International journal of application or innovation in engineering and management

ijaiem.com/Oct 2023/ Volume 12/Issue 2/Article No-1/24-36
ISSN: 2319-4847

Cybersecurity in Cloud Computing: Safeguarding Your Data

Ms. FARHEEN SULTANA[1], Mrs. NAZIA AMREEN[2], Mr. MOHAMMED SADDAM HUSSAIN[3]
Department of Information technology
Nawab Shah Alam Khan College of Engineering and Technology (NSAKCET)

Article Info

Received: 17-08-2023 Revised: 21 -09-2023 Accepted: 06-10-2023 Published:15/10/2023

ABSTRACT

In cloud computing, IT (Information Technology) resources like infrastructure, platform, and software can be used through the internet with web-based tools and apps. This Different businesses are going to the cloud at different speeds. But the company needs to think about a number of risks before going to the cloud. Risks to information security are the most important for many organisations. One reason for this is that protecting information can help keep intellectual property, trade secrets, personally identifiable information, or other private information safe. This study put cloud security into three groups based on the three types of cloud computing service models: SaaS, PaaS, and IaaS. It also lists and quickly describes the qualities of each type of protection. We looked at the security offered by some of the most well-known cloud service providers in the world, like Amazon AWS, Google App Engine, Windows Azure, and more, in terms of the cloud security area. Additionally, we included suggestions for businesses that have chosen to move their data to the cloud but aren't sure how to pick the safest service provider for their needs.

***KEYWORDS: Cloud** Computing, Information Security.*

1. INTRODUCTION

Cloud computing is a great idea for modern IT because it lets people access resources like infrastructure, platforms, or software-related services over the internet as needed. These resources can be quickly set up and taken down with little help from managers or service providers. There are four ways to set up cloud computing: privately, publicly, hybridally, and in a group. You can use Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS) in the cloud. According to the design of cloud computing, cloud service companies are very important for storing, changing, and moving data. This means that data protection is now one of the most important issues people are worried about.

This essay sorts cloud security into three groups based on the three service models of cloud computing and lists the features that make up each group. This also compares the security services that the biggest and best cloud service providers in the world offer. In Section 2, we talk about the history of cloud computing. In Section 3, we talk about the different security aspects of cloud computing. This part gives a short explanation of each security area and

compares the security of different cloud service providers in those areas. Finally, we will end our work with some suggestions.

2. BACKGROUND

In 1999, Salesforce.com came out. It was one of the first big steps forward in cloud computers. Salesforce.com was the first company to offer business apps on a simple website [5]. Amazon Web Services launched the Amazon Mechanical Turk in 2002 as a set of cloud-based services. These services include storage, computing, and human intelligence[5]. Their Elastic Compute Cloud (EC2) was first made public in 2006. It was a paid web service called EC2 that lets people and small businesses run their own computer programs. According to Jeremy Allaire, CEO of Brightcove, which gives its SaaS online video platform to UK TV stations and newspapers[5], Amazon EC2/S3 was the first cloud computing infrastructure service that a lot of people could use. Web 2.0 really took off in 2009, with a big event. Through services, Google and others began to offer browser-based business apps. Most people know this from Google Apps. The number of people using the cloud is growing. This subject is being talked about at conferences, meetings, and projects involving colleges, business groups, and governments. Deloitte[4] put together a study document for the Centre for the Protection of National Infrastructure (CPNI) that gave a full review of cloud computing. The document focused on the possible benefits and risks of cloud computing as well as ways to make it less vulnerable. The lecture was mostly for people who work in computer protection for businesses. Like CPNI, some studies and papers have already come out that talk about cloud security problems. However, as far as I know, there isn't a study that specifically talks about information security in cloud computing.

3. CLOUD SECURITY

Cloud computing services influence economies of scale and create robust, meshed infrastructures. It transfers our important business data from the corporate network to the cloud. To provide increased levels of security to support sensitive enterprise application or information, we recommend the following areas should be considered for the security of cloud computing:

3.1 Infrastructure Security

Infrastructure can be defined as services that make clouds and cloud services available to end- user clients and the transport mechanisms to the cloud and between the various components within the cloud. Whatever the cloud type is private or public and wherever the service is SAAS, PAAS or IAAS, the foundational infrastructure of a cloud must be inherently secure. Cloud computing providers distribute to data centres around the world where land and labour are less expensive to save money and keep costs low. Organizations need to confirm that their data is protected at a standardized level based on their requirements, not only on the laws of the country where the data is transacted, transmitted

or stored. Prior to signing with a provider these kinds of controls can be written into the service level agreement (SLA). To ensure infrastructure security some more points that need to be in the check list of cloud users are Physical Security, Network Infrastructure Security, Firewalls, Access Control Lists (ACLs), Availability (Performance and anti-DoS), Security Policies (Including facilities/services will be available to customers), Remote access, Mobile access and platforms, Virtualization issues, Environmental controls, Disaster recovery, Identity/authentication/federation, Staffing/employee background checks etc. TABLE I states comparison of six cloud service providing companies regarding infrastructure security.

Table 1. Comparison on Infrastructure Security

Sl No	Cloud Service Provider's Name	Description
1	Amazon AWS	AWS Datacenter are housed in a state of art facilities where physical access is strictly controlled not only at the perimeter but also at building ingress points. AWS authority use professional security staff, video surveillance, intrusion detection systems, and other electronic means. To access data centre, authorized staff need to pass two-factor authentication for at least two times. Unauthorized person like visitors, contractors, etc. are required to present identification, signed in and continually escorted by authorized staff. Datacenter information and access are provided to employees and only those contractors who have a legitimate business need for such privileges. For both employees and contractors, privileges for access to Datacenter is immediately revoked if his/her business need is fulfilled. Log of all physical access to Datacenter is routinely audited by the authority of AWS[3].
2	Force.com	Datacenter of Salesforce is top-tier Datacenter collocated in dedicated space. Security facilities like carrier-level support, including 24-hour manned security, foot patrols and perimeter inspections, biometric scanning for access, dedicated concrete-walled Datacenter rooms, computing equipment in access-controlled steel cages, video surveillance throughout facility and perimeter are provided. Beside this, building engineered for local seismic, storm and flood risks and tracking of asset removal also available[7].
3	Google App Engine	A full-time information security team is employed in Google. The team includes some of the world's foremost experts in information, application, and network security. Responsibilities for the company's perimeter defence systems, security review processes, and customized security infrastructure, as well as for developing,

ijaiem.com/Oct 2023/ Volume 12/Issue 2/Article No-1/24-36
ISSN: 2319-4847

		documenting, and implementing Google's security policies and standards is done by the security team[11].
4	Go Grid	GoGrid, AT&T and Verizon shares same Datacenter. The Datacenter is furnished with state-of-the-art video and audio monitoring equipment and 24 hours on-site guards. All people entering the building are required to register with the security office and leave a valid ID while in the building. Those not on the access list are not allowed into the building without an escort. Visitors are checked for second time prior to entry into Datacenter on the second floor. The GoGrid NOC is staffed for 24 hours all the year round and a direct line-of-site view into the Datacenter is provided[8].
5	Rack Space	Rack Space insures ID card protocols, biometric scanning protocols and round-the-clock internal and outside surveillance monitor access to every Datacenter. Only authorized Datacenter personnel are granted access credentials to Datacenter. No one else can enter the production area of the Datacenter without prior clearance and an appropriate escort. Every Datacenter employee undergoes multiple and thorough background security checks before they are hired[9].
6	Windows Azure	Windows Azure executes in geographically distributed Microsoft facilities It shares space and utilities with other Microsoft Online Services. Each facility is designed to run 24 hours and utilize various measures to help protect operations from network outages, power failure and physical intrusion. Datacenter of Windows Azure follows industry standards for physical security and reliability. They are administered, managed and monitored by Microsoft operations personnel. They are designed for “lights out” operation[12]. With traditional security measures like locks and keys, the security system also use alarms, biometrics cameras and card readers.

3.2 Application Security

Application security is the use of hardware, software, and procedures to keep apps safe from threats from the outside. There are security features built into apps. A good application security process can make it less likely for hackers to access, change, steal, or delete private data or mess with applications[6]. These days, it's easier to get to apps over networks, which leaves them open to a lot of different threats. At some point, security starts to become a bigger issue during creation. The most basic software defence is an application firewall. Here, "countermeasure" refers to the steps that are taken to protect the application.

When you run an app in the cloud, it changes how other systems work, such as Public Key Infrastructure (PKI) systems, security key services, Identity and Access Management (IAM) systems, and other application tiers like databases. Because these systems depend on each other, change management is harder to do than with standard setup. When it comes to

ijaiem.com/Oct 2023/ Volume 12/Issue 2/Article No-1/24-36
ISSN: 2319-4847

application security, things like the Security Design Life Cycle, Authentication, Session Management, Data Input Validation, Data Integration/Exchange, Vulnerability Testing, Error Handling, Anti-Malware, Anti-Spam, Patching, APIs, Proxies, Application Sandboxing, Incident Response, Bug/Issue Tracking, Versioning, and more need to be thought about. TABLE II shows a review of six cloud service providers in terms of how secure their apps are.

Table 2. Comparison on Application Security

Sl No	Cloud Service Name Provider's	Description
1	Amazon AWS	AWS provides a number of ways to identify user and securely access user's AWS account, the AWS services have signed up for, and the resources hosted by these services. AWS provide additional security options like Multi-Factor Authentication (MFA), Key Rotation and Identity and Access Management (IAM) which enable further protection of AWS account and control access. Amazon S3 provides further protection via Versioning. Versioning is used to restore, retrieve, and preserve all version of every object stored in Amazon S3 bucket. Easily recover from both unintended user actions and application failures are possible with Versioning. By default, most recently written version is retrieved by the requests. By specifying a version in the request, older versions of an object can be retrieved. Using Amazon S3 Versioning's MFA Delete feature we can use further protection of versions. Each version deletion request must include the six-digit code and serial number from users multi factor authentication device, if we enabled this feature for an S3 bucket [3].
2.	Force.com	Salesforce uses robust application security model which prevents one client's from accessing another's information. With every request, this security model is reapplied and imposed for the total duration of a user session. Salesforce account is accessible with a valid user name and password, which is encrypted via SSL while in transmission. Selecting weak or plain passwords are prevented and each user is uniquely identify by an encrypted session ID cookie. At regular intervals, the session key is automatically scrambled and re-established in the background[7].

3	Google App Engine	As part of the Secure Code development process, Google applications go through multiple security reviews. To maximize security, the environment of application development is carefully monitored and closely restricted. To provide additional assurance, external security audits are also conducted on regularly basis. 2- step verification is available for all Google Apps customers[11].
4	GoGrid	GoGrid gets SAS70 Type II certification for its own facilities. Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS) compliance requirements like custom network implementations, secure database servers and hardware firewalls are offered as infrastructure solutions to help customers meet[8].
5	RackSpace	The Rackspace security regime addresses the inherent vulnerabilities of Internet-oriented applications like FTP servers, mail services, DNS, Linux, Apache, Microsoft IIS, streaming media and organizations databases. To protect business applications Rackspace deactivates non-essential features and implements well-configured firewalls [9].
6	Windows Azure	To provide a way to integrate common identities Microsoft has .NET Access Control Service. It works with web applications and web services. The service will support popular identity providers. The Security Token Service (STS) creates Security Assertion Markup Language (SAML) tokens based on which applications determine whether a user is allowed to access or not. A digital signature is provided for each token by STS. For the STSs applications have trusted lists of digital certificates. An STS that issues a token to provide for identity federation and a trusted STS can create a trust relationship. STS runs in the cloud and it is an Access Control Service. STS creates and signs a new token for the client application after the validation of signature on the SAML token that is sent by the client application like a web browser to present to the cloud application[12].

ijaiem.com/Oct 2023/ Volume 12/Issue 2/Article No-1/24-36
ISSN: 2319-4847

3.3 Information Security

The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability[13]. Here, integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Confidentiality means preserving authorized restrictions on disclosure and access, including means for defending proprietary and personal privacy information. And availability means ensuring timely and reliable access to and use of information. Cloud computing provides computing and storage resources on demand without the need for internal infrastructure which ensures cost-saving benefits. As the technology arrangement becomes more popular, additional cloud computing security measures are necessary to ensure the continued protection of the confidentiality, availability, and integrity of enterprise data.

The physical boundaries of data and moving that data between trusted partners securely and reliably is changed by cloud computing. To ensure the latest security capabilities are being used properly, this capability of cloud computing will require encryption and trust models being constantly evaluated. By using the right service provider in the cloud, this capability may be enhanced. To ensure information security data storage and privacy security need to be consider.

3.3.1 Data Storage Security

For Data Storage Security Data storage zoning, Data tagging, Data retention policies, Data permanence/deletion, Data classification, Locality requirements, etc. have to be in the check list.

3.3.2 Data Privacy Security

Backup, Archiving, Multi-tenancy issues, Recovery, Privacy/privacy controls, prevention, Malicious data aggregation, Encryption (at-rest, in-transit, key management, Federal information processing standards/Federal information security management act), Digital signing/integrity, attestation, Data leak prevention etc. are need to be considered for Data Privacy Security.

Table 3 states comparison of six cloud service providing companies regarding information security.

ijaiem.com/Oct 2023/ Volume 12/Issue 2/Article No-1/24-36
ISSN: 2319-4847

Table 3. Comparison on Information Security

Sl No	Cloud Service Provider's Name	Description
1	Amazon AWS	As part of normal operation, data stored in Amazon Elastic Block Store (EBS), Amazon S3 or Amazon SimpleDB is redundantly stored in multiple physical locations. On the initial write by storing objects multiple times across multiple Availability Zones, Amazon S3 and Amazon SimpleDB provide object durability. In the event of device unavailability or detected bit-rot further replication is actively done. AWS procedures include a decommissioning process when a storage device has reached the end of its useful life. The process is designed to prevent customer data from being exposed to unauthorized individuals. As part of the decommissioning process AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data. In accordance with industry-standard practices a hardware device is degaussed or physically destroyed if the device will be unable to be decommissioned [3].
	Force.com	Salesforce.com guarantees that customer's data is protected with physical security, application security, user authentication and data encryption. It also ensures the latest standard-setting security practices and certifications, including: ISO27001, SOX, SysTrust certifications, third-party vulnerability and World-class security specifications SAS 70 Type II. It provides secure point- to-point data replication for data backup: Backup tapes for customer data never leave providers facilities—no tapes ever in transport. Salesforce.com uses 1024-bit RSA public keys and 128-bit VeriSign SSL Certification for ensuring strongest encryption products to protect customer data and communications. The lock icon in the browser indicates that data is fully shielded from access while in transit. Using RAID disks and multiple data paths, customer's data are stored on carrier- class disk

		storage. on a nightly basis, all customer data is automatically backed up to a primary tape library up to the last committed transaction. on regular basis to verify their integrity, backup tapes are immediately cloned and moved to fire-resistant, secure, off-site storage[7].
	Google Engine App	A distributed NoSQL data storage service is provided by App Engine with transactions and a query engine features. The distributed datastore grows with data like the distributed web server grows with traffic. Two different data storage options are available for customers. These data storage are differentiated by their availability and consistency guarantees. The App Engine datastore is not like a traditional relational database. Here data objects, or "entities," have a set and kind of properties, using which, queries can retrieve entities of a given kind filtered and sorted. Any of the supported property value types can be Property values. Here, datastore entities are "schemaless" and data entities structure are enforced and provided by customer's application code. The datastore uses optimistic concurrency control and is strongly consistent. If other processes are trying to update the same entity simultaneously, an update of entity occurs in a transaction that is retried a fixed number of times. ensuring the integrity of customer's data, customer application can execute multiple datastore operations in a single transaction which either all fail or all succeed. Using "entity groups", transactions are implemented across its distributed network. Entities are manipulated through a transaction within a single group. For efficient execution of transactions same group entities are stored together. When the entities are created, application can assign them to groups. In case of errors or system failure Google can recover data and restore accounts as they keeps multiple backup copies of customers' content. When customer asks to delete messages and content, Google make reasonable efforts to remove deleted information from their systems as quickly as is practicable[11].

	Go Grid	Go Grid offers disaster recovery and backup solutions i365 EVault SaaS for online data protection. For small and medium- sized businesses, a cost-effective recovery and backup solution is EVault SaaS. It provides efficient, reliable, secure protection of an organization's critical data through Internet. It automatically backs up server, desktop and laptop data from across the customer's organization. The customer can configure the retention schedule and monitor their backups using a web browser. Customer's data is reduplicated, compressed, encrypted, and then transmitted to a vault in one of i365's top- tier Datacenter[8].
	Rack Space	For secure collaboration, disaster recovery, and data access, Rackspace provides Cloud Drive. Cloud Drive automatically backs up any file type or file size—no restrictions. Here, files are kept secure using admin-controlled keys and AES-256 encryption [9].
	Windows Azure	To minimize the impact of hardware failures Windows Azure replicate data within the Fabric to three separate nodes. By creating a second Storage Account to provide hot-failover capability Windows Azure infrastructure leverage Customers with the geographically distributed nature. To synchronize and replicate data between Microsoft facilities, customers can create custom roles. Customers can also create customized roles to extract data from storage for off-site private backups. Strict hardware disposal processes and data handling procedures are followed by Microsoft operational personnel after systems end- of-life. Assets are classified to determine the strength of security controls to apply. To determine required protections, a defense- in-depth approach is taken. For example, when data assets are residing on removable media or when they are involved in external network transfers, fall into the moderate impact category and are subject to encryption requirements. For high impact data, in addition to those requirements, is subject to encryption requirements for network transfers, storage and for internal system as well. The SDL cryptographic standards list the acceptable and unacceptable cryptographic algorithms and all Microsoft products must meet that standards. For example,

ijaiem.com/Oct 2023/ Volume 12/Issue 2/Article No-1/24-36
ISSN: 2319-4847

		symmetric encryption is required for longer than 128-bits keys. When using asymmetric algorithms, keys of 2,048 bits or longer are required[12].

3.4 Audit and Legal Compliances

Audits and following the law are also very important for security. For security reasons, you need to think about a few things, such as forensics, auditing, SLAs, monitoring, accreditation, compliance, legal problems, regulations, public communication plans, local requirements, discovery, logging, and so on.

4. CONCLUSIONS

Cloud computing technology lets people get better, faster services while also saving money, making services stronger, and making them safer. The main features of cloud computing are on-demand supply, measured services, network access, flexibility, and resource sharing. These features greatly lower the costs of buying and running services and make them more efficient and effective. Companies that know this technology can help them are moving to the cloud, though some are moving faster than others. This comes with a number of risks that the companies need to think about. According to our study, the biggest risk is to the security of information, since cloud computing changes the physical limits of information and makes it possible to send that information safely and consistently to trusted partners. To make sure that all of your information is safe, you need to cover all of its security areas, such as infrastructure, applications, data storage, privacy, and legal problems. Moving data storage and apps to the cloud can be hard for some businesses because they don't have the right security infrastructure, control, risk profile, or clear understanding of their contractual responsibilities. To make sure that the newest security features are being used correctly, trust models need to be looked at all the time, and safe encryption will need extra attention. Picking the right cloud service company that fits the needs of the business can make it better. Before showing the seller, a company should know what kind of information is being kept or sent, as well as the specific law and security rules that apply to their business. Technology needs to keep getting better at protecting data in a way that service providers can easily use. So if safety and risk worries are the most important things, then all other results

It will be profitable to switch to cloud-based design for reasons of cost and features. When services get better in this way, both service companies and users will have alot of business.

REFERENCES

1. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, by Ronald L. Krutz and Russell Dean Vines, came out in 2010.

2. "Cloud Security Deep Dive: A New Security Model for a New Era," by Roger A. Grimes, Infoworld, August 2011, p.2.
3. Amazon Web Services: A Look at Their Security Measures, May 2011
4. Information security report 01/2010 from Deloitte to the Centre for the Protection of National Infrastructure(CPNI), March 2010.
5. Computerweekly.com, The history of cloud computing was first written in March 2009 and can be found at http://www.computerweekly.com.
6. TechTarget, https://searchsoftwarequality.techtarget.com/definition/application-security
7. This is what Salesforce.com Inc. says: https://trust.salesforce.com
8. GoGrid, which can be found at http://www.gogrid.com
9. Rackspace US, Inc., http://www.rackspace.com/
10. Amazon Web Services, https://aws.amazon.com/security
11. Google, https://www.google.com/apps/intl/en/business/infrastructure_security.html
12. Windows Azure Security Overview v1.01, August 2010, by Charlie Kaufman and Ramanathan Venkatapathy
13. The Legal Information Institute of Cornell University Law School, This link takes you to the US Code text for section 44-354.
14. The Structure of the New IT Frontier: Cloud Computing – Part I by Dexter Duncan, Xingchen Chu, Christian Vecchiola, and Rajkumar Buyya was published by Manjrasoft Pty Ltd and the Cloud Computing and Distributed Systems (CLOUDS) Laboratory at The University of Melbourne in Australia.
15. The Cloud Security Alliance put together Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 in December 2009.