





# CONTROLLING DATA IN THE CLOUD: OUTSOURCING COMPUTATION WITHOUT OUTSOURCING CONTROL

**Paper By:**

Chow, R; Golle, P; Jakobsson, M; Shai, E; Staddon, J From PARC  
&  
Masuoka, R And Mollina From Fujitsu Laboratories Of America


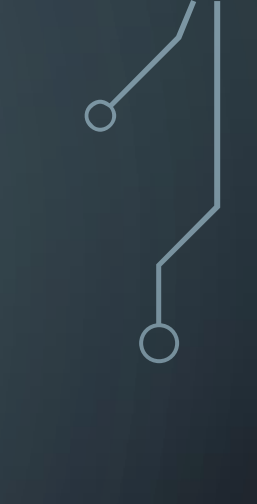
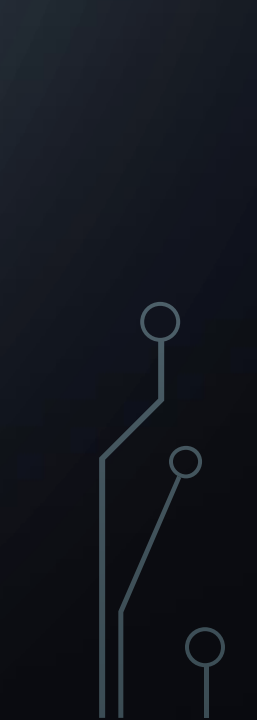
2009 ACM WORKSHOP ON CLOUD COMPUTING SECURITY (CCSW 2009)

**Presented By Talal Basaif**

CAP 6135 – SPRING 2014



# AGENDA

- Introduction
  - Current Fear of the Clouds
  - New problems that will arise later
  - New directions to solve some issues
- 
- 
- 

# INTRODUCTION

- Cloud computing is one of desirable technology for its cost-effective and reliability.
- However, several persistent concerns that might compromise the adoption of cloud computing as a new IT procurement model.
- The paper characterized the cloud computing issues and their impacts.
- The paper argue the concerns by highlighting some solution and researches on trusted computing and encryption can be advantageous from business intelligence point of view.

# FEAR OF THE CLOUD

- Study from IDC in 2008 Cloud Service User Survey of IT executive cite security is major challenge for enterprise to adopt cloud computing.
- The paper Categorized security concerns into:
  - Traditional Security
  - Availability
  - Third-Party data control.

# TRADITIONAL SECURITY

- It involves computer and network intrusions attacks threatening in the cloud.
- Cloud providers arguing this concern that their security measures and process are more mature and tested.
- Also, another argument by Jericho said that administering information by a third party is easier if companies worried from insider threat by enforcing security via contracts.

# TRADITIONAL SECURITY CONCERNS (CONT.)

- VM Level Attack due to potential vulnerabilities in the hypervisor. Vendor like Third Bridge mitigate this issue through monitoring and firewalls.
- Cloud provider vulnerability on platform level like SQL injection or cross-site scripting vulnerability. Example vendor like IBM has a solution by repositioning its Rational AppScan tool to scan for vulnerabilities in web services as a cloud security service.
- Phishing cloud provider and cloud customer.
- Expanded network attack surface as the cloud user should protect its infrastructure connecting to the cloud by using firewalls.
- Merging and extending enterprise authentication and authorization framework to the cloud to include cloud resource.
- Difficulty of cloud Forensic investigations.

# AVAILABILITY CONCERNS

- Service uptime as cloud providers claim that their server uptime compares well with the availability of user data. However, certain critical applications cannot be handled by third party cloud as it would be collapse like running billing information application for utility company, SAP's CEO.
- Despite of high availability claim, there are many Single point of failure and attack that affect the availability of the services in the cloud.
- Computational integrity assurance, as the enterprise can assure that the cloud provider will run the hosted application and return valid result.



# THIRD-PARTY DATA CONTROL

- The legal implications of data being held by a third party are complex and not well defined and there will be a lack of control and transparency.
- So some companies built private cloud to avoid these issues, for example: Scalent System's CEO said:

*“What I find as CEO of a software company in this space, Scalent Systems, is that most enterprises have a hard time trusting external clouds for their proprietary and high-availability systems. They are instead building internal “clouds”, or “utilities” to serve their internal customers in a more controlled way.”*

# THIRD-PARTY DATA CONTROL CONCERNS

- Cloud provider diligent response in required time frame in any case or legal actions.
- Lack of control can complicate auditing as it might be difficult to satisfy auditors that enterprise data is safe and secure and not viewed by others as enterprise doesn't have control over the cloud.
- Enterprise Information might be abused by cloud provider which compromise confidentiality and privacy of classified information.
  - Example Google Gmail and Google Apps, corporate users of these services are concerned about confidentiality and availability of their data. However, some consumer decided that the dangers of placing their data in the cloud were outweighed by the value they received.

## THIRD-PARTY DATA CONTROL CONCERNS (cont.)

- Data Lock-in with proprietary format which might complicate process when cloud provider changes.
  - For Example: Coghead as its cloud platform shutdown force customer to rewrite their applications to run on a different platform. So Standardizing cloud computing can solve this issue.
- Transitive nature where some cloud provider use subcontractors where cloud user doesn't have any control over subcontractors whenever failure happen from subcontractor side.

# NEW PROBLEMS

- With widespread adoption of cloud computing more problem can arise like:
  - Cheap data and data analysis
  - Cost effective defense of availability
  - Increased authentication demands

# NEW PROBLEMS: CHEAP DATA AND DATA ANALYSIS

- As the amount of user data collected in the cloud arise, cloud provider can abuse it for advertisement and analysis which impact the privacy of users' data.
- Also, attackers will have huge and centralized database for analysis and database mining.
- Example:
  - Google collect and analyze customers data for advertising network.
  - EPIC enterprise called to shutdown all its google applications in the cloud until appropriate privacy insurance in place.

# NEW PROBLEM: COST-EFFECTIVE DEFENSE OF AVAILABILITY

- Availability should be highly considered against any disruption activities for many reason like political conflicts like the cyber attack on Lithuania.
- The damages are not only related to the losses of productivity, but extend to losses due to the degraded trust in the infrastructure and costly backup measures.
- Also, cloud computing considered as single point of failure. So it is important to develop methods for high availability and for recovery after attack. So cloud will operate on the basis of losses minimization and required service level.

# NEW PROBLEM: INCREASED AUTHENTICATION DEMANDS

- The development of cloud computing allow the use of the thin client rather than a license purchased software installed in the client side to authenticate users to use cloud applications.
- This approach has couple advantages as:
  - Made software piracy difficult.
  - Centralized monitoring.
  - Prevent spread of sensitive data – on untrustworthy clients.
  - Managed security for the thin client by the cloud provider.
- As dependency on the cloud increased mobility importance increased. However, Lesser reliance on specific user machines (Thin Client) increase the threat of phishing and other issues aimed on stealing access credentials.

# NEW DIRECTIONS

- The paper provide some tools limiting cloud provider control over users' data ,which is the main issue, and enabling all cloud users to benefit from cloud data through enhanced business intelligence. Such as:
  - Information-Centric Security.
  - High-Assurance Remote Server Attestation.
  - Privacy-Enhanced Business Intelligence.



# NEW DIRECTION: INFORMATION-CENTRIC SECURITY

- To extend control of data in the cloud, author propose shifting from protecting data from outside to protect data from within where the data and information protecting itself.
- It required intelligence where the data should be self-describing and defending.
- Data should be encrypted and packed with use policy. When it is accessed, it consult its policy and attempt to created a secure environment and reveal itself if the environment is verified as trustworthy.
- It is an extension to finer, stronger and more usable data protection.

# NEW DIRECTIONS: HIGH-ASSURANCE REMOTE SERVER ATTESTATION

- Lack of transparency in the cloud discourage business to move their data to cloud for auditing purpose to ensure that data is not leaked or abused and have accurate audit information for data processing events.
- A promising approach to address this issue based on trusted computing by installing trusted monitoring tool to monitor and audit operations of the cloud server and provide proof of compliance to data owner.
- To produce proof of compliance the code of the monitor is signed so when it is received by data owner , it can be verified that the correct code is run and the cloud server has complied with access control policy.

# NEW DIRECTIONS: PRIVACY BUSINESS INTELLIGENCE

- Encrypting all cloud data will retain control of data by customer. However, encryption will limit data use specially with searching and indexing.
- The paper suggested some stat-of-the-art cryptography tools that allow operations and computation on cipher-text, example:
  - Searchable Encryption or Predicate encryption which allow data owner to compute by using his secret key. This key encode a search query then the cloud use the encoded search query to return matched data and information.
  - Holomorphic Encryption or Private Information Retrieval it performs computation on encrypted data without decrypting. (dig more in ref)

# NEW DIRECTIONS: PRIVACY BUSINESS INTELLIGENCE (cont.)

- Cryptography also can address other security problem beside privacy such as proof of retrievability in storage server which show a compact proof of correctly storing all of clients data.
- Still more research is needed for sufficient and practical cryptographic tool as it will enable cloud user to collaborated data and information in controlled manner, and encrypted data enable anomaly detection which is valuable for business intelligence.

# CONCLUSION

- Cloud computing is becoming popular now and it will impact software development as it did on hardware.
- Adoption of cloud computing is relying on overcoming the fears of the cloud.
- To overcome the fears of loss control of data in the cloud, the paper suggested to extend control from enterprise to the cloud by using trusted computing and cryptographic technique.
- Also, it relates to issues and abuses that will arise from reliance on cloud computing and how to mitigate them.



THANK YOU

Q & A