Digital Contents Security

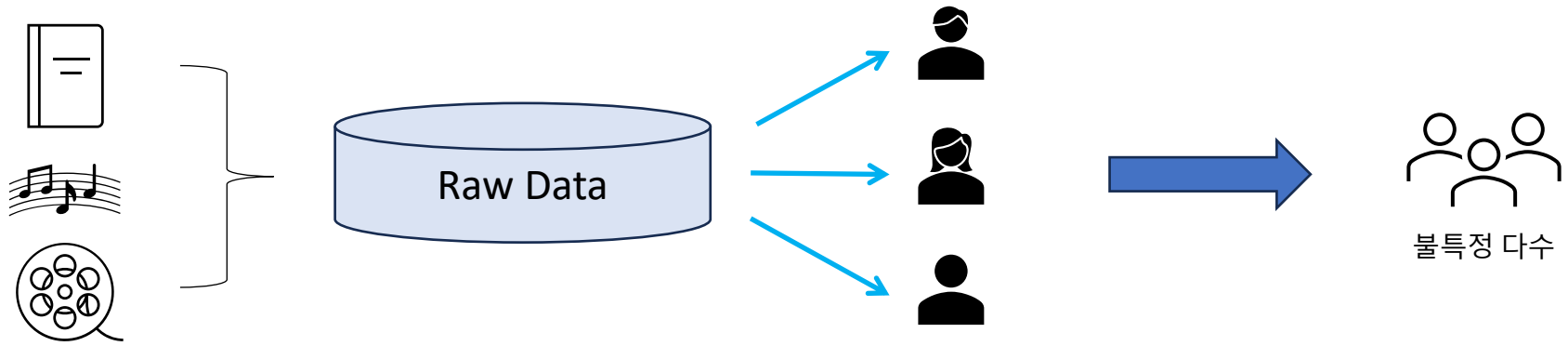
Vesper's

Advanced Features

for

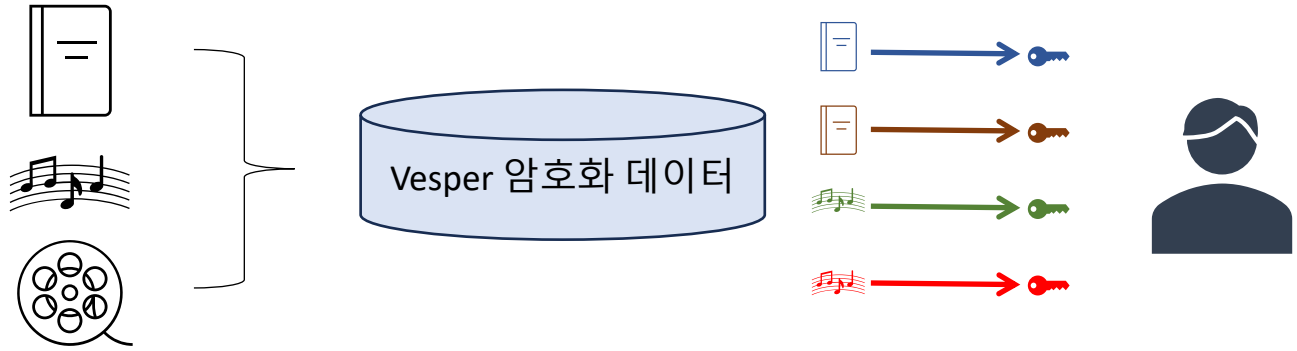
Enhanced Security

현재 디지털 컨텐츠 관리의 문제



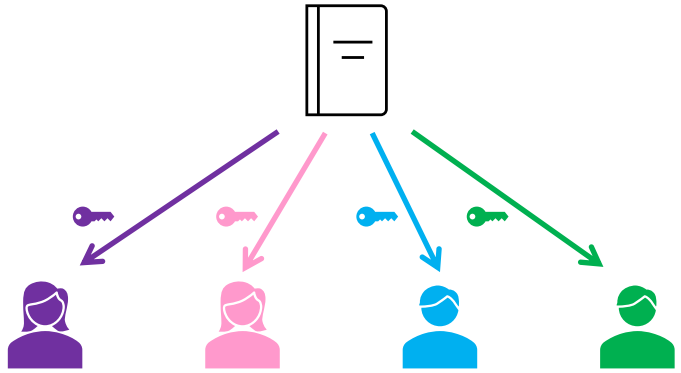
- 암호화되지 않은 데이터 관리
  - 문서, 음원, 영상 등 대부분의 컨텐츠는 서버에서 암호화되지 않은 평문으로 저장
  - 암호화되지 않은 상태로 사용자에게 전송
  - 한 명의 사용자로부터의 데이터 유출은 불특정 다수로의 배포를 의미: 명확한 저작권법 위반
- 불법적인 데이터 전송에 대한 방지책의 부재
  - 불법적으로 배포된 데이터는 원본과 동일: 출처의 불명확
- 현재 상용화된 암호체계의 한계
  - '모든 사용자'에게 전송된 '모든 데이터'를 개별적으로 관리할 방법이 없음

Vesper를 이용한 디지털 컨텐츠의 개별화



- 서버데이터의 암호화
  - 원본 데이터를 각 컨텐츠마다 별도로 Vesper를 이용하여 암호화된 상태로 서버에 저장
  - 데이터서버와는 별도의 키서버(key server)에서 키를 관리
- Vesper의 키모핑(key-morphing)을 이용한 사용자 별 컨텐츠의 개별화
  - Vesper 암호문 데이터는 사용자에게 전송될 때 개별적인 암호키(key)를 생성하여 새로운 암호문으로 전송
  - 동일한 컨텐츠(문서, 음원 등)라도 각 사용자 마다 다른 키의 암호문으로 전송
    - 사용자 'A'와 'B'가 동일한 컨텐츠를 구매하여 사용하여도 'A'의 키로 'B'의 컨텐츠를 사용할 수 없음
  - 동일한 사용자라도 각 컨텐츠 마다 다른 키를 사용함
    - 사용자 'A'가 컨텐츠 'X'와 'Y'를 구매하여도 X의 키로 Y를 사용할 수 없음

저작권자 및 판매자의 권리보호



- 컨텐츠 당 Vesper 키 생성횟수를 기준으로 실제 판매량을 측정
  - 불법복제 및 배포를 최소화하여 저작권자 및 판매자의 권리 보호
- 사용자 키 분실 시 새로운 키 생성
  - 사용자의 권리 보장
- Vesper 키 데이터의 응용 (1024 바이트 키의 경우)
  - 사용횟수 및 사용기간 설정
  - 판매 뿐만 아니라 대여 및 권리이전 등의 추가기능
- Steganography와 같은 디지털 지문 기술과 병행, 불법 배포물의 출처 확인 및 추적 가능