Biometric Data Emulation and Encryption for Sport Wearable Devices (A Case Study)

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

*Also Affiliated with Mathematics, Statistics, Physics, and Computer Science
Irving K. Barber School of Arts and Sciences, UBC Okanagan, BC Canada

Scott McMillan
XCo Tech Inc., Penticton, BC Canada
Email: scott@xco.io

Abstract—[illegible] N SQL [illegible] W [illegible] N SQL [illegible]

I. Introduction

XCo Tech Inc. (Xco), based in Penticton BC, Canada is developing an agnostic sensor platform for enabling interconnectivity, analysis and integration of information for sports, fitness and healthcare. The company's software system collects data from multiple sensors and transmits that data to servers where the data is integrated, synchronized, and analyzed. The data and derived analytics are then transmitted to other devices or persons where an app can use the data and analytics to present valuable real-time information to the user.

Critical to the value-add proposition of the system is the ability to measure a person's location with cm level precision

In the workshop paper [3], authors present work in progress where they utilize sensor-based wellness data to benefit teenage ice-hockey players in their hobby. They created an application concept and mock-ups of wearable sensors, and conducted a service design workshop with a teenage ice-hockey team. "Numerous sports tracking applications exist for mobile phones and smart watches, bracelets and other wearable sensors are becoming increasingly popular form factors for detecting location, physical activity and biometric data" [3].

In paper [16] authors discuss a new model of using NoSQL databases as a storage systems. The tell, that the "new generation of database systems with weaker data consistency models is content with using and managing locally attached individual storage devices and providing data reliability and availability through high-level software features and protocols". They examines the behavior of several NoSQL DBs: HBase and Cassandra. In Summary they conclude, that I/O profile does not differ greatly from traditional RDBMes, but what differs most is their approach to managing data.

On the other hand, authors in [12] investigated three NoSQL database (MongoDb V2.2, Cassandra V2.0 and Riak V1.4) performances for a large, distributed healthcare organization. In their testing, a typical workload and configuration produced throughput that varied from 225 to 3200 operations per second between database products, while read operation latency varied by a factor of 5 and write latency by a factor of 4. They found, that Cassandra DBMS provided the best throughput performance, but with the highest latency.

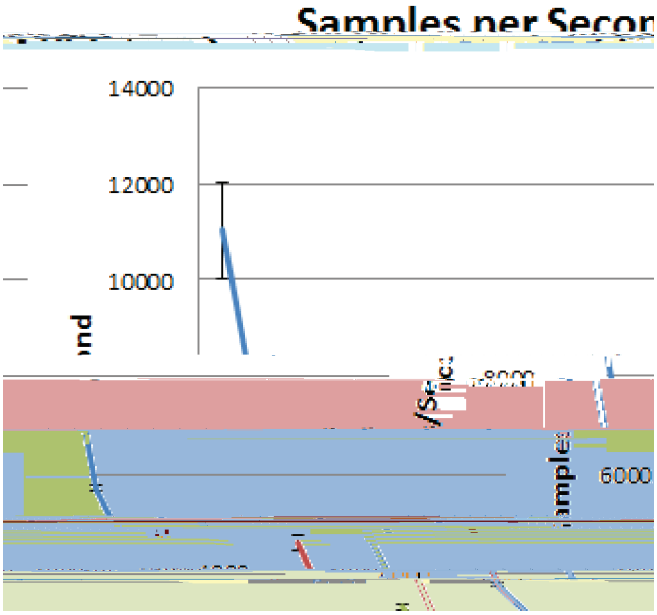
A Parallel Data Generation Framework (PDGF), a generic data generator is described in [7]. As they inform, "an extremely time and resource consuming task in the creation of new benchmarks is the development of benchmark generators, especially because benchmarks tend to become more and more complex". They presented PDGF Version 2, which contains extensions enabling the generation of update data as well.

Additionally to biometric data emulation and transmission we investigated different types of encryption algorithm for the secure data transmission and storage within a NoSQL database.

Fig. 1. Architecture of the Data Generation and Data Encryption/Decryption within NoSQL DBMS server.

Jira is a planning and collaboration tool that we used to plan our work and keep track of what needs to be done, and who is working on what. It is based around agile methodologies, and has a plug in for SCRUM which makes it a very good fit for our team.

A group of 9 students in COSC 470 Software (SW) Engineering at Okanagan College (OC) completed a 5 week spike project, in which a data generator was designed and implemented. The data generator emulates sensors data, and sends data across a network and into the database. The research goals of the spike project were to experiment with different en-


Samples per Secon
14000
12000
10000
6000

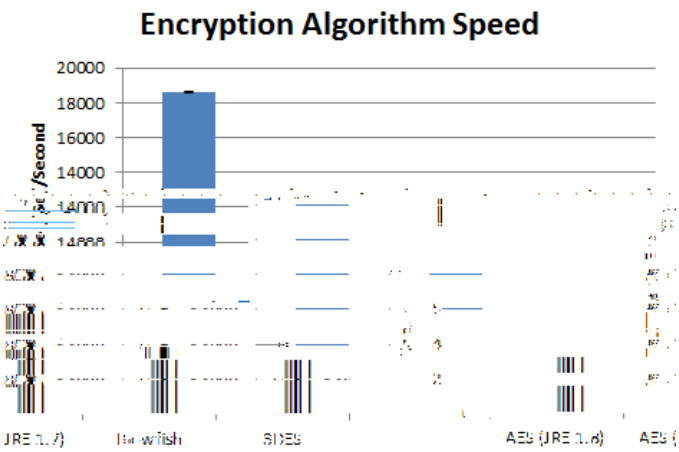


Fig. 4. Encryption Algorithm Performance

of 3DES because the DES algorithm was not designed to be used in this way, but no serious flaws have been found in its design, and it is still a widely used algorithm [8].

B. Encryption Algorithm Performance

We have implemented the previous three algorithms into the system and ran tests on them to see which one would be the best choice for us to implement in our system. In Fig. 4 we ran each encryption algorithm for a set amount of time to see how many 2491 Byte Json documents each of them could encrypt per second.

Theoretically Blowfish is a faster algorithm than AES, so we were surprised when tests were showing that AES more than twice as fast as Blowfish. The answer to this question of why AES is faster that Blowfish is optimization. In recent versions of Java there has been a lot of work done to optimize their implementation of AES and make use of Intel®'s AES-NI (AES New Instruction set); a set of instructions used to do AES encryption directly on the hardware which was introduced in 2010 [2] [19].

VI. Conclusion

In this paper we looked at how to generate data to emulate biometric sensors and investigated the effectiveness of different data encryptions for NoSQL document data bases for location and biometric data captured by sports wearable devices. Choosing an encryption method to use can be difficult, however through this research we have discovered 2 encryption methods that work well. The AES and blowfish algorithms seem to be the best choice for the system implemented. Blowfish can be implemented to be more secure than AES, however AES is faster when encrypting very large amounts of data, especially when using Intel® AES-IN. They outperform 3DES in both speed and security, 3DES is an outdated algorithm, and should not be implemented in new systems.

Acknowledgments

The research paper is based on the SW engineering spike project, which was developed by Computer Science students at Okanagan College within capstone project course COSC 470 "SW Engineering" in the Fall 2015, Bachelor of Information Systems (BCIS) program. The student project was in support to the NSERC CCI Engage College grant "GAUGE: Exact Positioning Systems For Sport and Healthcare Industries" (GAUGE). Our thanks to the COSC 470 students: Ahmed Abu Tayrah, Mohammed Aldaej, Khalid Almutiri, Yasir Asiri, Cheng-Kao Chiang, David Leader, Jon Ohlhauser and to the student research assistant Mikio Koga for their participation in development and testing of the software applications.

We would like to thank NSERC CCI Engage College program of Canada for supporting our GAUGE research project application in 2015. Our thank to Amazon Web Services, Inc. for supporting our capstone student software engineering and our student research projects by AWS Grants for Research and Education.

References

[1] Paarijaat Aditya, Victor Erdélyi, Matthew Lentz, Elaine Shi, Bobby Bhattacharjee, and Peter Druschel. Encore: Private, context-based communication for mobile social apps. In *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '14, pages 135–148, New York, NY, USA, 2014. ACM.

[2] Intel Corporation. Alexsey Ignatenko. Improved advanced encryption standard (aes) crypto performance on java with nss using intel® aes-ni instructions. https://software.intel.com/en-us/articles/improved-advanced-encryption-standard-aes-crypto-performance-on-java-with-nss-using-intel.

[3] Mira Alhonsuo, Jenni Hapuli, Lasse Virtanen, Ashley Colley, and Jonna Hakkila. Concepting wearables for ice-hockey youth. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, MobileHCI '15, pages 944–946, New York, NY, USA, 2015. ACM.

[4] M. Bellare. Block ciphers. http://cseweb.ucsd.edu/mihir/cse107/w-bc.pdf.

[5] Daniel Burmeister, Andreas Schrader, and Darren Carlson. A modular framework for ambient health monitoring. In *Proceedings of the 7th International Conference on Pervasive Computing Technologies for Healthcare*, PervasiveHealth '13, pages 401–404, ICST, Brussels, Belgium, Belgium, 2013. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[6] Hua Deng, Qianhong Wu, Bo Qin, Willy Susilo, Joseph Liu, and Wenchang Shi. Asymmetric cross-cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '15, pages 393–404, New York, NY, USA, 2015. ACM.

[7] Michael Frank, Meikel Poess, and Tilmann Rabl. Efficient update data generation for dbms benchmarks. In *Proceedings of the 3rd ACM/SPEC International Conference on Performance Engineering*, ICPE '12, pages 169–180, New York, NY, USA, 2012. ACM.

[8] A.A.Zaidan Hamid A.Jalab M.Shabbir Hamdan.O.Alanazi, B.B.Zaidan and Y. Al-Nabhani. New comparative study between des, 3des and aes within nine factors. *Journal of Computing*, 2, 2010.

[9] Seema Holla and Praveen Dala-Krishna. Medical data encryption for communication over a vulnerable system, September 4 2012. US Patent 8,260,709.

[10] SplashData Inc. Blowfish encryption. http://www.splashdata.com/splashid/blowfish.htm.

[11] Florian Kerschbaum. Searching over encrypted data in cloud systems. In *Proceedings of the 18th ACM Symposium on Access Control Models and Technologies*, SACMAT '13, pages 87–88, New York, NY, USA, 2013. ACM.

B, Da a S em, PABS '15, pages 5–10, New Yor , NY, USA, 2015. ACM.

[13] S. Marchesani, L. Pomante, F. Santucci, and M. Pugliese. A cryptographic scheme for real-world wireless sensor networ s applications. In *Pro ee n o e ACM/IEEE 4 In erna ona Con eren e on C er-P a S em*, ICCPS '13, pages 249–249, New Yor , NY, USA, 2013. ACM.

[14] Er Ashima Pansotra and Er Simar Preet. Singh. Cloud security algorithms. *In erna ona Jo rna o Se r an I A a on*, Vol. 9(No.10):pp. 353–360, 2015.

[15] Margaret Rouse. Advanced encryption standard (aes) definition. http://searchsecurity.techtarget.com/definition/advanced-encryption-standard.

[16] Jiri Schindler. Profiling and analyzing the i/o performance of nosql dbs. In *Pro ee n o e ACM SIGME ICS/In erna ona Con eren e on Mea remen an Mo e n o Com er S em*, SIGMETRICS '13, pages 389–390, New Yor , NY, USA, 2013. ACM.

[17] Bruce Schneier. The blowfish encryption algorithm https://www.schneier.com/blowfish.html.

[18] Darpan D Shah, Anami a Mittal, and Kuntesh K Jani. A new approach towards encryption technique: D's crypto-cipher technique (dcct). *A van e n Com er Se en e an In orma on e no (ACSI)*, 2(5):pp. 446–449, April-June 2015.

[19] Intel Corporation Shay Gueron. Intel® advanced encryption standard (aes) new instructions set. https://software.intel.com/sites/default/files/article/165683/aes-wp-2012-09-22-v01.pdf.

[20] A Al Tamimi. Performance analysis of data encryption algorithms. *e r.eve O o er*, 1, 2008.

[21] Ja ob Tholander and Stina Nylander. Snot, sweat, pain, mud, and snow: Performance and experience in the use of sports watches. In *Pro ee n o e 33 Ann a ACM Con eren e on H man Fa or n Com n S em*, CHI '15, pages 2913–2922, New Yor , NY, USA, 2015. ACM.

[22] Wouter Walmin , Danielle Wilde, and Florian 'Floyd' Mueller. Displaying heart rate data on a bicycle helmet to support social exertion experiences. In *Pro ee n o e 8 In erna ona Con eren e on an e, Em e an Em o In era on*, TEI '14, pages 97–104, New Yor , NY, USA, 2013. ACM.