1) What is the primary lesson you took away from this paper?

This paper thought more about public cloud data security. I learned from this paper about "hourglass schemes and protocols" framework, which provide a way to tenant and end user to validate and keep track of their data on cloud. Using encryption and cryptographic mechanism, we can build a mechanism to create a trust bond between cloud provider and tenant for trustiness and honesty.

2) What do you think would be the most interesting way to extend this work?

Since author done the experiments on Amazon EC2, I would like to see to extend this work to test on other cloud providers for instance, Rackspace, Google and Microsoft Azure. Moreover, to extend this framework to make a generalized solution that will work with any cloud provider and easily migratable between cloud providers.

3) If you had to list a criticism of this paper, what would it be?

Overall, this paper gave me a first steps towards creating solutions for cloud security considering honesty and trust between cloud providers and end user, so paper was well outlined and explained problems and solutions. So I don't have much to criticize except that if author would have provided some reactions and feedback from cloud providers and customer on their solution.

4) List the 3 references that you would be most interested in reading.


[14] P. Golle, S. Jarecki, and I. Mironov. Cryptographic...


1) Technical details (approach/technique) that you found novel/ something specific you learned that you didn't know before

Since less knowledge in cryptography domain, I found complete hourglass framework solution is novel for me. Moreover, I like watermarking concept to identify data leakage, which is useful to backtrack to source of cause.

2) Could I have done this work if I had the idea why or why not?

Considering less domain knowledge of cryptography, I couldn’t have done this work, even though this work need less resources and infrastructure.

3) Is there anything I could do to repeat or validate?

I could consider validating or repeating their claim about data linkage identification based on embedding of “provenance tags in files

4) What is my best idea for follow on work that I could personally do?

Best on this idea, I could personally keep on track on how can we make a general security as services in cloud using this hourglass framework. As per my knowledge this is the first work I see for cloud security considering trust between cloud providers and end users. Both of them can validate their
work on each other. We could consider this framework as a small part of building secure hybrid cloud framework.

5) What is my best idea for follow on work that I'd like to see the authors do?

Since author tested their solution only on Amazon EC2. I would like to see if he can provide or deploy this solution on other cloud as well. In addition to this, I would like to see him to think more on how can he make this solution to become a product or one of the cloud service for cloud providers as well as end user.

6) How does this compare to the other papers we read? Most similar? How different? Other comparisons?

This paper specially targeted for public cloud domain. The author tried to create a trust and honesty model which is benefit for end user as well as cloud providers. Though it’s come under cryptography and encryption, solution's goal is different. The papers we read about cloud security, this paper more towards trust and honesty between involved entities.