SNS COLLEGE OF TECHNOLOGY

(An Autonomous Institution)

Re-accredited by NAAC with A+ grade, Accredited by NBA(CSE, IT, ECE, EEE & Mechanical)

Approvedy by AICTE, New Delhi, Recognized by UGC, Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER APPLICATIONS

COURSE	UNIT V	TOPIC	Semester
23CAE717 Cloud Computing	**Security in the Cloud**	Data Security – Application Security – Virtual Machine Security	II Semester / I MCA

DATA SECURITY

- Primary and challenging issue
- Data are outsourced, user relived from the burden of storage and maintenance
- Data are scattered around the different physical locations
- Security issues in virtualization
- Data segregation
- Physical security in data center
- Cloud storage security

DATA SECURITY

- **Data Integrity**
  - protecting data from unauthorized deletion, modification, or fabrication
- **Data Confidentiality**
  - important for private or confidential data in the cloud
  - Authentication and access control strategies are used to ensure data confidentiality.
- **Data Availability**
  - Recovery mechanism, simplified audit mechanism
- **Data Privacy**
  - Sensitive data

DATA SECURITY

- Data security model must ensure
- Data must be encrypted automatically
- Use a strong encryption algorithm
- Algorithm must be fast to retrieve data
- Use strong authentication
- Ensure file integrity

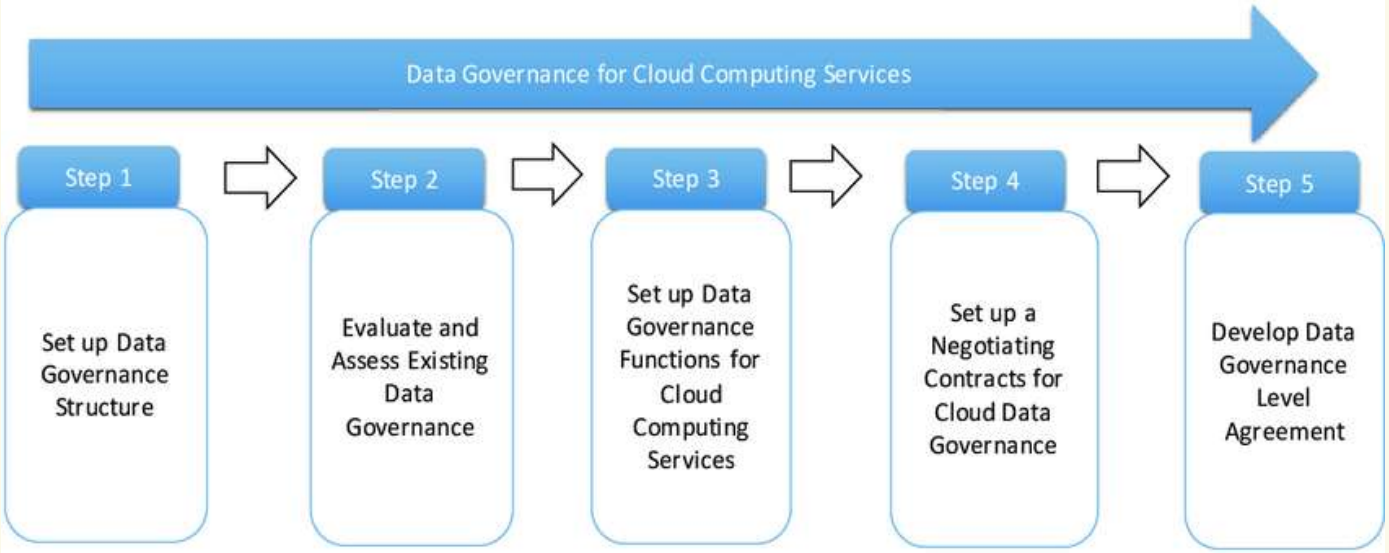
DATA SECURITY TECHNIQUES

- Data masking
- Secure logic migration and execution
- Data traceability
- Authentication and identity
- Algorithm must be fast to retrieve data
- Use strong authentication
- Ensure file integrity

DATA GOVERNANCE

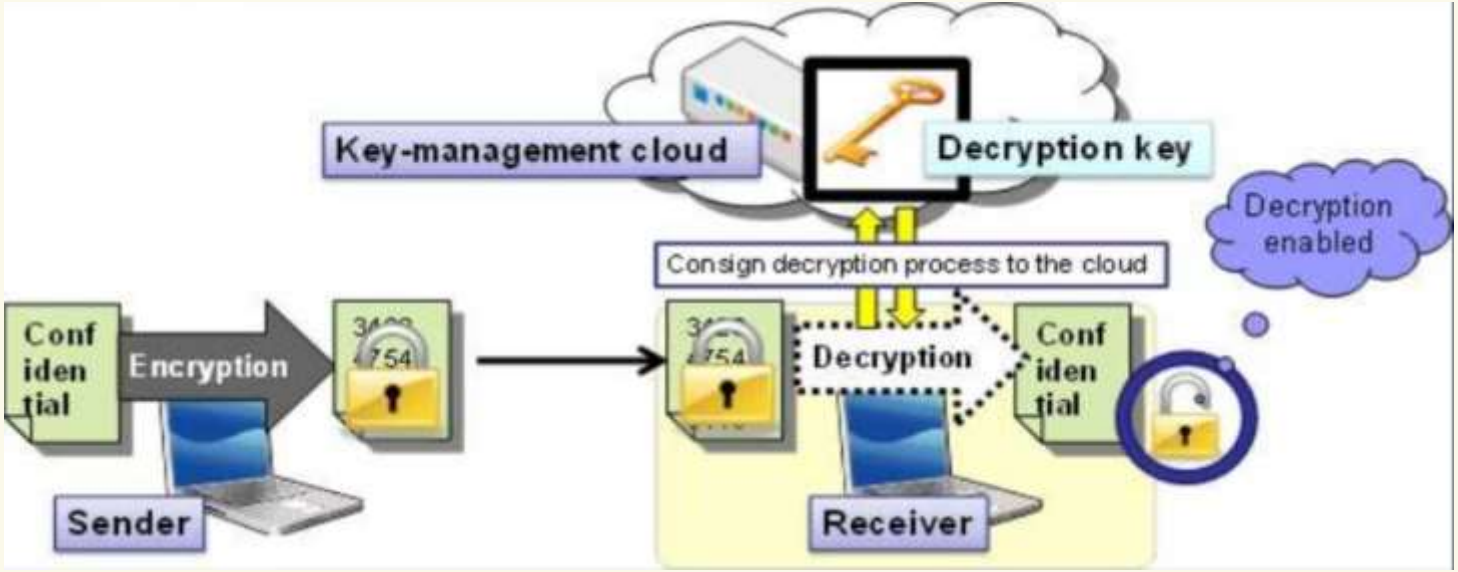
- Data governance framework to ensure the privacy, availability, integrity and overall security of data in different cloud models.
- It should include
  - Data inventory
  - Data classification
  - Data analysis (business intelligence)
  - Data protection
  - Data privacy
  - Data retention/recovery/discovery
  - Data destruction

DATA GOVERNANCE FRAMEWORK



OTP Authentication

OTP Authentication



Application Security - Types

- Identity based access
  - Using username and password
- Role based access
  - Like administrator, developer etc…
- Key based access
  - End user provided with key, stored in database in encryption form
- Claim based access
  - Using live ID like google ID, facebook ID

Application Security - Types

Hidden field manipulation	Certain fields are hidden in the web-site and it's used by the developers. Hacker can easily modify on the web pag	Avoid putting parameters into a query string
Dos Attack	Services used by the authorized user unable to be used by them.	Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks. Preventive tools are Firewalls,Switches,Routers
DDoS	DDoS attack results in making the service unavailable to the authorized.	Preventive tools are firewalls, Switches, Routers, Application front-end hardware, IPS based Prevention, etc
Google Hacking:-	Google search engine Best option for the hacker to access the sensitive information	Prevent sharing of any sensitive information Software solution such as Web Vulnerability Scanner
SQL injection	Malicious code is inserted into a standard SQL code and gain unauthorized access to a database	Avoiding the usage of dynamically generated SQL in the code
Cross site Scripting attak attacks	Inject the malicious scripts into web contents.	Various techniques to detect the security flaws like: Active Content Filtering, Content Based Data Leakage Prevention Technology

VM SECURITY - ISSUES

- collective measures, procedures &processes to ensure the protection of virtual environment
- A single system/VM attacked during scaling cause destruction to virtual environment
  - Resource attacks
  - Data attacks
  - DoS attacks
  - Backdoor

VM SECURITY - ISSUES

- Vulnerability of the underlying OS
- Sharing of files and data between the guest and the host
- Resource allocation
- Target Usage
- Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection on VM

VM Security - Types of Attacks

- **Service Provider Attacks**
  - attacker has physical access to the Cloud hardware, may run malicious code to damage VMs
- **Hypervisor Attacks**
  - program running in one VM can get root access to the host machine is called VM Escape
  - Cloud customer can lease a guest VM to install a malicious guest OS, which attacks hypervisor
- **VM Attacks**
  - deploy a software or application that stops VMs from using extra resources unless authorized

VM SECURITY - TYPES

❑ Guest Image Security

- Image files must be scanned for the detecting viruses, worms, spyware and rootkits
- use of filters, virus scanners and rootkit detectors to provide
- protection against potentially compromised images
- protect the backup VM images cryptographic techniques to be used
- Checkpoint attacks can be prevented by encrypting the checkpoint files

References

- Kai Hwang, Geoffrey C Fox, Jack G Dongarra, “Distributed and Cloud Computing, From Parallel Processing to the Internet of Things”, Morgan Kaufmann Publishers, 2012
- James E. Smith, Ravi Nair, “Virtual Machines: Versatile Platforms for Systems and Processes”, Elsevier/Morgan Kaufmann, 2005.
- Kumar Saurabh, “Cloud Computing – insights into New-Era Infrastructure”, Wiley India,2011.
- Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, TMH, 2009.
- John W.Rittinghouse and James F.Ransome, “Cloud Computing: Implementation, Management, and Security”, CRC Press, 201