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.

References

- http://www.homelandsecuritynewswire.com
/databreaches-Compromise-nearly-8-million-medicalrecords: Data breaches compromise nearly
8 million medical records, published 1 June 2011
- http://en.m.wikipedia.org/wiki/PlayStation_Network_outage: Playstation Network
outage.
- Carlos Aguilar Melchor and Philippe Gaborit, Javier Herranz, Additively Homomorphic
- Ivan Damgard, Mads Jurik: A Generalisation, a Simplification and Some Applications of
Paillier’s Probabilistic Public-Key System Public Key Cryptography 2001:119-136
- Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari
Balakrishnan," CryptDB: Protecting Confidentiality with Encrypted Query
Processing";, SOSP&amp;apos;11, October 23-26, 2011, Cascais, Portugal
- Yin Hu, A Dissertation on"Improving the Efficiency of Homomorphic Encryption
Schemes";, May 2013
- R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and
- T. Okamoto and S. Uchiyama. A New Public-Key Cryptosystem as Secure as
Factoring. Eurocrypt 08, LNCS 1403, pp. 308-318, 1998
- http://go.worldbank.org/M1JHE0Z280 (extracted on 18. 08. 2008)
cloud applying homomorphic encryption. In: Proceedings of the 5th IEEE International
(2011)
- Breuer, P. T. , Bowen, J. P. :Typed assembler for a RISC crypto-processor. In:Barthe,
Heidelberg (2012)
- Nektarios Georgios Tsoutsos and MichailManiatakos, "Investigating the Application
of One Instruction Set Computing for Encrypted Data Computation";, in proceeding of
SPACE 2013, Lecture Notes in Computer Science Volume 8204, 2013, pp21-37
- Halevi,S. ,Shoup, V. :Design and implementation of a homomorphic-encryption library
(2012)
- Brakerski, Z. , Gentry, C. , Vaikuntanathan, V. : (Leveled) fully homomorphic encryption
- Ron Rivest, Leonard Adleman,and Michael L. Dertouzos. On data banks and
- Craig Gentry. Fully homomorphic encryption using ideal lattices. In STOC,
- 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


References

http://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.
- http://www.verizonenterprise.com/DBIR
- About Zero Day Exploits (http://netsecurity.about)
Index Terms

Computer Science  Security

Keywords

Homomorphic encryption  CryptDB  Cloud Computing security  Social and Business applications