(ISC)²

SECURITY CONGRESS 2018

ENRICH
ENABLE
EXCEL

congress.isc2.org

#ISC2Congress

Protect Cloud Data from Prying Eyes!

Dr. Sarbari Gupta, CISSP, CISA

Agenda

- **Background**
  - ***Why Store Data in the Cloud?***
  - ***Cloud Storage - Uncertainties and Concerns***
  - ***Security Responsibility in Different Cloud Models***
  - ***Applying Cryptography to Cloud Services***
- **Cryptographic Key Management (KM)**
  - ***Life Cycle Operations***
  - ***Design Choices***
  - ***Documentation***
- **Design of a KM Solution for Cloud Data Encryption**
  - ***Define Solution Requirements***
  - ***Analyze Cloud Service Options***
  - ***Cloud KM Challenges***
  - ***Strategies and Best Practices***
- **Wrap-Up**
  - ***Summary***
  - ***Contact Information***

Why Store Data in the Cloud?

- **Staggering volumes of data (files, posts, messages, images, videos) being created daily**
  - ***Cloud Storage is a practical and viable option***

- **Cloud Value/Benefits**
  - ***Cost Effective***
  - ***Highly Scalable***
  - ***Easily Accessible***
  - ***Security Features***

- **Drawbacks/Concerns**
  - ***Security and Privacy***
  - ***Performance and Availability***
  - ***Poor Visibility into Cloud Operations***

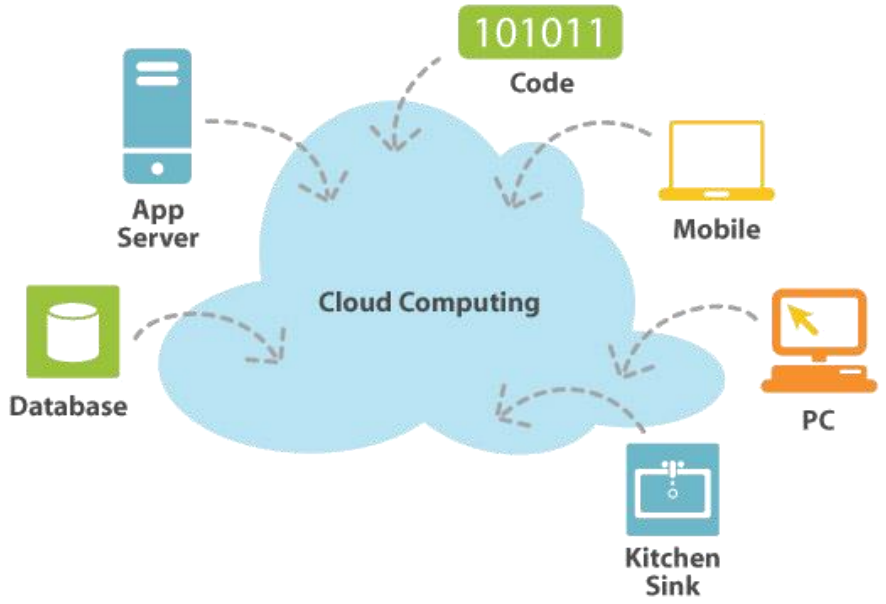
Cloud Storage – Uncertainties and Concerns

- **Data Storage**
  - ***Where does my data reside?***
  - ***Is my data co-resident with other users' data?***
  - ***Is my data encrypted at rest?***
- **Communication**
  - ***How does my CSP know who I am?***
  - ***How is the cloud connection protected?***
- **Administration**
  - ***Who administers the Cloud Infrastructure?***
  - ***Who has access to my data? My activities?***
- **Cryptographic Key Management**
  - ***Where and how are keys: Generated? Stored?***
  - ***How are keys: Distributed? Protected?***
  - ***How are keys and data recovered if lost?***
  - ***When and how are keys destroyed?***

Cloud Service Provider (CSP) - Models

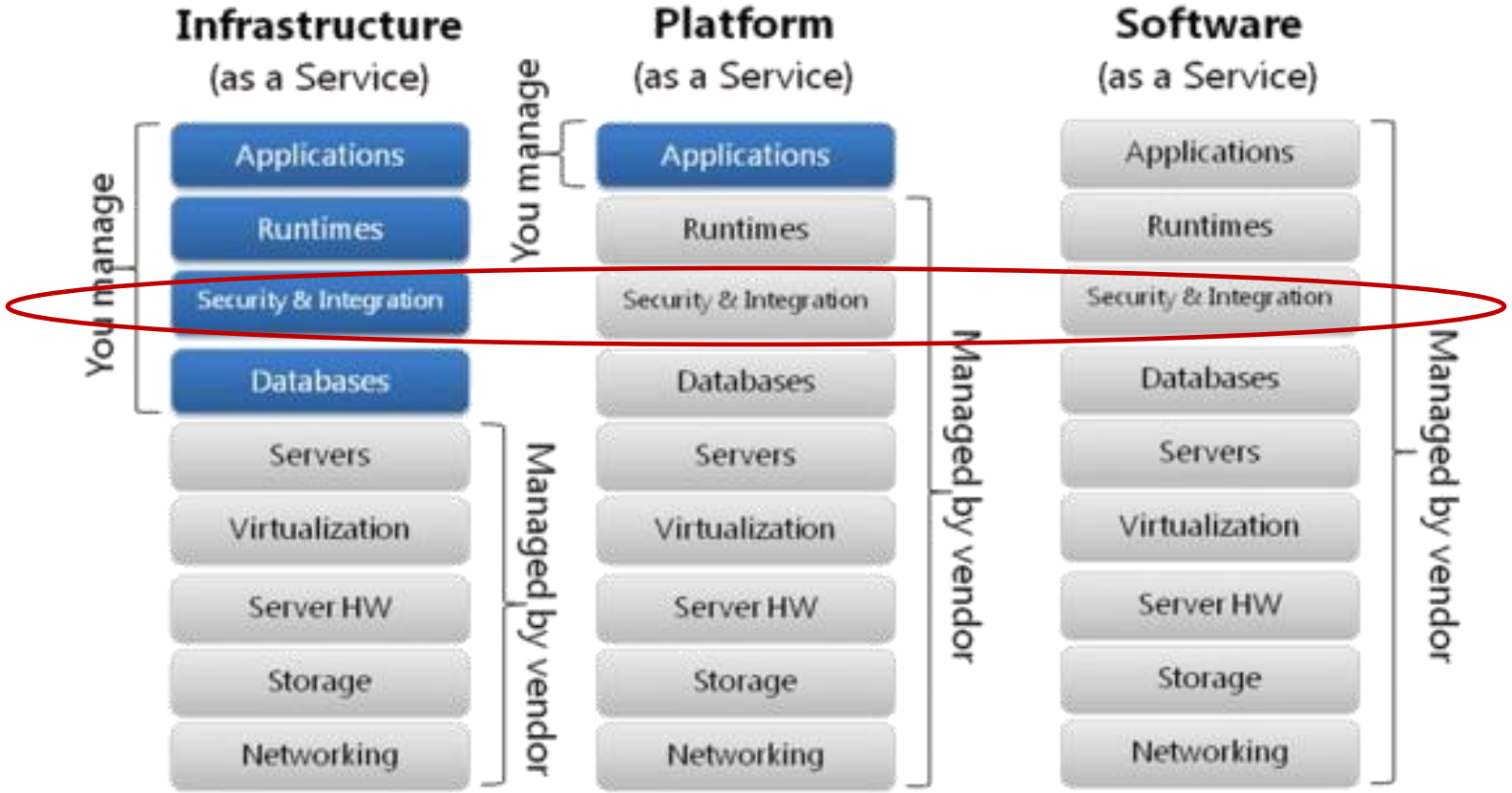
- **Cloud Service Models**
  - ***Software as a Service (SaaS) - Access to applications and services hosted in cloud***
  - ***Platform as a Service (PaaS) - Building blocks to rapidly develop/host cloud applications***
  - ***Infrastructure as a Service (Iaas) - Networked access to processing power, storage***

- **Cloud Deployment Models**
  - ***Public Cloud***
  - ***Private Cloud***
  - ***Community Cloud***
  - ***Hybrid Cloud***



Not all Clouds are created equal!

Security Responsibility in Cloud Service Models



- **SAAS** allows users to run online applications. Off-the-shelf applications are accessed over the Internet. The vendors own the applications and the users pay a fixed subscription fees.
- **PAAS** allows users to create their own cloud applications. Basically, provides an environment and set of tools to allow the creation of new web applications.
- **IAAS** allows users to run any applications they want to on cloud hardware of their choice. Existing applications can be run on the vendor's cloud hardware, potentially replacing a company's data center infrastructure.

Courtesy of CIO Research Council (CRC)

Protecting Cloud Services using Cryptography

- **Supports strong remote authentication**
  - ***Regular users (1- or 2-factor)***
  - ***Administrators (2-factor)***
- **Implements strong communication protocols**
  - ***Between user (browser) and cloud (SSL/TLS)***
- **Provides data confidentiality**
  - ***From Cloud administrators***
  - ***From Cloud co-tenants***
  - ***From Hackers***
- **Supports data integrity**
  - ***Tamper-detection of critical data through MACs and digital signatures***
- **Strengthens Audit Log Management**
  - ***Signed and time-stamped audit logs***

Encryption of Cloud Data at Rest (I)

- **SaaS Model**: CSP controls and implements encryption
  - ***Pros:***
    - Transparent to User
    - Scalable
    - Protection from Hackers
  - ***Cons:***
    - No control over strength of encryption
    - Data accessible to Cloud Admins

- **PaaS Model**: CSP provides encryption tools; User selects options and configurations
  - ***Pros:***
    - Some control over strength of encryption
    - Scalable
    - Protection from Hackers
  - ***Cons:***
    - More complex for User
    - Data accessible to Cloud Admins

Encryption of Cloud Data at Rest (II)

- **IaaS Model (Option 1): CSP provides encryption infrastructure (crypto services); User configures**
  - ***Pros:***
    - Full control over strength of encryption
    - Use of virtual Hardware/Software Security Modules
    - Keys may be stored separately from encrypted data
    - Protection from Hackers
  - ***Cons:***
    - Very complex for User
    - Data accessible to Cloud Admins

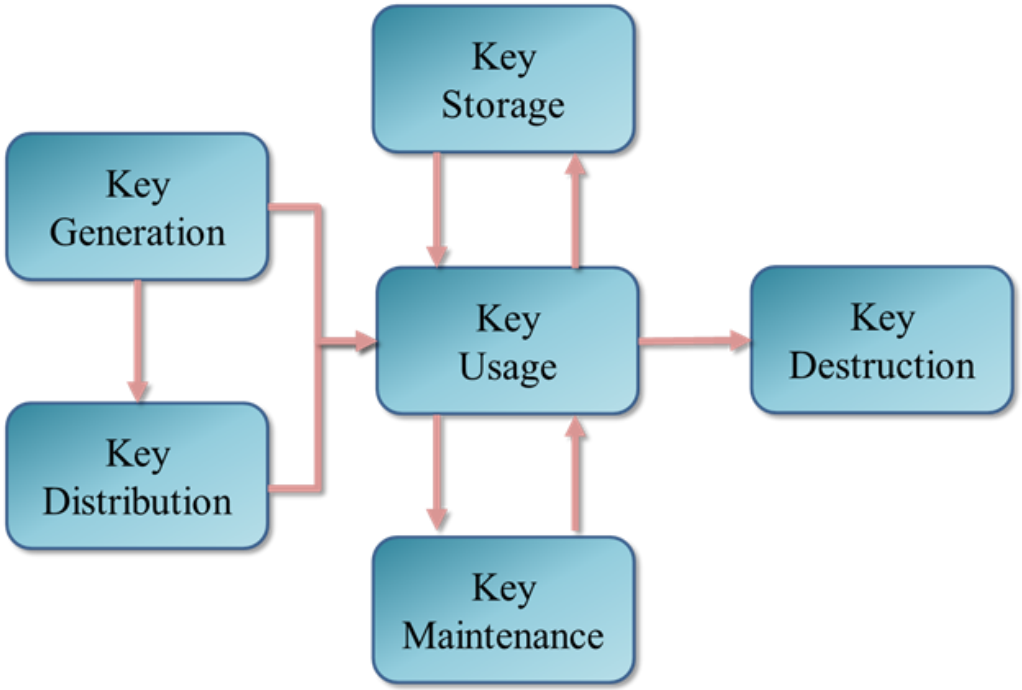
- **IaaS Model (Option 2): CSP provides storage; User encrypts using local tools**
  - ***Pros:***
    - Complete control over encryption tools/mechanisms
    - Keys can be stored separated from encrypted data
    - Data not accessible to Cloud Admins
  - ***Cons:***
    - Expensive and complex for User
    - Full responsibility for key management on User

Cryptographic Key Management

- **Key Management (KM)**
  - ***Encompasses the sum total of parameters and operations related to sustaining the key through its lifecycle***
  - ***KM design choices impact the functionality, performance and security of the overall solution***

Cryptographic Key Lifecycle Operations

- **Key Generation**
  - ***Creation of new cryptographic key***
- **Key Distribution**
  - ***Making key available to authorized users***
- **Key Usage**
  - ***Applying key for security operations***
- **Key Storage**
  - ***Saving key for future use***
- **Key Maintenance**
  - ***Operations to ensure key is ready for use (e.g. renewal, recovery)***
- **Key Destruction**
  - ***Terminating ability to use key***



Key Management Solution Design Choices (I)

- **Key Generation**
  - ***Key type (symmetric/asymmetric), algorithms, key strength, crypto-period, key parameters, hardware or software crypto module, source of entropy, etc.***
- **Key Distribution**
  - ***How exchanged, distributed and established, how protected in transit, how entities are authenticated, etc.***
- **Key Usage**
  - ***Granularity and volume of data to be protected, who has access to key, crypto module used for operations, how protected during and after use, etc.***

Key Management System Design Choices (II)

- **Key Storage**
  - ***Where stored, proximity to encrypted data, how protected, access control, auditability, etc.***
- **Key Maintenance**
  - ***What keys need to be recovered, who needs to recover keys, how quickly, how long keys need to be recoverable, how key recovery is audited, whether multi-party approvals are needed, etc.***
- **Key Destruction**
  - ***When destroyed, how destroyed, auditability, etc.***

Key Management Solution Documentation

- **Key Management Policy (KMP)**
  - ***Defines the objectives of the key management infrastructure***
- **Key Management Practices Statement (KMPS)**
  - ***Describes the parameters and processes selected to meet the objectives within the KMP***
- **The KMP/KMPS needs to address the essential key management lifecycle states and all of the key management design choices made.**

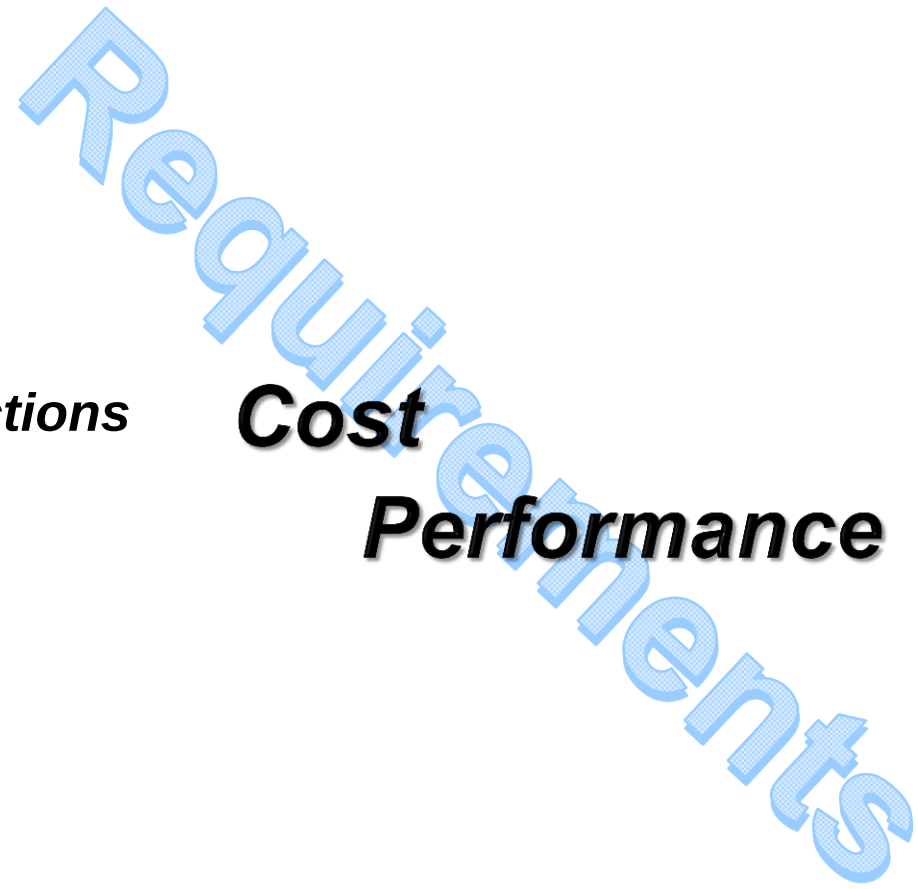
Cloud Storage KM Solution Design

Define Solution Requirements (I)

- **Functional Considerations**
  - ***Type(s) of Data to be Stored***
    - **Business or Personal Data**
    - **Transactional or Storage Data**
    - **Volume of Data**
    - **Value / Criticality /Sensitivity of Data**
    - **Modularity of the Data**
  - ***Duration of Storage and Availability***
  - ***Profile of Users***
    - **Types of Users (Public, Customers, Org Users, Family/Friends)**
    - **Platforms used by Target Users**

Define Solution Requirements (II)

- **Cost Considerations**
  - ***Initial Implementation Budget***
  - ***Expansion Cost per Unit***
- **Performance Considerations**
  - ***Average Data Size for Storage/Retrieval Actions***
  - ***Frequency of Access***
  - ***Serialized versus Simultaneous Access***
  - ***Round Trip Time***
  - ***Availability (e.g. five nines)***



Define Solution Requirements (III)

- **Security and Privacy Considerations**
  - ***Security Risk Category (High/Moderate/Low)***
  - ***Privacy protection***
  - ***Confidentiality, Integrity and Availability***
  - ***Applicable Threats Agents based on Industry/Sector***
  - ***Applicable Attacks***

- **Compliance Considerations**
  - ***Security Authorization/Accreditation***
  - ***Privacy and Data Protection***
  - ***Location of Cloud Servers (e.g., servers located in US)***
  - ***Citizenship and Clearance of Cloud Administrators***
  - ***Types of Cryptography (e.g., FIPS approved)***

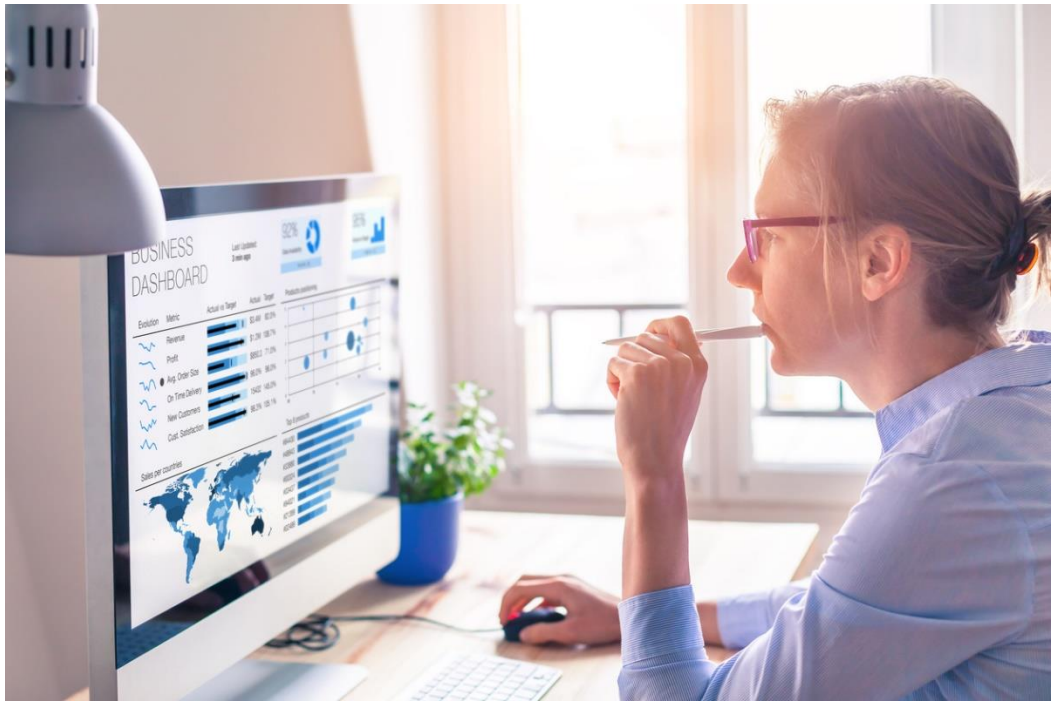
Requirements

Security, Privacy

Compliance

Analyze Cloud Service Options

- **Cloud Service Models**
  - ***IaaS/PaaS/SaaS***
- **Cost of Service**
- **Security Options**
  - ***Available Crypto Services***
  - ***Ease of Use***
  - ***Flexibility***
  - ***Configurability)***
- **Accreditation of Cloud Services**
  - ***FedRAMP***
- **Known Vulnerabilities and Limitations**



Cloud Key Management Challenges

- **Multiple Layers of Privileged Users**
  - ***Administrators for one of more CSPs***
  - ***Administrators for Cloud KM Solution***
- **Multi-Tenancy**
  - ***Co-Tenancy on VMs / Virtual Storage***
  - ***Co-Tenancy on Hardware***
- **Authentication of Remote Users**
- **Hardware Versus Software Cryptography**
  - ***Availability and Complexity of Hardware Crypto in the Cloud***
- **Availability of Data and Keys**
  - ***Making Keys Available to Users***

Cloud Data Encryption – Strategies and Best Practices

- Implement Strong (2-factor) User Authentication
- Use Approved Algorithms
- Use Validated Cryptographic (HW/SW) Modules
- Minimize Data to be Encrypted
- Minimize Impact of Key Compromise by Use of Multiple Keys
- Separate Encrypted Data from Keys
- Implement Key Recovery Mechanism (for Lost/Corrupted Key)
- Pre-think Long Term Availability of Encrypted Data

Summary

- **Data stored in cloud has higher exposure**
  - ***Larger set of insider and outsider threats***
- **Cryptography is essential in partitioning and protecting cloud data**
  - ***Cryptographic Key management (KM) defines strength and ease of use***
- **Design of a Cloud KM Solution is a balance of priorities**
  - ***Requirements***
  - ***Cost***
  - ***Security, Privacy***
  - ***Compliance***
- **Commonsense KM design choices and strategies can effectively *Protect Cloud Data from Prying Eyes***

Contact Information

- **Contact Info: Dr. Sarbari Gupta – Electrosoft**
  - ***Email: sarbari@electrosoft-inc.com;***
  - ***Phone: 703-437-9451 ext 12***
  - ***LinkedIn: http://www.linkedin.com/profile/view?id=8759633***

- **Electrosoft**
  - ***Web: http://www.electrosoft-inc.com***
  - ***LinkedIn: https://www.linkedin.com/company/electrosoft/***
  - ***Twitter: https://twitter.com/Electrosoft_Inc***
  - ***HQ: 1893 Metro Center Drive, Suite 228***
    Reston VA 22066
  - ***Tel: (703) 437-9451***
  - ***FAX: (703) 437-9452***