Building Your Private Cloud Storage on Public Cloud Service Using Embedded GPUs

Wangzhao Cheng[1,2,3], Fangyu Zheng[1,2(✉)], Wuqiong Pan[1,2], Jingqiang Lin[1,2], Huorong Li[1,2,3], and Bingyu Li[1,2,3]

[1] Data Assurance and Communication Security Research Center, Beijing, China
[2] State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing, China
{chengwangzhao,zhengfangyu,panwuqiong,linjingqiang,lihuorong,libingyu}@iie.ac.cn
[3] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

Abstract. When the public cloud provides infrastructure as a service (IaaS), the customer can outsource its data to the public cloud and release itself from the burden of storing data locally. At this point, the customer can not guarantee the security of the data in the public cloud. Encrypting data before using cloud storage is a viable solution, but frequent data encryption operations cause the original limited local computing resources to be even more stretched. In this paper, we used Jetson TX1 to build a client-side data encryption device that proxies the customer's data encryption and decryption operations. Firstly, a GPU-based SM4 implementation is carefully scheduled in the integrated GPU on Jetson TX1, including instruction-level optimization and variable improvement for data arrangement. Secondly, using zero-copy access on the device, we reduce the impact of explicit data transfer operations on overall performance. Finally, our SM4 kernel is capable of encrypting data at 30.30 Gbps on Jetson TX1, it is 26.6 times faster than the CPU-based implementation on the same platform. Furthermore, data processing throughput of the device reaches 30.19Gbps, a single Jetson TX1 owns sufficiently redundant computational power for the customer in 10 Gigabit fiber network environment.

Keywords: Symmetric cryptographic algorithm · Jetson TX1
CUDA · SM4 implementation · Virtual private cloud storage

W. Cheng—This work was partially supported by National 973 Program of China under Award No. 2014CB340603, National Natural Science Foundation of China under Award No. 61772518 and National Key R&D Program of China under Award No. 2017YFB0802103.

R. Beyah et al. (Eds.): SecureComm 2018, LNICST 254, pp. 512–528, 2018.
https://doi.org/10.1007/978-3-030-01701-9_28