

The cloud is as secure as  
you want it to be...

Debashis Banerjee

*Yahoo! India*

2<sup>nd</sup> IndicThreads.com Conference On  
Cloud Computing

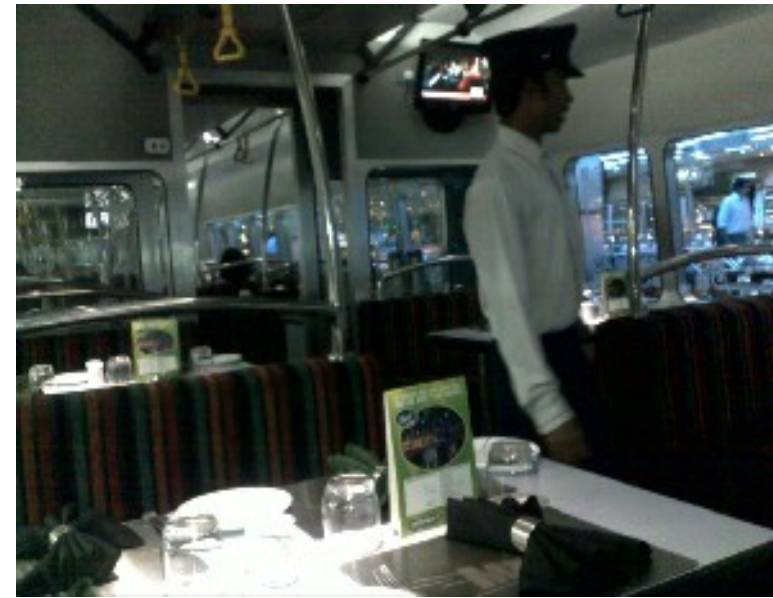
3,4 JUNE 2011



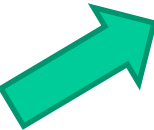
PUNE, INDIA



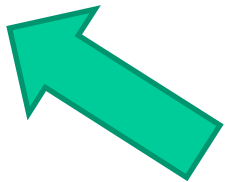
My son's first day at school



Catered Food on my anniversary party



Money in my bank



My seat on the plane



# Today's Journey

Refresher to  
the cloud

Multi device  
Cloud  
Security -  
Mobiles

Ensuring  
your cloud  
is secure

OTP, SMS  
based multi  
Factor auth

Public, Private  
and Hybrid  
Cloud Security

Secure  
APIs



# Cloud Computing - Refresher

- Key aspects of using the cloud: Elasticity, On Demand, Multi Tenancy, Multi Device, Ability to measure Service
- Type of Clouds - Public Clouds, Private Clouds, Hybrid Clouds, Community/Partner Clouds
- Deployment models : SaaS , PaaS , IaaS

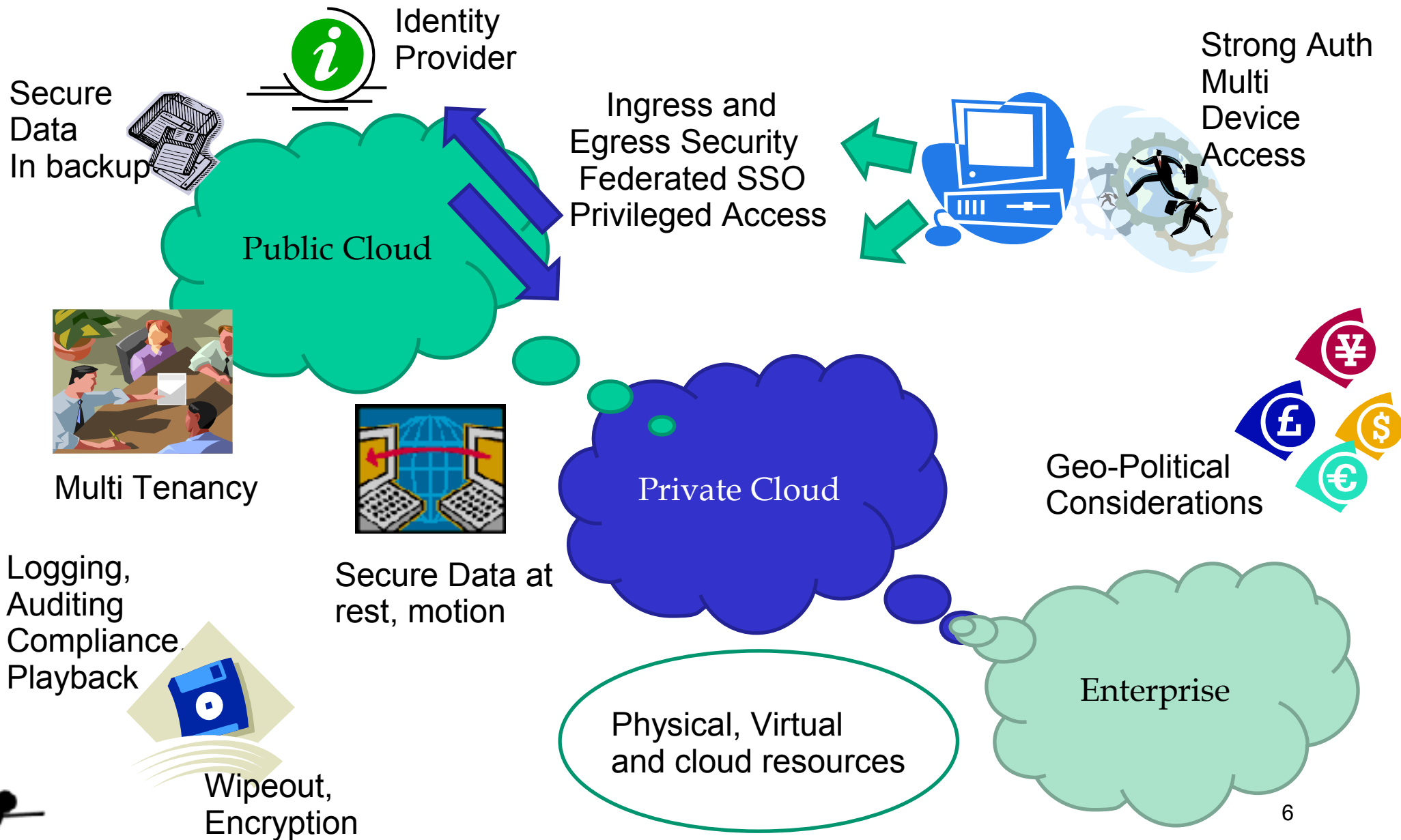


# Key questions to ask about security?

- What do you need to protect? Who are your users?
- Where does your data live? How does it flow? What geographies?
- What are your compliance, logging needs?
- Is there SSO and Identity management in place?
- Do you have a mix of physical , virtual, cloud?
- Who pays for security? Who is accountable for what aspect of
- security?
- How do you react if a security breach takes place?



# Ensuring your cloud solution is secure



# Security in Public Cloud Deployments

- Strong Identity management
- Privileged Account Management
- Place the appropriate type of data in the cloud
- Have access to compliance and logging , auditing
- Being a public cloud ensure you impose where you data can or cannot travel
- Wipeout policies
- Ensure you are comfortable with the security of multi tenancy
- Secure keys





# Security in the Private & Hybrid Cloud

## Private:

- Design such that there is scope to move to a hybrid model
- Impose SSO

## Hybrid:

- Segregate your data between clouds
- Use SAML and ensure appropriate enterprise credentials are within the perimeter
- Have your Federation set up correctly. Enable SSO.
- Ensuring enterprise credentials do not travel into the cloud





# Multi Device Cloud Security – Mobile Phones

- The mobile device as an extension of the Cloud
- Secure Mobile Apps on the cloud.
- On Cloud and On Device virus scanning
- Seamless policies for mobile devices
- Credential life cycle management
- Secure Roaming Users



# Multi Factor Auth – OTPs, SMS based

Use OTPs effectively to protect your data access to the cloud

GoldKey

Multi Factor Auth – AWS/Gemalto

2 Factor Auth using SMS

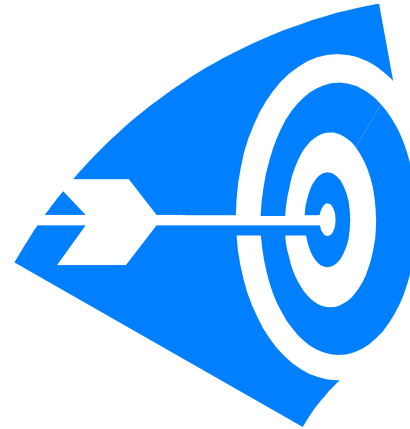


Image: <http://commons.wikimedia.org/wiki/File:RSA-SecurID-Tokens.jpg>



# Some APIs useful in cloud security

- Safe Browsing API
- VM Safe APIs



# In Conclusion

- Cloud Security is critical to succeed in the cloud
- Choose Private / Public / Hybrid cloud & SaaS / PaaS / IaaS
- Identity & Privileged User Management
- Compliance, Certification and Logging
- Consider Multi Device Scenarios
- Use Strong Authentication



## Remember your questions about security to

1. Your child's school
2. Your anniversary party caterers
3. Your airline
4. Your bank



And you won't go  
wrong with  
the Cloud Security !!!!

