

[16]. InformationWeek (February 2014) FedRAMP Cloud Security http://dc.ubm-us.com/i/244186

[17]. Bajpai, Shashank, Srivastava, Padmija (2009) A Fully Homomorphic Encryption Implementation on Cloud computing http://www.ripublication.com/irph/ijict_spl/ijictv4n8spl_05.pdf

[18]. Craig Gentry (2009), A Fully Homomorphic Encryption Scheme http://crypto.stanford.edu/craig/craig-thesis.pdf

[19]. EnCase https://www.guidancesoftware.com/products/Pages/EnCase-Cybersecurity/nist-cybersecurity-framework.aspx] accessed on 01/10/2015

[20]. Splunk (http://www.splunk.com/product) accessed on 01/10/2015

[21]. Scheier, Robert [2003] Web services security vendors focus on access control, XML firewallshttp://searchsecurity.techtarget.com/tip/Web-services-security-vendors-focus-on-access-control-XML-firewalls

[22]. Macmillan, Douglas. Yadron, Danny. "DropBox blames Security breach on Password Reuse" Wall Street Journal. Oct 14, 2014. Date accessed: Jan 01, 2015.

[23]. McCullagh, Declan "Dropbox confirms security glitch—no password required" CNET. Jun, 20, 2011. Date Accessed: Jan 01, 2015

[24]. Mell, Peter. Grance, Timothy. "The NIST Definition of Cloud computing" NIST. NIST special publication 800-145. Sep 2011

[25]. Idilio Drago, Marco Mellia, Maurizio Munafo, "Inside Dropbox: Understanding Personal Cloud Storage Services" Proceedings of the 2012 ACM conference on Internet measurement conference. Pages 481-494. 2012.

[26]. "How we've Scaled Dropbox" YouTube. YouTube. 10 Sept. 2010 Web. 04 Jan. 2015.

[27]. Adrian Crockcroft "NetflixOSS-A Cloud Native Architecture". Sept 2013. Date accessed: 01 Jan, 2013 http://laser.inf.ethz.ch/2013/material/cockcroft/LASER2.pdf

[28]. Jaspn, Chan. "Netflix's Journey to the Cloud: Lessons learned from Netflix migration to the public cloud" http://www.sfisaca.org/images/FC12Presentations/D1_2.pdf

[29]. "iCloud Design Guide." Apple Inc. 2014

[30]. "Google-Docs" Wikipedia. Wikipedia. Date accessed: 5 Jan, 2015 http://en.wikipedia.org/wiki/Google_Docs

[31]. Norton, Steven. Boulton, Steven. "Why Big companies Delay using the cloud for some applications". Wall Street Journal. 16 July, 2014. Date accessed: 1 Jan, 2015.

[32]. How docusign works. (2015, January). Retrieved from https://www.docusign.com/how-it-works

[33]. End-to-end solution in technology. (2006, March 30). Retrieved from http://dictionary.reference.com/browse/end-to-end solution

[34]. The global standard for digital transaction management. (2015, January). Retrieved from https://www.docusign.com/how-it-works/digital-transaction-management

[35]. Bank-grade security & operations. (2015, January). Retrieved from https://www.docusign.com/how-it-works/security

[36]. Industry leaders align on digital transaction management standard. (2014, March 5). Retrieved from https://www.docusign.com/press-releases/industry-leaders-align-on-digital-transaction-management-standard

[37]. Docusign customer information security breach. (2012, December 5). Retrieved from http://community.docusign.com/t5/Miscellaneous/DocuSign-customer-information-security-breach/m-p/14161

[38]. Understanding evernote sync. (2015). Retrieved from https://evernote.com/getting_started/

[39]. Walsh, E., & Cho, I. (2013). Using evernote as an electronic lab notebook in a translational science laboratory. Journal of Laboratory Automation, 18(3), 229-234. Retrieved from http://jla.sagepub.com/content/early/2012/12/26/2211068212471834.full

[40]. Ovide, S. (2013, March 2). Evernote discloses security breach. Wall Street Journal. Retrieved from http://www.wsj.com/articles/SB10001424127887323478304578336373531236296

[41]. King, L. (2014, June 11). Evernote pounded by aggressive cyber attack. Forbes. Retrieved from http://www.forbes.com/sites/leoking/2014/06/11/evernote-pounded-by-aggressive-cyber-attack/

[42]. Security overview. (2015). Retrieved from https://evernote.com/security/

[43]. Kaliski, B. (2000, September). Password-based cryptography specification. Retrieved from http://www.ietf.org/rfc/rfc2898.txt

[44]. One-time passwords - hotp and totp. (2015, February 28). Retrieved from http://blogs.forgerock.org/petermajor/2014/02/one-time-passwords-hotp-and-totp/

[45]. Fulton, S. (2011, November 02). Joukuu floats a web-based "cloud cloud" for online storage. Retrieved from http://readwrite.com/2011/11/02/joukuu-floats-a-web-based-clou

[46]. Smollinger, M. (2011, March 22). Joukuu reviewed. Retrieved from http://www.smallnetbuilder.com/other/cloud/cloud-services-apps/301-joukuu-reviewed

[47]. Rouse, M. (2014, July). Linkedin. Retrieved from http://whatis.techtarget.com/definition/LinkedIn

[48]. Schwartz, M. (2012, June 20). Linkedin security breach triggers $5 million lawsuit. Retrieved from http://www.darkreading.com/risk-management/linkedin-security-breach-triggers-$5-million-lawsuit/d/d-id/1104943?

[49]. Silveira, M. (2012, June 06). An update on linkedin member passwords compromised. Retrieved from http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/

[50]. Linkedin security features. (2015). Retrieved from https://help.linkedin.com/app/safety/answers/detail/a_id/3702

[51]. Google 2-step verification. (2015). Retrieved from https://www.google.com/landing/2step/

[52]. Bisong, Anthony and Rahman, Syed[2011] An Overview of the Security Concerns In Enterprise Cloud Computing.

[53]. N Nayab, Jean Scheid "Is Google Docs Secure Enough for Your Company's Data?". 8 Aug, 2011. BrightHub. Retrieved from http://www.brighthub.com/computing/enterprise-security/articles/122102.aspx

[54]. Ryan Singel "NetFlix Cancels Recommendation Contest After Privacy Lawsuit". WIRED. 3 May, 2010. Retrieved from http://www.wired.com/2010/03/netflix-cancels-contest/

[55]. Jill Scharr "Criminals Target Netflix Users via Microsoft Flaws" toms Guide US. 20 March, 2014. Retrieved from http://www.tomsguide.com/us/cybercriminals-netflix-microsoft-silverlight,news-18807.html