Title of Pre-Conference Tutorial: Fully Homomorphic Encryption: Cryptography's Holy Grail

Theme: Information Security and Cryptography, Key Management

Duration in Hours: 3 hours

Abstract:

In the Cloud-based Data-centric world that we live in today, there is a potential threat to our privacy because of the large amount of personal data that we voluntarily or inadvertently reveal to the cloud when using different services on the web. Coupled with the proliferation of ubiquitous web-enabled computing devices and advancement in statistical and computational methods for machine intelligence, it has now become easy to draw vital inferences drawn from the data we submit, and associate to the identity of an individual - sacrificing the privacy. One of the panaceas to the problem of ensuring protection of our individual privacy is through the controlled release of our data. That is, it is tempting to infer that if submit only the encrypted data to the cloud when using web services, our individual privacy is ensured. However, this is a fallacy since without revealing the decryption key to the cloud; we cannot expect the data to be processed by the cloud – the purpose for which it was submitted in the first place.

Hence, an important question that we raise here is as follows: Is it possible to have an encryption mechanism that allows computations on encrypted data to be performed by the cloud – thus obviating the need for the sender to also submit the decryption key? Well, the answer to this question is indeed in the affirmative – resort to Homomorphic Encryption.

In this tutorial, we plan to take the audience through an excursion of the different encryption techniques viz. Symmetric key, Asymmetric key, Identity based Encryption, Attribute Based Encryption and highlight various candidate schemes therein that lack the property of Homomorphic Encryption. Then, we plan to expose the audience to a few of Homomorphic Encryption algorithms - that are additively or multiplicatively homomorphic. We illustrate the use of these algorithms in typical Cloud based applications. In the process, we also illustrate how Homomorphic Encryption goes beyond ensuring plain data security and ensures privacy of our data submitted to the cloud.