Case Study

Banking and Financial Services
Intel® Processor, Intel® Distribution of OpenVINO™ Toolkit

Ensuring a safer ATM experience

IntelliVIX and Intel deliver an anomaly detection solution to help customers transact safely at ATM touchpoints.

"We are proud to unveil an innovative Vision-AI-based solution designed to protect customers from ATM fraud and phishing scams. Implementing real-time video analysis using deep learning on ATMs, which lack sufficient computing resources, posed a significant challenge. Thanks to the Intel® OpenVINO™ toolkit, we successfully developed a real-time anomaly detection system, achieving our target performance even on ATMs with limited computing power. We are looking forward to extending and enhancing our Vision-AI solutions for various business areas in collaboration with Intel."

- Jeong-Hun Jang,
CTO, IntelliVIX

In the modern banking landscape, where convenience meets complexity, ensuring secure transactions is paramount. The rise of ATM fraud in South Korea, has necessitated a paradigm shift in security strategies.

IntelliVIX, in collaboration with Intel, built a sophisticated anomaly detection system capable of discerning genuine transactions from fraudulent activities. By leveraging the seamless integration of Vision AI and Intel's technologies, this solution addresses the vulnerabilities inherent in traditional security measures.

The Need for Safer ATMs

In recent years, South Korea has grappled with a persistent and evolving challenge: Automated Teller Machine (ATM) fraud. Criminals have ingeniously exploited the trust people place in legitimate organizations, particularly targeting vulnerable groups such as senior citizens. In this context, the need for advanced security solutions becomes paramount.

According to South Korea's Financial Supervisory Service, a total of 227,126 scams were reported from 2018 to 2022, and the expense of reported loss from these scams was some 1.66 trillion won.[1]

To counteract these losses South Korea is turning to technological innovation. In a pioneering move, the country introduced facial recognition devices integrated into cash machines, aiming to enhance security measures. The deployment of this technology is set to transform the banking landscape, ensuring transactions are conducted securely and efficiently.

Addressing Challenges of ATM Frauds

ATMs are vital conduits, facilitating millions of transactions daily. However, the rise of ATM fraud, especially through methods like phone scams and identity theft, poses a significant threat to both financial institutions and their customers. According to the Seoul police department, a total of 28,619 phishing cases were detected last year in which victims were tricked into sending cash to scammers via their bank accounts.[2] This surge in ATM fraud has not only caused substantial financial losses but is also eroding public trust.

Traditional security measures have proven insufficient in deterring criminals who exploit technological loopholes to target vulnerable individuals. As the incidents of fraud escalate, financial institutions face a pressing challenge: how to innovate and fortify security protocols without compromising user experience and privacy.

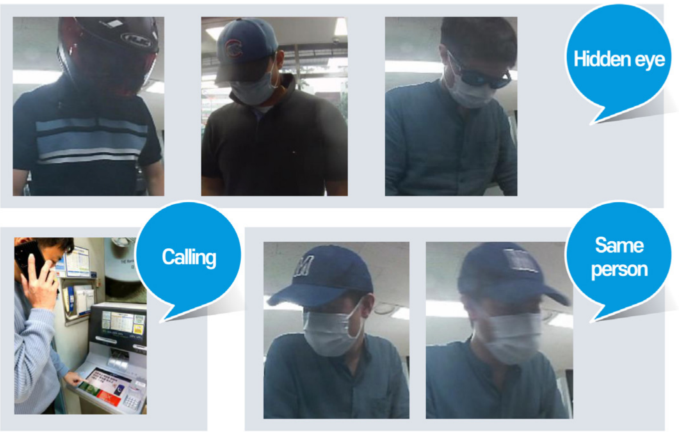


Figure 1: Anomalous behavior at ATMs with subjects obscuring their faces using helmets, sunglasses, face masks, etc.

Enabling Safe and Risk-free Transactions at ATMs

It is within this backdrop that IntelliVIX, a leading developer of Vision AI technology, collaborated with Intel to develop a groundbreaking solution. This collaboration aimed not just to address the immediate concerns related to ATM fraud but also to revolutionize the way security is approached in banking.

By harnessing the power of Intel® Distribution of OpenVINO™ Toolkit and IntelliVIX's expertise in Vision AI technology, the team set out to create an anomaly detection system capable of discerning legitimate transactions from fraudulent activities.

Anomalies, in this context, encompass a range of activities: covering faces, talking excessively during transactions, or conducting multiple transactions in quick succession. Identifying these patterns is pivotal in distinguishing genuine transactions from potentially fraudulent ones.

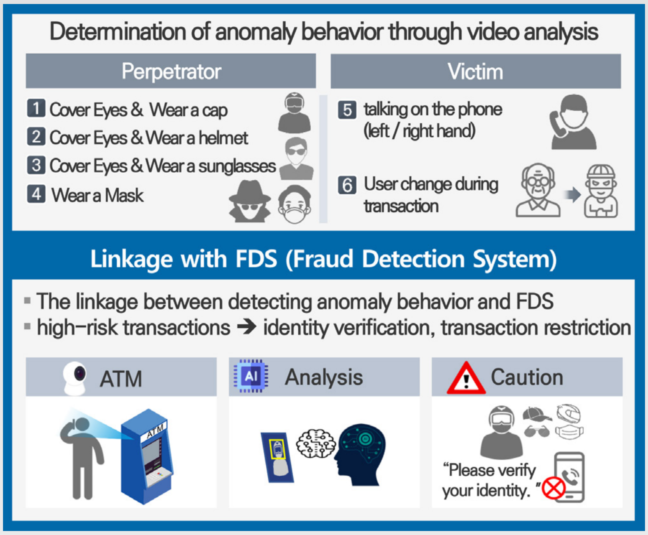

Determination of anomaly behavior through video analysis
Perpetrator
Victim
1 Cover Eyes & Wear a cap
2 Cover Eyes & Wear a helmet
3 Cover Eyes & Wear a sunglasses
4 Wear a Mask
5 talking on the phone (left / right hand)
6 User change during transaction
Linkage with FDS (Fraud Detection System)
▪ The linkage between detecting anomaly behavior and FDS
▪ high-risk transactions ➔ identity verification, transaction restriction
ATM
Analysis
Caution
ATM
AI
"Please verify your identity."

Figure 2: How IntelliVIX's solution identifies anomalous behavior at ATMs through real-time video analysis of subjects. Its linkage to the Fraud Detection System (FDS) allows it to then verify the subject's identity and issue a warning to flag potential frauds or risky transactions

Enhancing Anomalous Behavior Detection with Vision AI

Vision AI technology, with its robust object detection and image classification capabilities, plays a pivotal role in this detection process. Through advanced algorithms, the system recognizes specific attributes like head movements, facial expressions, and transaction frequency. By employing Vision AI, the ATM's built-in cameras become vigilant watch systems, capable of discerning minute details that elude the human eye.

When the system detects suspicious behavior, it acts promptly and decisively. For potential victims of voice phishing, immediate alerts are triggered, warning them of the ongoing scam. Simultaneously, these anomalies flag high-risk transactions, initiating additional security measures.

For flagged, high-risk transactions, the system employs multi-layered security protocols. Identity verification steps, such as secondary authentication prompts or biometric scans, add an extra layer of assurance. Additionally, transaction restrictions can be dynamically enforced, preventing large withdrawals or transfers until the user's identity is unequivocally verified. This real-time, adaptive approach ensures that even if a scam attempt is made, the system is primed to thwart it, safeguarding both the financial institution and the account holder.

The seamless integration of anomaly detection into the broader Fraud Detection System (FDS) is what makes this initiative truly groundbreaking. FDS, bolstered by Vision AI, becomes a proactive shield against emerging threats. It doesn't just react to incidents; it anticipates and prevents them, offering a robust defense against voice phishing and other forms of financial fraud.

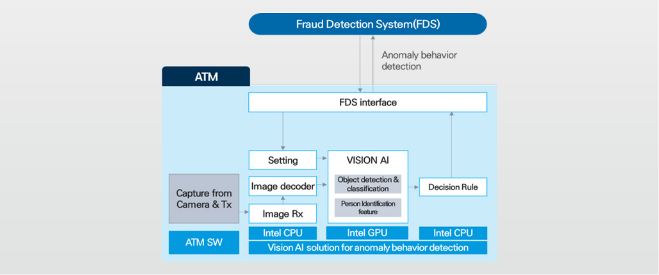

Fraud Detection System(FDS)
Anomaly behavior detection
ATM
FDS interface
Setting
VISION AI
Object detection & classification
Person Identification feature
Decision Rule
Capture from Camera & Tx
Image decoder
Image Rx
ATM SW
Intel CPU
Intel GPU
Intel CPU
Vision AI solution for anomaly behavior detection

Figure 3: An overview of the Fraud Detection System (FDS)

Empowering Vision AI with OpenVINO™

Intel® Distribution of OpenVINO™ Toolkit designed specifically for optimizing deep learning models, is central to this innovative approach to ATM security. IntelliVIX utilized the OpenVINO™ Toolkit to balance accuracy and resource utilization. This approach minimized false positives, ensuring precise anomaly detection while maximizing efficiency.

The solution's adaptability to various Intel® processors ensured flexibility and scalability for future applications. OpenVINO™ Toolkit's transformative impact lies in its ability to seamlessly harness the potential of Intel's hardware, including CPUs and GPUs, for deep neural network (DNN) inference. By providing a unified environment for diverse neural network architectures, OpenVINO™ Toolkit ensures efficient execution across Intel® platforms. In the context of ATM anomaly detection, this translates to unparalleled speed and accuracy, enabling real-time analysis of transactions.

ATMs, as edge devices, face inherent limitations in computational resources. OpenVINO™ Toolkit, tailored for edge computing scenarios, becomes a game-changer. By enabling sophisticated DNN-based vision AI services on low-spec CPUs, OpenVINO™ Toolkit empowers a myriad of edge devices, transforming them into intelligent, proactive guardians against financial fraud.

Beyond speed and efficiency, OpenVINO™ Toolkit simplifies the development process. Its open-source nature fosters a collaborative ecosystem, allowing developers to leverage a wealth of resources, guides, and community support. This collaborative synergy accelerates innovation, ensuring that the solution remains at the forefront of technological advancements.

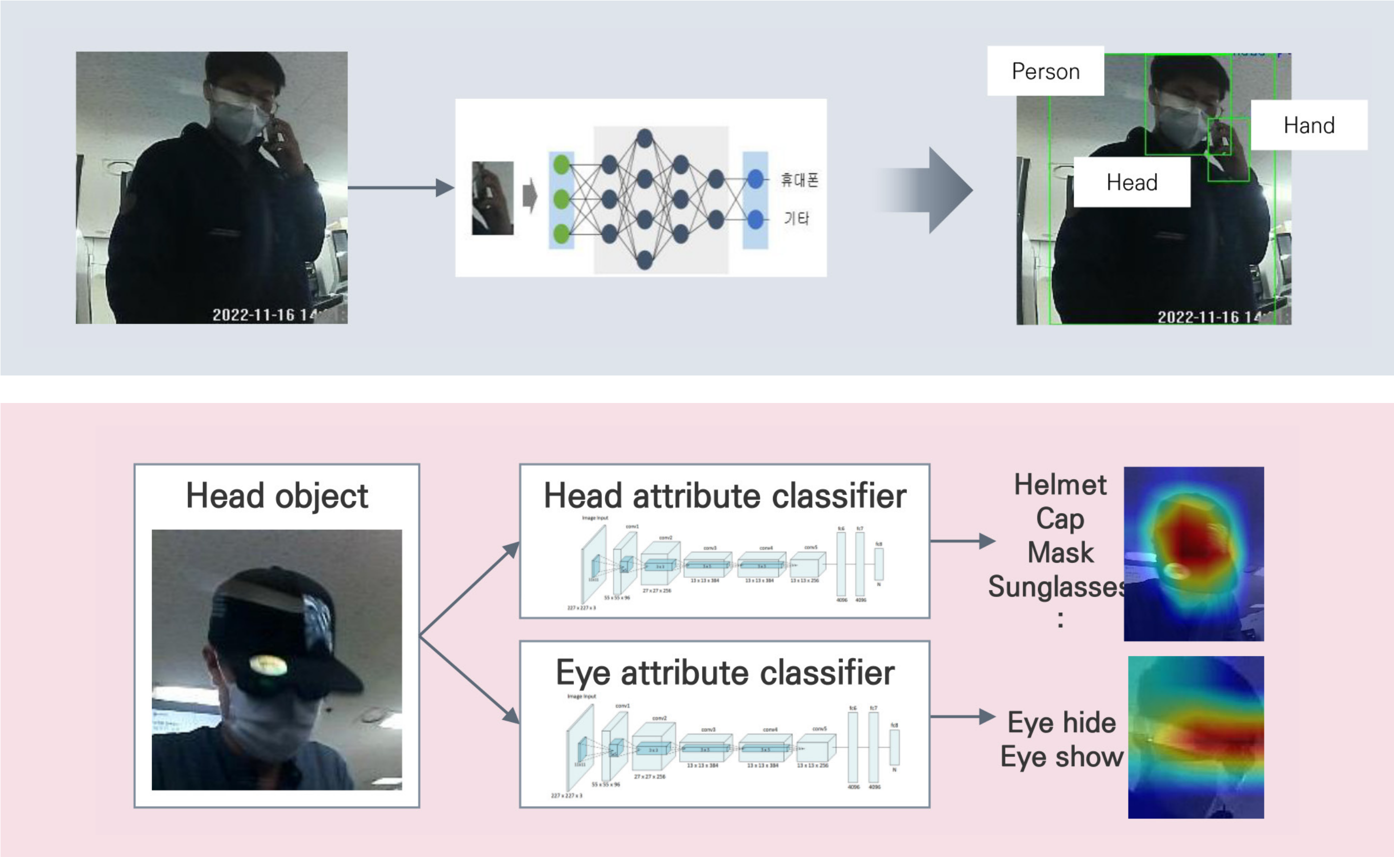


Figure 4: The system enables more efficient video analysis in real time at ATMs through an analysis of different facial and physical attributes related to the head, eyes and hands of subjects

Transforming ATM Security and Building Trust with Precision and Speed

In the financial security landscape, where every millisecond matters, the impact of the OpenVINO™- based anomaly detection solution is nothing short of revolutionary. By delving into the quantifiable impact numbers, the magnitude of this transformative collaboration becomes vividly clear.

Drastic reduction in processing time by using Intel® G3420 CPUs and Intel® i5-6500/ Intel® HD Graphics 530 GPUs

Before Integration	After Optimization
Without the optimization prowess of OpenVINO™ Toolkit, the system grappled with a processing time of 326 milliseconds per image. This delay not only hindered real-time analysis but also posed a potential inconvenience to users.	With the seamless integration of OpenVINO™ - based INT8 calibration, the processing time plummeted to 55 milliseconds per image - enabling swift transactions & immediate responses to any anomalies detected.

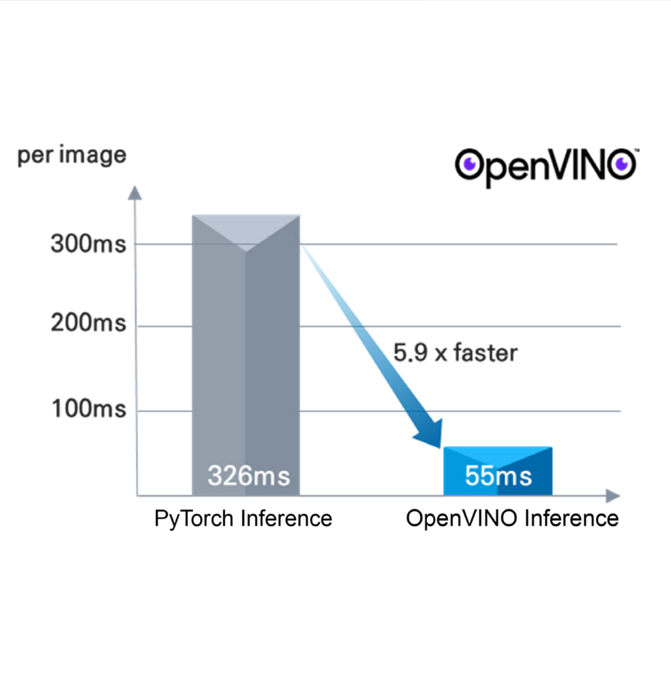


Figure 5: PyTorch vs. OpenVINO inference times for anomaly detection showing the magnitude at which the solution speeds up image analysis (5.9x faster)*

Delivering the Benefits ATMs Need

Enhanced User Experience

- **Minimized Transaction Delays:** The swift processing facilitated by Intel® processors and OpenVINO™ Toolkit translate into minimal transaction delays for ATM users. Transactions are executed seamlessly, enhancing user satisfaction and trust in the banking system.
- **Proactive Fraud Detection:** Real-time analysis means that potentially fraudulent activities are flagged and addressed promptly. This proactive approach not only safeguards users but also bolsters the overall security posture of financial institutions.

Reduction in False Positives

- **Precision in Anomaly Detection:** OpenVINO™ Toolkit's optimization techniques contribute to a significant reduction in false positives. By fine-tuning the deep learning models, the system delivers a high level of accuracy, ensuring that only genuine anomalies are flagged.
- **Enhanced Fraud Prevention:** The ability to distinguish genuine threats from benign transactions elevates the efficacy of fraud prevention efforts. Financial institutions can focus their resources on addressing actual risks, thereby maximizing the impact of their security measures.

Cost-Efficiency and Scalability

- **Cost Reduction:** By optimizing existing hardware with OpenVINO™ Toolkit, financial institutions can experience cost efficiencies. The need for expensive, specialized hardware is mitigated, leading to substantial cost reductions in both deployment and maintenance.
- **Scalability:** The streamlined process means that financial institutions could extend the anomaly detection system across a vast network of ATMs. The collaboration between Intel and IntelliVIX has led to the deployment of advanced AI solutions on over 5,000 ATMs across South Korea .

Societal Impact and Trust Building

- **Creating a Safer Financial Ecosystem:** The robust anomaly detection system plays a pivotal role in preventing financial crimes such as voice phishing. By deterring fraud and ensuring the safety of users' funds, the solution can enable a safer and trusted financial ecosystem.

Ensuring Ethical AI: Upholding Privacy and Integrity

In the world of AI, ethical principles and user privacy are of paramount importance. The anomaly detection solution places a strong emphasis on adhering to ethical guidelines and safeguarding user privacy. Here's how the solution aligns with AI ethics and personal data protection laws.

Stringent Data Protection: The anomaly detection solution operates in strict compliance with the Personal Data Protection Law, ensuring the complete avoidance of storing any photos or personal information. This approach upholds the highest standards of data protection, safeguarding user privacy.

Ethical Facial Analysis: The solution refrains from including facial recognition or face analysis functions, such as gender, age, and expression estimation, to mitigate potential biases and ethical dilemmas. By excluding these functionalities, the system eliminates the risk of perpetuating biases through AI analysis, ensuring fairness and integrity.

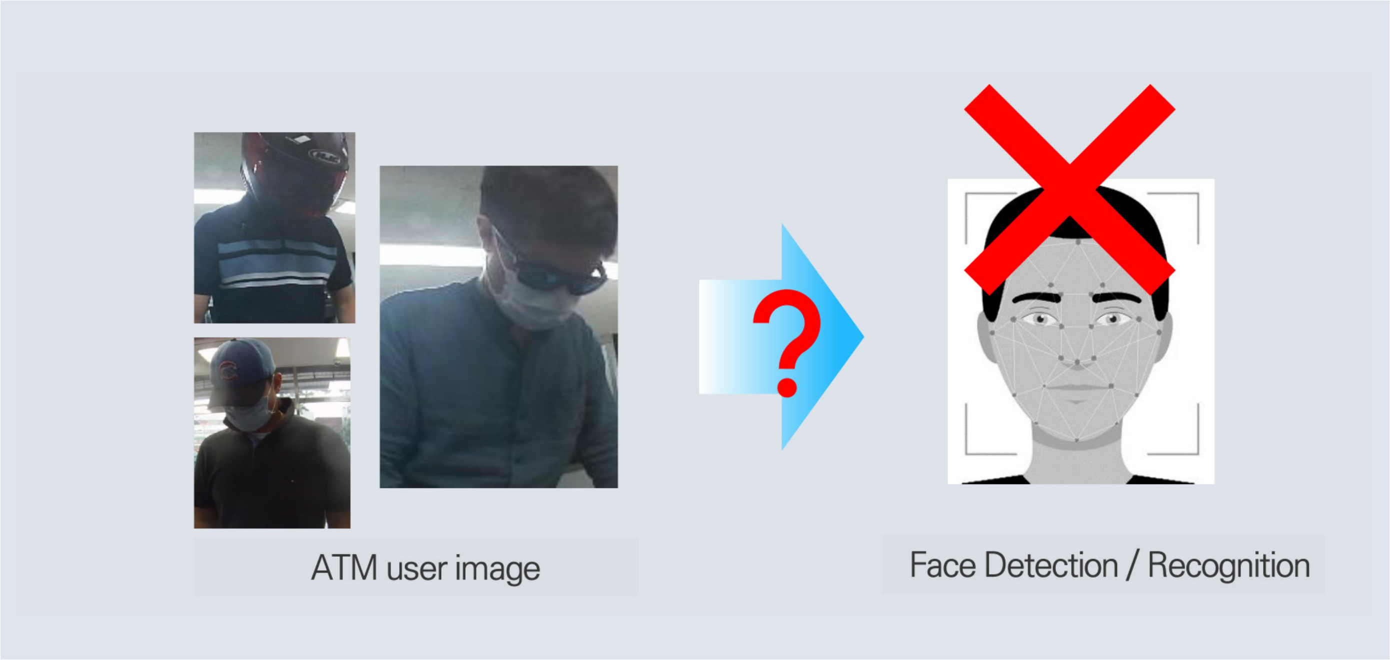
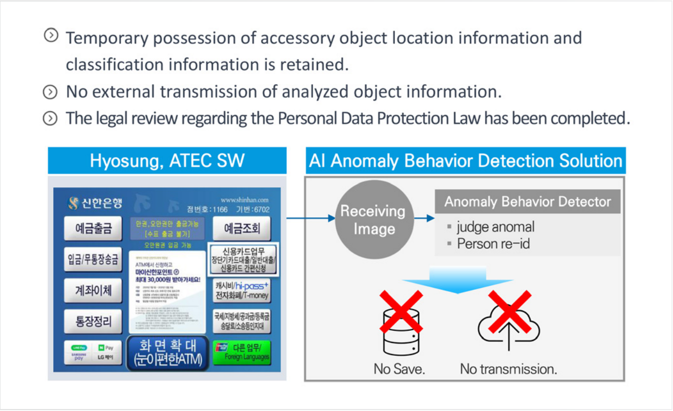


Figure 6.1: The solution enables compliance with data protection and privacy regulations by excluding analysis of gender, age and expressions to mitigate biases

Accessory and Full-Body Analysis: To address challenges related to facial disguises, the solution adopts a holistic approach. Prioritizing AI ethics, the system focuses on accessory analysis and full-body analysis. By analyzing accessory object location and classification information, the solution ensures accurate anomaly detection without compromising user privacy or ethical standards.



- Temporary possession of accessory object location information and classification information is retained.
- No external transmission of analyzed object information.
- The legal review regarding the Personal Data Protection Law has been completed.

Hyosung, ATEC SW
AI Anomaly Behavior Detection Solution
신한은행
www.shinhan.com
점번호:1166 기번:6702
예금출금
입금/무통장송금
계좌이체
통장정리
예금조회
신용카드업무 장단기카드대출/일반대출/신용카드 간편신청
캐시비/hi-pass+ 전자화폐/T-money
국세/지방세/공과금/등록금 송달료/소송등인지대
다른 업무/ Foreign Languages
화 면 확 대 (눈이편한ATM)
Receiving Image
Anomaly Behavior Detector
judge anomal
Person re-id
No Save.
No transmission.

Figure 6.2: The system neither saves, stores nor transmits any information and data from object analysis

This collaborative effort also adheres to the principle of temporary data retention during accessory object analysis. Accessory object location information and classification details are retained only for the duration necessary to facilitate anomaly detection. Once the analysis is complete, there is no external transmission of analyzed object information, respecting user privacy rights.

The solution has also undergone rigorous legal review, ensuring alignment with the Personal Data Protection Law and ethical imperatives. This scrutiny demonstrates the commitment to ethical AI development and responsible data usage, reinforcing the system's integrity and reliability.

Roadmap for a Secure Future

IntelliVIX and Intel look ahead to expand their collaboration into various industries such as retail, automation, and factory settings. The success of this ATM anomaly detection solution exemplifies how Intel's innovative technologies are shaping the future of AI applications globally. IntelliVIX and Intel's collaboration demonstrates the power of combining Vision AI technology with Intel's advanced hardware solutions. By enhancing ATM security and paving the way for unmanned applications, they are not just ensuring safer transactions but also driving innovation across diverse industries.

[1] https://www.koreaherald.com/view.php?ud=20230221000590

[2] https://www.upi.com/Top_News/World-News/2023/03/03/Shinhan-Bank-AI-ATM-phishing-scams/9181677861566/

Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel's Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.

*Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.