
Emerging Technologies

컴퓨터개론

(Introduction to Computer Systems)

GEN1030

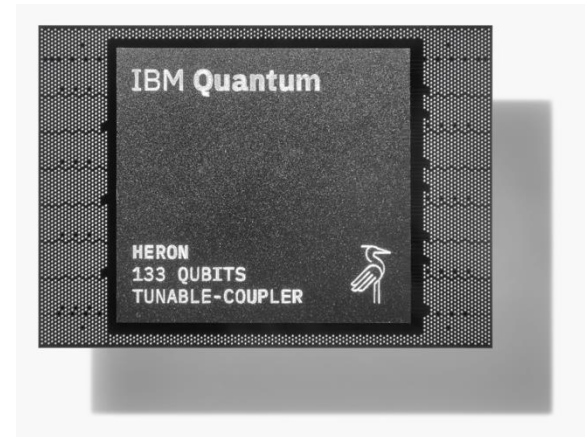
Quantum Computing

양자컴퓨팅

- 양자역학의 원리인 '중첩'과 '얽힘'을 활용해 기존 슈퍼컴퓨터로 수천 년이 걸릴 복잡한 연산을 몇 분 만에 해결할 수 있는 기술
 - 중첩(Superposition)
 - 기존 비트: 0 또는 1
 - 큐비트(Qubit): 양자컴퓨터에서 정보처리하는 단위
 - 정보를 0, 1 또는 0과 1의 중첩으로 처리
 - 얽힘(Entanglement)
 - 두 큐비트가 얽힌 상태
 - 수백 개의 큐비트를 얽어서 협력적으로 연산에 활용 → 큐비트 수가 늘어날수록 처리 능력이 기하급수적으로 증가

양자컴퓨터

- Google Willow (2024)
 - 105 큐비트
 - 기존 컴퓨터가 10^{25} 년 걸릴 연산 5분에 처리
- IBM Quantum System 2
 - 433 큐비트
 - 클라우드로 양자컴퓨터 접근 서비스 제공



양자컴퓨터와 보안

- 현재 인터넷 보안은 두 가지 수학적 난제에 기반
 - 소인수분해의 어려움(RSA 암호)
 - 이산 로그 문제의 어려움(ECC 암호)
- Shor algorithm
 - 양자컴퓨터에서 실행되는 알고리즘
 - 소인수분해와 이산 로그 문제를 다항식 시간에 풀 수 있음
→ 기존 암호 방식이 보장하는 안정성이 무너질 수 있음
- “Harvest Now, Decrypt Later”
 - 암호화 된 데이터를 지금 수집해 둔 후, 나중에 양자컴퓨팅 기술이 완성되면 그때 해독
 - 국가 기밀, 금융 거래 등 장기적으로 민감한 데이터 위험

Post-Quantum Cryptography (PQC)

- 양자 내성 암호
 - 양자컴퓨터로도 풀기 어려운 수학적 난제를 기반으로 한 암호 체계
- 미국 국립표준기술연구소(NIST) 표준화
 - 2024년 PQC 표준 발표
- Challenges
 - 기존 알고리즘(RSA/ECC)들이 인프라에 깊게 자리잡고 있음
 - 알고리즘 동작에 필요한 컴퓨팅 자원이 비교적 큼
 - 네트워크 오버헤드도 훨씬 큼
 - 저사양/저전력 기기에서 구동이 어려울 수 있음
- Post-Quantum TLS (PQTLS)
 - TLS handshake 과정에서 기존 알고리즘(ex. RSA/ECC) 대신 PQC 알고리즘을 사용
 - 통신 구조 자체는 TLS와 동일, 내부 암호 알고리즘만 교체
 - 표준화 진행 중

Big Data

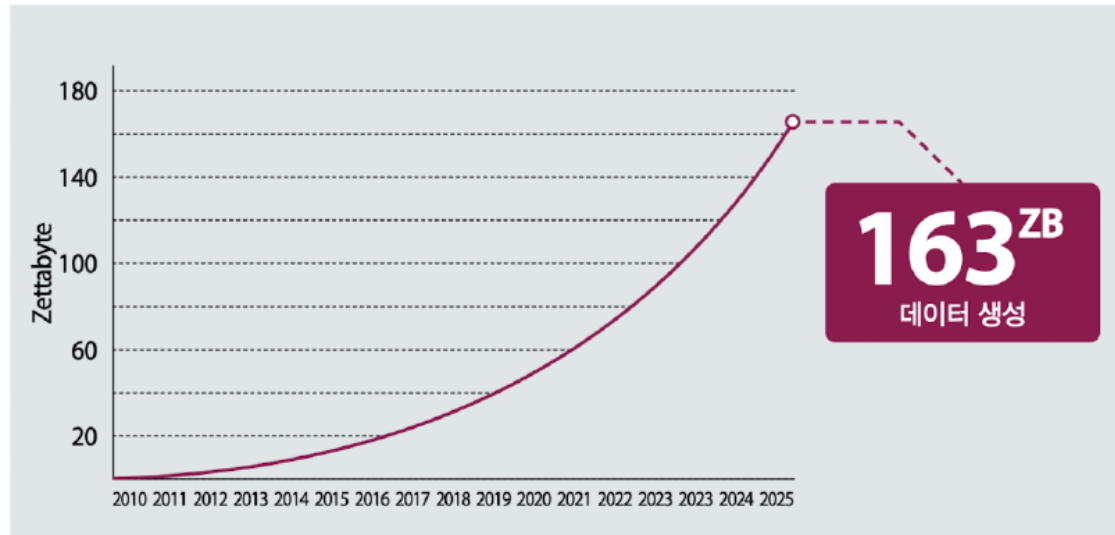
빅데이터(Big Data)

- 일반적인 데이터베이스로는 처리하기 어려운 정도의 큰 규모의 데이터
 - 기존 방식으로는 저장/처리/분석이 어려운 규모의 초대용량
 - Petabyte (PB), Exabyte (EB), Zettabyte (ZB) 단위
- 컴퓨터의 발전 및 보급이 확산됨에 따라 중요도 증가
 - 스마트폰 보급 → 1인당 데이터 생산량 증가
 - IoT 기기 확산 → 기계들이 끊임없이 데이터 생성
 - SNS, 스트리밍 등의 서비스 발달

빅데이터(Big Data)

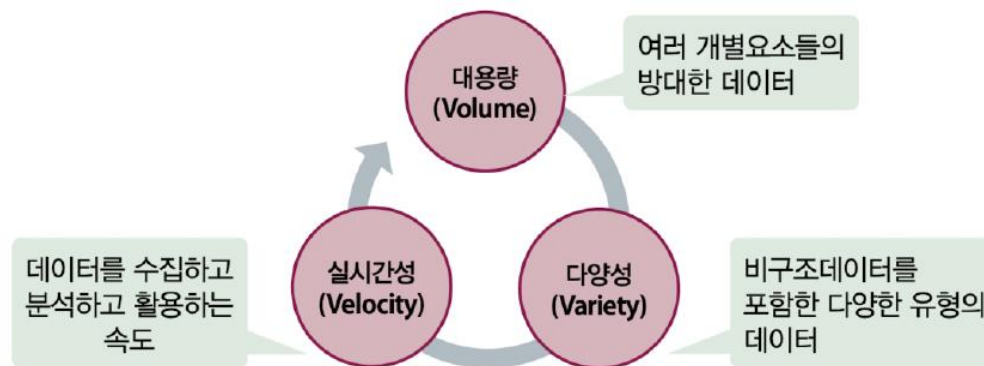
- 일반적인 데이터베이스로는 처리하기 어려운 정도의 큰 규모의 데이터
 - 기존 방식으로는 저장/처리/분석이 어려운 규모의 초대용량
 - Petabyte (PB), Exabyte (EB), Zettabyte (ZB) 단위

Yotta Byte(YB)	10^{24}
Zetta Byte(ZB)	10^{21}
Exa Byte(EB)	10^{18}
Peta Byte(PB)	10^{15}
Tera Byte(TB)	10^{12}
Giga Byte(GB)	10^9



빅데이터의 특징

- 빅데이터 3V
 - Volume (규모)
 - 방대한 데이터
 - 페타, 엑사, 제타바이트 단위
 - Variety (다양성)
 - 정수/실수, 텍스트, 음성, 이미지, 동영상 등 정형 데이터, 비정형 데이터 모두 포함
 - Velocity (속도)
 - 실시간으로 생성되고 처리되어야 하는 데이터



빅데이터의 특징

- 빅데이터의 가치
 - 이전에 관리되지 않던 새로운 데이터를 수집/분석함으로써 새로운 가치를 창출
 - 빅데이터 분석을 통해 의미 있는 정보를 실시간으로 도출
 - 이상 현상 감지, 트렌드 파악, 미래 예측, 마케팅, 의사 결정 등의 분야에서 활용
- 활용 사례
 - 영화 추천 알고리즘
 - 실시간 교통 정보
 - 질병 예측
 - 이상 거래 탐지

빅데이터 처리

1. 수집(Collection)

- 웹 크롤링(crawling), IoT 센서 데이터 등

2. 저장(Storage)

- Hadoop HDFS: 대용량 파일을 여러 서버에 분산 저장

3. 처리(Processing)

- Hadoop MapReduce, Apache Spark 등
- 배치 처리, 스트림 처리

4. 분석(Analysis)

- Python, R, SQL 등

5. 시각화/활용(Visualization)

- 분석 결과를 의사결정, 추천 시스템, 예측 모델에 적용