Faculity of engineering and technology

Computer Science Department

COMP4381(Cloud computing and data security)

Instructor : Dr. Ruba Awadallah

Student : Yahya Aburayyan

Student ID : 1221971

Project: Cloud computing and data security

Proposal for **TechSolutionsInc.**

We as **Amazon AWS** cloud computing service provider are glad that yours company TechSolutionsInc. Is looking to move to the cloud and take benefits of its services ,this is our proposal for you that may have all the details that you want to know about all the Scenarios that you may think of.

1- Available Cloud products for you :

Since you are looking to migrate your IT infrastructure to the cloud , so you need one of our many IaaS (Infrastructure as a Service) products to improve scalability, accessibility and cost-effectiveness of your company.

Also we have another cloud services such as PaaS (Platform as a Service) and SaaS (Software as a Service), PaaS is mainly used as a runtime environment to test you applications as a programmer . On the other hand , SaaS is the service that the end user needs only simple web access to use the applications. The consumer does not have to worry about making updates, adding security codes, and ensuring the availability of the service.

In addition Amazon AWS has cloud services in a lot of categories including :

Compute, Storage, Database, Analytics, and Machine Learning exc. .

And the best Amazon AWS IaaS product for you is : **Amazon EC2**

AWS deployment modals : Cloud ,Hybrid , On-premises.

Since your company TechSolutionsInc. Is concerned about security risks we recommend you the **On-premises (private) deployment modal** of the cloud.

But ,let's take a look at the most important characteristics that Amazon AWS gives you as a mid-sized technology company :

1- Resilience and elasticity :

cloud computing offers unlimited storage space and better computing power than the traditional IT infrastructure , allowing applications to run faster. Also You can focus on your core business activities because others fully manage the IT infrastructure and computing resources.

2- Flexibility and Scalability :

cloud services offer on-demand virtual boundless distributed computing space and have various server resources. Thus, cloud servers can scale up or down depending on the activity level. Also IaaS solutions give you a lot more options that you can use to both increase compute performance and reduce network latency.

3- Backup and recovery :

IaaS providers give you access to unlimited infrastructure for backup and disaster recovery. For example, you can duplicate your applications across multiple servers so that if one fails, another takes over.

4- Cost :

IaaS is a cloud computing model in which customers pay only for the resources they use. Such a setup encourages more efficient IT resource management and promotes innovation by making cloud services affordable to small businesses.

2-Possible Cloud Computing Security risks and challenges and there vulnerabilities :

Even though cloud computing have a lot of benefits , this benefits must be weighed against the security concerns. So, since the cloud computing services is a collection of different and mixed technologies , it's make the data in the cloud vulnerable to threats.

Cloud computing risks are summarized in four management areas:

1- Governance management risk.
2- Enterprise management risk.
3- Information management risk.
4- Information security.

Data Breaches : Data is considered breached once its information is disclosed, manipulated, or used by unauthorized parties. And breaches occur duo to human mistake, implementation flaws , insufficient security measures.

Data breach threats lead to three main violations:

1-Data privacy violations .

2-Data confidentiality violations.

3-Data integrity violations.

Contracts:

Contracts is used to define a formal relationship and guarantee between providers and customers, it's the primary tool of governance between cloud provider and client ,so this contract must be clear and included of all the expected good or bad scenarios between CSP and client .

Cloud Security Alliance (CSA):

Is a nonprofit organization that create a shared responsibility model for both CSPs and cloud clients. The CSA study collected the most critical cloud computing security flaws or issues that result in various attacks: Identity spoofing, Data repudiation ,Information leakage ,Denial of service , Privilege elevation.

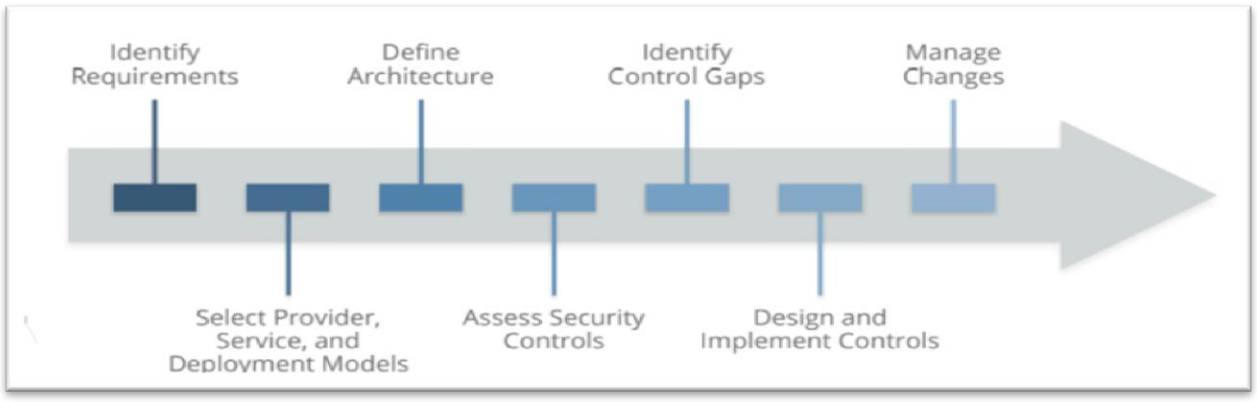


Figure 1: CSA process modal for security

The roles of cloud service providers and clients in ensuring security:

The CSP responsibilities :

1- Using the Consensus Assessments Initiative Questionnaire (CAIQ) tool to Develop and execute such policies.
2- Responsible for ensuring high availability and reliability of their services. This includes maintaining data centers, network connectivity, and hardware to minimize downtime.

The cloud client responsibilities :

1- deciding which data you store in the services you use.
2- Using the Cloud Controls Matrix (CCM) tool to track duties.
3- Securely configuring the services that you have chosen to use.

Vulnerability : is any weakness or gaps in an information system, system security operations, central administration, or application that could be misused or controlled by a remote attacker that he could gain unauthorized ,steal data.

The vulnerabilities related to data breaches are categorized into four:

1. Data Storage Cryptography Vulnerabilities.

2. Data Access Vulnerabilities.

3. Data Storage Location, Backup and Recovery Vulnerabilities

4. Data Sanitization Vulnerabilities.

A quick explanation for some of them :

Data Storage Cryptography Vulnerabilities: Lack of encryption presents a significant vulnerability in cloud storage, allowing unauthorized individuals to access sensitive data if they manage to sneak to the cloud environment. Some of its examples : Poor key management ,and insecure encryption technique.

Data Access Vulnerabilities : it's an Vulnerability that come from outsiders like attackers and others , or from insider and both of them are unauthorized . also we consider the insider attacker is much dangerous than the outsider because of the permissions that the insider have to the data. For example : an IT employee who has access to sensitive data in the Database ,like the marks of students and he changed them for bribe (رشوة).

Data Storage Location, Backup and Recovery Vulnerabilities : Cybercriminals can use such configuration mistakes to get configuration information and stored data, and in many cases, can also tamper or play with the data itself, including the copies used to protect the data . for example : information disclosure and data loss, loss of control , data locality.

We as Amazon AWS provide over 300 security measures and features that are suitable for your company TechSolutionsInc. So since we in AWS the security is our top priority we gained the trust of millions of customers.

Some of these security measures in AWS :

1- **Detect** : Gain visibility into your organization's security posture with logging and monitoring services.
2- **Identify**: Understand and manage risk with deep visibility and automation.
3- **Prevent**: Define user permissions and identities, infrastructure protection and data protection measures for a smooth and planned AWS adoption strategy.

3- Developing data security strategies that matches your requirements :

To guarantee a secure cloud computing service we need to consider these security requirements in hands (name with simple definition):

1. **Privacy** : the client's critical data is not disclosed to any unauthorized proses .

2. **Confidentiality** : Data is used from who is allowed to only .

3. **Integrity** : Data is saved and secured from and changing or destroy on it.

4. **Availability** : Data is ready and available when its required.

5. **Accountability** : Every activity information is known to the CSP.

6. **Authentication** : the proses of verify who you claim you are.

7. **Authorization** : the proses of giving the authenticated user level of access.

To consider the security of data in the cloud we need to develop a data security strategy that consider the data security requirements , and this strategy get done by applying security countermeasures for data breaches.

Security Countermeasures : are methods, actions, devices, procedures, or techniques that reduce or prevent threat, vulnerability, or attack by minimizing the harm it can cause **,such as :**

1- Encryption and Key Management
2- Data Classification and Access Control
3- Digital Signature and hashing
4- Trust Framework
5- Data Integrity and Availability
6- Identity and Access Management
7- Intrusion Detection and Prevention System
8- Location, Backup and Recovery Transparency
9- Data Sanitization

So we in Amazon AWS think this **strategy** is the best for your company **TechSolutionsInc**. :

We are going to apply some countermeasures that get some of data security requirements vivificated :

1- Encryption and Key Management :

A good encryption algorithms and strong Key management mechanism have a directly impact on data confidentiality and privacy .on the other hand if the algorithms and the mechanisms are weak this well lead to data storage susceptible to threats .

So we AWS recommend many schemes **that classify data confidentially and privacy such as** :

Symmetric key encryption scheme : Advanced Encryption Standard (AES).

Asymmetric key encryption scheme : RSA , ElGamal and Gentry.

2- Data Classification and Access Control :

Data Classification : It's based on the degree sensitivity of the data , so by assigning classification levels : manage , protect, and handle data assets , also prioritize resources and apply security measures on each data category . Data classified using : Advanced algorithms to scan and analyze data ,matching it to the defined categories based on data attributes, Or manual classification .

Data can be classified into three levels :

1- Primary (non-sensitive data) .

2- Confidential (personal information).

3- Highly confidential, stored data (financial, political, Health) .

Identity and Access Management (IAM) : the security discipline that permits the appropriate users to access the right resources at the correct time for the proper purposes. And manages user authentication and authorization at all cloud environment layers .

Both Data classification and IAM provide together data **confidentiality** which is provided by the classifying of the data , **authentication** ,and **authorization** which is provided by IAM .

3-Digital Signature and Hashing :

Digital Signature : is an electronic , encrypted stamp (ختم) or a mathematical technique used to validate the authenticity and integrity of a digital document, massage or software . and it uses to keys in its mechanism Public key and Private key.

Digital signature public key : is openly available and used by both client and CSP to encrypt the data .

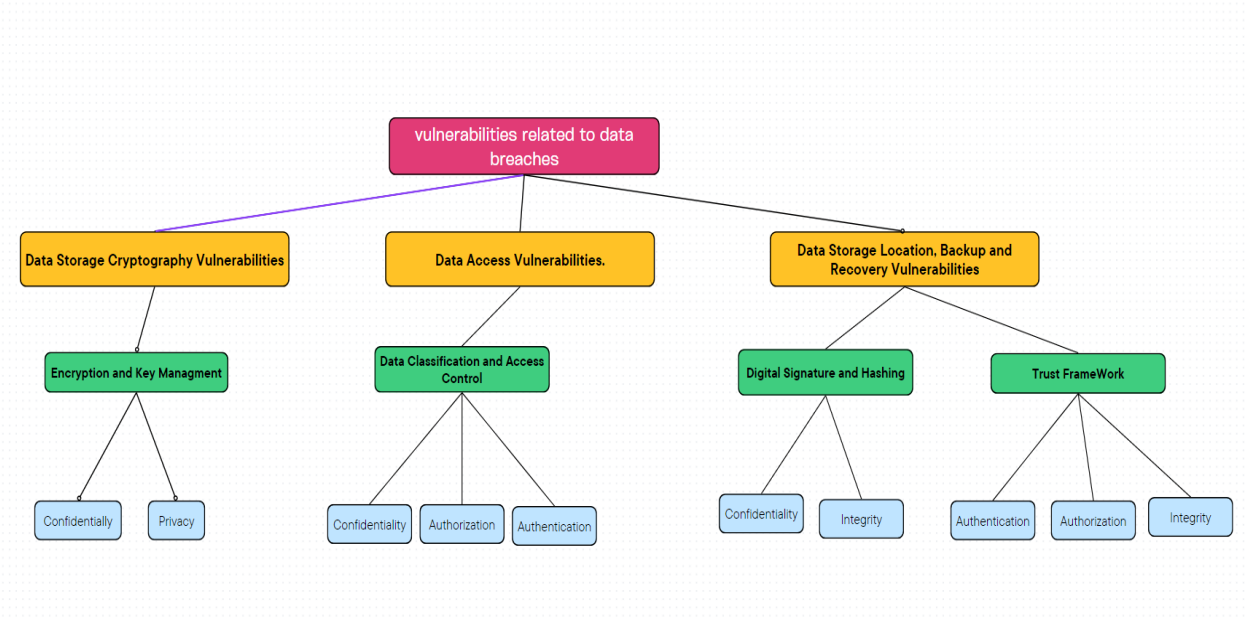
Digital signature Private key : after the client encrypt the data with the public key and send the data to the CSP with the public key so if the CSP wants to do any operations on the data he can but without be able to understand the data . by side the public key the client (who encrypt the data with the public key) a private key is created which get kept with the client to decrypt the data after doing operations on it.

Hash function or hashing: A one-way algorithm that converts input data of any size (a file, text, image, etc.) to an array of numbers and letters of a fixed length. Examples: MD5 and SHA.

So both Digital Signature and Hashing provide data confidentiality and integrity.

And there is a lot of Security countermeasures methods used such as : virtual trusted platform module (VTPM) ,Trusted cloud computing platform (TCCP) ,Identity and access management (IAM) including Single-sign-on(SSO) and Multifactor authentication (MFA) and Session management , ClearBox , NIST , Secure Data Deletion (SoK) ,and other methods.

4-Flowchart :



So since our proposal covers the three vulnerabilities : Data Storage Cryptography , Data Access , and Data Storage Location , Backup and Recovery , we give this flow chart to summarize our security strategy . First we identify the three vulnerabilities , then connect the related countermeasure that is implemented to mitigate the vulnerability . Finally , connect the security requirement that the implemented countermeasure covers.

References :

- **Amazon AWS Website.**
- **Wikipedia.**
- **Cloud Security Alliance (CSA).**
- **The course Slides (Dr. Ruba Awadallah COMP4381 Slides).**
- **Microsoft Support Web page.**