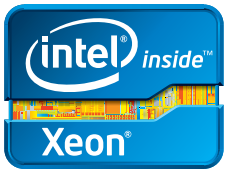
SOLUTION BRIEF
Intel® AES-NI
Healthcare IT

High Performance Encryption for Electronic Health Record Databases

Using Intel® Advanced Encryption Standard New Instructions with InterSystems Caché* EHR database substantially improves encryption performance and reduces computational overhead.



"The promise of electronic health records will be realized only if built on a trusted foundation of secure, high-performing computing end-to-end. Encryption is a key means to minimize security risks as protected health information moves among platforms, places, and people in the healthcare continuum."

—Eric Dishman
General Manager, Health Strategy and Solutions Group, Intel Corporation

Executive Summary

Electronic health record (EHR) server databases, implemented using InterSystems Caché, are increasingly being encrypted to protect the confidentiality of sensitive healthcare data. However, employing encryption on such databases can require significant computational resources. Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), included in the Intel® Xeon® processor X5670 and Intel® Xeon® processor E5-2680 (and more recent Intel Xeon processor families), accelerates encryption and greatly reduces computational overhead.

Key findings:

- Tests show that even as data and computational time increase, there is negligible degradation in performance for encryption or decryption.
- Use of Intel AES-NI with Caché's interleaved cipher blocks can speed up encryption by a factor of 20 or more.

Securing Sensitive Data to Prevent Breach

According to the U.S. Health and Human Services report, *Breaches Affecting 500 or More Individuals*, many data breaches involve compromised servers and backups.[1] While such events are less likely than the loss or theft of mobile devices, when server or backup breaches do occur, the number of patient records compromised is often much larger and the business impact much greater.

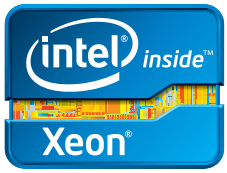
The Ponemon Institute's *2011 Cost of Data Breach Study: United States* estimates the average total cost of a data breach at USD 5.2 million.[2] To mitigate this type of risk, healthcare organizations are increasingly employing encryption on EHR databases. However, encryption can require additional computational resources, and this can in turn impact application scalability and increase the cost of deployment.

With the right combination of database platform, high-end processors, and encryption/decryption solution, cost-effective, scalable security for EHR is possible.

Intel AES-NI for Encryption/Decryption

Intel AES-NI[3] implements strong encryption and decryption while greatly reducing the associated processing time required. It consists of a new set of seven instructions, four of which implement the core of the AES algorithm and accelerate data encryption and decryption on the Intel® Xeon® processor X5670, Intel® Xeon® processor E5-2680, and more recent Intel Xeon processor families.

By accelerating performance, Intel AES-NI provides improved application scalability and more affordable data protection. These benefits are maximized by using Intel AES-NI in a mode that interleaves the processing of multiple cipher blocks.[4]



"Encryption is now a requirement for data in many domains. We've had an efficient implementation, and now with the hardware assist from Intel, we can offer encryption with much lower impact on overall system performance."

—Robert Nagle
Vice President of Software Development, InterSystems Corporation

InterSystems Caché Database for EHR

InterSystems Caché is a high-performance database and rapid application development and deployment platform that powers many large-scale EHR systems. The Caché high-performance database engine stores data in highly compressed, sparse multi-dimensional arrays called "globals." Application programmers can access and manipulate this data through objects, SQL, or direct access to the underlying structure.

Caché database files consist of sequential fixed-size blocks, 8 KB, 16 KB, 32 KB, or 64 KB in size. Blocks contain application data, indices, or metadata such as directories, pointers, or allocation maps. A single Caché instance can have many databases, with each database using one of these block sizes and each stored in a separate disk file. When in use by applications, database block images are stored in shared memory buffers.

Caché distributes application processing among many processes. When a process needs data that is in a database block not currently resident in a shared memory buffer, that process allocates a free buffer and reads the needed database block from disk. Other processes are not affected.

When the numbers of modified, unmodified, and free shared memory buffers hit any of several thresholds, or a maximum time interval elapses, a set of write daemon processes writes the contents of the modified buffers back to disk. This allows for efficient bulk processing of disk writes and allows application processes to continue while disk writes are in progress.

Reducing Computational Overhead

Databases that contain sensitive data should be encrypted in order to prevent compromise. The Caché database encryption feature was designed to meet the following goals:

- The entire contents of the database, including all structural metadata except for the single initial label block, are encrypted.
- The encryption operation is size-preserving, to maintain the efficient mapping of database blocks to disk hardware.
- The encryption and decryption operations are completely transparent to applications and the database engine.
- Identical data stored in different database blocks is encrypted differently, to minimize information leakage.
- Encrypted databases are completely portable between Caché instances running on different hardware and OS platforms.

Caché database encryption uses the AES algorithm in Cipher Block Chaining (CBC) mode at the database block level, with an initialization vector derived by encrypting the database block number.[5,6] Database encryption and decryption are performed at the interface between the Caché engine and the OS file system.

Block-level database encryption provides high performance by amortizing fixed initialization overhead over large blocks. The choice to encrypt fixed-sized database blocks also allows for optimal exploitation of instruction-level hardware encryption. The AES algorithm operates on 16-byte cipher blocks, performing 10 to 14 rounds (depending on the key length) of multiple cryptographic primitives on each cipher block, using a different 128-bit round key for each round. Intel AES-NI instructions perform one complete round on one cipher block as a single instruction.

Because Intel Xeon processor families implement a pipelined architecture and Intel AES-NI instructions take multiple clock cycles to complete, multiple cipher blocks must be interleaved at each round for maximum processor utilization. In CBC mode, the processing of each cipher block requires the encrypted data from the previous cipher block. Cipher block interleaving is therefore straightforward for decryption, when all the encrypted cipher blocks are initially available and multiple cipher blocks can be interleaved in the instruction pipeline, but is not possible

for encryption in the general case. Because Caché encrypts the contents of a large pool of fixed-sized shared memory buffers during write daemon processing, it can interleave cipher blocks from multiple buffers to achieve the same CPU utilization for encryption as for decryption. Caché automatically detects the Intel Xeon processor family on which it is running and optimizes the interleaving factor to maximize performance.

Case Study: Encryption Performance Testing

We measured the computational overhead of Caché AES-CBC database encryption and decryption. Measurements were made on an unencrypted database, an encrypted database using an optimized AES-CBC software implementation ("software"), and an encrypted database using an interleaved AES-CBC implementation with Intel AES-NI hardware ("interleaved Intel® AES-NI").

Figure 1 shows the results of these measurements on a 2.93 GHz Intel Xeon processor X5670, and Figure 2 shows the results on a 2.7 GHz Intel Xeon processor E5-2680. The benefits of hardware encryption are striking. While unencrypted data will always process faster, with Intel AES-NI, there is little degradation in performance even as time and data increase. Table 1 lists the computational overhead and speed-up factors by test case and processor.

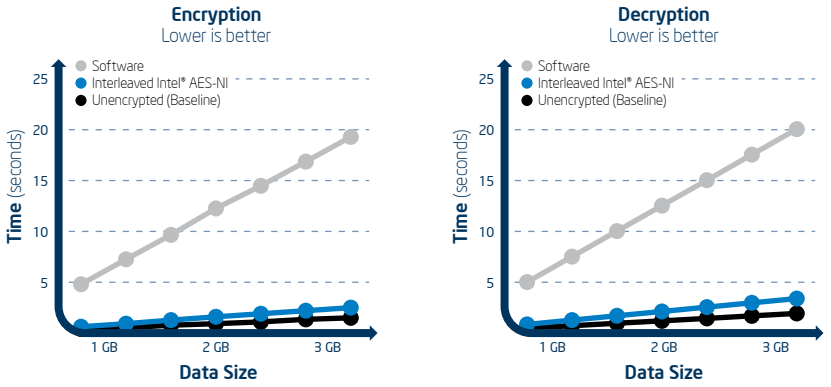


Figure 1. Performance results of encryption (left) and decryption (right) on a 2.93 GHz Intel® Xeon® processor X5670. Note: "Software" refers to the optimized AES-CBC software implementation and "interleaved Intel® AES-NI," the interleaved AES-CBC implementation with Intel AES-NI hardware.

Performance test results show Intel® AES-NI tracks nearly identical to the baseline of unencrypted data.

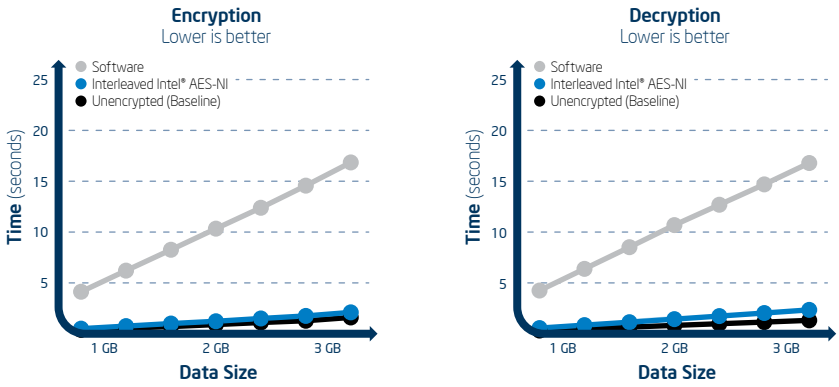


Figure 2. Performance results of encryption (left) and decryption (right) on a 2.7 GHz Intel® Xeon® processor E5-2680. Note: "Software" refers to the optimized AES-CBC software implementation and "interleaved Intel® AES-NI," the interleaved AES-CBC implementation with Intel AES-NI hardware.

Table 1. Observed computational overhead and speed-up factors, translated into clock-speed invariant units.

Implementation		Intel® Xeon® Processor X5670		Intel® Xeon® Processor E5-2680	
		Computational Overhead (clocks/byte)	**Speed-up Factor**	**Computational Overhead** (clocks/byte)	**Speed-up Factor**
Encryption	Software	16.0		12.0	
	Interleaved Intel® AES-NI	1.0	16x	0.5	24x
Decryption	Software	16.0		12.0	
	Interleaved Intel® AES-NI	1.3	12x	0.8	15x

Conclusion

The design of InterSystems Caché database encryption allows maximally efficient utilization of the Intel AES-NI capability implemented in the latest Intel Xeon processor families. Intel AES-NI allows Caché to perform encryption and decryption faster, enabling it to handle an ever-increasing amount of sensitive data at reduced hardware cost. In addition to servers and backups, Intel AES-NI hardware-assisted encryption and decryption can also be useful for client platforms and encryption of data in transit.

For More Information

InterSystems Caché: Protecting Data at Rest, by David Shambroom
www.intersystems.com/dcdownloads/ProtectingDataAtRest.pdf

Intel Xeon processor families
www.intel.com/xeon

FACTORS TO CONSIDER FOR DATABASE ENCRYPTION SOLUTIONS

Consider these factors to make use of this advanced capability:

1. Be aware of regulations, data protection laws, and breach notification rules applicable for your geographic location(s) of business, and their requirements for protecting confidentiality of sensitive healthcare data.
2. Be aware of the increasing risk of breaches from compromised servers and address these types of risks in your risk assessments.
3. Consider server database encryption a key safeguard as part of a holistic approach to protect confidentiality of sensitive healthcare data, and avoid breach.[7]
4. If database encryption is part of your solution, consider the advantages of deploying InterSystems Caché on hardware that supports Intel AES-NI.

For more information on InterSystems Caché visit InterSystems Caché Technology Guide at **www.intersystems.com/cache/technology/techguide**

For more information about Intel Advanced Encryption Standard New Instructions visit **www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html**

[1] Ponemon Institute. 2011 Cost of a Data Breach Study in the U.S. March, 2012. http://bit.ly/xBF6vr.

[2] U.S. Department of Health and Human Services. Breaches Affecting 500 or More Individuals. www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

[3] Intel Advanced Encryption Standard New Instructions (Intel® AES-NI) is a set of instructions that consolidates mathematical operations used in the Advanced Encryption Standard algorithm. Enabling Intel AES-NI requires a computer system with an Intel AES-NI-enabled processor as well as non-Intel software to execute the instructions in the correct sequence. For availability of Intel AES-NI enabled processors or systems, check with your reseller or system manufacturer.

[4] Secure Cloud with High Performing Intel Data Protection Technologies. www.youtube.com/watch?v=I0ALeQjS7FA].

[5] Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[6] National Institute of Standards and Technology. Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation. http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

[7] Houlding, David. Healthcare information at Risk - Encryption is Not a Panacea. Intel® Solution Brief. http://premierit.intel.com/servlet/JiveServlet/previewBody/6367-102-1-9576/Healthcare_Information_Risk-Encryption_is_Not_a_Panacea.pdf.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, reference www.intel.com/performance/resources/benchmark_limitations.htm or call (U.S.) 1-800-628-8686 or 1-916-356-3104.

Printed in USA 1012/DHOU/KC/PDF ♻ Please Recycle 327957-001US