Abstract

Confidentiality in third party services like cloud computing has become a major concern. IT industry and government organizations are very serious about security factor in cloud computing, because its usage has reached all the way from a common man having a mobile phone to large scale business enterprises. In this paper, we present security threats in social and business applications accessing the data stored in cloud computing scenario. Also, we critically discuss homomorphic encryption and CryptDB schemes which are applicable to protect data from malicious third party service environments (cloud computing) and also from insiders for these applications. We also present empirical results of partial homomorphic encryption algorithms over one lakh 10-digit numbers, using Linux virtual machine on VirtualBox, VMPlayer and KVM. The result for four algorithms (namely Paillier, ElGamal, RSA and Benaloh) as performed on the above four different platforms are computed to show their respective overhead values as compared to plain data operations. In case of Paillier Algorithm the overhead is 17, 15, 22 and 12 times for addition operation and 278, 399,518 and 346 times for multiplication operation respectively. Similarly, in case of Elgamal algorithm 1. 72, 1. 6, 11. 7 and 8. 9 times for multiplication operation; in case of RSA algorithm 1. 79, 1. 5, 3. 48 and 1. 5 times for multiplication operation and in case of Benaloh algorithm is 5. 6, 5. 36, 5. 48 and 3. 5 times for addition operation respectively. These performances clearly indicate that these
algorithms are quite feasible enough to be used in context of social and business applications by third party service providers.
- LinkedIn passwords leaked by hackers: http://www.bbc.co.uk/news/technology-18338956
- Matt Bishop and David Wagner, "Inside Risks", November 2007/Vol. 50, No. 11

COMMUNICATIONS OF THE ACM
Applicability of Homomorphic Encryption and CryptDB in Social and Business Applications: Securing Data Stored on the Third Party Servers while Processing through Applications

J. Lieberman, National Security Aspects of the Global Migration of the U. S. Semiconductor Industry, white paper, Airland Subcommittee, US Senate Armed Services Committee, June 2003; References:

- https://hcrypt.com/scarab-library/
- "Parents: Cyber Bullying Led to Teen's Suicide: Megan Meier's Parents Now Want Measures to Protect Children Online"; ABC News 29 November 2007.
- Craig Gentry and Shai Halevi, Implementing Gentry's fully-homomorphic encryption scheme; Advances in Cryptology - EUROCRYPT 2011, pp. 129-148, 2011
- http://www.verizonenterprise.com/DBIR
- About Zero Day Exploits (http://netsecurity.about.)
Applicability of Homomorphic Encryption and CryptDB in Social and Business Applications: Securing Data Stored on the Third Party Servers while Processing through Applications


- D. Borelli. The name Edward Snowden should be sending shivers up CEO spines. Forbes, Sept. 2

Index Terms

Computer Science
Security

Keywords
Homomorphic encryption  CryptDB  Cloud Computing security  Social and Business applications