Case Study

Intel® Advanced Encryption Standard New Instructions

Healthcare

Healthcare, Security, Big Data Analytics, Population Analytics,
HIPAA, Genomics, Clinical Genomics

Intel® AES-NI hardware-accelerated encryption boosts security and performance of GenoSpace Population Analytics application

GENOSPACE™
Digital Architects of Genomic Medicine

The science of genomics, which studies the sequencing and analysis of DNA structures, has revolutionized healthcare. Advances in genomics are enabling personalized treatments and potential cures by testing genetic variants and comparing these to what is known about various therapies and drugs. The confluence of genomics and information technology has yielded advanced software tools that are helping researchers, laboratories, clinicians, and community healthcare providers compile and interpret large, complex data sets. Significant breakthroughs in the development and application of new, more precise therapies for cancer and inherited disease indications are in large part due to innovative genetic analysis.

GenoSpace, headquartered in Cambridge, Massachusetts, is a fast-growing company that offers cloud-based software services designed to be HIPAA-compliant and applied across research, clinical development, pathology, and clinical care. The company's offerings include data integration, modeling, analysis, interpretation, visualization, and collaboration capabilities for genomic and other biomedical data. Since maintaining the confidentiality of human genetic data is of paramount importance to GenoSpace, the company has made security a top priority. In an environment where breaches involving healthcare data have reached alarming levels, GenoSpace understands the costly business impact of noncompliance with HIPAA patient privacy regulations and industry-leading data security practices. For example, the Identity Theft Resource Center's 2014 annual list of security breaches points out that the medical/healthcare sector accounted for more than 42.5% of all the breaches listed, topping all other categories.[1] Since reporting requirements began, the US Department of Health and Human Services has tracked 944 incidents involving approximately 30 million individuals.[2]

Along with the persistence and enormity of this problem comes financial fallout. For example, in its study, *2014 Cost of Data Breach Study: Global Analysis*, the Ponemon Institute estimated that the average cost of a data breach in 2014 was $3.5 million, an increase of 15% over 2013. Additionally, the average cost per record across all sectors also increased, from $188 to $201—and the per capita cost for healthcare was the highest across all industries at $316 per patient. And the typical fine for a data breach runs up to $1.5 million per incident. The cost of breaches to the healthcare sector overall is estimated at $5.6 billion annually.[3]

> "For more than a decade, the MMRF has worked to develop the world's most comprehensive clinical and genomic data on multiple myeloma patients, from mapping the myeloma genome to launching the CoMMpass study—dedicating all data to the public domain to accelerate discoveries, treatments, and a cure. But what's the point if people aren't using it? A critical, missing piece was the system to put all of the data into the hands of researchers, clinicians, and bioinformatics specialists who could use it. GenoSpace stepped in to provide an analytics solution with robust and high-performance encryption to ensure the security and privacy of patient data."
>
> – Kathy Giusti, Founder and Executive Chairman, The Multiple Myeloma Research Foundation and Member of President Obama's Precision Medicine Initiative Working Group

Security from the Ground Up

Since the company's inception, GenoSpace's software development practices have incorporated the strongest possible data encryption to help secure these highly sensitive data sets and meet HIPAA compliance standards. On its website, HealthIT.gov, part of the US Department of Health and Human Services, highly recommends encryption as an integral part of a broader holistic and multilayered approach to securing healthcare data and minimizing the probability of damaging breaches. The HITECH Act of 2009 expanded HIPAA data breach reporting requirements and requires disclosure of breaches involving unprotected patient health data. The HITECH Act states that while encryption of data at rest and in transit is not required, it is certainly "addressable."[4] Failure to encrypt patient healthcare data can have significant ramifications, including steep fines.

The GenoSpace architecture is hosted on Amazon Web Services (AWS), which provides flexibility and scalability for its developers and customers. To ensure the utmost security for this public cloud implementation, GenoSpace takes a ground-up approach to encryption. Its solutions gather all of the data that will be subject to analysis and layer encryption on top of that to safeguard the confidentiality of sensitive healthcare data stored on AWS or data that travels over the Internet. This adds an important extra measure of protection to AWS built-in security features.

Recently, GenoSpace evaluated the benefits of Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), a silicon-based instruction set that accelerates encryption on Intel® Xeon® processors, which GenoSpace uses to process data. Meeting its customers' performance and usability demands was a key objective for GenoSpace, given the amount of encryption and decryption that occurs when its software is used for analytics. To determine how the query response time of its population analytics application would be affected by encryption and by the hardware encryption acceleration that Intel® AES-NI provides, GenoSpace ran a series of tests focused on measuring the performance aspects of encrypting and decrypting stored data.

The study consisted of two phases:

Phase 1: GenoSpace sought to determine how configurations for the application's Java environment would impact Intel® AES-NI performance. Key parameters included:

- The version of Java Runtime Environment (JRE), which is an important component of building Java-based web applications.
- Cryptography provider libraries, which are application programming interfaces that implement Advanced Encryption Standard (AES) in Java. Libraries tested included Network Security Services (NSS), Bouncy Castle (BC), and Java Sun Cryptography Extension (SunJCE).
- Language implementation: Java or Groovy.
- Rates of performance on larger versus smaller data block sizes.
- Encryption key sizes: 128-bit keys versus the longer, more secure 256-bit keys.
- AES modes—Electronic Codebook (ECB), Cipher Block Chaining (CBC), CounTeR (CTR), and others—which define the types of block cipher mode of operation used.

Phase 2: The GenoSpace team tested production deployments of GenoSpace Population Analytics applied to real-world data with Intel® AES-NI enabled and disabled on sample data sets of various sizes: 1,000 patients, 10,000 patients, and 100,000 patients. In this application, data is generally written and encrypted once, but accessed and read multiple times and decrypted, so the performance of decryption was of particular interest.

Intel® AES-NI-Enhanced Encryption Improves Performance Significantly

The key findings of this test revealed that Intel® AES-NI-enhanced encryption had a markedly positive influence on the performance of the GenoSpace Population Analytics application.

- **Provider library choice significantly impacts results.** The choice of encryption provider library and AES mode had the largest impact on performance. While Bouncy Castle showed no appreciable improvement with respect to Intel® AES-NI, the NSS library with Intel® AES-NI enabled performed more than 78% faster than Bouncy Castle and is the obvious choice for encryption. For decryption, NSS was approximately 96% faster than Bouncy Castle and 90% faster than SunJCE.

  With respect to AES modes, ECB, which is the simplest algorithm, outperformed other modes. However, because ECB is less secure than the other modes, and given the sensitivity of healthcare data, it is generally not appropriate for healthcare applications. For best performance and security, test results implied that the combination of CBC and the NSS provider library should be used, as it has the shortest routine time.

- **Intel® AES-NI significantly decreases the impact of increasing key length.** Typically, increasing the length of the AES encryption key (which functions much like a password) to strengthen security also increases encryption/decryption time.

  As key length increases, one expects a near linear increase in encrypt/decrypt times. But the study showed that by using NSS with Intel® AES-NI, the impact of doubling key length was reduced twenty-fold.

- **The benefits of Intel® AES-NI increase with the size of data sets.** In Phase 2 of the study, where sample genomic data was used, GenoSpace found that enabling Intel® AES-NI improves request times by nearly 9%. In fact as the size of the data sets scales up, there are even greater performance gains—an almost 14% improvement.

- **Intel® AES-NI had less impact on the application's overall performance.** GenoSpace concluded that with Intel® AES-NI, encryption can scale more efficiently than other operations, such as data serialization, sorting, and filtering.

Use Cases

The Multiple Myeloma Research Foundation (MMRF)

MMRF was involved in the launch of a 10-year study with approximately 50 participating cancer hospitals that collected and analyzed genomic data from nearly 1,000 multiple myeloma patients. Multiple myeloma, a type of cancer that affects white blood cells found in bone marrow, can severely compromise a patient's immune system. MMRF's goal was to help develop targeted treatments based on each patient's unique genomic markers. The study generated complex data from diverse clinical and laboratory sites that was collected using a range of procedures.

To accelerate innovation and foster collaboration, MMRF wanted to pull all the valuable data it had amassed and make it publicly available to clinicians, researchers, and bioinformatics specialists through the **Multiple Myeloma Research Gateway**. GenoSpace solved the dilemma by providing researchers with a custom solution that integrates genomic and clinical data from molecular laboratories, clinical sites, and contract research organizations. Leveraging Intel® AES-NI, GenoSpace provides a high-performance, secure environment that delivers the analytics MMRF requires to further its mission.

> "Like many providers pushing the envelope of genomic medicine, we needed an effective solution to the challenge of making petabytes of genomic data accessible to the scientists and physicians in our organization. GenoSpace enables our staff to efficiently gain insight from large quantities of complex information. We also like the fact that GenoSpace leverages Intel® AES-NI encryption acceleration technology, so we can be assured both that patient health data is secure and we get maximum performance and usability with the GenoSpace solution."
>
> – Greg Eley, Chief Technology Officer, ITMI

Intel® AES-NI both enhances usability of the analytics tool and offers a critical layer of protection for HIPAA-regulated genomic data used in MMRF's research projects.

Inova Translational Medicine Institute (ITMI)

ITMI, a division of nonprofit healthcare provider Inova Health System, brings genomic medicine into the community hospital environment. The organization has sequenced more than 8,000 genomes from individuals representing more than 100 countries. These sequences are linked to clinical data with the goal of discovering genetic factors that may be associated with a wide spectrum of diseases. ITMI chose the GenoSpace platform because it provided a scalable, intuitive tool that could enable the discovery of disease associations within these large data sets and the translation of these correlations into data that could be used by medical practitioners. As a company that is committed to maintaining the security and privacy of patient data, ITMI values the fact that the GenoSpace platform takes full advantage of Intel® AES-NI.

Why It Matters

Intel® AES-NI-enhanced encryption significantly enhances the performance and usability of the GenoSpace Population Analytics offering, which, in turn, results in increased user productivity and satisfaction with the overall solution. Enabling high-performance and secure solutions paves the way for healthcare organizations to embrace the use of genetic population analytics to significantly increase the effectiveness of research, healthcare, and disease treatment options. While healthcare workers and researchers put these tools to work, they can be confident that Intel® AES-NI accelerated and hardened encryption can help mitigate serious security breaches.

For organizations that avail themselves of the rich intelligence available through genomic analysis, there are several ways to ensure the security and privacy of the highly sensitive patient data they work with.

- Conduct security and privacy risk assessments to identify, prioritize, and triage risks, and address deficiencies in safeguards to improve security posture. McAfee® Foundstone® Professional Services, a part of Intel Security, offers consultation services and tools to pinpoint vulnerabilities, quickly identify a breach, and help apply appropriate remediations.
- To substantially reduce the risk of a breach, while reducing performance impact, consider applying hardware-accelerated and hardened encryption using Intel® AES-NI in combination with administrative and physical security controls for effective mitigation of risks and to maintain confidentiality of healthcare information.
- Check to see if your hardware and software can enable the use of encryption acceleration, and activate it to maximize the performance and usability of the solution.

> "We view patient privacy as a paramount concern, even at the cost of application performance. Intel® AES-NI allows us to employ the strongest encryption standard when scaling to massive population studies without making performance tradeoffs."
>
> – Niall O'Connor, Chief Technology Officer, GenoSpace

For additional information on security to mitigate risk of breaches in healthcare, see **http://www.intel.com/healthcare/security/breaches**.

To learn more about Intel® AES-NI-enhanced encryption and how it can help healthcare and life sciences organizations meet compliance requirements and secure patient data, visit **http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html.**

[1] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.

[2] http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/

[3] http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

[4] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

This document and the information given are for the convenience of Intel's customer base and are provided "AS IS" WITH NO WARRANTIES WHATSOEVER, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. Receipt or possession of this document does not grant any license to any of the intellectual property described, displayed, or contained herein. Intel® products are not intended for use in medical, lifesaving, life-sustaining, critical control, or safety systems, or in nuclear facility applications.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to http://www.intel.com/performance.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration.

Intel® Data Protection Technology: No computer system can be absolutely secure. Requires an enabled Intel® processor, system and software designed to use the technology. Check with your manufacturer or retailer. Intel® Data Protection Technology with AES-NI and Secure Key

Printed in USA 0415/DH/ETMG/001/PDF ♻ Please Recycle HLS-2015-001US