ENEE 759-L: Cloud Computing Security

Spring 2014

Instructor: Charalampos (Babis) Papamanthou

Course description:

In the age of big data, cloud computing plays a major role in processing and analyzing massive amounts of information. Services like Amazon S3 and EC2 offer easily accessible outsourced storage and computation, gradually replacing our local hard drives and desktop machines. Nevertheless, many security concerns have arisen in this new paradigm, preventing both individual users and large corporations to use cloud computing services. For example, in an untrusted cloud setting, users' data and computations can be potentially tampered with and sensitive data could be leaked to unauthorized parties.

In this class, we will study current research work (both theoretical and applied) on protocols and systems that provide security in the cloud. Most of the class will focus on reading and presenting research papers. By the end of the class the students will be expected to have a good knowledge of the current cloud computing security research landscape (i.e., most important technologies, techniques and algorithms) and to be able to contribute to both theoretical and applied research in the field.

Course prerequisites:

ENEE 641 or CMSC651 or permission by the instructor.

Topic prerequisites:

Basic knowledge of algorithms, data structures and programming.

Tentative list of topics:

1. Secure storage and memory checking
2. Advanced authenticated data structures (streaming queries, geometric queries, set queries)

3. Generalized verifiable computation
4. Provable data possession and proofs of retrievability
5. Database integrity and privacy
6. Searchable encryption
7. Oblivious algorithms
8. (Somewhat) homomorphic encryption and applications
9. Practical multiparty computation
10. Side channel attacks
11. Remote code attestation

Grading policy:
Class participation: 10%
Paper presentations: 40%
Project: 50%

Major conferences in the field:
1. ACM Conference on Computer and Communications Security (CCS)
2. ACM Workshop on Cloud Computing Security (CCSW)
3. Network and Distributed System Security Symposium (NDSS)
4. IEEE Symposium on Security and Privacy (SSP)
5. International Cryptology Conference (CRYPTO)
6. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)

Useful books:
1. Introduction to Modern Cryptography (Katz and Lindell, Chapman & Hall/CRC, 2007).
2. Introduction to Algorithms (Cormen, Leiserson, Rivest and Stein, MIT press, 2009).