



KOÇ UNIVERSITY

the perfect view



<http://www.ku.edu.tr>



PROJECT IDEAS 1: The Economics of Delivering Secure Cloud Storage Services

- Create an economic model for; Customers, Service Providers
- Show that secure cloud services are profitable for both parties
- Come up with an optimal pricing scheme
- Create a comparison method for customers (price vs. security)
- Avoid legal costs incurred due to legal issues
- For venture capitalists: Which cloud startup to fund based on prices vs. security?

(Submitted ICT-7- 2014 on April 2014)

Dr. Alptekin KUPCU

Core Research: Cryptography, Security, Privacy

Application Areas: Cloud Computation, Cloud Storage, Peer-to-Peer Systems, Electronic Cash, Electronic ID Cards, Password-based Authentication.

<http://crypto.ku.edu.tr> ; akupcu@ku.edu.tr





PROJECT IDEAS 2: Secure Mobile Cloud Storage Systems Peer-to-Peer and Energy-Efficient Secure Cloud Storage Systems

- A secure cloud storage system is a system in which there are two main parties: a client and a server. To be useful and successful, such a system needs to provide some guarantees to the client. Unfortunately, current cloud storage systems fail to provide such guarantees.
- With the emergence of the cloud computing paradigm as a way to support user demands for computing power and storage, energy consumption will most likely increase and hence there is a severe need for energy-aware solutions.
- We envisage that energy efficiency of security mechanisms for cloud storage are very significant, and benefits of peer-to-peer (P2P) network principles can be utilized in this context.
- To the best of our knowledge, *no research has been done on having a mobile, energy-efficient, and P2P secure cloud storage system*. Designing energy-efficient P2P algorithms and applications is significant and an active area of research. In this project, the main idea is to develop a secure mobile cloud storage system in which the client can challenge the storage server for a proof that her files are kept intact.

<http://crypto.ku.edu.tr> ; akupcu@ku.edu.tr





PROJECT IDEAS 3: **Fairness in the Cloud**

- Secure two-party and multi-party computation which are the leading research areas in cloud computing. But the existing systems fail to provide fairness to the participants, it is possible for one participant to obtain the result of the joint computation while others lack this knowledge
- Lastly, the techniques used by **Küpçü and Lysyanskaya** involve **advanced techniques like *electronic cash (e-cash)* and *verifiable encryption***. Transferring such techniques to these new domains will bring challenges and yet novel solutions. Their protocol, including these advanced cryptographic primitives were **implemented in a cryptographic library** [Library], and one of the goals of this project is to integrate the novel solutions developed to this library, hence enabling their use and adoption by the whole society.
- **within the context of this project include: - Peer-to-peer file sharing systems, - Dynamic agreement protocols and cloud storage systems, - Cloud computation systems, Secure two-party and multi-party computation systems**

<http://crypto.ku.edu.tr> ; akupcu@ku.edu.tr





PROJECT IDEAS 4: Instrumenting Selected Cloud Programming Model

- DesCloud, for systematic simulation of programs written for a cloud platform. DesCloud will explore on a desktop different possible scenarios a program can encounter on the cloud, and will make possible practical iterative development of cloud programs.
- As a result, there are several sources of non-determinism and uncertainty, such as creation and migration of task instances, and re-ordering of messages sent between tasks.





PROJECT IDEAS 4: Instrumenting Selected Cloud Programming Model

- DesCloud aims to help the programmer with the challenge of verifying that his program handles the uncertainties it faces on a cloud platform, and does not experience data loss or corruption, or unacceptable interruption to services.
- DesCloud will run on a desktop and will control and orchestrate different sources of uncertainty. It will allow recording, replay and systematic exploration of executions to reproduce detected errors for debugging purposes. We believe providing these capabilities as a desktop tool before actual large-scale deployment will be a valuable aid to cloud programmers.

Prof.Serdar Tasiran: stasiran@ku.edu.tr ;
<http://home.ku.edu.tr/~stasiran>



Thank you!
<http://tto.ku.edu.tr/>
tto@ku.edu.tr

