CASE STUDY
Intel® Xeon® Processor
Intel® Advanced Encryption Standard New Instructions
Cloud Computing and Data Storage Security

Enhanced Data and Cloud Storage Security

South Korean mobile telecom company chooses hardware-based Intel® Advanced Encryption Standard New Instructions powered by Intel® Xeon® processors for enhanced data and cloud storage security

SK Telecom is a leading mobile communications company Korea. The company has successfully enhanced its security by deploying hardware-based Intel AES-NI powered by Intel Xeon processors and plans to extend it to its data centers to offer customers reliable and secured services.

CHALLENGES

- **Comprehensive security strategies**
  The company needed strategies for a powerful enterprise security system to respond to today's most complex and sophisticated security threats.
- **Minimize server slowdown.**
  To quickly respond to security threats, the company needed a security system that encrypts data while minimizing server slowdown.

SOLUTIONS

- **Hardware-based Intel AES-NI powered by Intel Xeon processors.**
  SK Telecom adopted the hardware-based Intel AES-NI powered by Intel Xeon processors for the cloud storage system for enhanced security.

IMPACT

- **Hardware-based security solution.**
  The hardware-based Intel AES-NI powered by Intel Xeon processors performs the encryption easily, quickly, and completely in the hardware without affecting overall system performance.
- **Enhanced security in virtual environments.**
  SK Telecom offered highly-reliable services to its users by successfully addressing the security issues, one of the biggest threats in cloud environments.

"With the launch of new cloud services, we needed a more powerful security system to protect the user's private data. That is why we chose the hardware-based Intel® AES-NI powered by Intel® Xeon® processors."

Nam-Seuk Han
Head of the Information Technology R&D Center, SK Telecom

Need for powerful security system to protect the user's private data

SK Telecom, a leading mobile telecommunications company in South Korea, adopted the hardware-based Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) powered by Intel® Xeon® processors to enhance its data storage security and build a cloud system for cloud storage services. With ever-increasing complexity and sophistication of security threats, SK Telecom was looking for a fast-responding, comprehensive security system to protect its customers' personal data and provide them with secured services. The hardware-based Intel AES-NI powered by Intel Xeon processors led this company to deploy a system that performs data encryption with minimized server slowdown.

Deploying a powerful and comprehensive security system

Enterprises are becoming increasingly concerned about their IT security systems as hackers are getting smarter every day. With the launch of new cloud services, SK Telecom, Korea's No. 1 mobile communications carrier, was eager to find a comprehensive and strong security strategy to secure its sensitive data and information assets as well as to protect its computer systems from potentially devastating cyber attacks. Unencrypted data transfer between the networks and difficulty in controlling and maintaining required security features are the two root causes of security problems. Database and document encryption is the most efficient and essential way to improve security. Unfortunately, encryption often results in a serious server slowdown, which holds back many companies from actively adopting it.

With a primary PoC successfully completed, SK Telecom decided to extend the Intel® AES-NI to its cloud data centers to eliminate customers' potential concerns about security vulnerabilities.

"What we like the most about this technology is that we can provide more enhanced data security, since there is no risk of key exposure, unlike other software encryption. Also, no other devices but Intel® Xeon® processors are needed for AES encryption."

Nam-Seuk Han
Head of the Information Technology R&D Center, SK Telecom

Minimized server slowdown with Intel's hardware-based encryption

SK Telecom, a leading mobile communications company in South Korea, successfully deployed a document encryption feature on its cloud systems using the hardware-based Intel AES-NI powered by Intel Xeon processors without compromising system performance.

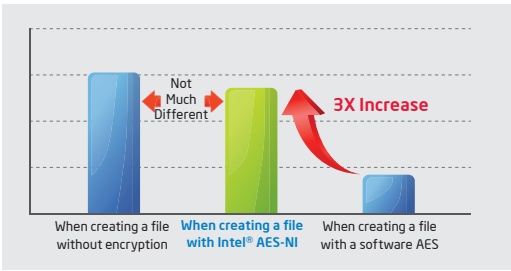
Unlike conventional software-based encryption technologies, Intel AES-NI, powered by Intel Xeon processors, is based on the hardware, and SK Telecom enjoyed a three-times increased system performance with Intel AES-NI. The perfomance was even comparable to when they did not use encryption.
In a conventional software encryption approach, there is a high data exposure risk to hackers during AES encryption.

Intel AES-NI, powered by Intel Xeon processors, completely addresses such concerns. Since the Intel Xeon processors perform AES encryption without the need for additional hardware, companies can also enjoy streamlined system maintenance in the future.

Nam-Seuk Han, head of the Information Technology R&D Center for SK Telecom, said, "With a primary proof of concept successfully completed, SK Telecom decided to extend the Intel AES-NI to its cloud data centers to eliminate customers' potential concerns about security vulnerabilities. As a result, SK Telecom has been able to offer users highly reliable services by successfully addressing the security issues–one of the biggest threats in cloud environments-with the hardware-based Intel AES-NI powered by Intel Xeon processors.

Performance Test on Encrypted File Creation[1]

The following graph shows encryption/decryption performance per second (MB/sec) measured upon file creation in SSD under different conditions (with Intel® AES-NI, software AES, or no encryption process).



Find a solution that is right for your organization. Contact your Intel representative or visit Intel.com

SOLUTION PROVIDED BY:

[1] **Excerpted from SK Telecom's conference paper at Mobile World Congress 2011:**

- Test condition: the duration in creating 1,000 x 5 MB files was measured given that the I/O buffer size is 4 KB. Total encrypted file size was 5 GB.
- File creation time of the three models was compared: one with no encryption, another with Intel® AES-NI, and the other without Intel® AES-NI.
- This test was run on the system with the Intel® Xeon® E5606 CPU (2.13 GHz, quad-core) and 2GB memory.

For more information on Intel AES-NI, visit www.intel.com/technology/dataprotection/index.htm.

0711/JML/PMG/200/PDF 325907-001KR