Data Security Issues in Cloud Computing

Y. V. Lokeswari
AP / CSE
SSN College of Engineering

Data Security Issues

- When multiple organizations share resources there is a risk of data misuse.
- So, to avoid risk it is necessary to secure data repositories and also the data that involves storage, transit or process.
- Protection of data is the most important challenges in cloud computing.
- To enhance the security in cloud computing, it is important to provide authentication, authorization and access control for data stored in cloud.

Data Security Issues

- **Confidentiality**
  - Top vulnerabilities are to be checked to ensure that data is protected from any attacks.
  - So security test has to be done to protect data from malicious user such as Cross-site Scripting, Access Control mechanisms etc..,.
- **Integrity**
  - To provide security to the client data, thin clients are used where only few resources are available.
  - Users should not store their personal data such as passwords so that integrity can be assured.
- **Availability**
  - Availability is the most important issue in several organizations facing downtime as a major issue.
  - It depends on the agreement between vendor and the client.

Data Security Issues

- ***Locality***
  - In cloud computing, the data is distributed over the number of regions and to find the location of data is difficult.
  - When the data is moved to different geographic locations the laws governing on that data can also change. So there is an issue of compliance and data privacy laws in cloud computing.
  - Customers should know their data location and it is to be intimated by the service provider

Data Security Issues

- ***Integrity***
  - The system should maintain security such that data can be only modified by the authorized person.
  - In cloud based environment, data integrity must be maintained correctly to avoid the data lost. In general every transactions in cloud computing should follow ACID Properties to preserver data integrity.
- ***Confidentiality***
  - Data is stored on remote servers by the cloud users and content such as data, videos etc.., can be stored with the single or multi cloud providers.
  - When data is stored in the remote server, data confidentiality is one of the important requirements.
  - To maintain confidentiality data understanding and its classification, users should be aware of which data is stored in cloud and its accessibility

Data Security Issues

- ***Breaches***
  - Data Breaches is another important security issue to be concentrated in cloud.
  - Since large data from various users are stored in the cloud, there is a possibility of malicious user entering the cloud such that the entire cloud environment is prone to a high value attack.
  - A breach can occur due to various accidental transmission issues or due to insider attack.

Data Security Issues

- ***Access***
  - Data access mainly refers to the data security policies. In an organization, the employees will be given access to the section of data based on their company security policies.
  - The same data cannot be accessed by the other employee working in the same organization.
  - Various encryption techniques and key management mechanisms are used to ensure that data are shared only with the valid users.
  - The key is distributed only to the authorized parties using various key distribution mechanisms.

Data Security Issues

- ***Segregation***
  - One the major characteristics of cloud computing is multi-tenancy.
  - Since multi-tenancy allows to store data by multiple users on cloud servers there is a possibility of data intrusion.
  - By injecting a client code or by using any application, data can be intruded.
  - So there is a necessity to store data separately from the remaining customer's data.
  - Vulnerabilities with data segregation can be detected or found out using the tests such as SQL injection aws, Data validation and insecure storage

Data Security Issues

- ***Storage***
  - The data stored in virtual machines have many issues one such issue is reliability of data storage.
  - Virtual machines needs to be stored in a physical infrastructure which may cause security risk.
- ***Data Center Operation***
  - In case of data transfer bottlenecks and disaster, organizations using cloud computing applications needs to protect the user's data without any loss.
  - If data is not managed properly, then there is an issue of data storage and data access.
  - In case of disaster, the cloud providers are responsible for the loss of data.

Solutions to Data Security Challenges

- Encryption is suggested as a better solution to secure information. Before storing data in cloud server it is better to encrypt data.
- Data Owner can give permission to particular group member such that data can be easily accessed by them.
- A data security model comprises of authentication, data encryption and data integrity, data recovery, user protection has to be designed to improve the data security over cloud.
- Before uploading data into the cloud the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged.
- Calculate the hash of the file before uploading to cloud servers will ensure that the data is not altered.
- RSA based data integrity check can be provided by combining identity based cryptography and RSA Signature

Solutions to Data Security Challenges

- SaaS ensures that there must be clear boundaries both at the physical level and application level to segregate data from different users.
- Distributed access control architecture can be used for access management in cloud computing.
- To identify unauthorized users, using of credential or attributed based policies are better.
- Fine grained access control mechanism enables the owner to delegate most of computation intensive tasks to cloud servers without disclosing the data contents.
- Network based intrusion prevention system is used to detect threats in real-time.
- To compute large files with different sizes and to address remote data security RSA based storage security method can be used.

Solution for each Data Security Issue

- **Confidentiality : Authorization & Encryption**
- **Integrity : Hash and RSA based Signatures**
- **Availability: Strict SLOs & SLAs**
- ***Locality : Customers should know their data location***
- ***Breaches : Intrusion Detection and Prevention System***
- ***Access: Fine- grained Access Control Policies and Credentials***
- ***Segregation: Clear boundaries for Physical and application level***
- ***Storage : RSA based storage security***
- ***Data Center Operation : Backup data before outsourcing to cloud***

References

- Rao, R. Velumadhava, and K. Selvamani. “Data Security Challenges and Its Solutions in Cloud Computing”. International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014). *Procedia Computer Science* 48 (2015): 204-209.