Improving security in the cloud

December 15 2011

Less and less of today's computing is done on desktop computers; cloud computing, in which operations are carried out on a network of shared, remote servers, is expected to rise as the demand for computing power increases. This raises some crucial questions about security: Can we, for instance, perform computations on data stored in 'the cloud' without letting anyone else see our information? Research carried out at the Weizmann Institute and MIT is moving us closer to the ability to work on data while it is still encrypted, giving an encrypted result that can later be securely deciphered.

Attempting computation on sensitive data stored on shared servers leaves that data exposed in ways that traditional encryption techniques can't protect against. The main problem is that to manipulate the data, it has to be first decoded. 'Until a few years ago, no one knew if the encryption needed for this sort of online security was even possible,' says Dr. Zvika Brakerski, who recently completed his Ph.D. in the group of Prof. Shafi Goldwasser of the Computer Science and Applied Mathematics Department. In 2009, however, a Ph.D. student at Stanford University named Craig Gentry provided the first demonstration of so-called fully homomorphic encryption (FHE). But the original method was extraordinarily time consuming and unwieldy, making it highly impractical. Gentry constructed his FHE system by using fairly sophisticated math, based on so-called ideal lattices, and this required him to make new and unfamiliar complexity assumptions to prove security. Gentry's use of ideal lattices seemed inherent to fully homomorphic encryption; researchers assumed that they were necessary for the server to perform such basic operations as addition and

multiplication on encrypted data.

Brakerski, together with Dr. Vinod Vaikuntanathan (who was a student of Goldwasser's at MIT), surprised the computer security world earlier this year with two recent papers in which they described several new ways of making fully homomorphic encryption more efficient. For one thing, they managed to make FHE work with much simpler arithmetic, which speeds up processing time. And a surprise discovery showed that a mathematical construct used to generate the encryption keys could be simplified without compromising security. Gentry's original ideal lattices are theoretical collections of points that can be added together – as in an ordinary lattice structure – but also multiplied. But the new research shows that the lattice does not have to be ideal, which simplifies the construction immensely. 'The fact that it worked was something like magic, and it has challenged our assumptions about the function of the ideal lattices in homomorphic encryption,' says Brakerski.

Their result promises to pave a path to applying FHE in practice. Optimized versions of the new system could be hundreds – or even thousands of times faster than Gentry's original construction. Indeed, Brakerski and Vaikuntanathan have managed to advance the theory behind fully homomorphic encryption to the point that computer engineers can begin to work on applications. These might include, for instance, securing medical information for research: A third party could perform large medical studies on encrypted medical records without having access to the individuals' information.

Provided by Weizmann Institute of Science