Protect Cloud Data from Prying Eyes!

Dr. Sarbari Gupta

President and CEO, Electrosoft

ISACA Cloud Computing Conference 2019

September 18, 2019

Holiday Inn Rosslyn, VA

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
FAX: (703) 437-9452

Security in the Cloud?

**"Are you sure our data is secure on the cloud?
I just saw my spreadsheet on the weather channel!"**

Agenda

- **Background**
  - ***Why Store Data in the Cloud?***
  - ***Cloud Storage – Questions and Uncertainties***
  - ***Security Responsibility in Cloud Service Models***
- **Protecting Cloud Services using Cryptography**
  - ***Cryptographic Key Lifecycle Operations***
  - ***Encryption of Cloud Data at Rest***
- **Cloud Data Encryption Solution Design**
  - ***Define Solution Requirements***
  - ***Analyze Cloud Service Options***
  - ***Identify Residual Risk***
  - ***Implement Controls to Mitigate Risk***
- **Wrap-Up**

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***

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

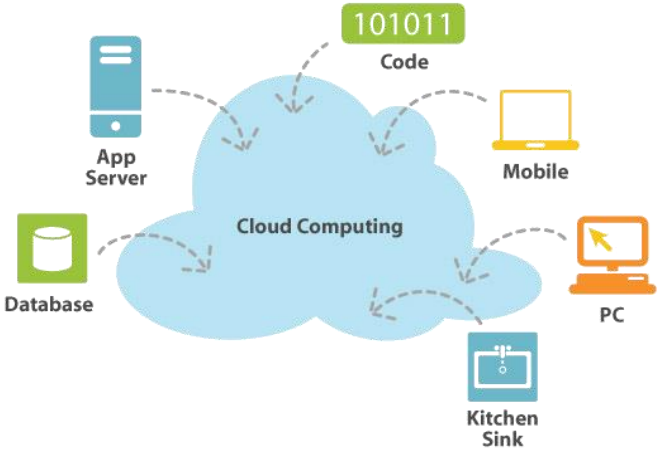
Cloud Storage – Questions and Uncertainties

- **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

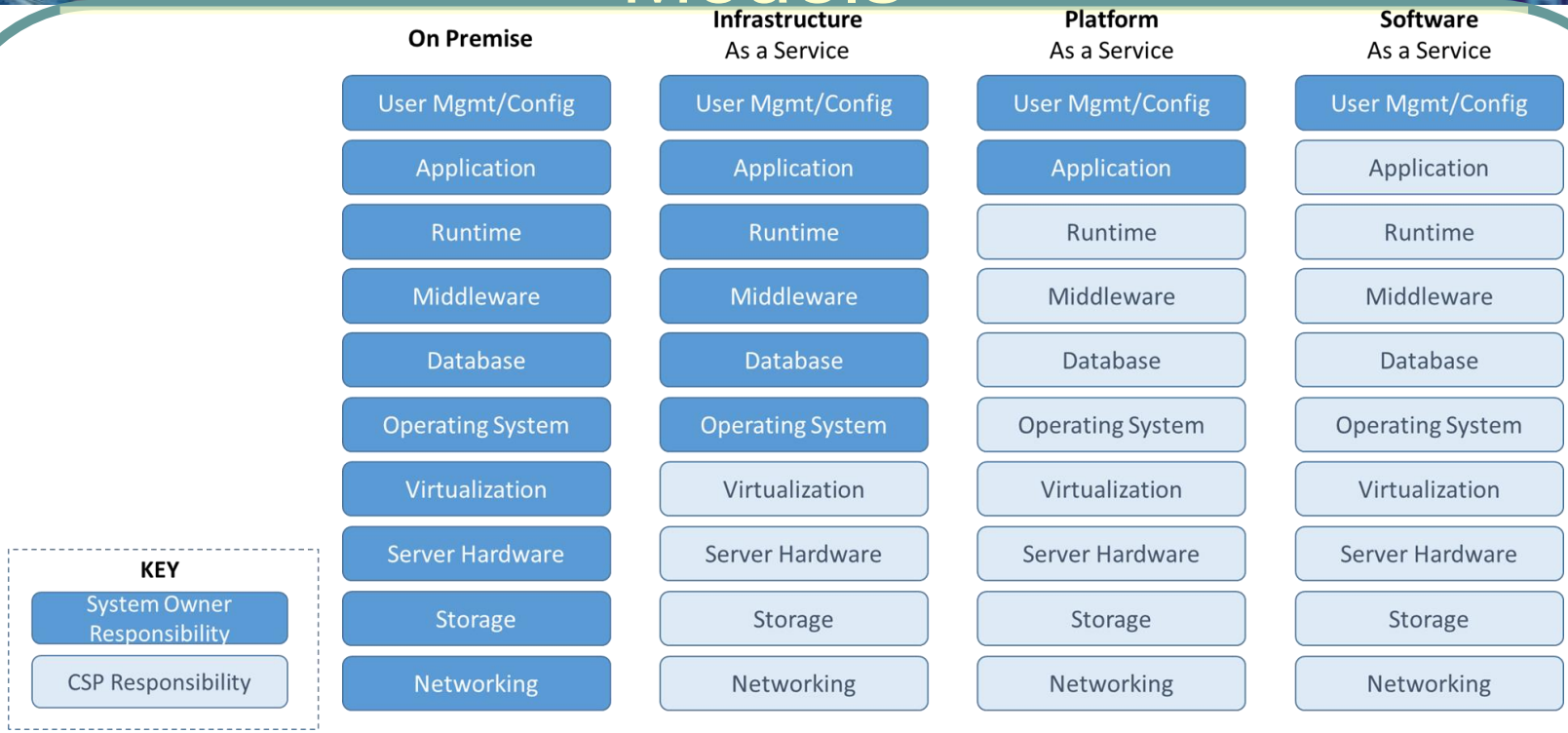
- **Cloud Service Models**
  - ***Software as a Service (SaaS) - Access to applications and services hosted in cloud***
  - ***Platform as a Service (PaaS) - Building blocks to rapidly develop/host cloud applications***
  - ***Infrastructure as a Service (Iaas) - Networked access to processing power,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

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



Not all Clouds are created equal!

Security Responsibility in Cloud Service Models



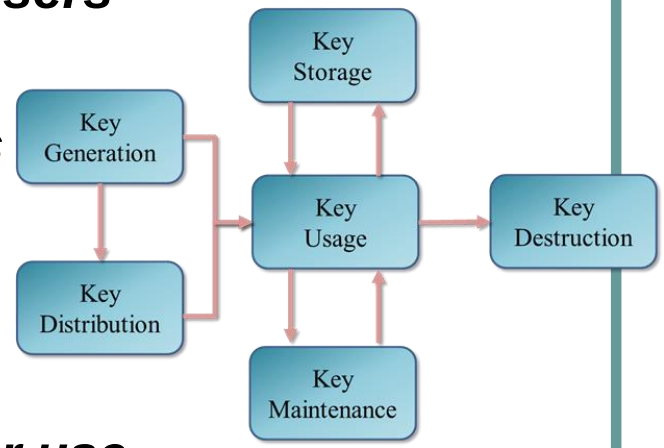
- **SAAS** allows users to run online applications. Off-the-shelf applications are accessed over the Internet. The CSP owns the application and users pay subscription fees.
- **PAAS** allows users to create their own cloud applications. The CSP provides an environment and set of tools to allow the creation of new web applications.
- **IAAS** allows users to run new and existing applications on cloud infrastructure provided by the CSP.

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***

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*



Encryption of Cloud Data at Rest (I)

- **SaaS Model**: CSP controls and implements encryption
  - ***Pros:***
    - Transparent to User
    - Scalable
    - Provides Protection from Hackers
  - ***Cons:***
    - No control over strength of encryption
    - User Data may be accessible to Cloud Admins
- **PaaS Model**: CSP provides encryption tools; User selects options and configurations
  - ***Pros:***
    - Some control over strength of encryption
    - Scalable
    - Provides Protection from Hackers
  - ***Cons:***
    - More complex for User
    - User Data may be 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
    - Provides Protection from Hackers
  - ***Cons:***
    - Very complex for User
    - User Data may still be accessible to Cloud Admins
- **IaaS Model (Option 2): CSP provides storage; User encrypts using separate tools/services**
  - ***Pros:***
    - Complete control over encryption tools/mechanisms
    - Keys can be stored separated from encrypted data
    - User Data is not accessible to Cloud Admins
  - ***Cons:***
    - Expensive and complex for User
    - User has full responsibility for Cryptographic Key Management

Cloud Data Encryption Solution Design

1. Define Solution Requirements
2. Analyze Cloud Service Options
3. Identify Residual Risk
4. Implement Controls to Mitigate Risk

1. 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**

1. 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)***

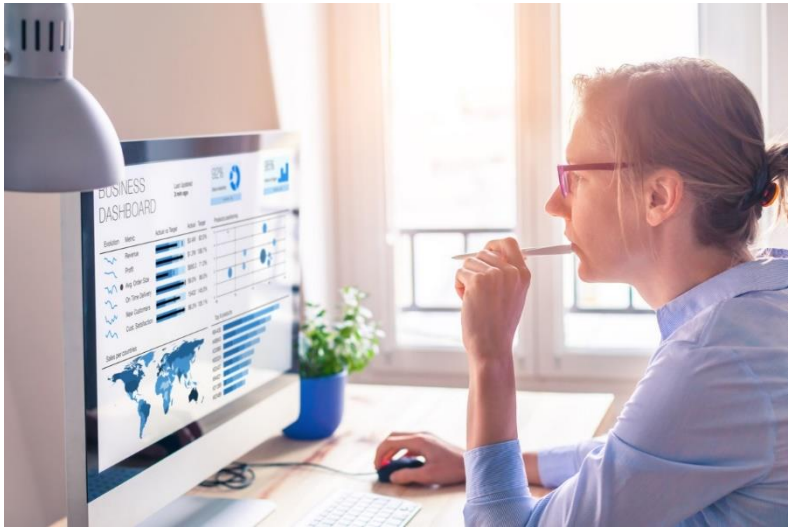
1. Define Solution Requirements (III)

- **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)***

2. 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**

3. Identify Residual Risk

- **Cloud Data Encryption – Typical 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 (all Users are Remote!)***
  - ***Hardware Versus Software Cryptography***
    - Availability and Complexity of Hardware Crypto in the Cloud
  - ***Availability of Data and Keys***
    - Making Keys Available to Users

4. Implement Controls to Mitigate Risk

- **Cloud Data Encryption – Strategies and Best Practices**
  - ***Implement Strong (2-factor) User Authentication***
  - ***Use Approved Cryptographic 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**
- **Design of a Cloud Data Encryption Solution is a balance of priorities**
  - ***Requirements***
  - ***Cost***
  - ***Security, Privacy***
  - ***Compliance***
- **Commonsense design choices and strategies can effectively *Protect Cloud Data from Prying Eyes!***

Questions/Comments

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