A Survey on Security Mechanisms of Leading Cloud Service Providers

Deepak Panth
Associate Software Engineer
Accenture Services Pvt. Ltd.

Dhananjay Mehta
Software Engineer
Accenture Services Pvt. Ltd

Rituparna Shelgaonkar
Software Engineer
Accenture Services Pvt. Ltd

ABSTRACT
With an unprecedented pace of developments in Cloud computing technology, there has been an exponential increase of users of these services and an equal rise of cloud services providers. Clouding Computing is a virtual pool of resources provided to users as service through a web interface. These resources may include Software, Infrastructure, Storage, Network, Platform etc. With more and more organizations migrating their data over cloud, it is imperative to ensure security and integrity of their data. In this paper we 1) discuss the security challenges posed to data on the cloud computing. 2) Survey cryptographic algorithms that can be used to overcome these challenges. 3) Survey Security designs of 5 leading cloud service providers. 4) Perform a comparative study of security and features of these providers.

Keywords
Cloud Computing, Cryptography, Encryption, AES, DES, TDES, Blowfish, RSA, DSA, ELGAMAL, ECC, AWS, SmartCloud, Azure, Google Cloud Platform, Rackspace.

1. INTRODUCTION
When photos are stored online rather than on PC or if documents are shared over "dropbox" then an underlying service called "Cloud Computing" is used. Cloud computing is a concept where the applications do not reside on a specific piece of hardware but involves a geographically spread; distributed network of several computers. These interconnected networks provide a computing platform offering a shared pool of services including data storage, network services, computational services etc. These services mainly include Software (Software as a Service (SaaS)), Infrastructure (Infrastructure as a Service (IaaS)) and Platform (Platform as a Service (PaaS)). These services are presented as an integrated system through a web interface. Today cloud services are provided by numerous companies, some prominent names in this arena include Amazon (Amazon Web Services), Google (Google App Engine), Microsoft (Azure), IBM (Smartcloud), Rackspace. Cloud services can be deployed depending upon the requirements and usage by the end customers. A public cloud offers services open for all whereas a private cloud is closed and can be used by a single organization. A community cloud share resources between different organizations whereas a hybrid cloud combines two or more clouds offering benefits of multiple deployments[1] [2].The key features of cloud computing distinguishing it from traditional computing are resource abstraction, network centric services, agility, rapid and elastic scaling, location independence, no maintenance, zero up-front cost and per usage payment[2] [3]. Unlike traditional computing, Cloud computing do not require setting up a physical infrastructure that includes Datacenters, Severs, Cooling systems, purchasing software license etc. Rather it offers traditional computing as a service like communication services are provided by a telecom companies i.e. a "pay per use". These factors have encouraged more and more organizations to migrate to cloud platform. With rise in acceptance and popularity for cloud computing, there are several challenges faced today and data protection tops the list of these challenges.

2. RESEARCH DESIGN
In this paper, the major security challenges related to cloud environment will be reviewed first, then survey the existing encryption algorithms that can be adopted to provide data security for cloud computing followed by a survey of the security designs and encryption techniques adopted by major cloud services providers for data storage on cloud.

3. SECURITY CHALLENGES IN CLOUD COMPUTING
The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing. With change in thinking, design and delivery of the computing technology, cloud computing faces some major security challenges as mentioned below:

Data Security: Data security was the most important concern that had hindered the acceptance of the cloud computing initially. Storing and processing the data, running software, using CPU and virtual Machines on others' infrastructure were some serious concerns for the users initially. Data breach, data integrity and data loss are major security issues that posed threats to organization's data and software. Moreover, the multi-tenancy model and pooled computing resources over cloud have introduced new security challenges requiring new techniques to tackle with [4] [5] [6].

Data Loss: Data loss or leakage is another major concern. This may occur due to catastrophe, accidental deletion or even by the user itself but shall be a grave concern if CSPs (Cloud Service Provider) are held liable for the loss. Under the EU (European Union) data protection rules data destruction and corruption of personal data are considered forms of data breaches and would require appropriate notifications [6]. Incomplete data deletion is another concern which invites data scavenging [5] [9] [11] [12]. This also evoke a need of careful control over data mobility as this is guided by government rules and directives like EU Privacy Act or US Patriotic Act which allows data to flow within restricted geographies.

Account or Service Traffic Hijacking: Attacks such as phishing, fraud, botnet (running remotely on a collection of machines), side channel attack, man-in-the-middle attack and exploitation of software vulnerabilities lead to account or

service hijack. This leads to stolen credentials and passwords that are often misused for eavesdrop activities and transactions, manipulate data, return falsified information, and even redirect clients to illegitimate sites. This compromises the confidentiality, integrity and availability of the services [6].

Insecure Interfaces and APIs: Cloud computing services are offered to customers though web interfaces (a set of software interfaces or APIs). Security of these basic APIs determines security and availability of general cloud services [10]. Therefore from authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability [8] [6].

Denial of Service: Denial-of-service attacks prevent users of a cloud service from being able to access their data or applications. These attacks lead to exponential increase in consumption of system resources such as processor power, memory, disk space or network bandwidth. This lead to an intolerable system slowdown, leaving all the service users confused and frustrated over slow service response [6] [7].

Network Security: As data on cloud is stored on hardware outside the organization it can only be accessed through a web interface. Therefore network security is a major challenge. There are various issues that occur over cloud which include man in middle attack, net sniffing, port scanning, SQL injection, flooding attack and others [13].

Malicious Insider: The most feared and debated threat to cloud security is the risk of a malicious insider which can have access to potentially sensitive information. A malicious insider can be of any form as a current or a former employee, contractor, business partner, administrator or any person associated with organization and possess access to the cloud [6].

Shared technology vulnerabilities: Cloud services are delivered by sharing infrastructure, platforms, and applications. A single vulnerability or misconfiguration over the cloud can compromise entire provider's cloud. For example, as users share virtual resources it is possible that a user is prone to a side channel attack where the neighboring virtual machine might sneak upon the user[12] [14]. A defensive in-depth strategy is recommended which should include compute, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS [6].

4. TECHNIQUES TO COUNTER THREATS AND VULNERABILITIES IN CLOUD

There are different levels in a cloud at which the security measures are required in order to ensure the data security pertaining to the distributed architecture of cloud computing. This may involve implementation of security measures at the kernel level, storage level, at the transmission level, at the access level and at several other levels. Traditionally firewalls and intrusion detection systems have been used but they are not sufficient in cloud computing. Here we list some techniques used over cloud to counter the vulnerabilities and threats encountered on cloud [15].

Table1. Techniques to counter threats and vulnerabilities on cloud platform.

Security Challenges : Threats and Vulnerabilities	Countermeasures
Data Security	Ensure data Security compliance (e.g. ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SSAE 16, CoBIT5, PCI-DSS), Encryption and Encryption Key Management, Multi-factor Authentication, Tokenization [10], Identity and Access Management [16], Dynamic credential [17], Creating a Data Asset Catalog [9], User roles and access management.
Data Loss	Digital Signatures [18], Encryption [19], Homomorphic encryption [20], Secure Disposal guidelines in Service Level Agreement, Internal and External Data Audits, SAS70 Auditing Standards, Fragmentation-redundancy-scattering (FRS) technique.
Account or Service Traffic Hijacking	Identity and Access management, Dynamic Credentials[21], Secure API and strong Browser Security, HyperSafe, PALM[98], TCCP (Trusted Cloud Computing Platform), Audit Logging, Intrusion Detection, LDAP and Active Directory[6], Traffic Screening and Surveillance[9].
Insecure Interfaces and APIs	External Identity Providers, Identity and Access Management Guidance, User Access Authorization, LDAP and Active Directory [6], Single Sign-On.
Denial of Service	Resource and capacity planning, Backup planning, Security Assessment, Traffic Screening and filtering, Quality of Service.
Network Security	Network Traffic Screening, Access Validation, Web Application Screening, Firewalls, IPsec (Internet Protocol Security), Virtual network framework based on Xen network modes [22].
Malicious Insider	Identity and Access Audit, Ownership, Third Party Audits, Access Authorization and segregation, Federated Identity Management.
Shared Technologies vulnerability	HyperSafe [23],TCCP (Trusted Cloud Computing Platform) [22],VNSS[99], Mirage, TVDc (Trusted Virtual Datacenter) [24, 25], Isolating Clients from Each Other[9]

5. ENCRYPTION ALGORITHM USED IN CLOUD ENVIRONMENT

As data security is the biggest concern for cloud computing, this surveys the prevailing encryption algorithms that can play the role. Encryption involves scrambling of data called "Plaintext", such as text, image, audio; video etc. to make this data unreadable, invisible or meaningless called "Ciphertext" during transmission or storage. The opposite process of getting back the original data from the encrypted data is called "Decryption", which restores the scrambled data to its original form [32]. Cryptography can be broadly classified as:

5.1 Symmetric Key Encryption

The most commonly used of all the encryptions, Symmetric-key algorithms use a common key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms is simpler and faster as it does not consume too much of computing power and has high speed in encryption [35].

Symmetric-key algorithms are divided into two types [32]:

1. Block Cipher: In block cipher cryptography a group of plaintext of fixed size is taken as a block depending on the type of a symmetric encryption used. A key of fixed size is then applied on this block of plaintext that transforms it to a block of ciphertext of the same size.

2. Stream Cipher: In stream cipher each plaintext digit is combined with a random cipher digit thereby giving a stream of ciphertext. Stream cipher is also sometimes called as 'State cipher' as encryption of each digit is dependent on current state

Some popular Symmetric-key algorithms used in cloud computing includes:

1. Data Encryption Standard (DES),
2. Triple-DES (TDES),
3. Advanced Encryption Standard (AES),
4. Blowfish

Table2: Comparison of TES, TDES, AES and Blowfish encryption algorithms.

	TES	TDES	AES	Blowfish
Block size	64 bit	64 bit	128bits	64 bit
Key Size	56 bit	56,112,168 bit	128, 192, 256 bit	32-448 bit
Algorithm	Fiestel Scheme	Fiestel Scheme	Substitution Permutation	Fiestel Scheme
Encryption Rounds	16	16,24,48	9,11,13	16
Vulnerability	Brute Force attack, Linear Cryptanalysis	Meet-in-the-middle, Chosen Plaintext Attack	Side Channel Attack, Related key Attack	Susceptible to attack on reflective weak keys

5.2 Asymmetric Key Encryption

Asymmetric-key encryption often termed as public-key cryptography use a set of keys for encryption and decryption. These two keys are called Private Key and Public Key. The Public key is used for encryption by the sender whereas the private key is used by the receiver for decryption of data [32]. In cloud computing asymmetric-key algorithms are used to generate keys for encryption. Some popular Asymmetric-key algorithms used in cloud computing includes [27]:

1. RSA.
2. Digital Signature Algorithm (DSA)
3. ElGamal Encryption
4. Elliptic Curve Cryptography (ECC)

Table3: Comparison of RSA and DSA encryption algorithms.

	DSA	RSA
Algorithm	Based on Discrete Logarithm problem	Based on difficulty of factorization of large integers
Usage	Can only be used for Authentication	Used for both Authentication and Encryption
Efficiency	Faster key Generation	Faster Encryption
Performance	DSA faster at signing and slow in verification	RSA is fast at encryption
Signature	Generates a smaller signature file	Generates larger signature file
Vulnerability	280 bit DSA cracked.	RSA 512 bit key cracked.

6. SURVEY OF VARIOUS SECURITY MECHANISMS PROVIDED BY LEADING CLOUD SERVICE PROVIDERS (CSP)

With the global cloud computing market expected to grow at a 30% compound annual growth rate reaching $270 billion in 2020[28], state and federal governments around the globe have passed various legislation pertaining to safeguard of sensitive or private information. This has introduced new security standards and regulations in the technology industry. In the United States various laws have been enacted addressing the data privacy and security provision that include HIPAA, USA Patriot Act, Gramm–Leach–Bliley Act [97], HITECH, etc. Similarly the European Union has Data Protection Directive including Information Directive 1995[29] and Privacy and Electronic Communications Directive 2002[30]. As per the guidelines provided in the cloud computing technology roadmap of US

Government [31] encryption is required for systems that are assigned a FISMA impact level of moderate or above. FISMA requires FIPS 140-2 encryption of data, both at rest and in transit. This way, even if devices are lost or stolen or transmissions intercepted, data remains protected. Under these guidelines the cloud provider must provide a FIPS140-2 validated encryption algorithm for cloud consumers to establish their own encryption keys rather than the encryption key. These keys must be managed separately from data and require higher privileges. Encryption keys shall be changed on a regular basis, decrypting data and re-encrypting with the new key [32]. There are other security standards that are being followed worldwide which include the PCI-DSS, ISO 27001 certification and others [33]. A survey on security design of leading cloud service provider to comply with the new security trends is presented here. This will highlight the key security measures implemented by them to ensure confidentiality, integrity and availability of customer data.

6.1 Amazon Web Services (AWS)

Amazon.com offers its cloud computing services through AWS. Officially launched in 2006, AWS is the most prominent cloud services provider today and is located in 10 geographical "regions"[36a]. Some well-known cloud services provided by AWS are EC2 [34] and S3 [35], these services have different purpose and use different databases such as RDS [36], DynamoDB [37] and Elastic Cache [38].

Security Mechanism: All AWS data centers in worldwide include the ISO 27001 certification [39]. Entire vendor applications are on Amazon's PCI-compliant technology [39] infrastructure. AWS holds the FISMA moderate certification also it operates over the FIPS 140-2 validated hardware [40]. AWS holds number of features to ensure security in cloud environment. It uses cryptographic method to validate the users over HTTPS web service. It also offers configurable network access and firewall access [41]. AWS eliminates need to share passwords or access keys by allowing multiple user creation and permission management, it also uses different security credentials [42]. Adhering to the FISMA guidelines AWS rotates keys. Amazon provides reporting processes for security vulnerabilities [43] and penetration testing [44]. Amazon offers its customers an ability to apply penetration testing to evaluate and assess potential reported vulnerabilities to their services. To manage access to data, AWS uses Identity and Access management (IAM) [45] allowing creation and management of multiple users under single account. Amazon's customers can have the data and objects they store in Amazon S3, Glacier, Redshift, and Oracle RDS encrypted automatically using AES-256 and RSA [46]. For customers who require additional measures to comply with US ITAR regulations, AWS provides an entirely separate region called AWS GovCloud (US)[47] that provides an environment where customers can run ITAR-compliant applications and provides special endpoints that utilize only FIPS 140-2 encryption [47]. Important security measures includes DDoS protection, brute-force detection, secure HTTPS access using SSL, built in firewall, multi-factor authentication, private subnet etc.[48].

6.2 Google Cloud Platform

Google's cloud platform is a portfolio of cloud computing products offered by Google Inc. These services include App Engine (PaaS), Compute Engine (IaaS), Storage, BigQuery and other cloud services. The Google App Engine, first released in 2008 is cloud computing platform for developing and hosting web applications in Google-managed data centers and infrastructure [49][50]. Google Cloud Storage allows storage, access, and protection of data [52]. Google BigQuery is a fully managed cloud based interactive query services for massive datasets [53].

Security Mechanism: With datacenters spread across 12 places around globe [54], Google implements various industry standards to ensure the security over cloud such as FISMA Moderate, HIPAA, PCI DSS, SSAE 16 and ISAE 3402 Type II [55]. Data is protected through redundant storage at multiple physical locations. OAuth and granular access controls form strong, configurable security. Google offers two options to control access to Google Cloud Storage objects and buckets 1) Access Control Lists (ACLs), which uses Google accounts and provides longer term access. 2) Signed URLs (Query String Authentication), which does not use Google accounts, but provides "valet-key" type access for a limited time [56]. Google uses Google Cloud SQL, a web service that provides a highly available, fully-managed, hosted SQL storage solution for App Engine applications. Data for a Google Cloud SQL instance is stored in datacenters; these instances can have synchronous or asynchronous replication of data. The data is encrypted using the 128-bit AES-128 [96es] or better, with symmetric keys: that is, the same key is used to encrypt the data when it is stored, and to decrypt it when it is used. These data keys are themselves encrypted using a master key, stored in a secure keystore, and changed regularly [57]. Google uses manual and automated scans to find websites that can be the source of malware or phishing. To ensure network security Google implement firewalls, ACLs, periodic log examination. Also the traffic is routed through customized front-end servers.

6.3 Windows Azure (Microsoft)

Microsoft Azure or Windows Azure is a cloud computing platform created by Microsoft for building, deploying and managing applications and services through Microsoft managed datacenters. Released on February 1, 2010 it provides both IaaS and PaaS services [51].

Security Mechanism: Azure ensures data security for user through various security mechanisms such as identity and access management, isolation, encryption, Security Token Service (STS) etc. [58] [59]. Microsoft Azure integrates Microsoft's Security Development Lifecycle (SDL) guidelines [60]. Identity and access management systems are used to avoid unwarranted access to users. Azure SMAPI (Service Management API) provides the web services via Representational State Transfer protocol (REST), a remote procedure call that runs on SSL and authenticated with certificate and private key[61] [62]. To bolster the user's protection the applications are run on a least privilege environment that avoid granting the administrative access to the user's VM reducing the probability of side kick attack. Also all the communications between the internal components of Azure are protected with SSL thereby avoiding possibilities of packet snooping within the cloud. To lower the risk of exposing, the certificates and private keys of user Azure saves them as PKCS12 (PFX) files that may be password protected [62]. Microsoft is the first public cloud platform to achieve he FedRAMP JAB P-ATO for Windows Azure. Multifactor authentication offer additional protection to stored data by thwarting unauthorized access to Azure accounts [63]. Data encryption is provided by Azure to ensure confidentiality of data. Several encryption algorithms are used such as Microsoft's core .NET libraries (with Cryptographic classes), Symmetric

key algorithm AES-256, Cryptographic hash algorithms MD5 and SHA used for detecting duplicate data, hash table indexes, message signatures and password verification. The RNGCryptoServiceProvider .net class can be used to generate random numbers for cryptography that ensures very high level of entropy of the random numbers generated by applications making it hard to guess at the patterns[64] [58] [61]. For Hybrid storage frequently used data is accessed locally. Data is de-duplicated, compressed, and encrypted before sending. Data can be recovered from virtually any location with an Internet connection. Cloud based data backup provides protection against data loss [65] [66]. On-premises identities are synchronized with Windows Azure Active Directory that enables single sign-on to simplify user access to cloud applications thereby making easy for end users to quickly and effectively launch cloud applications with a single set of credentials[67] [68].

6.4 IBM SmartCloud

SmartCloud is an enterprise cloud computing solution offered by IBM. The services include IaaS, SaaS, PaaS offered on public, private and hybrid cloud networks.

Security Mechanism: SmartCloud offers a cloud security portfolio spanning across all security domains—people, data, applications and infrastructure—based on the IBM Security framework combined with its enterprise grade expertise. User identities are managed with comprehensive administration and security capabilities, thereby securing endpoints and defending workloads against sophisticated network attacks within the cloud [69]. SmartCloud manages data using encryption and deduplication technologies. Encryption masks the data whereas deduplication is a compression technique that prevents unauthorized access to stored data [69]. SmartCloud backs data using 128-bit client side file-level data encryption. It also allows users to generate a 63-bit encryption key [69]. To comply with the FFIEC standards SmartCloud encrypts data stored on tape drives. IBM uses TKLM Software with full KMIP to support encryption of stored data. TKLM supports 256-bit AES data encryption and allows users to implement and manage a revolving set of keys that can be scheduled to automatically change on a calendar basis. Additionally, FIPS 140-2 Level 1 certified encryption services are available to provide the off-site backups requiring the highest standards of protection [70]. Data deduplication is an important security attribute offered by SmartCloud that provides advanced compression that prevents others from reading data at the remote vault location. IBM Security Identity and Access Assurance helps users gain access to cloud resources, while also monitoring, controlling and reporting on the identities of the systems, database administrators and other privileged users. IBM Tivoli Federated Identity Manager (FIM) provides authentication to multiple cloud applications with a single ID and password. Database Security solutions offer capabilities to help protect cloud-based customer information and intellectual property from both external and internal threats. These enterprise grade solutions help prevent unauthorized changes to sensitive cloud-based data by privileged users. IBM Security Privileged Identity Manager helps manage and control access to critical cloud resources by the organization's employees and/or personnel who work for cloud providers and have high-level privileged access thereby preventing the risk of malicious insiders. IBM Security Network Intrusion Prevention System provides advanced network-level protection against emerging threats and vulnerabilities. The IBM Security zSecure suite provides cost-effective security administration, improves service by detecting threats and reduces risk with automated audit and compliance reporting [69].

6.5 Rackspace

Rackspace is a leading hybrid cloud services provider based in Windcrest, Texas, USA with services including IaaS and SaaS [71]. Two main service segments include managed and intensive support. Rackspace provides its clients servers on demand, cloud hosting services for websites and files, block storage, free DNS management and private cloud. Rackspace is open cloud company and supported by OpenStack, an open source operating system [72] [73].

Security Mechanism: Rackspace provides various security mechanisms to protect the data and safeguard against service interruptions by adopting various industry security standards. These may include ISO 27001, SSAE16, FISMA, HIPAA, ISO 14001 (UK), BSOHSAS 18001 (UK), ISO9001 [74] [75] [76]. Within Rackspace the user identities are authenticated using protocols like LDAP and Active Directory. In Rackspace private cloud, the management and internal services are offered on separate network. The internal communications in OpenStack are made through the REST API calls that are secured via SSL/TSL certifications. Rackspace allows third party encryption including SSL/TSL certifications for data backup [74]. Customer's sensitive data is encrypted for storage on cloud in order to preserve confidentiality. Rackspace provide enterprise-grade encryption Advanced Encryption Standard, 256 bit key for the encryption of data over the cloud. Rackspace offers "private cloud" [78] facility to increase privacy and security.

Table 4: Comparison of the security and features of leading cloud services provider in the industry

Cloud Providers	Industrial Security Standards [79]	Products and Services Provided	Encryption Techniques	Vulnerabilities and Demerits
Amazon Web Services (AWS)	SAS70 Type II Audits, SOC 1 Type 1&2 reports, SOC2, SSAE16 Standards, ISAE 3402 standards, ISO27001	EC2(Elastic Cloud Computing), S3(Simple Storage Service), ELB(Elastic Load Balancer),Glacier, EBS(Elastic Block Store), DynamoDB, VPC(Virtual Private Cloud), RDS(Rational Database Service), AWS GovCloud (US),	AES- 256 RSA – 4096	Amazon lacks the depth of enterprise segment experience. The service for Dropbox, that uses AWS were unavailable for an entire day, on 10, Jan, 2013[81]. In April 2010, Amazon experienced a

	certification, PCI/DSS, HIPAA-BAA, CVSS, Safe Harbor, FISMA , ITAR, FIPS, Fed RAMP	RedShift , Amazon Elastic Cache, Route53, CloudFront, EMR(Elastic Map Reduce), Kinesis, SWF(Simple Workforce Service), SNS(Simple Notification Service), SES(Simple Email service),SQS(Simple Queue Service), IAM(Identity and Access Management), CloudWatch, FPS(Flexible Payment Services) [80].		Cross-Site Scripting (XSS) bug that allowed attackers to hijack credentials from the site. In 2009, numerous Amazon systems were hijacked to run Zeus botnet nodes. [82] AWS EC2 was used by hackers in April, 2011 to siphon off personal details of over 80 million users from Sony's PlayStation Network (PSN) [83] [84].
Google Cloud Services	SAS70 Type II Audits, SOC 1 Type 1&2 reports,SOC2, SSAE16 Standards, ISAE 3402 standards ISO27001 certification PCI/DSS, HIPAA-BAA, Safe Harbor FISMA, FedRAMP.	Compute Engine (IaaS), App Engine (PaaS), Cloud SQL (Rational MySQL database), Cloud Storage (Object storage Service), Cloud DataStore, Cloud DNS Cloud Endpoints, Prediction API (Machine Learning Algorithm), Big Query (Big Data). [86]	AES-128 or better	On Monday March 18, 2013 Google users faced slow load times or time-out while accessing the Google Drive Documents [87]. This service uses Google's cloud storage facility. Twitter had admitted in past that a hacker had accessed a substantial amount of company data stored on Google Apps [88].
Microsoft Azure	SAS70 Type II Audits, SOC 1 Type 1&2 reports SSAE16 Standards ISAE 3402 standards ISO27001 certification PCI/DSS HIPAA-BAA CVSS Safe Harbor FISMA , ITAR, FIPS , FedRAMP, UK G-Cloud	I. Computation Services (Virtual Machines , Websites, Mobile Services, Cloud Services) II. Data Services (Storage, SQL Database, HDInsight, Cache, Backup, Recovery Manager) III. App Services (Media Services, Service Bus, Notification Hub, Scheduler, Automation, BizTalk Services, Visual Studio Online, Multi-Factor Authentication, API management, Azure RemoteApp) IV. Network (ExpressRoute, Virtual Network, Traffic Manager, CDN(content delivery network)) V. Microsoft Azure Government Cloud (In Testing) [89].	AES-256	Dedoose, a data analytics system that operates on Azure cloud suffered a failure on Azure that left three weeks of lost data for customers [90]. Microsoft's Office 365(a cloud service by Microsoft) editing suite and Outlook.com mail service both stuttered on Feb, 2013. Users were unable to access the services for about two hours [91].
IBM SmartCloud	SAS70 Type II Audits, SOC 1 Type 1&2 reports SOC2 SSAE16 Standards ISO27001 certification PCI/DSS HIPAA-BAA CVSS Safe Harbor FISMA , ITAR, FIPS, FedRAMP, EU Data Privacy	I. Infrastructure and Platform Services [92]- Dedicated Bare metal Servers, Managed cloud environment for System Z, Content Management Service, Virtualized Server Recovery, Managed Security Services, Cloud environment for SAP and ORACLE applications, Business storage Cloud, Virtual Private Cloud, Hybrid Cloud, Big Data, and Disaster Recovery. II. Software as a Service& Business Process as a Service [93]- IBM Sterling(Network Services) ,IBM DemandTec (Trading services), IBM Emptoris,	AES-256	N/A

		IBM Digital Analytics, IBM Live Email, IBM Kenexa(Talent Management Services), IBM Cognos.		
Rackspace	ISO 27001, SSAE16, FISMA, HIPAA, ISO 14001 (UK), BSOHSAS 18001 (UK), ISO9001 SOC 1 Type 1&2 reports SOC2, SOC3 Safe Harbor, PCI DSS, CDSA	I. Cloud Services (Public Cloud, Private Cloud, Hybrid and Enterprise) II. Cloud Servers (Cloud storage, web hosting, virtualization, servers) III. Storage (Cloud Block Storage, Cloud backup, Cloud files) IV. Databases (Cloud Database, Big data platform) V. Network (Queues, Load Balancers, DNS, Networks) VI. Email (Email hosting, Microsoft exchange, Rackspace email) VII. Applications (Microsoft SharePoint, WordPress, Marketplace) [94]	AES-256	Rackspace was vulnerable to external access to user credentials; this was later rectified by them. [95] Context (a security consultancy) during its survey was able to access remnants of data belonging to previous customers, by reading "beyond the file system" of virtual machines that it rented from Rackspace [77].

7. CONCLUSION

Today, cloud computing is being embraced across all fields of business and a huge volume of data being entrusted by the organizations to CSP. However, despite a huge surge in adoption of this technology significant number of concerns are still looming that have impeded the pace of growth of a ubiquitous cloud platform. Some organizations are yet to adopt cloud computing whereas those who have adopted cloud have put only less sensitive data on it. There is still reluctance among the cloud users as they fear vulnerabilities of using cloud as a computing platform and entrusting their data to a third party. As cloud computing model is different from the traditional computing, it possesses newer threats and risks and therefore requires different strategies to encounter them. This paper has highlighted some major security challenges currently faced by cloud computing. Also various mechanisms are stated that are available to counter threats and vulnerabilities on cloud computing and how some of the leading CSP are implementing them to counter these challenges. Cloud computing is inevitably the future for sustainable and economically viable computing. This will increase the roles and responsibilities of the CSP to ensure the safety of the data and to avoid any risk, threat or vulnerability posed to data placed over cloud.

8. REFERENCES

[1] Cloud computing, Wikipedia. At: http://en.wikipedia.org/wiki/Cloud_computing

[2] Gordon Haff.2013. INTRODUCTION TO CLOUD COMPUTING, Red Hat Inc.

[3] Introduction to Cloud Computing, 2010 Dialogic Corporation, pp 4-5.

[4] Kuyoro S. O., Ibikunle F. &AwodeleO. 2011. Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011, pp 252-253 .

[5] Jaydip Sen, Security and Privacy Issues in Cloud Computing. Innovation Labs, Tata Consultancy Services Ltd., Kolkata, India, pp 10-12.

[6] Cloud Security Alliance (February, 2013).The Notorious Nine, Cloud Computing Top Threats in 2013.

[7] Securosis (November 7, 2012). Defending Against Denial of Service Attacks V 1.3

[8] Bryan Sullivan, Said Tabet, Edward Bonver, Judith Furlong, Steve Orrin & Peleus Uhley (December 5, 2013). Practices for Secure Development of Cloud Applications. SAFECode & Cloud Security Alliance.

[9] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA

[10] Cloud Security Alliance (2010), Top Threats to Cloud Computing V1.0.

[11] Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36-42.

[12] Grobauer B, Walloschek T, Stocker E (2011) Understanding Cloud Computing vulnerabilities.IEEE Security Privacy 9(2), pp 50-57.

[13] Muhammad Imran Tariq, University of Lahore, Pakistan (2012). Towards Information Security Metrics Framework for Cloud Computing, International Journal of Cloud Computing and Services Science (IJ-CLOSER). Vol.1, No.4, October 2012, pp 210-211.

[14] Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security. Technical report, Helsinki University of Technology, October 2007.

[15] Keiko Hashizume, David G Rosado, Eduardo Fernandez-Medina and Eduardo B Fernandez (2013), An analysis of security issues for cloud computing. Hashizume et al. Journal of Internet Services and Applications 2013.

[16] Cloud Security Alliance (2012) SecaaS implementation guidance, category 1: identity and Access management.

[17] Xiao S, Gong W (2010) Mobility Can help: protect user identity with dynamic credential. In: Eleventh International conference on Mobile data Management (MDM). IEEE Computer Society, Washington, DC, USA, pp 378-380.

[18] Somani U, Lakhani K, Mundra M (2010) Implementing digital signature withRSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing. In: 1st International conference on parallel distributed and grid Computing (PDGC). IEEE Computer Society Washington, DC, USA, pp 211-216.

[19] Harnik D, Pinkas B, Shulman-Peleg A (2010) Side channels in Cloud services:deduplication in Cloud Storage. IEEE Security Privacy 8(6), pp 40-47.

[20] Tebaa M, El Hajji S, El Ghazi A (2012) Homomorphic encryption method applied to Cloud Computing. In: National Days of Network Security and Systems (JNS2). IEEE Computer Society, Washington, DC, USA, pp 86-89

[21] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications Sector (Directive on privacy and electronic communications).

[22] Wu H, Ding Y, Winer C, Yao L (2010)Network Security for virtual machine in Cloud Computing. 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18-21

[23] Wang Z, Jiang X (2010) HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity. In: Proceedings of the IEEE symposium on Security and privacy. IEEE Computer Society, Washington, DC, USA pp 380-395.

[24] Berger S, Caceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D (2008) TVDc: managing Security in the trusted virtual datacenter. SIGOPS Oper. Syst. Rev. 42(1), pp 40-47.

[25] Berger S, Caceres R, Goldman K, Pendarakis D, Perez R, Rao JR, Rom E, SailerR, Schildhauer W, Srinivasan D, Tal S, Valdez E (2009) Security for the Cloud infrastructure: trusted virtual data center implementation. IBM J Res Dev, pp 560-571.

[26] ShafiGoldwasser, & MihirBellare (July,2008). Lecture Notes on Cryptography.

[27] Public-key cryptography, Wikipedia. At: http://en.wikipedia.org/wiki/Public-key_cryptography

[28] Global Cloud Computing Market Forecast 2015-2020, Market Research Media.

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of , Official Journal L 281, 23/11/1995

[30] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications Sector (Directive on privacy and electronic communications).

[31] National Institute of Standards and Technology (November 2011), US Government Cloud Computing Technology Roadmap Volume II (Release 1.0). Useful Information for Cloud Adopters.

[32] Cloud Security Alliance (2009) Security best practices for cloud computing.

[33] Cloud Computing Security (May, 2010), A Trend Micro Whitepaper.

[34] Amazon S2, Amazon web services. At: http://aws.amazon.com/ec2/

[35] Amazon S3, Amazon web services. At: http://aws.amazon.com/s3/

[36] Amazon RDS, Amazon web services. At: http://aws.amazon.com/rds/

[37] Amazon DynamoDB, Amazon web services. At: http://aws.amazon.com/dynamodb/

[38] Amazon ElastiCache, Amazon web services. At: http://aws.amazon.com/elasticache/

[39] AWS ISO 27001 FAQs, Amazon Web Services. At: http://aws.amazon.com/security/iso-27001-certification-faqs/

[40] AWS GovCloud (US) Region – Government Cloud Computing. At: http://aws.amazon.com/govcloud-us/

[41]Amazon Web Services: Overview of Security Processes (November 2013), At: http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

[42] US Patriot Act, US Government Information. 107th Congress.

[43] Vulnerability Reporting, Amazon web services. At: http://aws.amazon.com/security/vulnerability-reporting/

[44] Penetration Testing, Amazon Web Services. At: http://aws.amazon.com/security/penetration-testing/

[45] AWS Identity and Access Management (IAM), At: http://aws.amazon.com/iam/

[46]AWS PGP Public Key, Amazon Web Services, At: https://aws.amazon.com/security/aws-pgp-public-key/

[47] AWS GovCloud (US) Region – Government Cloud Computing. At: http://aws.amazon.com/govcloud-us/

[48] Security Bulletins, Amazon Web services. At: https://aws.amazon.com/security/security-bulletins/

[49] Google App Engine, Wikipedia. At: http://en.wikipedia.org/wiki/Google_App_Engine

[50] Google App Engine, At: https://developers.google.com/appengine/docs/whatisgoogleappengine

[51] Google Cloud Storage – a simple way to store, protect, and share data (2012). Google Inc.

[52] An Inside Look at Google BigQuery(2012), Google Inc.

[53] Google, data centers. At: https://www.google.com/about/datacenters/inside/locations/index.html

[54] Google Apps Administrator, Google Inc.

[55] Google Cloud Storage, Google Inc.

[56] Google Cloud SQL, Google Inc. At: https://developers.google.com/cloud-sql/faq#whatissql

[57] Microsoft Azure, Wikipedia. At: http://en.wikipedia.org/wiki/Microsoft_Azure

[58] Deb Shinder(2009,Nov 11), Microsoft Azure: Security in the Cloud, WindowSecurity.com.

[59] Tata Consultancy Services, Windows Azure – The Cloud Computing Platform.

[60] Microsoft Security Development Lifecycle (SDL), Microsoft.

[61] Charlie Kaufman and Ramanathan Venkatapathy(2010, August), Windows Azure Security Overview, Windows Azure.

[62] Jonathan Wiggs (2010, January) Crypto Services and Data Security in Microsoft Azure, MSDN Magazine.

[63] Pedro Hernandez(2013-10-01),Microsoft's Windows Azure Meets Federal Security Standards.eWEEK.com

[64] Security Best Practices Windows Azure, Microsoft.

[65] Storage, Backup, and Recovery, Microsoft Azure, Microsoft.

[66] Azure Active Directory, Microsoft Azure, Microsoft.

[67] David Chappel (2010, October) Introducing the Windows Azure Platform. David and Chappel Associates.

[68] Microsoft Azure, Microsoft. http://www.microsoft.com/windowsazure

[69] Karin Beaty and Chris Bode(2012, September). A "how-to" guide on using cloud services for security-rich data backup. IBM Global Technology Services.

[70] IBM solutions for cloud and virtualization in enterprise environments(2013, May), IBM Software.

[71] Rackspace. http://www.rackspace.com/

[72] OpenStack, http://www.rackspace.com/cloud/openstack/

[73] OpenStack, http://www.openstack.org/

[74] Joe Burke, Rackspace Private Cloud Security, Rackspace US, Inc.

[75] Rackspace Bolsters Expanding List of Security Credentials (March 13, 2013), Rackspace Hosting, Rackspace.

[76] RACKSPACE SECURITY & COMPLIANCE , Rackspace US, Inc.

[77] Information Age (21 May 2012), Exposing the cracks in cloud security, Information-age.com.

[78] Rackspace Private Cloud, Rackspace US, Inc. At: http://www.rackspace.com/cloud/private/

[79] Alex Pucher, Stratos Dimopoulos, A Survey on Cloud Provider Security Measures.

[80] Products & Services, Amazon Web Services. At: https://aws.amazon.com/products/

[81] JR Raphael, InfoWorld, July 1, 2013. The worst cloud outages of 2013. JR Raphael (July 1, 2013) The worst cloud outages of 2013- slide4. InfoWorld.

[82] Top Threats Working Group (Feb, 2013). The Notorious Nine, Cloud Computing Top Threats in 2013. Cloud Security Alliance.

[83] Carl Bagh (May16, 2014). Sony PlayStation Network attack shows Amazon EC2 a hackers' paradise. Ibtimes.com

[84] By Pavel Alpeyev, Joseph Galante and Mariko Yasu (May 15, 2011). Amazon.com Server Said to Have Been Used in Sony Attack, Bloomberg.com.

[86] Google Cloud Platform, At: https://cloud.google.com/

[87] JR Raphael (July 1, 2013) The worst cloud outages of 2013- slide12. InfoWorld.

[88] Twitter breach revives security issues with cloud computing, CloudCenter News Article, ClearCenter Corp.

[89] Microsoft Azure. At: http://azure.microsoft.com/en-us/services/

[90] Charles Babcock (May 14, 2014). Social Science Site Using Azure Loses Data. Informationweek.com

[91] JR Raphael (July 1, 2013), The worst cloud outages of 2013- Slide 8, InfoWorld.

[92] SmartCloud, Infrastructure and platform services. IBM Inc.

[93] SmartCloud, Cloud Applications (SaaS , PaaS). IBM Inc.

[94] Rackspace. At: http://www.rackspace.com/

[95] Ben Greiner(December 23, 2013), Rackspace Email Security Breach. Source: forgetcomputers.zendesk.com

[96] Google Encryption Standard. At: https://developers.google.com/cloud-sql/faq

[97] Gramm–Leach–Bliley Act, PUBLIC LAW 106–102—NOV. 12, 1999, 106th Congress

[98]] Zhang F, Huang Y, Wang H, Chen H, Zang B (2008) PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In:Trusted Infrastructure Technologies Conference, 2008. APTC'08, Third Asia-Pacific. IEEE Computer Society, Washington, DC, USA, pp 9–18

[99] Xiaopeng G, Sumei W, Xianqin C (2010) VNSS: a Network Security sandbox for virtual Computing environment. In: IEEE youth conference on information Computing and telecommunications (YC-ICT). IEEE Computer Society, Washington DC, USA, pp 395 –398.

9. APPENDIX

1. **ISO** - International Standard Organization
2. **ISO/IEC 27001** - Information security management standard which helps organizations keep information assets secure.

3. **ISO/IEC 27017** - Standard recommending relevant information security controls for cloud computing, based on and extending recommendations by ISO/IEC 27002.
4. **ISO/IEC 27018** - Standard aimed at ensuring cloud service providers offer suitable information security controls to protect the privacy of their customers' clients by securing PII (Personally Identifiable Information) entrusted to them.
5. **ISO 14001** - Standard that a company or organization can follow to set up an effective environmental management system, to improve resource efficiency, reduce waste, and drive down costs.
6. **ISO 9001** - Standard for the quality management of businesses.
7. **SSAE 16** - Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization
8. **SAS 70** - Statement on Auditing Standards (SAS) No. 70 and third-party assurance for service organizations.
9. **COBIT5** - Business framework for the governance and management of enterprise IT.
10. **PCI-DSS** - Payment Card Industry Data Security Standard
11. **LDAP** - Lightweight Directory Access Protocol
12. **HIPAA** - Health Insurance Portability and Accountability Act of 1996
13. **HITECH** - Health Information Technology for Economic and Clinical Health Act of 2009
14. **FISMA** - Federal Information Security Management Act of 2002
15. **FIPS** - Federal Information Processing Standards
16. **JAB -** Joint Authorization Board
17. **P-ATO -** Provisional Authorities to Operate
18. **BSOHSAS 18001** – Health and safety management system with systematic and process driven approach to control and monitor risks that can arise from the company's day to day activities.
19. **US ITAR** - United States (US) International Traffic in Arms Regulations (ITAR)
20. **ISAE 3402** - International Standards for Assurance Engagements (ISAE) No. 3402