CLOUD SERVICES

S Thenmozhi

Department of Computer Applications

CLOUD SERVICES

Cloud Application Design

S Thenmozhi
Department of Computer Applications

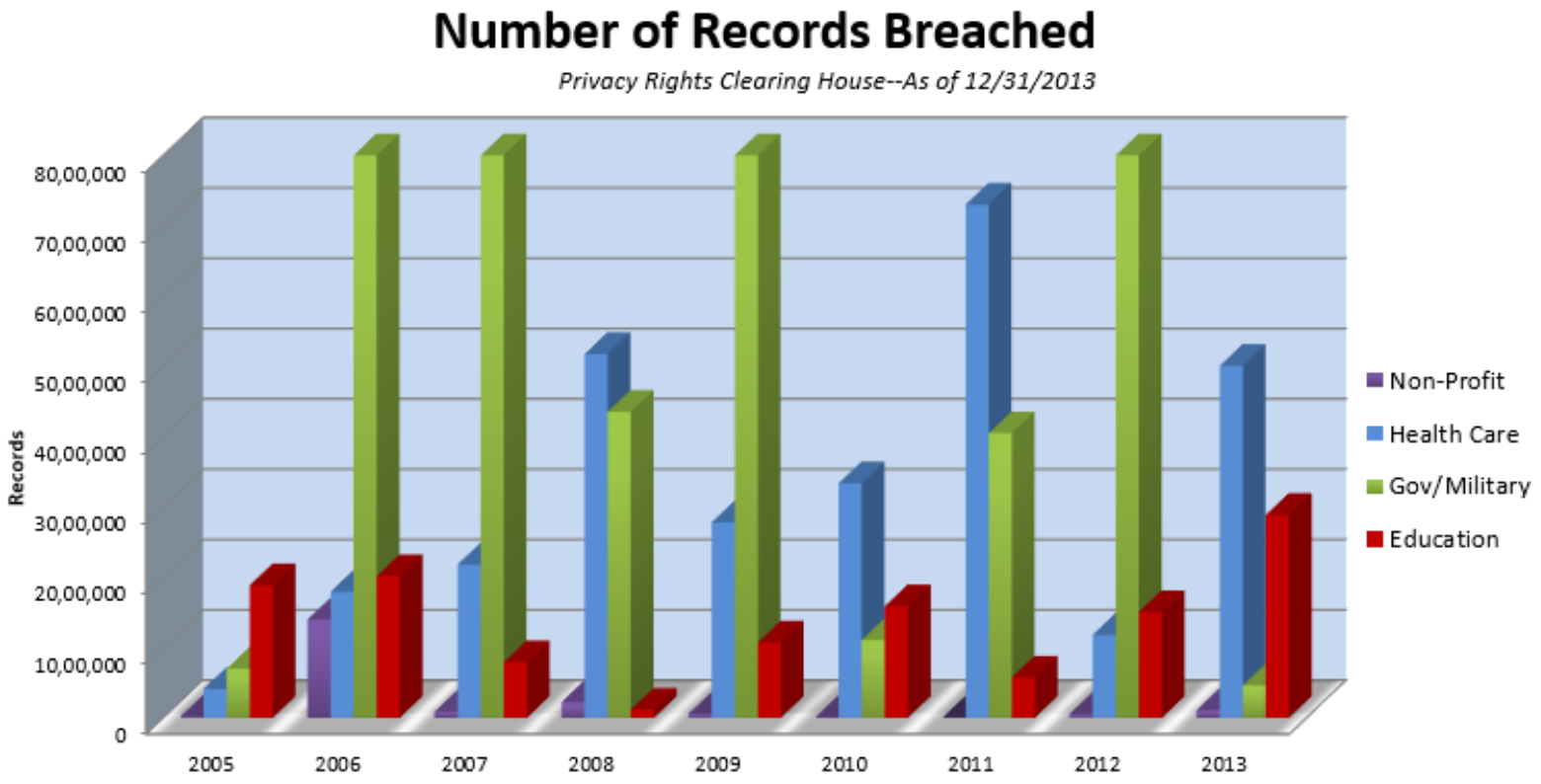
CLOUD SERVICES

Cloud Security Requirements

- Challenges of Cloud Computing
  - Shared Infrastructure
  - Rapid movement of the servers
  - Workload in the infrastructure

CLOUD SERVICES

Cloud Security Requirements



Cloud Security Requirements

- The cloud infrastructure can be partitioned as **Physical and Virtual infrastructure**
- Based on these factors security can fall into
  - **Physical Security**
  - **Virtual Security**
- Basic Requirements
  - Confidentiality – no unauthorised access to functions of the cloud
  - Integrity – cloud system should be protected against tampering by implanting viruses or stealing of passwords etc.
  - Availability – No denial of service for the legitimate users.

Cloud Security Requirements

- Additional requirements
  - Cost-effectiveness
  - Reliability and performance
- **Physical Security**
  - Data center should be secured from the physical threats
  - Measures to avoid penetration from intruders and from natural calamities
  - Better: multi-layered security
    - Central monitoring and control with dedicated staff
    - Separate monitoring for each threat
    - Training of staff in response to threat situation
    - Manual or automated backups for the systems
    - Secure access to the facility

Cloud Security Requirements

- **Virtual Security**
  - **Cloud Time Service** – all data centres are synchronized to same clock. **Network Time Protocol** can be implemented which synchronizes the clock on a computer to a reference source on internet.
  - **Identity Management** – foundation for confidentiality, integrity and availability
    - Scale to number of users found in the cloud system
    - Ensure single identity and single sign on across multiple types of system
    - IM should satisfy the legal and policy requirements (deleting of users and services)
    - Maintain historical records for future investigation.

Cloud Security Requirements

- **Access Management**
  - Allow implementation of multi-factor authentication for sensitive operations
  - Restrict access to cloud management personnel
  - Disallow shared accounts
  - Implement white-listing of IP addresses for remote administrative actions
- **Break Glass procedures** – alarming system for the data centers
- **Key Management** – encrypting the key and ensure isolation to access.
  - Specific methods for generation, assignment, revocation and archiving of keys
  - Procedures for recovering from compromised keys

Cloud Security Requirements

- **Auditing**
  - Auditing is required for all system and network components.
  - Audit should capture all security-related events
  - Audit log should be centrally maintained
  - Stripped down logs should be made available to the cloud customers
  - Assistance to the customers for analysing the logs
- **Security Monitoring**
  - Cloud-wide intrusion and anomaly detection system
  - Should be installed both on the network as well as the host nodes.

Cloud Security Requirements

- **Security Testing**
  - Test all software before deployment
  - Test beds should be isolated from deployment and production

PES UNIVERSITY

CELEBRATING 50 YEARS

THANK YOU

S Thenmozhi

Department of Computer Applications

thenmozhis@pes.edu

+91 80 6666 3333 Extn 393