Artificial Intelligence and Homomorphic Encryption

정윤서

Contents

Artificial Intelligence and Homomorphic Encryption

What is Homomorphic Encryption

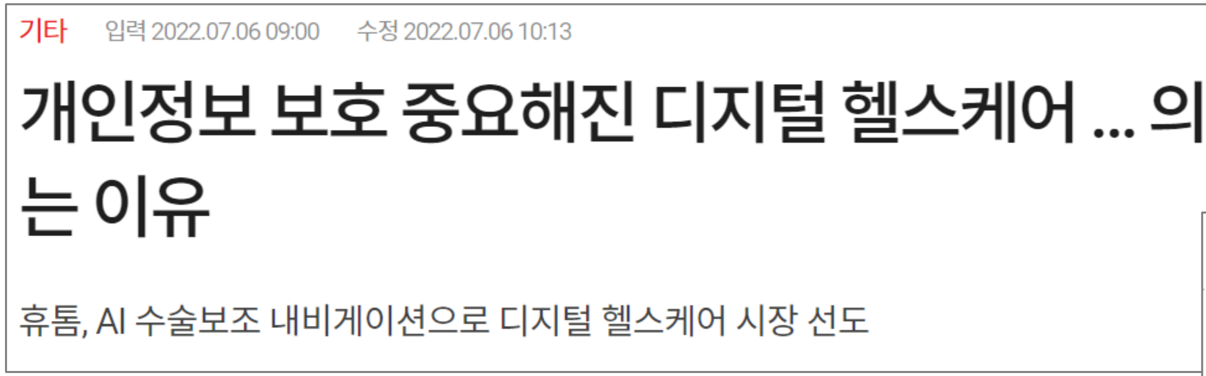
Specific Ways HE is Used in AI

Current Progress of the Study

AI and HE

AI and Privacy

AI and Privacy



기타 입력 2022.07.06 09:00 수정 2022.07.06 10:13

개인정보 보호 중요해진 디지털 헬스케어 ... 의료 AI 기업 움직임 주목받는 이유

휴톰, AI 수술보조 내비게이션으로 디지털 헬스케어 시장 선도

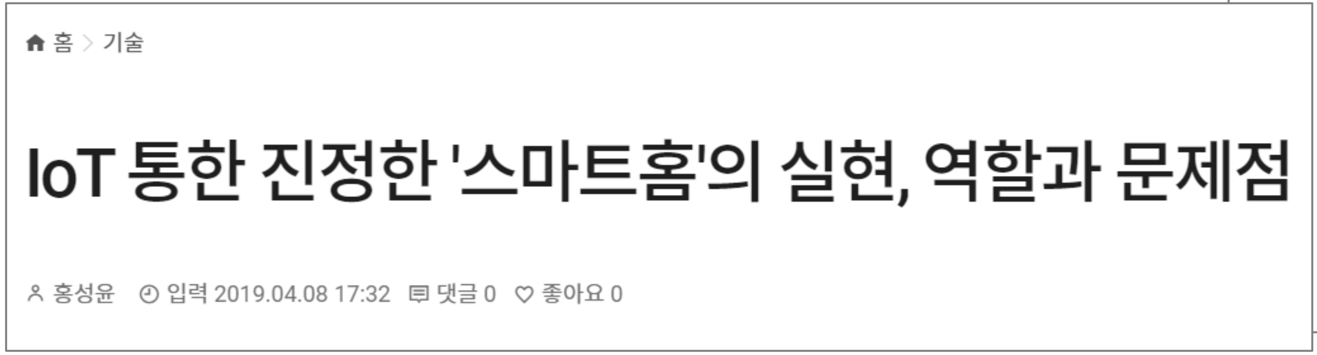
ETRI Insight

Insight Report 2019-59

국가지능화 특집

개인 맞춤형 의료: AI 적용과 당면과제

박종현 ● stephanos@etri.re.kr
기술정책연구본부



홈 > 기술

IoT 통한 진정한 '스마트홈'의 실현, 역할과 문제점

홍성윤 입력 2019.04.08 17:32 댓글 0 좋아요 0

AI and Privacy

1. Data Protection
2. Privacy Regulation
3. Cybersecurity
4. Algorithmic Bias
5. Accountability and Transparency

What is Homomorphic Encryption

Homomorphism

Homomorphic Encryption

Homomorphism

$$If < G,\blacksquare > and < H,* > are\ groups\ and\ f: G \to H,$$
$$then\ f\ is\ called\ a\ group\ homomorphism$$
$$if\ for\ all\ a, b\ \in G, f(a \blacksquare b) = f(a) * f(b).$$

$(example)$

$Consider < Z,+> and < Z_4,+>. Define\ f: Z\ \to Z_4\ by\ f(x) = [x] = \{x + 4k \mid k \in Z\}.$

$For\ all\ a, b \in Z, f(a + b) = [a + b] = [a] + [b] = f(a) + f(b).$

$f(7 + 5) = [7 + 5] = [12] = [0] = [7] + [5] = f(7) + f(5)$

Homomorphism

- A mathematical function that preserves the structure between two algebraic systems.
- A function that maps one algebraic system to another in a way that preserves certain operations or properties between them.

Homomorphic Encryption

A type of encryption that preserves certain operations on ciphertexts.

→ allows computations to be performed on encrypted data,

without the need to first decrypt the data.

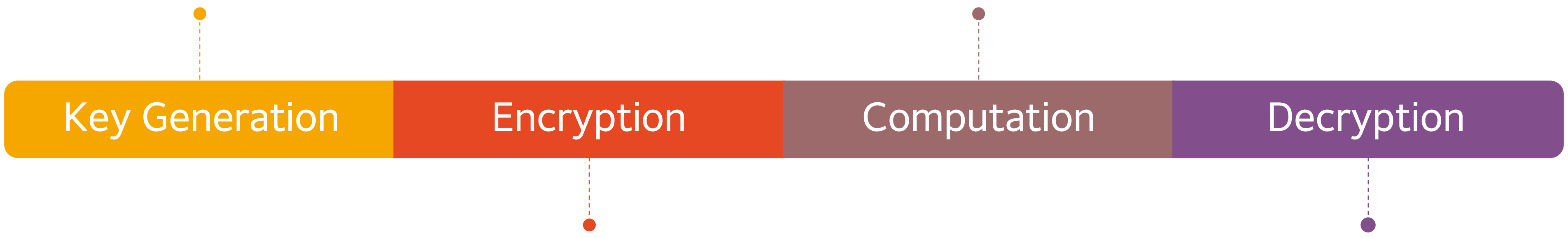
Homomorphic Encryption

Partial Homomorphic Encryption

Somewhat Homomorphic Encryption

Fully Homomorphic Encryption

How It Works



public key: encrypt data

secret key: decrypt data

1. a message → a mathematical representation,
2. the public key → encrypt the message →

   a ciphertext that appears as a random string of numbers and letters

When a computation is performed on two ciphertexts, the result is another ciphertext that can be decrypted to reveal the result of the computation.

When a computation is performed on encrypted data, the resulting ciphertext can be decrypted using the secret key to reveal the result of the computation.

How is HE used in AI?

Specific Ways

Medical Research

- Collaboration on sensitive medical data without compromising privacy.
- Researchers can encrypt their respective medical data sets and share them with each other, without the need to decrypt them.
- Protect against unauthorized access or data breaches.

Financial Industry

- Risk analysis on encrypted customer data.
- Instead of sharing the customers' sensitive credit data, the bank can encrypt the data and send it to a third-party analysis provider.
- Perform data analytics on large data sets, including financial market data.

Smart Home and IoT

- Privacy protection of data generated by smart devices.
- Encrypt the data before it is transmitted from the device to a central server or cloud storage system.
- Enable secure processing of the encrypted data without requiring the decryption of the data.
- Enable secure sharing of encrypted data between smart devi ces, without requiring that the devices decrypt the data.

Collaborative Machine Learning

- Shared training of AI models with multiple parties contributing data.
- Allows each party to keep their data private and secure, while still contributing to the overall accuracy of the model.
- By sharing the encrypted data, parties can collectively learn from the data without ever revealing their sensitive information to each other.

Current Progress of the Study

Limitations

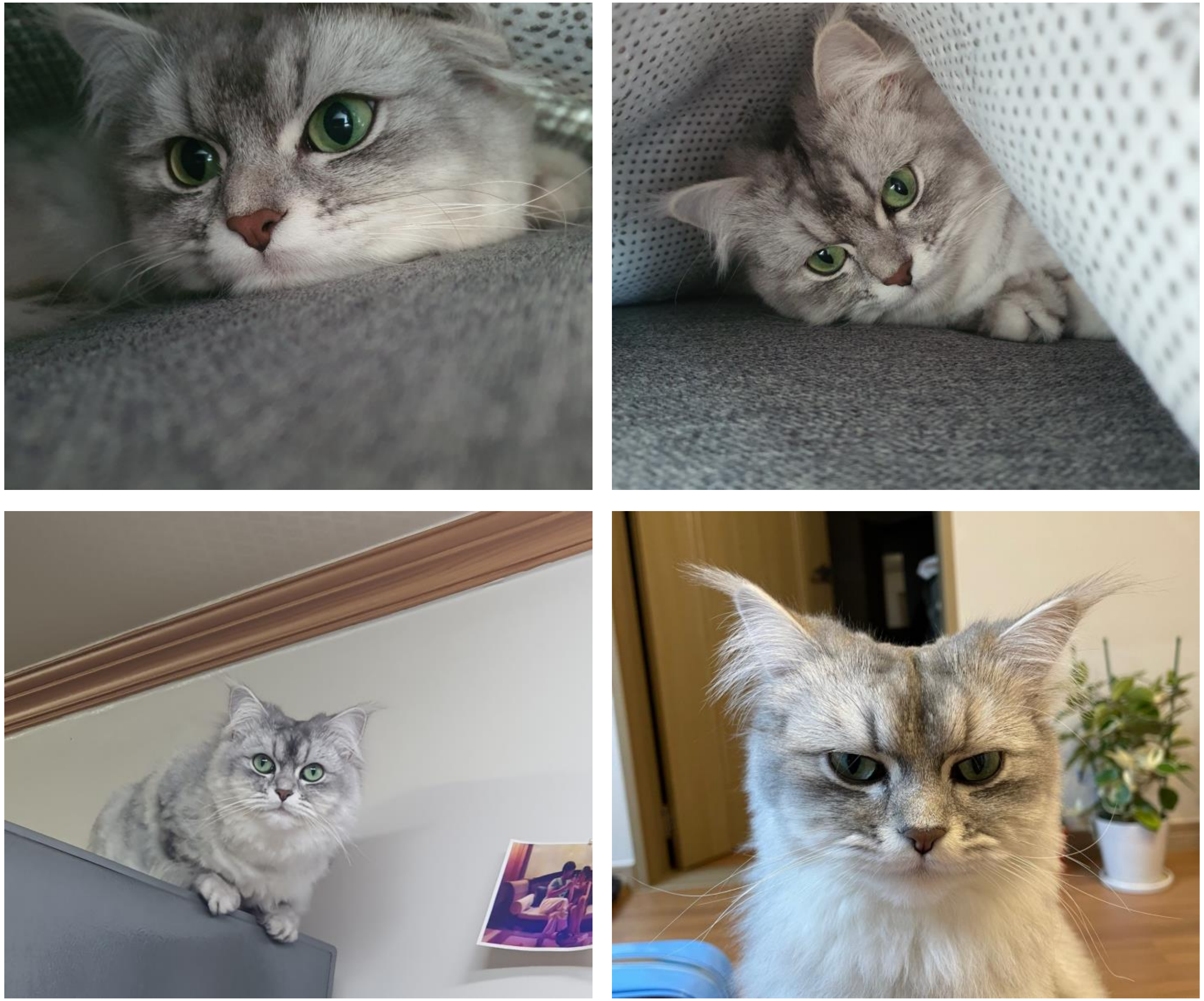
HEaaN

Current State of HE and its Limitations

- Computational complexity
- High communication and storage overhead
- Limited in the types of computations it can perform

HEaaN (혜안)

- A hybridencryption scheme that combines the benefits of both the fully homomorphic encryption (FHE) and the somewhat homomorphic encryption (SHE).
- Supports arbitrary computations on encrypted data while m aintaining a high level of security.



감사합니다.

정운서

216yoon@naver.com