INFORMATION SECURITY IN CLOUD COMPUTING

Lipi Akter[1], Prof. Dr. S M Monzurur Rahman[2] and Md. Hasan[3]

[1,2,3]Department of Computer Science & Engineering, United International University, Dhaka, Bangladesh.

[1]lipiakter@yahoo.com, [2]mrahman99@yahoo.com, [3]hasan@infobase.com.bd

ABSTRACT

In cloud computing IT (Information Technology) related resources like infrastructure, platform and software can be utilized using web based tools and application through internet. Here Organizations are moving to the cloud computing some faster than others. However, moving to the cloud presents the organization with a number of risks to assess. Information security is the most critical risk for many organizations. This is because the intellectual property, trade secrets, personally identifiable information, or other sensitive information can be powered by protecting information. This paper classified cloud security based on the three service models of cloud computing SaaS, PaaS and IaaS. Attributes for each type of security has also identified and briefly described here. We compared securities provided in different services by world's best known cloud service providing companies such as Amazon AWS, Google App Engine, Windows Azure etc. considering cloud security category. Furthermore, we included recommendations for organizations who have decided to move their data into the cloud, but confused to choose the best service provider for their organization regarding information security.

KEYWORDS

Cloud Computing, Information Security.

1. INTRODUCTION

The concept of cloud computing is a blessing of modern IT where resources like infrastructure, or platform, or software related services can be available through internet as an on-demand self service basis which can be rapidly provisioned and released with minimum management effort or service providers interaction. Private, public, hybrid and community are the four deployment models of cloud computing. Three service models of cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The cloud computing architecture follows such a principle that for any given model cloud service providers play a vital role for storage, manipulation and transportation of information so security of information has become a highly important concerns at present.

This paper classified cloud security based on the three service models of cloud computing and identifies attributes for each type of security. This also compares security services provided by world's best known cloud services providing companies. Section 2 describes the background of cloud computing. Section 3 identifies different security areas of cloud computing. This section briefly describes each security area including comparison of cloud service providing companies on corresponding areas. Lastly, we will conclude our paper with recommendations.

2. BACKGROUND

Salesforce.com arrived in 1999. It was one of the first milestone in cloud computing. Salesforce.com was the pioneer of delivering enterprise applications via a simple website [5]. In 2002, Amazon Web Services provided a suite of cloud-based services through the Amazon Mechanical Turk which include storage, computation and human intelligence[5]. In 2006, Amazon launched its Elastic Compute Cloud (EC2). EC2 was a commercial web service which allows small companies and individuals to run their own computer applications. "Amazon EC2/S3 was the first widely accessible cloud computing infrastructure service", said Jeremy Allaire, CEO of Brightcove, which provides its SaaS online video platform to UK TV stations and newspapers[5]. In 2009, a big milestone came as Web 2.0 hit its stride. Google and others started to offer browser-based enterprise applications, through services. Google Apps. is the best example of this. Cloud adoption sees increased growth. Conferences, workshops, projects comprising universities, industry associations and governments are dealing with this topic. On the research document compiled on behalf of Center for the Protection of National Infrastructure (CPNI), a detailed overview of cloud computing, focusing on the potential benefits and risks as well as identifying mitigation advice to reduce vulnerability was provided by Deloitte[4]. Main target of that briefing was information security practitioners from organizations. Like CPNI some reports and papers have already been published discussing cloud security related issues but to the best of my knowledge no paper exactly on information security in cloud computing is published yet.

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, 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

Sl No	Cloud Service Provider's Name	Description
		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

Using hardware, software and procedural methods to protect applications from external threats is called application security. Security measures built into applications. The probability to access, modify, steal or delete sensitive data or manipulate applications by hackers can be minimized by a sound application security routine[6]. Nowadays, applications become more frequently accessible over networks, as a result, vulnerable to a wide variety of threats. Ultimately, security becomes an increasingly important concern during development. Application firewall is the most basic software countermeasure. Here countermeasure means actions taken to ensure application security.

The operation of other systems like, Public Key Infrastructure (PKI) systems, security token services, Identity and Access Management (IAM) systems and other application tiers (e.g. databases) affects while running an application in the cloud. Dependencies on these systems render configuration management more complex than with traditional deployment. In the case of application security points like 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 Sand-boxing, Incident response, Bug/Issue Tracking, Versioning etc. are need to be considered. TABLE II states comparison of six cloud service providing companies regarding application security.

Table 2. Comparison on Application Security

Sl No	Cloud Service Provider's Name	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

Sl No	Cloud Service Provider's Name	Description
		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].

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.

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

Sl No	Cloud Service Provider's Name	Description
		accordance with industry-standard practices a hardware device is degaussed or physically destroyed if the device will be unable to be decommissioned [3].
2	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].
3	Google App Engine	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

Sl No	Cloud Service Provider's Name	Description
		remove deleted information from their systems as quickly as is practicable[11].
4	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].
5	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].
6	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, 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

Audit and legal compliances also play a vital role to ensure security. Few components like Fraud detection, Forensics, Auditing, SLAs, Monitoring, Accreditation, Compliance, Legal issues, Regulations, Public communication plans, Locality requirements, Discovery, Logging etc. are need to be considered for security reasons.

4. RECOMMENDATIONS

Target audience of this section are those organizations who have already decided to move their data into the cloud, and now choosing which service provider will be best for their organization regarding information security. We recommend the following will help them to pick right one.

i) Decide sensitivity of your organization's data with respect to protect sensitive information like personally identifiable information, intellectual property, or other trade secrets. Now, considering the importance of your data choose the right deployment model such as private model, public model, hybrid model or community model of cloud.

ii) All cloud providers offer a certain level of security benefits for their clients, but according to your own security needs create a check-list with the help of an information security expert. Make sure that your IT department experts remain involved while preparing the check-list.

iii) Also consider geographical location of Datacenter's of cloud service providers.

iv) Now choose which cloud service provider serves you best according to the check-list.

v) To reduce threats, review the cloud provider's software/hardware/other equipment sourcing security, employee background check process, supply chain practices and HR.

vi) To reduce the assurance burden, common controls reviews need to be used based on ISO 27000 and 28000 standards.

vii) The legal risks like subpoenas, e-discovery and jurisdictional issues as well as technology licensing issues need to be addressed in the contract.

viii) Obviously, there will be a shift in skills in IT departments as companies migrate to the cloud. Our recommendation is to train organization's people and help them achieve that skill shift so that organization can be much more successful as it moves forward.

ix) Finally, within 24 hours language mandatory immediate notification of serious security events with ongoing security reviews need to considered in the contract with cloud service provider.

5. CONCLUSIONS

Cloud computing technology allows users for improved, quicker services and to save resources, strengthen services, and better security. The essential characteristics of cloud computing is it's on-demand provisioning, measured services, network access, elasticity and resource pooling which dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services. Organizations, have realized the benefits of this technology are moving to the cloud some faster than others which presents the organization with a number of risks to assess. Our study recommend, security of information is the most critical risk as cloud computing conveys a modification in the physical boundaries of information and moving that information between trusted partners reliably and securely. To ensure total information security all areas of security like infrastructure, application, data storage and privacy and legal issues are need to be covered. An organization requires carefully analyse its security infrastructure, oversight ability, risk profile and contractual obligations clearly as they are significant obstacles to moving data storage and applications to the cloud environment. To ensure the latest security capabilities are being used properly, trust models need to be constantly evaluated and special attention will require on secure encryption. It can be enhanced by choosing the right service provider in the cloud that meets organizations business needs. Before presenting the vendor, an organization should prepared the nature of the information being stored or transacted with detailed security and legal requirements applicable to their business needs. Technology must continue to advance in securing data more robustly which may be easily implemented by the service providers. So if risk and security concerns are at the forefront with all other performance

and feature concerns, moving to cloud based architecture will be lucrative. If services get better this way, business for both providers and customers will flourish to new level of acceptance.

REFERENCES

[1] Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, 2010.
[2] Roger A. Grimes, Cloud Security Deep Dive: A new security model for a new era, Info world, SPECIAL REPORT, AUGUST 2011
[3] Amazon Web Services: Overview of Security Processes, May 2011
[4] Deloitte, Information security briefing 01/2010, center for the protection of national infrastructure(CPNI) , march 2010
[5] computerweekly.com, A history of cloud computing, first published in March 2009, Available from: http://www.computerweekly.com
[6] TechTarget, http://searchsoftwarequality.techtarget.com/definition/application-security
[7] Salesforce.com inc., https://trust.salesforce.com
[8] GoGrid, http://www.gogrid.com
[9] Rackspace US inc., http://www.rackspace.com
[10] Amazon Web Services, http://aws.amazon.com/security
[11] Google, http://www.google.com/apps/intl/en/business/ infrastructure_security.html
[12] Charlie Kaufman, Ramanathan Venkatapathy, Windows Azure Security Overview v1.01, August, 2010
[13] Legal Information Institute of Cornell University Law School, http://www.law.cornell.edu/uscode/text/44/3542
[14] Dexter Duncan, Xingchen Chu, Christian Vecchiola and Rajkumar Buyya, The Structure of the New IT Frontier: Cloud Computing – Part I, Manjrasoft Pty Ltd and Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computer Science and Software Engineering, The University of Melbourne, Australia
[15] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Prepared by the Cloud Security Alliance, December 2009

Authors

Lipi Akter received her M.Sc Degree from United International University, Bangladesh, Post Graduate Diploma in ICT from Bangladesh University of Engineering & Technology (BUET), Bangladesh and- B.Sc from National University, Bangladesh. Presently, she is a Programmer in Bangladesh Open University, Bangladesh.

S M Monzurur Rahman received his Ph.D in Data mining (Australia), M.Sc in Machine Learning (Australia), B.Sc Engg (CSE, BUET). Presently, he is a Professor in CSE Department, United International University, Bangladesh.

Md. Hasan received his M.Sc Degree from United International University, Bangladesh, B.Sc Degree from National University, Bangladesh. Presently, he is a Executive Director in Infobase Ltd. Bangladesh.