New Threats of cloud computing and solutions

Bin Yu

Student ID: 250***

Submit Date: 2013/5/31

Structure of the presentation

- What is this research about ?
- What are the research problems in this area ?
- What researchers have done in this area ?
- How is this research carried out ?
- What are the novelties about this research ?
- What are the contributions and limitations ?

What is this research about?

- This study addresses the **new** security threats in Cloud Computing and proposes possible solutions.
- This study aims to examine contemporary and historical perspectives from industry and academia, and concentrate on CC security issues that are fundamentally new or intractable like multi-party trust considerations and the ensuing needs for mutual audit ability. After study this threats possible solutions will be proposed.

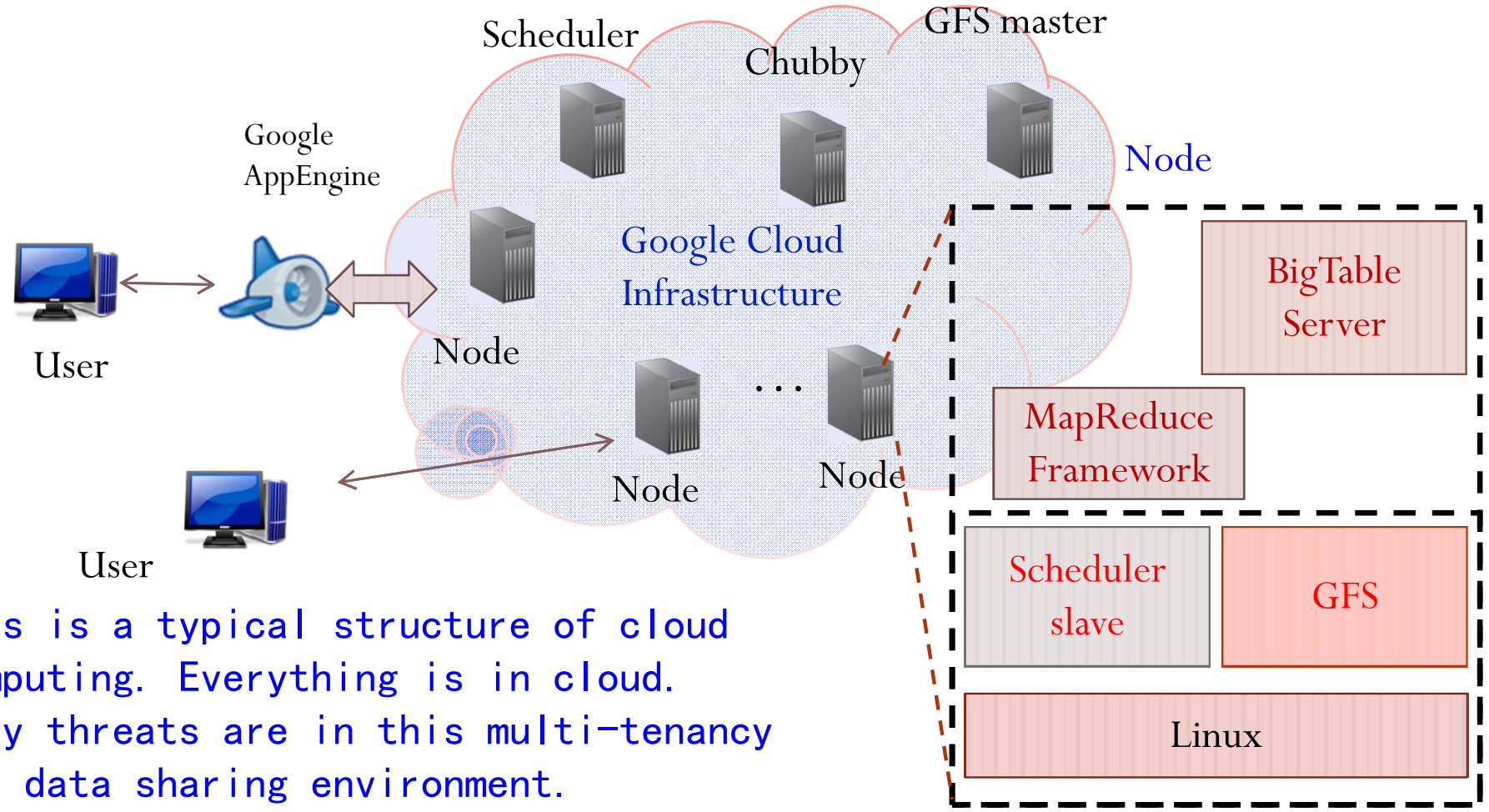
What are the research problems in this area?

- The new security threats in cloud computing environment are quite different from the traditional network threats. Many of the traditional incidents described as “cloud security” in fact just reflect web application and data-hosting problems. As cloud computing offers the most freedom of resources utilization to the cloud users, these new threats are difficult to detected, classified and managed. Also as many resources are shared in the clouding environment, the threats are more destructive. These new security threats issues have emerged as arguably the most significant barrier to faster and more widespread adoption of cloud computing.

What are the research problems in this area? (CONT)

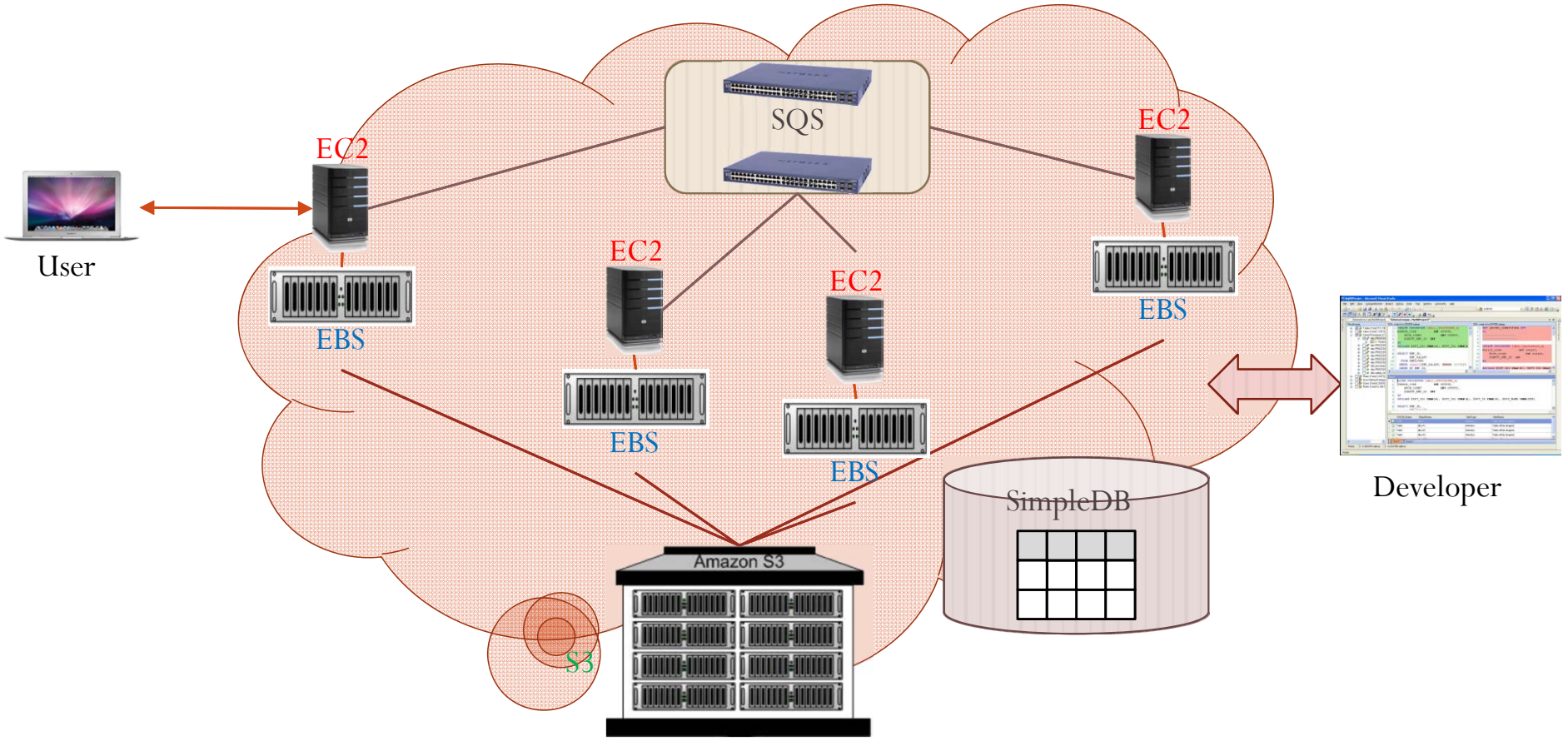
- Security threats cases
  - Amazon EC2 spam blacklist incident.
  - FBI raid on Texas database centers in April 2009.
  - Few security mechanism in OpenStack.

What are the research problems in this area? (CONT)



This is a typical structure of cloud computing. Everything is in cloud. Many threats are in this multi-tenancy and data sharing environment.

What are the research problems in this area? (CONT)



SQS: Simple Queue Service
EC2: Running Instance of Virtual Machines
EBS: Elastic Block Service, Providing the Block Interface, Storing Virtual Machine Images
S3: Simple Storage Service, SOAP, Object Interface
SimpleDB: Simplified Database

What are the research problems in this area? (CONT)

- Many of the new threats comes from the cloud structure itself. It is hard to identify. Because traditional security rules are trying to separate the whole system into trust and entrust area (Firewall). The cloud computing environment often regarded as trust area. It more like our immune system that has not obvious reaction on cancer. Because cancer is the functionality disorder of our cells themselves.

What researchers have done in this area?

- Firesmith provides taxonomy of security sub-factors that can be used as a basis for organizing and identifying different security threats. Many published papers focus on the security issues like web security , data outsourcing and assurance and virtual machines securities . Subashini and Kavitha address the new threats in cloud computing, but not investigate these threats in a certain depth.

How is this research carried out?

- We will use general cloud stack (IAAS,PAAS,SAAS) to investigate the cloud system find the threats in different level.
- According to the general cloud stack we will study these threats classify and manage them
- According to different threats and the different security levels, security models will be built.
- According to the security models, possible solutions will be proposed.

What are the novelties about this research?

- First, this paper regards data and software are not the only assets worth protecting. Activity patterns also need to be protected.
- This paper proposes a trust chain in cloud computing threats model.
- We built the security threats model, we also take participants behavior into consideration.
- This paper regards more of the new security threats come from the inner of cloud computing system compared with outer of cloud computing system.

What are the contributions and limitations?

- Contributions:
  - It is an original contribution to addressing the new threats in cloud computing and proposing the possible solutions.
  - Addresses the needs to pay more attention on flexibility and multi-tenancy in cloud computing.
  - Provides the introduction to the new issues in cloud computing which can be used for further study.

What are the contributions and limitations? (CONT)

- Limitations:
  - The general cloud stack is too rough model and not accurate enough for some threats.
  - There are no best solutions for one fixed threats. As the threats are so complicated, the solution for one threat may only solve the issues to some extent. And may bring other efficiency or security issues.

REFERENCES

- D. Firesmith, "Specifying reusable security requirements," *Journal of Object Technology*, vol. 3, pp. 61-75, 2004.

- K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 187-198, 2009,.

- J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, "Managing security of virtual machine images in a cloud environment," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 91-96 , 2009.

- S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, pp. 1-11, 2011.

- A. Aviram, S. Hu, B. Ford, and R. Gummadi, "Determinating timing channels in compute clouds," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, pp. 103-108 , 2010.