Sport Wearable Biometric Data Encrypted Emulation and Storage in Cloud

Nick Mcdonald, Daniel Atkinson and Youry Khmelevsky*
Computer Science, Okanagan College, Kelowna, BC, Canada
Emails: nick.mcdonald.94@gmail.com, daniel_atkinson@mail.com, and ykhmelevsky@okanagan.bc.ca

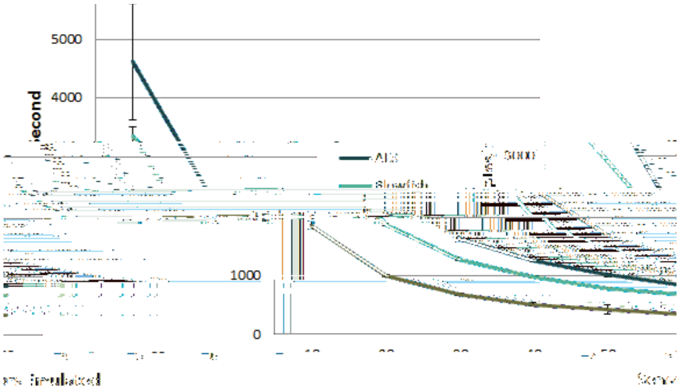
Scott McMillan
Co ech nc., enticton, BC Canada
Email: scott@ co.io

*Also A liated with Mathematics, Statistics, hysics, and Computer Science
rving K. Barber School o Arts and Sciences, BC Okanagan, BC Canada

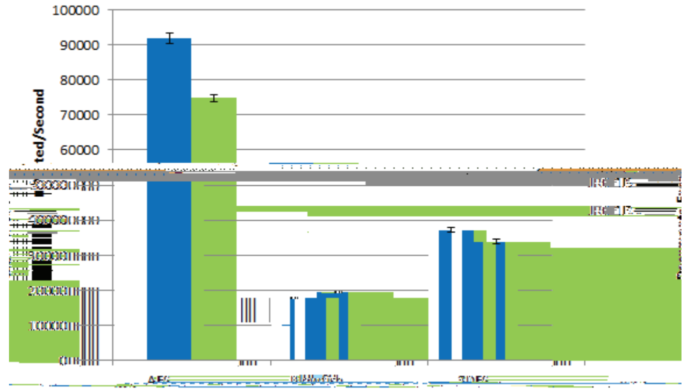
Abstract

or optimi ed batched writes Cassandra is twice better than Base. On the other hand, they ound that Base is about 0% better than Cassandra or low-density data read.

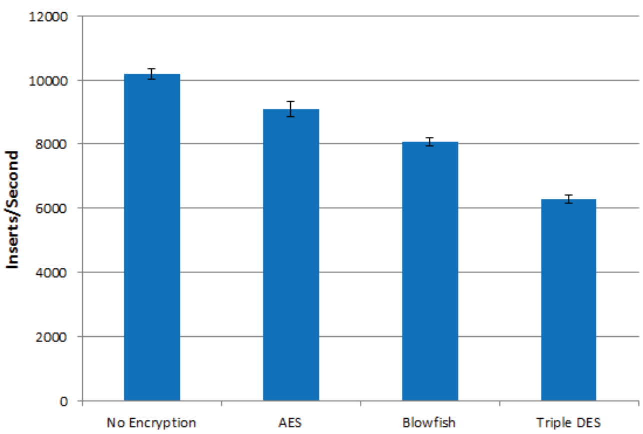
A new encryption paradigm, re erred to as asymmetric cross-cryptosystem re-encryption (ACC E) was presented in 10 . A cipherte t conversion mechanism that allows an authori ed pro y to convert a complicated BBE cipherte t into a simple BE cipherte t a ordable to mobile devices, without



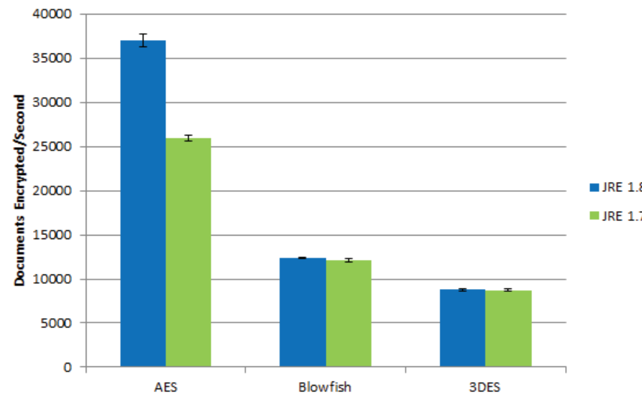
ig. 1. Data enerator er ormance



ig. . Encryption Algorithm er ormance or 100 Byte Documents



ig. 2. NoS L Database er ormance



ig. 4. Encryption Algorithm er ormance or 1 Kilobyte Documents

n addition to being the most widely used encryption algorithms they were selected or their stability, security, and ease o implementation. he algorithms addressed in this paper are the AES, Blow sh, and DES algorithms.

A. AES vs Blowfish vs 3DES

1) AES Encryption: An AES encryption algorithm 1 utili es two symmetric keys to code and decode data (meaning that the same key will encrypt and decrypt data). Keys constructed by this algorithm can be 12 , 192, or 2 bits.

2) Blowfish: Blow sh 1 , 19 employs keys with lengths 2 bits - 44 bits using a block si e 4 bits. As o now there is no known attack which can success ully break Blow sh.

3) 3DES: Data Encryption Standard (DES) 20 makes use o a -bit encryption key with a block si e 4 bits. o counter DES' vulnerability to brute- orce attacks, due to a small key si e and advancements in computer hardware, DES was introduced, which e ectively repeated the DES algorithm three times to increase key length rom bits to 1 bits.

B. Encryption Algorithm Performance

he a orementioned algorithms were integrated into the system and each was tested to determine which one was the best t or our system. n ig. and ig. 4 we tested each algorithm by having the repeadedly encrypt SON documents over a period o time to determine how many documents per second each algorithm could encrypt. he tests were ran or seconds and repeated 20 times to provide an accurate average. We chose 100 Bytes and 1 Kilobyte as our document si es because they best t the si e o data that this system and similar systems would be handling.

Our hypothesis was that Blow sh would encrypt aster than AES and DES, but surprisingly we ound that AES encrypted more than twice the number o documents as Blow sh. Looking into this peculiarity we discovered that the answer lies in optimi ation. n recent iterations o ava there have been great e orts to optimi e their AES implementation including most notably making use o ntel©'s AES-N (AES New nstruction set) 21 which conducts AES encryption directly on hardware.

ig. and ig. 4 show how each algorithm per ormed and di erent versions o ava and on di erent si es o data. We ound that AES out per ormed Blow sh and DES in both cases, and has improved greatly in recent versions o ava. Blow sh did not per orm well with the small amount o data and was outper ormed by DES, but Blow sh per ormed better than DES with larger amounts o data. Subse uent tests showed that as the si e o the data got larger Blow sh per ormed even better than DES but AES was still by ar the astest.