ICT의 가치를 이끄는 사람들!!

128회

정보관리기술사 기출풀이 4교시

T 02.724.1831 E kpcitpe@kpc.or.kr H www.kpc.or.kr C cafe.naver.com/kpcitpe

국가기술자격 기술사 시험문제

정보처리기술사 제 128 회 제 4 교시

분야	정보통신	종목	정보관리기술사	수험번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 25 점)

1. 최근 NFT(Non-Fungible Token) 시장의 활성화 및 생태계 형성의 견인차인 NFT 마켓 플레이스가 해커들의 주요 타겟이 되고 있다. 대형 거래소인 Opensea 의 보안 침해사례를 기반으로 NFT 특성과 마켓 플레이스에서의 보안 취약점을 설명하시오.

2. 웹서버의 안전한 운영을 위해 다양한 방안을 고려할 수 있다. 다음을 설명하시오.
   가. 리버스 프록시(Reverse Proxy)의 개념, 동작원리, 설정방법
   나. DDoS 사이버대피소

3. 6G 이동통신을 위한 위성-상공-지상 통합형 무선 네트워크(Satellite-Aerial-Terrestrial Integrated Network, SATIN)에 대하여 다음을 설명하시오.
   가. SATIN 의 개념 및 네트워크 특징
   나. SATIN 의 재난대비, UAV(Unmanned Aerial Vehcle) 활용, 낙후지역 네트워크 서비스에 활용방법

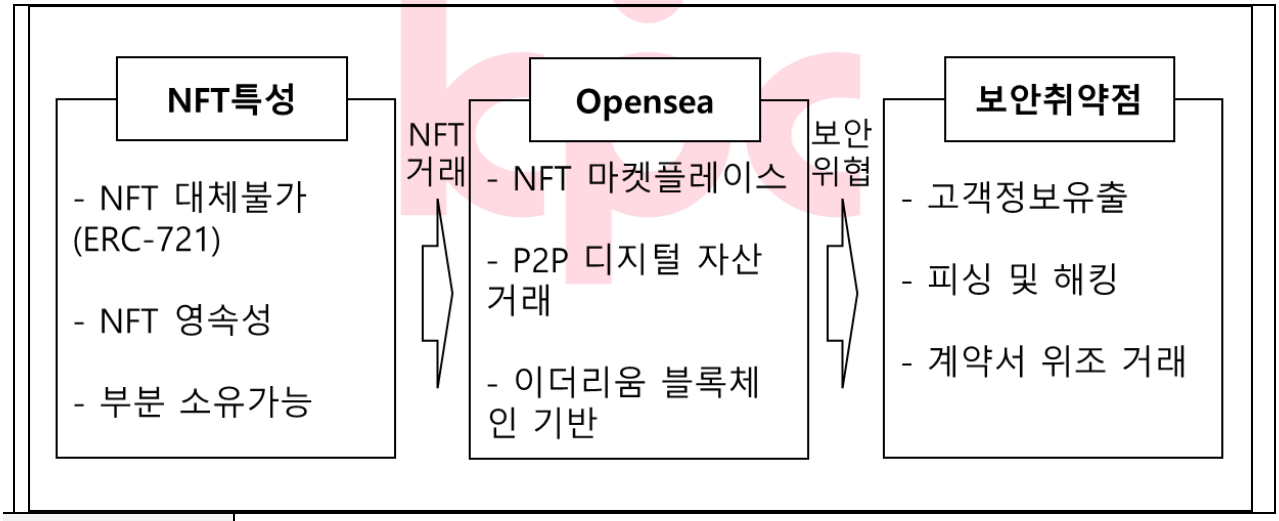
4. 최근 정보통신의 발전으로 인해 도감청이 불가능한 양자암호통신에 대한 관심이 높아지고 있다. 양자암호통신에 대하여 다음을 설명하시오.
   가. 양자암호통신의 암호키 분배방식
   나. 양자암호통신의 주요기술
   다. 양자암호통신의 취약점

5. 데이터베이스의 병행제어(Concurrency Control)에 대하여 다음을 설명하시오.
   가. 병행제어의 정의
   나. 병행제어의 기법의 종류
   다. 병행제어의 문제점

6. 식별(Identification)과 인증(Authentication)에 대하여 다음을 설명하시오.
   가. 개인 식별과 사용자 인증의 정의 및 차이점
   나. 사용자 인증 시 보안 요구 사항
   다. 인증 방식에 따른 4가지 유형 및 유형별 특징

문 제	**1. 최근 NFT(Non-Fungible Token) 시장의 활성화 및 생태계 형성의 견인차인 NFT 마켓 플레이스가 해커들의 주요 타겟이 되고 있다. 대형 거래소인 Opensea 의 보안 침해사례를 기반으로 NFT 특성과 마켓 플레이스에서의 보안 취약점을 설명하시오**
출 제 영 역	디지털서비스 / 난 이 도 ★★★☆☆
출 제 배 경	- NFT 의 활성화로 대형 NFT 마켓플레이스인 Opensea 의 보안 침해사례 발생으로, NFT 를 구매 및 판매하기 위한 중개자 역할을 하는 마켓 플레이스의 보안 취약점 인식 및 대응 방안 고려
출 제 빈 도	- 126 회 컴퓨터시스템응용기술사 (2 교시)
참 고 자 료	- 해시넷 (대체불가토큰) - http://www.thescoop.co.kr/news/articleView.html?idxno=53720 - https://blog.naver.com/phemex2019/222481373021
Keyword	- NFT, ERC-721, 마켓 플레이스, 서명탈취, 플러그인 취약점, 고객정보 유출, 에어드랍, 익스플로잇
풀 이	박영길(126 회 정보관리기술사)

1. Opensea NFT(Non-Fungible Token) 마켓 플레이스 보안침해 개요

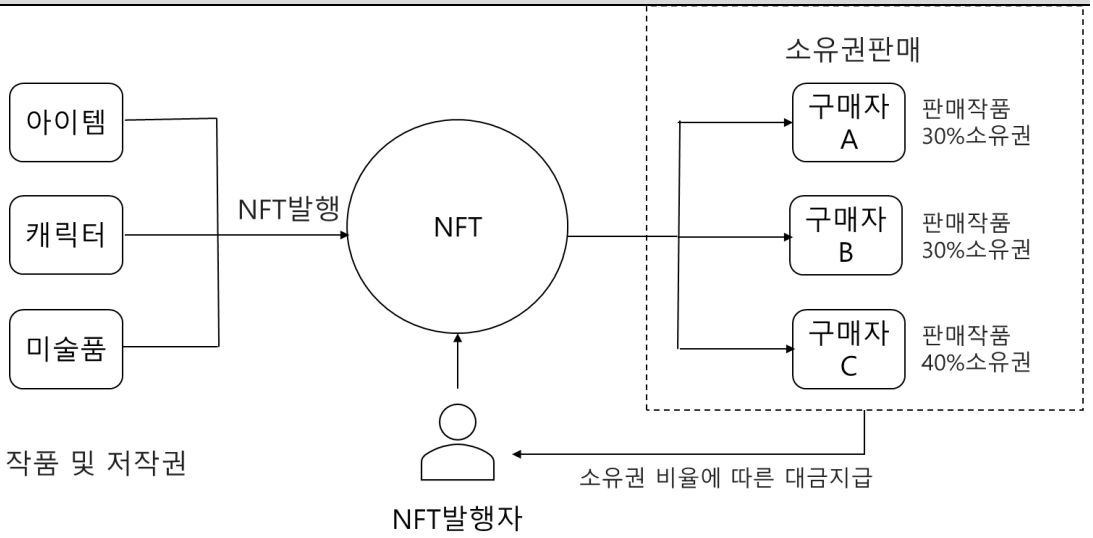


Opensea	- NFT(대체불가토큰)를 판매하고 구입할 수 있는 마켓 플레이스로서 암호화폐 소장품 NFT 등 다양한 아이템을 경매 등의 방식으로 거래할 수 있는 사이트	
Opensea 보안침해사례	**- 고객정보유출**	- Opensea 내부 감독 부실로, 협력사 직원 통한 고객 개인정보 외부 유출
	- 피싱/해킹	- 공식 소셜 네트워크 계정, 디스코드 해킹 통해 피싱 사이트 광고로 사용자를 악성 피싱 사이트로 유도해 NFT 탈취
	- 위조계약서 활용한 NFT 탈취	- 와이번 프로토콜의 유연성을 이용하여 고객 서명 탈취 후 오프체인에서 고객서명 이용해 위조계약서를 작성하여 NFT 탈취

- NFT 의 활성화로 대형 마켓 플레이스인 Opensea 가 대중화되자 피싱, 사용자 부주의, 위조계약서 통한 NFT 자산 탈취 등 다양한 보안 침해 사건 발생
- Opensea 는 P2P 기반 마켓 플레이스로 소장하고 있는 NFT 를 익명의 사용자에게 구매 또는 판매 가능.

2. NFT(Non-Fungible Token)의 특성

가. NFT 개념 및 개념도

구분	설명	
개념도		
개념	- 디지털 자산의 고유한 가치와 소유권을 기록하기 위해 블록체인 ERC721 표준 기반 고유한 값을 가지고 상호 교환할 수 없는 토큰	
NFT 유형	- 예술작품	- 디지털 작품, 드로잉, 사진 등 이미지를 NFT 로 생성, 이미지를 하나의 NFT 로 만들어 판매하거나, 여러 개의 이미지를 하나의 컬렉션으로 묶어서 제공
	- 게임자산	- 게임내 능력치 부여 아이템, 가상 부동산과 같은 게임자산을 NFT 로 제공
	- 도메인이름	- ETH 같은 분산형 도메인을 이더리움 네임 서비스(ENS)에서 NFT 로 등록 및 판매

- NFT 는 추적성, 거래간소화, 부분소유, 희소성, 프로그램화 가능과 같은 NFT 만의 고유한 특성이 존재

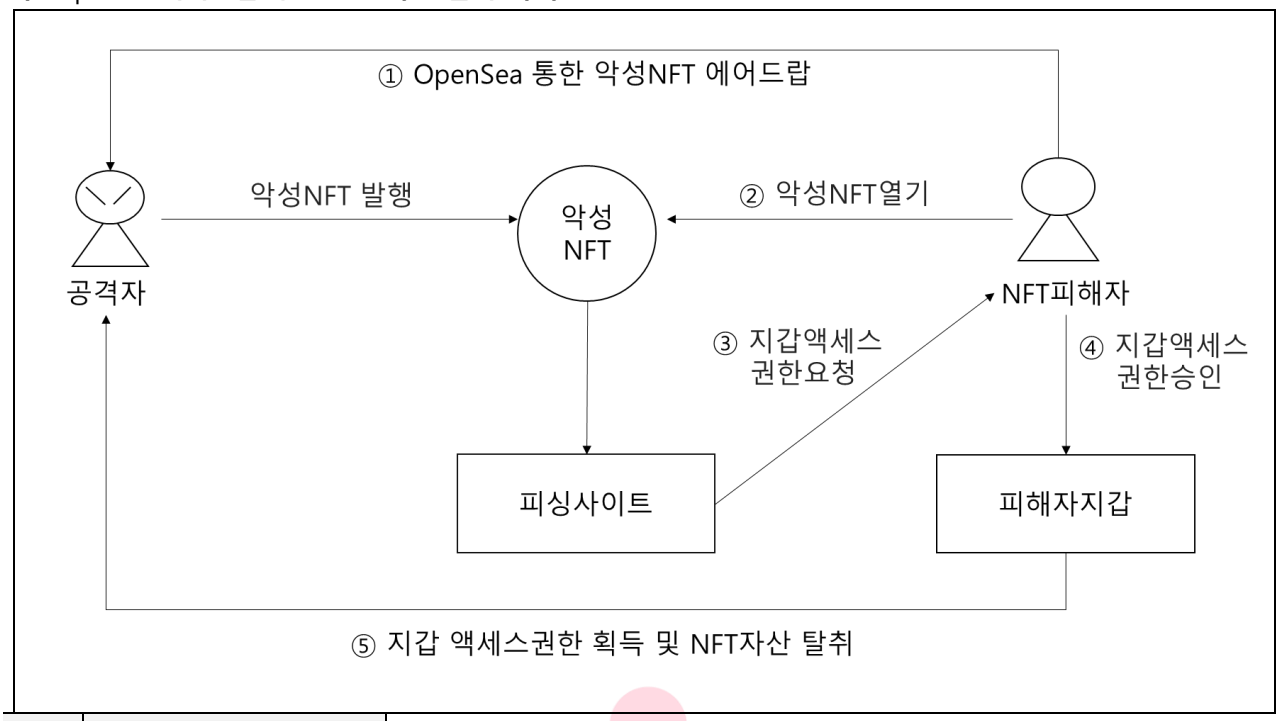
나. NFT 특성

특성	설명
- 추적성	- NFT 는 자산에 대한 기록이 블록체인을 통해 이루어지기 때문에 누구나 NFT 의 출처, 발행 시간, 소유자 내역 및 기타 정보 확인 가능
- 소유권 증명	- 위 변조가 불가능한 블록체인의 특성을 통해 소유한 NFT 에 대한 소유 내역을 증명 가능
- 부분 소유	- NFT 는 부분에 대한 소유권을 인정해 하나의 NFT 에 대해 1/N 으로 나누어서 부분 소유 가능
- 쉬운 거래	- NFT 는 공급량, 판매 방법, 결제 방법까지 본인이 결정할 수 있어 디지털 자산 거래소를 통해 손쉽게 매매 가능
- 희소성	- 디지털 자산의 가장 큰 약점인 무한 복제로 인한 가치화가 어렵기 때문에 NFT 를 통한 희소성 부여 가능
- 프로그램화 가능	- 스마트 컨트랙트를 이용해서 NFT 작품에 대해 원하는 거래조건 및 기능을 직접 스마트 컨트랙트에 작성하고 블록체인에 직접 민팅 가능

- NFT 를 통한 자산화가 증가함에 따라 대형 NFT 마켓플레이스인 Opensea 에서 보안 취약점을 통한 지갑 탈취, 사용자 정보를 통한 피싱 등을 통한 금전적 피해 사례 발생

3. 마켓 플레이스에서의 보안 취약점 설명

가. Opensea 에어드랍 통한 NFT 자산 탈취 사례



1	- 악성 NFT 에어드랍	- 공격자 악성 NFT 를 발행 후 피해자의 선물함에 에어드랍 * 에어드랍 : 사용자에게 무상으로 코인을 배분하여 지급하는 행위
2	- 악성 NFT 열기	- 피해자는 악성 NFT 를 받기 위해 Opensea 선물함에서 NFT 열기 수행
3	- 지갑 액세스 승인요청	- NFT 열기 수행 시 공격자 피싱 사이트로 이동, 가상화폐 지갑에서 자신의 지갑으로 인출하는 NFT 거래화면을 보여줌
4	- 지갑 액세스 권한승인	- 피해자가 NFT 거래내역을 제대로 보지 않고 거래화면의 승인 버튼을 누르면 피해자의 서명을 통해 피해자 지갑 접근 권한 승인
5	- 피해자 NFT 가상자산 이전	- 공격자가 거래에 요청한 거래내역에 따라 피해자의 가상자산을 피해자 지갑에서 공격자 지갑으로 이전

- 에어드랍을 통한 보안취약점은 피해자의 부주의를 노린 사회적공학 방식의 공격으로 사용자의 부주의를 통해 서명정보를 탈취하여 피해자 지갑의 액세스 권한 획득

나. NFT 마켓플레이스 보안 취약점 설명

구분	보안 취약점	설명
사회공학적 공격	- 내부 정보 거래	- 사내 정보를 이용해 상품을 게시하기 전 비밀리에 NFT 를 구매하여 초기 구매 가격의 두 배에서 다섯 배에 달하는 수익 취득
	- 고객 정보 유출	- 고객 정보를 관리하는 직원 및 관계자에 의한 고객정보 유출
피싱/해킹	- 소셜 네트워크 공식 계정 해킹	- 소셜 네트워크 공식 계정 해킹 통해 신규 NFT 민팅(발행) 광고를 공격자가 등록, 피해자가 광고를 클릭 시 광고를 통해 피싱 사이트로 이동 후 NFT 탈취
	- e 메일광고 피싱	- NFT 를 무료로 제공하는 광고 이메일 발송, NFT 를 받기 위해 이메일 링크를 클릭하면 지갑 플러그인(메타마스크 등)을 통해 피해자 자산을 공격자 지갑으로 전송

NFT 마켓 플레이스 취약점	- 익스플로잇 공격	- 보유 NFT 를 기본지갑에서 보조지갑으로 이전 후 다시 기본지갑으로 전송하면 가스를 별도로 들이지 않고 NFT 희망가를 새로 등록 가능. 하지만 마켓 플레이스 리스트에는 이전 희망가격이 여전이 존재하여 공격자는 가장 저렴했던 희망가격을 마켓 플레이스의 OpenAPI 를 통해 NFT 를 저렴하게 구입 후 재판매
	- 웹 플러그인 취약점	- 마켓 플레이스 선물함 내 에어드랍으로 들어와 있는 NFT 클릭시 악성 피싱 사이트로 이동, NFT 탈취 위한 거래계약서를 피해자가 확인하지 않고 메타마스크와 같은 웹 플러그인을 통해 거래계약에 승인하면, 피해자 자산을 공격자 지갑으로 자산 이전

- Opensea 고객 개인식별번호 유출로 인한 피싱, 이전(Transfer) 기능. API 취약점을 이용한 익스플로잇 공격 등 NFT 마켓플레이스에 대한 해킹 사례로 2 단계 인증 등 안전한 마켓 플레이스 거래 위한 장치 필요

4. NFT 마켓 플레이스 보안 취약점 대응방안

구분	대응방안	설명
사회공학적 공격대응	- 보안교육	- NFT 마켓플레이스 고객 정보 유출 방지를 위한 정기적인 정보보안교육 수행
	- 접근제어	- 내부자원에 대한 ACL(Access Control List) 활용 - MAC/DAC/RBAC 에 기반한 접근제어 수행
	- 2 단계인증	- 2 단계 인증 활성화로 NFT 거래 시 이용자 거래 내역 재확인으로 계약 조건 오인 방지
피싱/해킹	- NFT 보안정책과 가이드라인 활용	- 과학기술정보통신부 NFT 보안협의체를 통한 NFT 보안이슈 사전대응, 가이드라인 제정으로 안전한 NFT 활용
NFT 마켓 플레이스 취약점	- 에어드랍 보안 패치	- 에어드랍 또는 내가 원하지 않거나 알지 못하는 사람이 보내준 NFT 는 Hidden 탭에 자동으로 분류
	- NFT 리스팅 관리자 툴 패치	- 이전(Transfer) 버그를 활용한 익스플로잇 공격을 원천 봉쇄하기 위해 기존에 등록한 NFT 를 반드시 취소해야만 NFT 마켓 플레이스에 NFT 를 가격을 등록할 수 있는 리스팅 관리자 툴 기능 제공
	- EIP712 적용	- 사용자가 서명시 해시 값을 확인하기 힘든 문제를 해결하기 위해 사용자에게 해시 값이 아닌 사용자가 알기 쉬운 언어로 서명 내용을 보여주기 위한 스마트 계약인 EIP-712 활용

- NFT 자체는 데이터 위조/변조에는 강한 특성을 가지나 NFT 마켓플레이스는 중계사이트로써 보안 면에서는 일반 사이트와 다르지 않아 주의 필요

"끝"

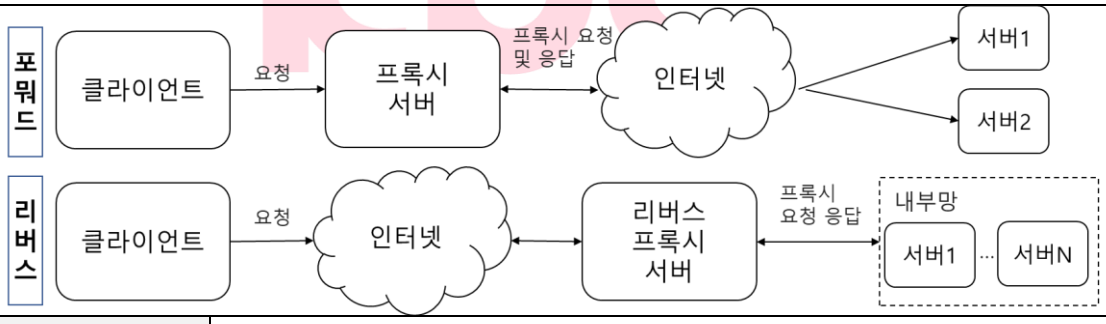
기출풀이 의견

1. 대형 NFT마켓플레이스인 Opensea의 사례 기반으로 NFT의 특성. 보안 취약 사례에 대해 풍부하게 작성하시면 좋습니다. 만약 Opensea의 보안 취약점 사례를 알지 못할 경우 일반적인 NFT 보안 취약점 사례로 대응하시면 좋겠습니다.

문 제	2. 웹서버의 안전한 운영을 위해 다양한 방안을 고려할 수 있다. 다음을 설명하시오. 가. 리버스 프록시(Reverse Proxy)의 개념, 동작원리, 설정방법 나. DDoS 사이버대피소		
출 제 영 역	정보보안	난 이 도	★★★☆☆
출 제 배 경	- DDoS 발생시 피해를 최소화할 수 있는 DDoS 사이버대피소에 대한 이해 및 사이버대피소를 구현하기 위한 기반 기술인 리버스 프록시 기술에 대한 이해		
출 제 빈 도	110 회 정보관리기술사 (1 교시)		
참 고 자 료	- Http 완벽가이드 - Apache(https://httpd.apache.org/), Nginx(https://www.nginx.com/)		
K e y w o r d	- 포워드 프록시, 리버스 프록시, Apache, NginX, KISA 사이버대피소, 트래픽 우회, DDoS 차단		
풀 이	박영길(126 회 정보관리기술사)		

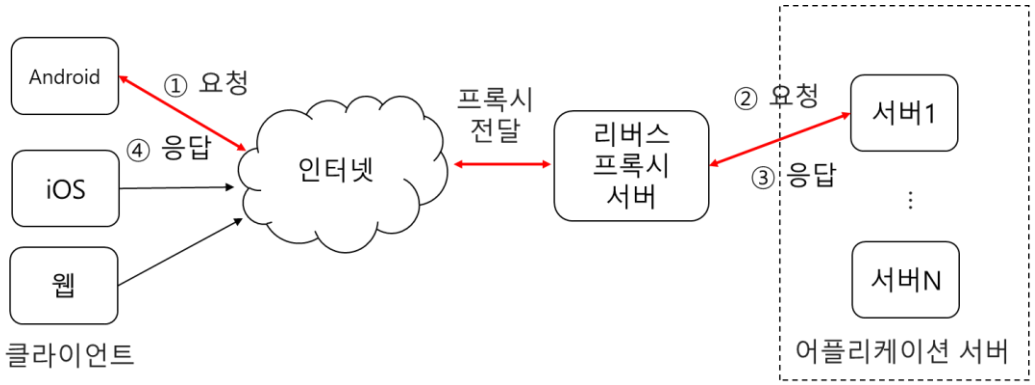
1. 리버스 프록시(Reverse Proxy)의 개념 및 동작원리

가. 리버스 프록시(Reverse Proxy)의 개념 및 특징

구분	설명	
개념	- 외부에 리버스 프록시 서버주소를 노출하여 클라이언트의 서비스 요청 시 리버스 프록시 서버가 직접 요청을 받아 실제 서버의 처리결과를 전달하는 장치	
개념도		
특징	- 로드밸런싱	- 리버스 프록시 뒤에 여러 개의 WAS 를 둠으로써, 사용자 요청을 분산 - End-point 마다 호출 서버를 설정할 수 있으며, 역할에 따라 서버의 트래픽을 분산 가능
	- 보안	- 내부 IP 노출 방지 등, 보안 상의 이유로 서버에 직접 접근하는 것을 막기 위해 DMZ 같은 네트워크에 리버스 프록시를 구성하여 접근
	- 성능 향상	- 리버스 프록시의 캐싱정보를 통해 캐싱된 정보가 있으면 내부망을 거치지 않고 캐싱 정보를 전달함으로써 성능 향상

- 포워드 프록시는 클라이언트에서 서버로 리소스를 요청할 때 서버로 직접 요청하지 않고 프록시 서버를 통해 요청 후 인터넷에 연결하여 요청 대리 수행 (클라이언트 숨김)
- 리버스 프록시는 포워드 프록시의 반대 개념으로 클라이언트가 서버를 요청할 경우 리버스 프록시를 호출하고, 리버스 프록시가 서버로부터 응답을 전달받아 다시 클라이언트에게 전송 (서버 숨김)

나. 리버스 프록시(Reverse Proxy)의 동작원리

구분	설명	
개념도		
동작원리	**1) 클라이언트 요청**	- 클라이언트가 인터넷을 통해 리버스 프록시 서버에 요청
	2) 프록시 서버 요청 전달	- 리버스 프록시 서버는 내부망의 어플리케이션 서버에 클라이언트 요청 전달
	3) 프록시 서버 응답 전달	- 내부망에 전달된 요청을 처리 후 리버스 프록시를 통해 응답 전달
	4) 클라이언트 응답	- 프록시 서버를 통해 내부망 응답을 클라이언트에 전달

- 리버스 프록시는 Apache, Nginx 와 같은 웹서버 소프트웨어를 이용하며 간단한 설정파일 수정으로 구현 가능

2. 리버스 프록시(Reverse Proxy) 설정방법

가. Apache 리버스 프록시 설정방법

```
# /etc/apache2/sites-available/000-default.conf 설정파일 수정
  <VirtualHost *:80>
    ...
    ProxyPass / https://www.kpc.or.kr/
    ProxyPassReverse / https://www.kpc.or.kr/
    ...
</VirtualHost>
```

1) Apache 설정파일 열기	- /etc/apache2/sites-available/ 경로의 Apache 설정파일 열기 - http 설정경로 : /etc/apache2/sites-available/000-default.conf - SSL 설정경로 : /etc/apache2/sites-available/000-default-le-ssl.conf
2) 리버스 프록시 경로 설정	- VirtualHost 태그 내의 ProxyPass, ProxyPassReverse 항목을 리버스 프록시 서버의 경로로 설정
3) Apache 서버 재시작	- 변경된 리버스 프록시 경로 적용을 위해 systemctl status apache2.service 명령어를 통해 Apache 서버 재시작
4) 리버스 프록시 서버 동작 확인	- 2)에서 설정한 리버스 프록시 서버 URL 로 접속 후 정상 작동 여부 확인

- ProxyPass 는 / 로 들어오는 요청을 https://www.kpc.or.kr 로 보낸다는 의미
- ProxyPassReverse 는 클라이언트 우회를 방지위해 응답 헤더의 https://www.kpc.or.kr 을 / 주소로 변경하라는 의미

나. Nginx 리버스 프록시 설정방법

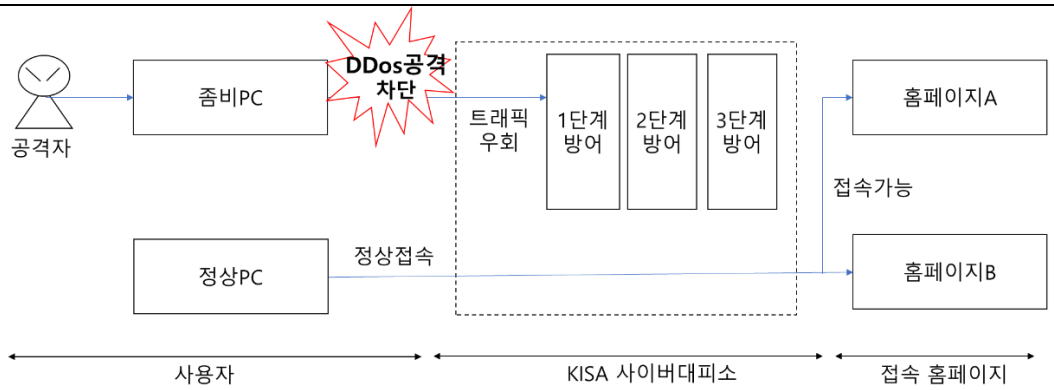
```
# /etc/nginx/conf.d/default.conf 설정 파일 수정
server {
        listen 80;
          ...
        location / {
          proxy_pass https://www.kpc.or.kr/
          ...
        }
}
```

1) Nginx 설정파일 열기	- /etc/nginx/conf.d/default.conf 경로의 Nginx 설정파일 열기
2) 리버스 프록시 경로 설정	- location 경로 내의 proxy_pass 항목을 통해 리버스 프록시 서버의 경로 설정 - 위의 예제에서 / 주소로 접근 시 https://kpc.or.kr 주소로 연결
3) Nginx 설정적용	- 변경된 리버스 프록시 경로 적용을 위해 nginx -s reload 명령어 통해 nginx 설정 적용 * restart 는 서버 재 기동, reload 는 변경된 설정만 적용
4) 리버스 프록시 서버 동작 확인	- 2)에서 설정한 리버스 프록시 서버 URL 로 접속 후 정상 작동 여부 확인

- 리버스 프록시를 활용하여 DDos 공격시 DDos 트래픽을 우회 및 차단하는 DDos 사이버 대피소로 활용 가능

3. DDos 사이버 대피소 설명

가. DDos 사이버 대피소 정의 및 개념도

구분	설명
개념	- DDoS 공격시 피해 웹사이트로 향하는 DDoS 트래픽을 대피소로 우회하여 분석, 차단함으로써 정상적으로 운영될 수 있도록 KISA 에서 제공하는 중소기업 무료지원 서비스
개념도	

- 사이버대피소는 웹사이트 접속 시 수행되는 도메인 질의 값을 대피소에서 준비한 IP 로 변경함으로써 공격을 하는 좀비 PC 를 비롯한 모든 접속요청을 대피소로 전달하여 공격 트래픽을 구별
- 즉, 웹사이트에 접속하는 일반 사용자는 사이버대피소의 IP 로 콘텐츠를 요청하고 이를 대피소에서 응답해 물리적인 시스템 변경 없이 웹사이트가 운영되는 한편, IP 가 변경됨으로써 디도스 공격 트래픽은 목표로 한 웹사이트에 피해를 입힐 수 없음

나. DDos 사이버대피소 구성요소

구분	구성요소	설명
사용자	- 좀비 PC	- 공격자에 의해 감염되어 DDoS 공격을 수행하는 공격 PC
	- 정상 PC	- 정상적으로 웹사이트를 이용하는 사용자 PC
사이버 대피소	- 1 단계 방어 (네트워크 소모성 공격 방어)	- DDoS 전용 대응장비와 ISP 와의 협 업을 통해 UDP. ICMP Flooding 과 같은 전통적인 네트워크 자원 소모성 공격에 대한 방어를 수행
	- 2 단계 방어 (IP 를 통한 사용자 구분)	- QoS 장비를 활용하여 사이버대피소로 유입되는 발신지 IP 를 좀비 PC 와 정상 사용자로 구분하여 적절한 가용량을 할당
	- 3 단계 방어 (가용성 확보)	- L7 스위치와 웹 캐싱을 통해 트래픽을 단순화하고 부하를 분산시켜 공격대상 웹서버의 가용성 확보
접속 홈페이지	- 홈페이지 서버	- DDoS 공격 대상 홈페이지 서버, 사이버 대피소에 의해 DDos 공격 트래픽은 우회되며, 일반적인 사용자는 정상 이용가능

- DDos 사이버 대피소는 중소기업기본법 제 2 조 및 중소기업기본법 시행령 제 3 조에 해당하는 중소기업이 활용
- DDos 사이버 대피소는 대응 구분에 따라 사전/긴급으로 구성되며 사전에 미 등록된 웹사이트도 이용가능

4. DDos 사이버 대피소의 사전/긴급 대응 절차

- 실제 디도스 공격이 발생하기 전 사전등록 신청서를 제출해 실제 공격 발생 시 소요되는 시간 절약 가능
- 사전 등록을 하지 않은 상황에서 공격이 시작됐다면 긴급대응 서비스를 이용 가능. 행정적인 절차를 사후에 처리하고 기본적인 웹사이트 운영 환경만 확인해 방어 서비스를 운영

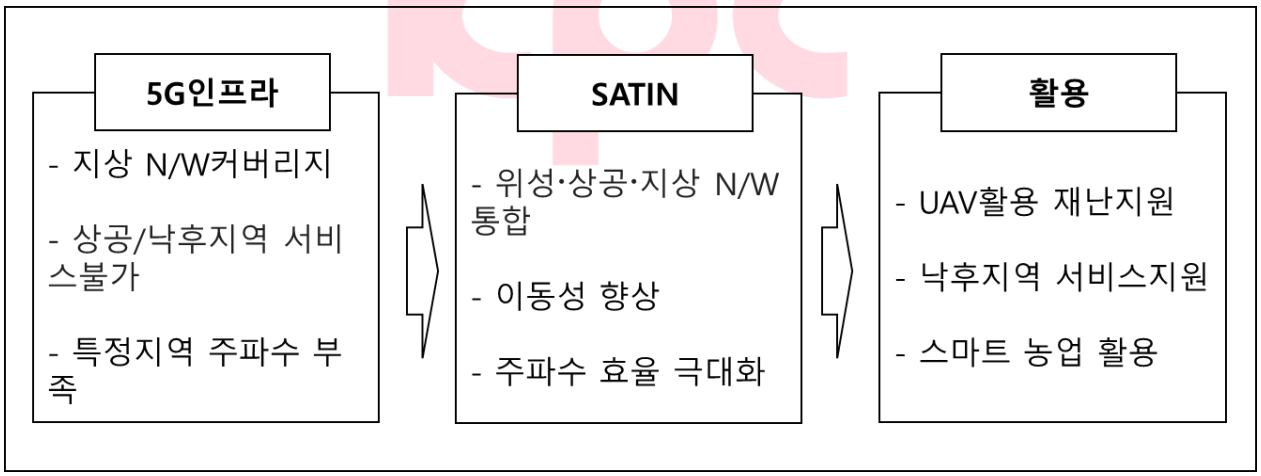
"끝"

기출풀이 의견

2. 제시된 문제에 맞추어 리버스 프록시에 대한 내용을 풍부하게 작성하시고, 사이버 대피소의 세부 내용과 리버스 프록시와의 관계를 작성하시면 차별화된 답안이 가능합니다. 4단락으로 DDoS 사이버 대피소의 사전/긴급 대응 외 해외 적용 사례 및 대응 방안에 대해 작성하셔도 좋습니다.

문 제	3. 6G 이동통신을 위한 위성-상공-지상 통합형 무선 네트워크(Satellite-Aerial-Terrestrial Integrated Network, SATIN)에 대하여 다음을 설명하시오. 가. SATIN 의 개념 및 네트워크 특징 나. SATIN 의 재난대비, UAV(Unmanned Aerial Vehicle) 활용, 낙후지역 네트워크 서비스에 활용방법		
출 제 영 역	네트워크	난 이 도	★★★★★
출 제 배 경	- 지상 위주 서비스 기술인 5G 이동통신 기술의 단점을 극복하기 위해 위성, 상공, 자상 전체를 서비스할 수 있는 SATIN 기술 이해		
출 제 빈 도	미 출제		
참 고 자 료	- 6G 이동통신을 위한 위성-상공-지상 통합형 무선 접속 네트워크 연구 (https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10671673)		
Keyword	- 위성 RAN, 상공 RAN, 지상 RAN, 다중접속제어, 인지스팩트럼, 공동간섭제어, 이동성관리, UAV		
풀 이	박영길(126 회 정보관리기술사)		

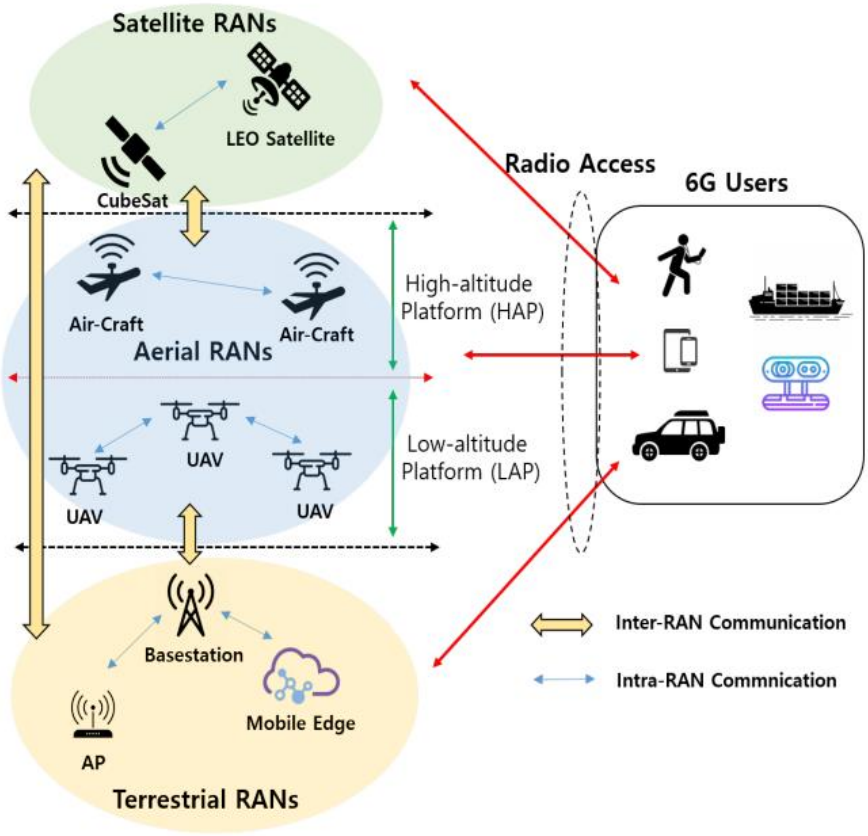
1. 5G 인프라 단점 극복 SATIN 의 개요



- 현재의 5G 인프라 구조는 지상 커버리지만 고려하여 설계되어 있기 때문에 인프라가 구축되지 않은 낙후된 공간이나 상공에서 고속으로 이동하는 이동물체 (드론, 항공선) 등에 서비스 전달이 힘들 뿐만 아니라 특정공간에 다수의 유저가 모이는 환경 (대규모 공연장, 스포츠 경기장)에서 주파수가 부족할 수 있는 문제점 존재
- 최근에는 한정된 커버리지, 주파수 부족 등 5G 서비스의 문제점들을 해결하기 위해서 6G 이동통신에서는 위성-상공-지상의 네트워크를 통합한 통합형 무선 접속네트워크 (Satellite-Aerial- Terrestrial Integrated Network, SATIN) 구조에 대한 연구가 진행 중
- 기존의 지상망에 상공의 영역의 네트워크를 통합함으로써 좀 더 나은 채널 액세스 환경을 제공하고 확장된 네트워크 커버리지를 통해 UAV 를 통한 이동성을 넓혀주어 재난지원, 낙후지역 네트워크 서비스에 활용 가능

2. SATIN 의 개념 및 네트워크 특징

가. 5G 인프라 단점 극복위한 SATIN 의 개념

구분	설명
개념	- 5G 의 단점인 지상 커버리지만 고려한 설계를 개선, 기존의 지상망에 상공, 위성 네트워크를 통합해서 채널 액세스 환경과 네트워크 커버리지를 증가시키는 기술
개념도	

- SATIN 은 위성(Satellite), 상공(Aerial), 지상(Terrestrial) RAN 을 서로 연계하여 통신 수행
- SATIN 을 통해 상공을 이동하는 UAV 로으로 네트워크 인프라가 활성화되지 않은 지역 이용가능

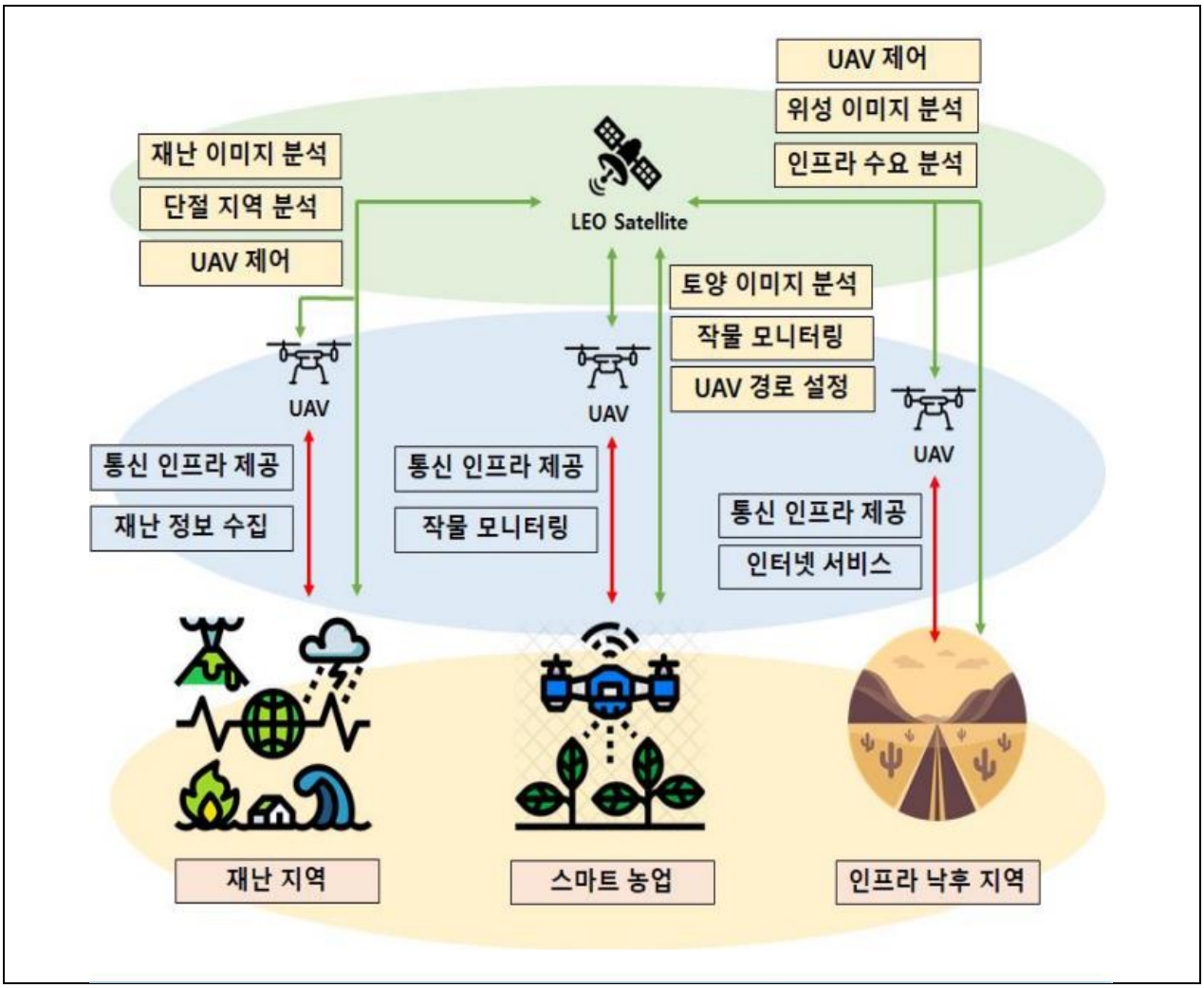
나. SATIN 네트워크 특징

특징	설명
- 다중 접속 제어 (Multiple Access Control)	- 직교 다중 접속과 비 직교 다중 접속을 통해 서로 다른 사용자의 신호를 다중화.
- 인지 스펙트럼 활용 (Cognitive Spectrum Utilization)	- 위성-상공-지상의 다양한 네트워크 간섭을 피하기 위해 인지 스펙트럼을 활용하여 네트워크 간섭을 최소화
- 공동 간섭 및 자원 관리 (Joint Interference and Resource Management)	- 지상, 상공, 위성 RAN 등 각 세그먼트의 특성을 고려한 간섭 제거 및 SATIN 공동 자원 스케줄링을 통한 무선 자원 관리 수행
- 이동성 관리 (Mobility Management)	- 지상, 상공에서 단말들의 빠른 핸드오버를 해결하기 위해 정교하고 효율적인 수평적, 수직적 핸드오버 수행

- SATIN 의 네트워크 특징을 활용하여, 네트워크가 불가능한 재난상황의 대처, 통신 인프라가 부족한 낙후지역의 UAV(Unmanned Aerial Vehicle)를 통한 네트워크 서비스 지원 가능

3. SATIN 의 재난대비, UAV(Unmanned Aerial Vehicle) 활용, 낙후지역 네트워크 서비스 활용방법

가. SATIN 의 재난대비, UAV 통한 스마트 농업, 낙후지역 네트워크 서비스 활용 개념도



- SATIN 을 활용하여 재난지역의 통신 인프라 제공, 재난지역 분석 및 인지 수행
- UAV 를 활용 스마트 농업, 네트워크 인프라가 부족한 낙후지역에서의 네트워크 통신 수행 가능

나. SATIN 의 재난대비, UAV 통한 스마트 농업, 낙후지역 네트워크 서비스 활용 세부설명

구분	주요 서비스	설명
재난대비	- UAV 제어	- 재난 시 통신이 안될 상황을 대비하여 UAV 배치 통한 기지국 기능을 제공
	- 통신 인프라 제공	- 재난 시 상공의 RAN 의 자원을 활용하여 안정적인 통신 링크를 제공
	- 재난 정보 수집 및 감지	- 위성시스템을 활용한 이미지 분석을 통해 재난 감지 정확도 향상
UAV 활용 (스마트 농업)	- 농작물 모니터링	- UAV 및 위성을 통해 농작물 모니터링으로 작물 건강 모니터링, 해충관리, 식물 품질 평가 수행
낙후지역	- 상공 무선 셀룰러 네트워크	- 지상 기지국과 위성 통신을 통해 인구 밀도가 낮은 지역 (숲, 사막, 바다 등)에 인터넷 서비스 제공

- 현재 3GPP, IEEE 등 다양한 표준화 단체들이 SATIN 을 표준화하기 위한 연구 중

4. SATIN 의 표준화 및 산업 동향

표준화 단체	설명
3GPP	- 지상, 상공, 위성 RAN 의 통합을 위한 잠재적 솔루션을 조사 및 R16 의 일부로 상공 RAN 을 5G 망에 통합하려는 연구 수행 - 5G 에서 위성 액세스를 수용하기 위한 향상된 네트워크 아키텍처에 대해 연구 수행
RAN WG	- NTN (Non-Terrestrial Network)을 지원하기 위해 새로운 무선 주파수에 대한 조사
ETSI SCN TC-SES	- 2018 년 말까지 위성과 고 궤도 플랫폼 (HAP) 스테이션을 5G 로 통합하기 위한 잠재적 아키텍처를 완성 - 위성 멀티캐스트를 통해 5G 용 에지 콘텐츠 전송 작업을 하고 있으며 2019 년에 위성 통신 시스템에 NFV 프레임워크를 도입할 예정
ITU-R WG 4B	- 위성 기술을 차세대 액세스 시스템에 통합하기 위한 핵심 구성 요소 연구
IEEE	- 5G 및 그 이상을 위한 기술 로드맵을 정의하기 위해 5G 위성 WG 를 설립하여 연구 중

- 현재 SATIN 활용 위해 SATIN 의 유즈케이스, 요구사항, 기술적 이슈 등의 관점에서 활발하게 논의 중

"끝"

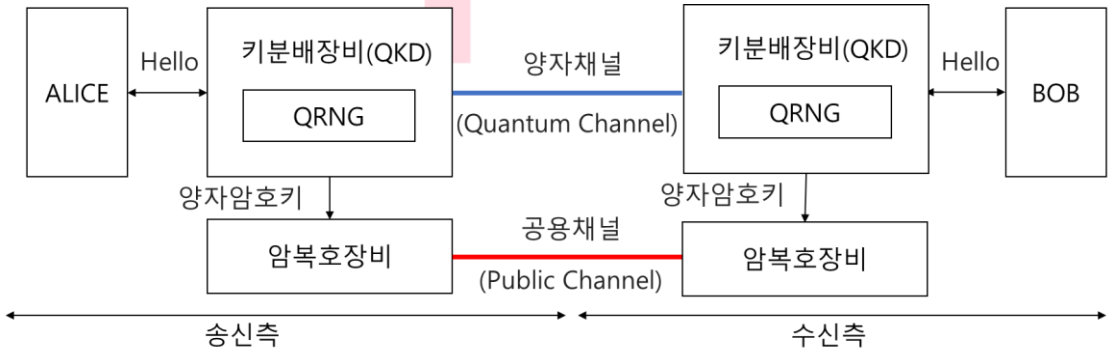
기출풀이 의견

3. 문제에서 물어본 것과 같이 SATIN에 대한 일반적인 개념과 네트워크 특징에 대해 작성해 주시면 좋겠습니다. SATIN을 모르더라도 5G의 단점을 통해 SATIN을 유추해서 6G기반으로 작성하신다면 문제에 대한 대응이 가능합니다.

문 제	**4. 최근 정보통신의 발전으로 인해 도감청이 불가능한 양자암호통신에 대한 관심이 높아지고 있다. 양자암호통신에 대하여 다음을 설명하시오.** **가. 양자암호통신의 암호키 분배방식** **나. 양자암호통신의 주요기술** **다. 양자암호통신의 취약점**
출 제 영 역	정보보안 / 난 이 도 ★★★★☆
출 제 배 경	- UAM(도심항공모빌리티) 연구가 활발해지며 기체가 안전하게 이동하기 위한 필수 기술로 차세대 보안기술인 양자암호통신이 주목받고 있으며, 양자암호통신 시장이 급증할 것으로 예측
출 제 빈 도	117 회 정보관리기술사 (1 교시)
참 고 자 료	- 해시넷 (양자키분배) - 양자암호통신 기술 https://ettrends.etri.re.kr/ettrends/95/0905000628/20-5_070_083.pdf
Keyword	- QKD, BB84, B92, 큐비트, 양자검출기, 양자통신기술, 양자난수, 양자암호키, plug&play, 양자인증
풀 이	박영길(126 회 정보관리기술사)

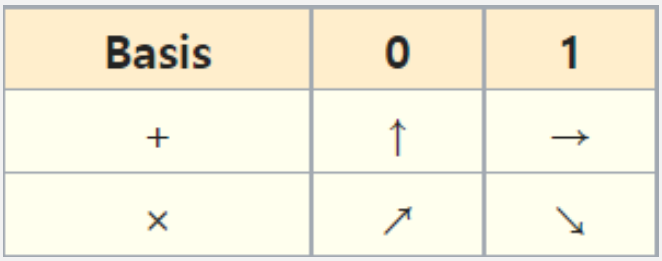
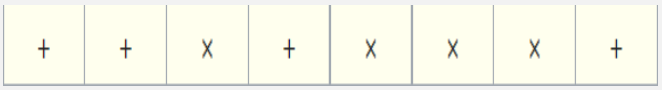
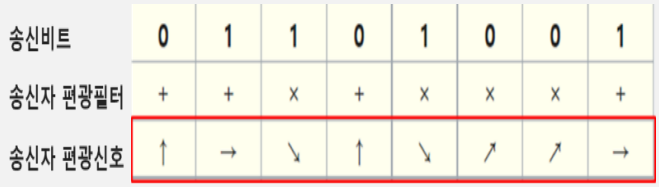
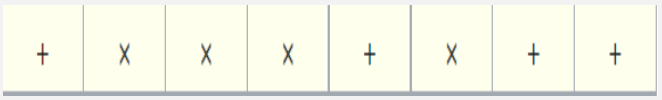
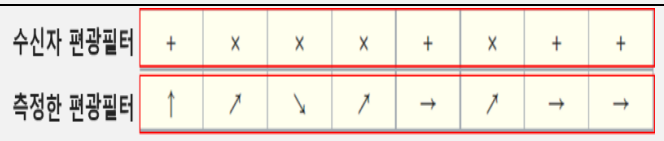
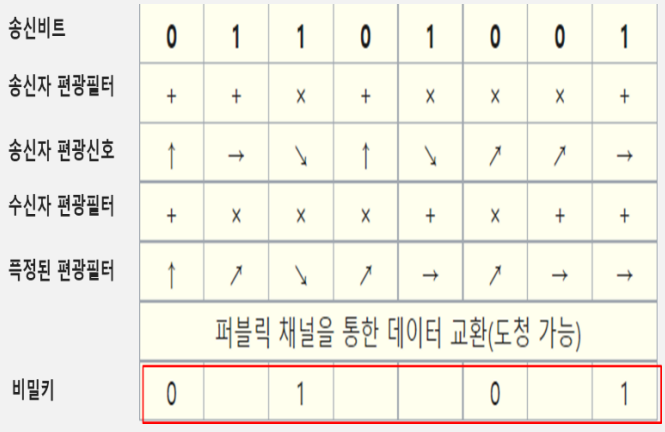
1. 양자암호통신의 암호키 분배방식

가. 양자를 이용한 비밀키 분배 양자키 분배방식 개념 및 특징

구분	설명	
개념	- 보안이 필요한 송수신자 사이에 양자 암호 키 분배(**QKD: Quantum** Key Distribution) 기술을 사용하여 암호화에 필요한 비밀키를 통신상에서 실시간으로 분배하기 위한 양자암호키 분배 기술	
개념도		
구성 요소	**- 양자채널**	- 양자암호키 분배 위해 편광신호를 전송하기 위한 양자전용채널
	- 공용채널	- 기존의 통신망을 이용해 송수신자간 편광필터를 송신, TCP/IP 프로토콜을 활용
	- QRNG	- 반복되는 주기를 예측하기 어려운 진정 난수를 생성하기 위한 장치

- 기존의 암호키 분배는 송신자의 암호화, 수신자의 복호화 방식으로 분배 수행, 양자암호통신은 송신자와 수신자가 양자전용채널을 통해 암호를 생성 후, QKD 기술을 통해 양자를 주고받으며 양자의 특성(불확정성)을 활용해 암호키를 생성
- 양자암호통신 암호키 분배는 광자 단위의 편광이나 위상차를 이용하여 신호를 전송하고 편광패드를 통해 수신
- 양자암호통신 프로토콜로 BB84, B92, EPR 등의 프로토콜 존재

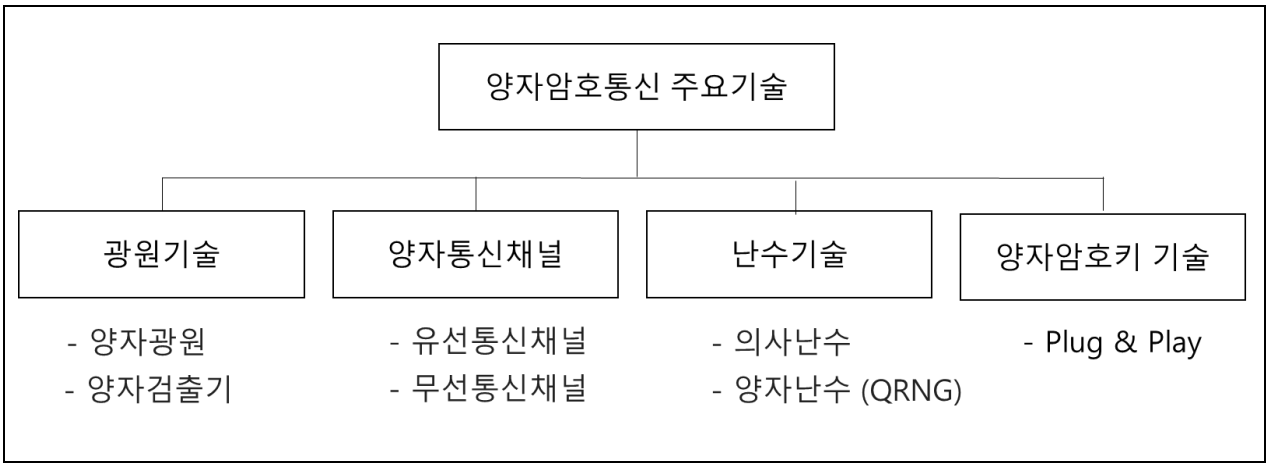
나. 양자암호통신(BB84) 암호키 분배 방식 설명

절차	개념도	설명
1)편광필터 선택		- 양자암호통신에 사용될 편광 필터 선택 - +, ↑ 는 비트 0 대응 - +, → 는 비트 1 대응 - x, ↗는 비트 0 대응 - x, ↘는 비트 1 대응
2)송신비트 생성		- 송신자가 수신자에게 보낼 임의 비트 생성 * 송신비트는 01101001
3)송신자 편광필터 임의선택		- 송신자는 수신자에 보내기 위한 편광신호로 변환하기 위한 임의의 편광필터 선택
4)편광신호 생성과 수신자 전송		- 필터에 대응되는 편광신호를 생성 후 양자 채널로 전송 * 송신비트 01101001 과 3)에서 선택한 편광필터를 통해 4)의 편광신호 생성 * 편광신호 생성시 1)의 편광필터 참조하여 편광신호 생성
5)수신자 편광필터 임의선택		- 수신자는 송신자 신호 측정 위해 편광필터 임의 선택
6)수신자 편광필터 측정		- 선택한 편광필터로 값 측정 * 5)의 수신자 편광필터로 4)의 편광신호 측정 결과 6) 생성
7)비밀키 생성		- 송신자와 수신자는 퍼블릭 채널로 동일한 필터 사용 여부를 확인 - 다른 필터를 사용한 비트를 제외하고 동일한 필터를 사용한 비트만 저장 - 송신자와 수신자가 저장한 데이터는 같은 값을 공유하며 비밀키로 사용

- 송신자와 수신자간 최종 비밀키는 10001 이며 해당 비밀키를 사용해서 양자암호통신 수행
- 양자암호통신의 주요기술로 양자를 생성 및 검출 위한 광원기술 키분배를 위한 키 분배 기술, 난수를 생성하기위한 QNG 기술 양자암호통신을 위한 프로토콜로 구분가능

2. 양자암호통신의 주요기술

가. 양자암호통신의 주요기술 유형



- 양자암호통신 기술로 광원 검출위한 광원기술, 통신위한 유무선 통신채널, 난수를 통한 암호키 생성기능 필요.

나. 양자암호통신의 주요기술 설명

주요기술	기술요소	설명
광원 기술	- 양자 광원	- 단일 광자에서 양자 얽힘 상태를 구현하기 위한 기술
	- 광자 검출기	- 양자효율과 잡음의 양자암호통신의 에러율과 직접적 관련되는 시스템 성능을 좌우하는 검출기술
양자통신채널 기술	- 유선통신채널 (광섬유)	- 단일모드 광섬유를 사용하여 네트워크 구축 - 투과손실이 낮아 장거리 통신에 활용
	- 무선통신채널 (대기이용)	- 위성과 지상 사이를 대기를 통해 QKD 암호 통신 - 날씨의 영향을 많이 받아 단거리 통신에 이용
난수 기술	- 의사 난수	- 프로그램을 통해 인위적으로 생성한 난수
	- 양자 난수 (QRNG)	- 암호키 생성 과정 중 필요한 완전 난수를 진정 난수로 생성하며, 초고속으로 난수를 생성하는 기술 * 도청자도 예측할 수 없는 무작위(난수)를 생성
양자 암호키 구현 기술	- Plug & Play	- FM(Faraday Mirror)를 이용해서 자동으로 위상과 편광을 보정하여 양자 암호통신 암호 키 구현 - 광섬유를 통한 장거리 전송에 적합
양자암호 프로토콜	- BB84	- 송 수신자간의 OTP 생성하여 시스템의 안정적인 동작을 수행하는 Plug & Play 방식의 TwoWay 프로토콜
	- COW04	- 환경변화에 민감하나 고속으로 동작하는 OneWay 방식 프로토콜
시스템 고도화 기술	- 양자중계기	- 광섬유 기반의 장거리 양자암호통신을 위한 증폭기 – 양자상태 유지하며 신호 전달
	- 양자다중화 중계기	- 다대다 양자암호통신 가능한 양자전용중계기
	- 양자인증, 서명	- 기밀성, 인증, 무결성, 부인방지 기능 제공

- 유선 QKD 시스템에서는 통신 파장영역에서의 광 흡수율이 높고, 구동전압이 낮은 APD(Avalanche Photodiode)를 단일 광자 검출 소자로 많이 이용하며 APD 의 오작동을 유도한 이용한 취약점이 존재

3. 양자암호통신의 취약점

구분	취약점	설명
큐비트 분석 공격	- 차단-재송신 공격(intercept-resend attack)	- 송신자가 수신자에게 보내는 큐비트를 공격자가 가로채서 자신이 원하는 측정 후 수신자에게 공격자가 자신에게 유리한 상태의 큐비트를 보내는 방법.
	- 복제 공격법(cloning attack, symmetric individual attack)	- 전달되고 있는 큐비트에 양자 복제(quantum cloning) 해서 방법으로 양자 역학적으로 완전한 복제는 불가능하지만 암호 키에 대해 일부 정보를 얻는 형태의 공격.
QKD 공격	- 광자 분리 공격 (PNS Attack, Photon Number Splitting Attack)	- 전달되는 큐비트의 상태에 영향을 주지 않으면서 그 펄스에 포함된 광자의 개수가 여러 개일 때 다중 광자 펄스 중 일부 광자를 조금씩 나누어 가진 후 송수신지 몰래 비밀키를 탈취하는 공격 방법 * 실제 물리적으로 구현된 양자채널은 손실(loss)이 존재, 손실로 인해 단일 광자로 보내야 하는 광자가 2 개 이상의 다중 광자 펄스로 분리됨. 공격자는 이를 악용하여 다중 광자 중 몇 개를 탈취해 비밀키 생성 * 양자 비 파괴 공격 (quantum non-demolition attack)이라고 불림
양자 검출기 공격	- Blinding 공격	- 도청자가 APD 에 의도적으로 강한 빛을 보내 APD 를 가열시킨 다음, 낮아진 인가 전압(Bias voltage)와 광 검출 효율(Detect efficiency)을 이용해 정보 탈취
	- After-gate 공격	- APD 의 게이트 타이밍(Gate timing) 이후에 강한 빛을 APD 에 입사시켜 Dead time 을 만들거나 선형 동작 클릭(Linear operation click)을 이용하여 검출기의 작동을 조절하여 비밀키 탈취 - 도청자는 이를 통해 송신자와 수신자 사이에서 광자를 가로채서 측정하여 비밀키 전체를 탈취..
	- Time-shift 공격	- 한 시점에서 두 개의 APD 간의 검출효율이 다른 경우를 이용한 공격 - 도청자가 송신자로부터 광자를 가로채 확인 후 광자의 타이밍을 조절해서 수신자에게 보내면, 수신자의 APD 작동을 조절할 수 있게 되고 이를 통해 정보 탈취
	- Trojan-horse 공격	- QKD 시스템을 가동하지 않는 시간에 도청자가 송신자와 수신자 간의 광섬유를 통해 수신자 쪽으로 레이저를 보내어 되돌아오는 빛을 분석하여 정보를 탈취

- 양자암호통신의 취약점으로 큐비트 단일신호, 다중신호를 통한 분석, 양자를 검출하기 위한 검출기 취약점을 통해 양자암호통신 정보 취득가능

4. 양자암호통신 취약점 대응방안

구분	취약점	대응방안
큐비트 분석 공격	- 차단-재송신 공격 - 복제 공격법	- BB84 보다 개선된 프로토콜 사용으로 양자암호통신의 불확실성 증가로 공격 회피 (**오류 검출률 증가**)
		- **Six-state QKD 프로토콜** : BB84 프로토콜에 Y 기저를 추가하여 총 3 개의 기저 (6 개의 상태)로 QKD 를 수행하는 프로토콜 사용
		- **이중 큐비트 QKD** : 단일 광자에 서로 다른 두개의 코딩을 하여, 단일 큐비트 QKD 프로토콜에 비해 훨씬 높은 오류 검출 가능한 이중 큐비트 사용 * 단일 큐비트 : 2 가지 기저와 4 가지 상태를 가짐 * 이중 큐비트 : 4 가지 기저와 16 가지의 상태를 가짐
QKD 공격	- 광자 분리 공격(PNS Attack, Photon Number Splitting Attack)	- Decoy state method, SARG04 등 개선된 프로토콜을 사용해서 광자 분리 공격 회피
		- 셋 이상의 경로를 통한 위상 차이를 이용, 위장용 펄스를 사용하는 프로토콜을 통해 광자 분리 공격 대응
		- 다중 광자 상태를 만들어 내게 될 확률을 특정 기준 이하로 유지하여 광자 분리 공격 대응
광자 검출기 공격	- Blinding 공격	- APD 에 강한 빛이 들어오는지 여부를 모니터링 함으로써 도청 회피
	- After-gate 공격	- APD 에 들어오는 빛의 세기를 실시간으로 모니터링 하여 After-gate 공격 대응
	- Time-shift 공격	- 도청자가 알아차리지 못할 정도로 미세한 Delay line 을 만들어 검출효율을 모니터링 하여 Time-shift 공격 대응
	- Trojan-horse 공격	- QKD 시스템을 가동하지 않는 시간에는 수신자 측 장비를 닫아 두거나 수신자 측에 들어오는 빛을 모니터링 하여 Trojan-horse 공격 대응

- 양자암호통신의 취약점 해결위해 개선된 양자암호통신 프로토콜 이용 및 실시간 모니터링으로 안전한 양자암호통신 활용 가능

"끝"

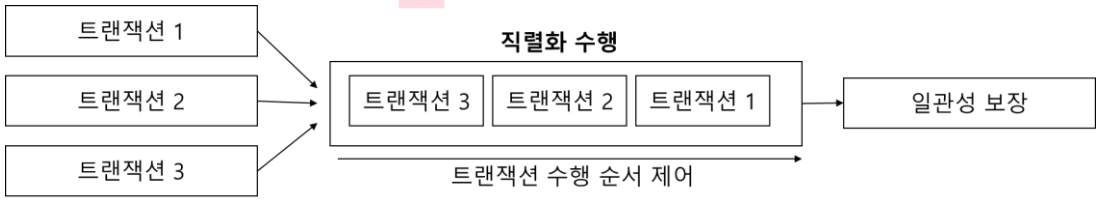
기출풀이 의견

4. 양자암호통신의 암호키 분배방식의 기본적인 개념과 요소를 작성해주시고, 암호키 분배방식을 잘 모를 경우 BB84프로토콜로 대응해주시면 좋습니다. 취약점을 모를 경우에는 일반적인 보안 취약점인 중간자 공격, DDos공격으로 대처해 주시면 좋습니다.

문 제	5. 데이터베이스의 병행제어(Concurrency Control)에 대하여 다음을 설명하시오. 가. 병행제어의 정의 나. 병행제어의 기법의 종류 다. 병행제어의 문제점		
출 제 영 역	데이터베이스	난 이 도	★★☆☆☆
출 제 배 경	- 데이터베이스의 기본 토픽인 데이터베이스의 병렬성을 위한 병행제어에 대한 개념 이해와 기법 문제점에 대한 지식 확인		
출 제 빈 도	111 회 정보관리기술사 (1 교시), 121 회 정보관리기술사 (2 교시)		
참 고 자 료	- 도리의 디지털라이프 (데이터베이스 동시성 제어) - https://needjarvis.tistory.com/589		
Keyword	- Locking, 2PL, Timestamp, 낙관적 병행제어, MVCC, 갱신손실, 현황파악오류, 모순성, 연쇄복귀		
풀 이	박영길(126 회 정보관리기술사)		

1. 데이터베이스 일관성 제어 병행제어의 정의

가. 병행제어의 개념 및 개념도

구분	설명
개념	- 데이터베이스에서 빠른 처리를 위해 여러 트랜잭션을 동시적 수행할 경우, 트랜잭션 간의 병행성을 제어하여 데이터베이스의 일관성을 유지하는 제어 기술
개념도	

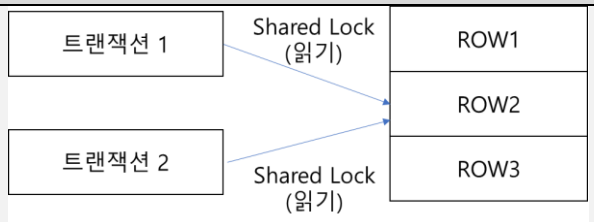
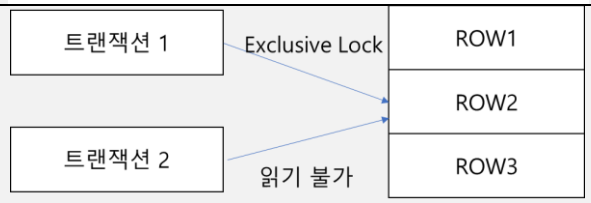
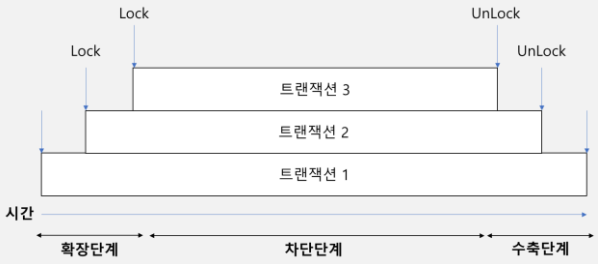
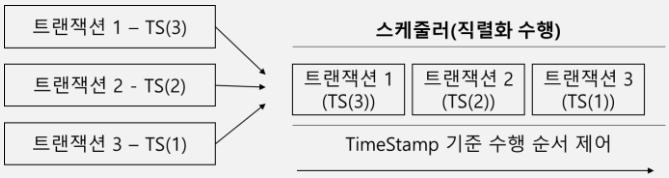
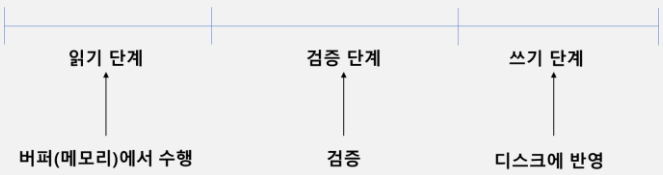
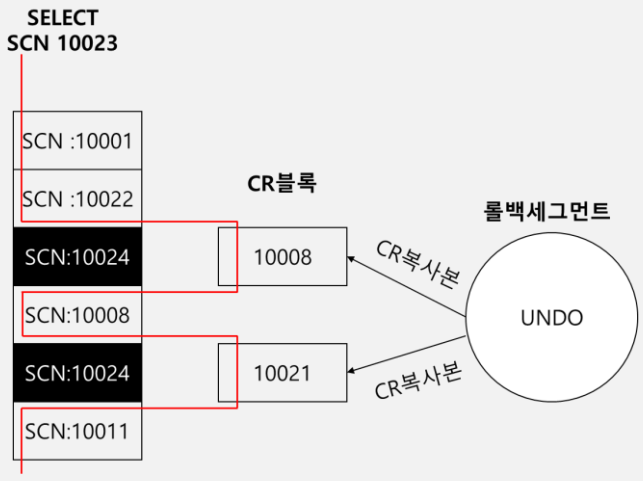
- 병행성이란 여러 개의 트랜잭션들이 동시에 인터리빙(Interleaving)하게 실행되는 것을 의미
- 인터리빙(Interleaving) : 트랜잭션들이 번갈아 가며 조금씩 자신이 처리해야 할 일을 처리하는 것

나. 병행제어의 목적

목적	설명
- 시스템 활용도 최대화	- 트랜잭션의 직렬성 보장으로, 동시 수행 트랜잭션 처리량 최대화
- 사용자에 대한 응답시간 최소화	- 트랜잭션의 병렬 처리로 사용자 응답 시간 최소화
- 데이터베이스 공유 최대화	- 공유도 최대, 응답 시간 최소, 시스템 활동의 최대 보장
- 데이터베이스 일관성 유지	- 수행 트랜잭션의 직렬화를 통한 데이터의 무결성 및 일관성 보장

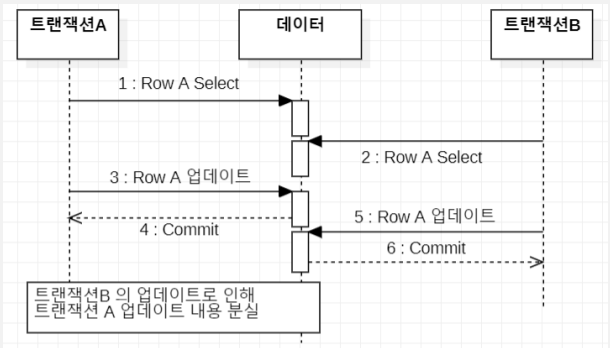
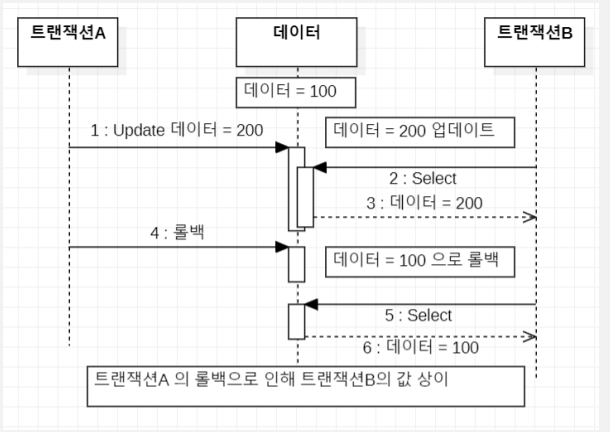
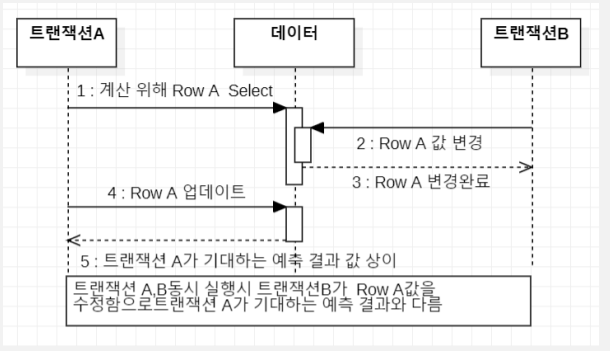
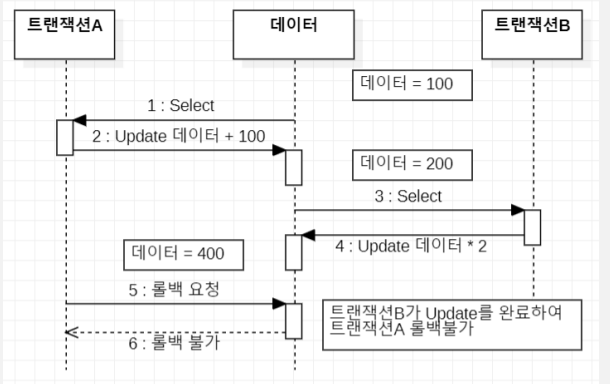
- 병행제어 기법으로 Locking, 2PL(2Phase Locking), 타임스탬프(Timestamp), 낙관적 병행제어, MVCC(Multi Version Concurrency Control)등의 방식 존재

2. 병행제어의 기법의 종류

구분	개념도	설명
Locking		- Shared Lock : 공유에 사용되는 락, 읽기에 사용 - Shared Lock 이 걸려있을 때 다른 Shared Lock 수행 가능
		- Exclusive Lock : 공유할 수 없는 락, 쓰기에 사용 - Exclusive Lock 이 걸려 있을 경우 다른 트랜잭션 수행 불가
2 단계 로킹 (Two-Phase Locking)		- 확장단계를 통한 Lock 축소단계의 Unlock 을 통해 트랜잭션의 직렬성을 보장하는 병행제어 기법
타임스탬프 (Time Stamp)		- 트랜잭션에 Timestamp 를 부여하여 Timestamp 순서로 직렬화 하는 병행제어 기법 * TS(T)는 트랜잭션 T 의 타임스탬프.
낙관적 병행제어		- 트랜잭션 수행 중 어떠한 검증도 수행하지 않고, 트랜잭션을 종료할 때 검증을 수행하여 데이터베이스에 반영하는 병행제어 기법
다중 버전 병행제어		- 트랜잭션에서 데이터에 접근하는 경우 데이터의 다중버전 상태 중 보장되는 버전에 맞는 CR 복사본을 롤백 세그먼트에서 반환하여 처리하는 병행제어 기법 - SCN 10023 번 시점에 시작된 쿼리가 10023 번 이후에 변경된 데이터를 만나면 롤백 세그먼트의 CR 복사본을 참고하여 10023 을 넘지 않는 데이터 중 최신 데이터 Read 수행

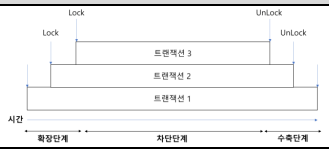
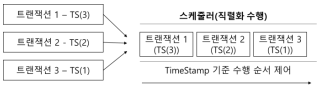
- 병행제어를 수행하지 않을 경우 갱신부실, 현황파악오류, 모순성, 연쇄복귀 등의 문제점 발생

3. 병행제어의 문제점

문제점	개념도	설명
갱신 손실 (Lost Update)		- 트랜잭션들이 동일 데이터를 동시에 갱신할 경우 트랜잭션 값이 갱신으로 분실되는 문제 - 트랜잭션 A 가 데이터를 갱신한 후 트랜잭션을 종료하기 전에 나중 트랜잭션 B 가 갱신 값을 덮어쓰는 경우 발생
현황파악오류 (Dirty Read)		- 트랜잭션 B 가 같은 데이터를 2 번 읽었을 때 서로 다른 결과가 나오는 문제 - 읽기 작업을 하는 트랜잭션 B 가 쓰기 작업을 하는 트랜잭션 A 가 작업한 중간 데이터를 읽어서 발생하는 문제
모순성 (Inconsistency)		- 두 트랜잭션이 동시에 실행할 때 DB 가 일관성이 없는 상태로 남는 문제 - 다수의 트랜잭션이 동시에 DB 를 액세스, 갱신을 해서 DB 내 데이터가 일치하지 않거나 출력 정보가 기대 값과 모순되는 경우
연쇄복귀 (Cascading Rollback)		- 두 트랜잭션이 동시에 실행할 때 Commit 으로 인하여 롤백이 불가능한 문제 - 복수의 트랜잭션이 데이터 공유 시 특정 트랜잭션이 처리를 취소할 경우 다른 트랜잭션이 처리한 부분에 대해 취소 불가한 문제

- 웹 페이지 등의 조회를 중심으로 처리하는 업무는 바로 실행 가능하고, 조회만 처리하므로 Timestamp Ordering 방식 추천
- 업무적인 구분이 명확하여 서로 중복이 거의 없다면, Validation 동시성 제어 기법 적용 권장

4. 병행제어 기법 비교

구분	2 단계 로킹	Timestamp Ordering	낙관적 검증기법
개념			
동작방식	- 확장 단계 : 트랜잭션 lock 권한 획득 - 차단 단계 : 데이터 연산(SQL) - 수축 단계 : 트랜잭션 Lock 권한 반납	- Timestamp 부여 : 트랜잭션 수행 시 고유한 timestamp 부여 - 직렬화 : 트랜잭션을 읽어오거나 수정할 때마다 트랜잭션의 timestamp 비교 후 처리	- Read : 트랜잭션 읽음 - Validation : DB 반영전 직렬 가능성의 위반여부를 확인 - Write : 확인: 통과시 실행결과를 DB 에 반영
장점	- 직렬성 보장	- 직렬화 가능 - 교착상태 방지	- 동작이 단순 - 동시 처리능력 증가
단점	- 연쇄복귀 발생 - 교착상태 발생	- 연쇄복귀 발생 - 기아상태 발생	- 장기 트랜잭션 철회 자원낭비

- 트랜잭션 동시성 보장기법 적용시 환경에 맞는 동시성 보장 적용으로 최적화, 일관성 있는 동시성 환경 제공

"끝"

기출풀이 의견

5. 병행제어의 명확한 정의와. 방법, 발생시 문제점을 제시된 문제에 맞게 관련 내용을 풍부하게 작성해 주시면 좋겠습니다.

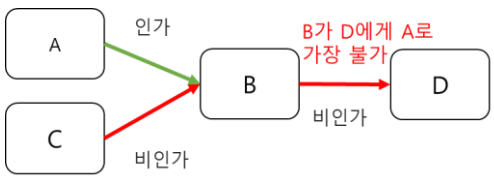
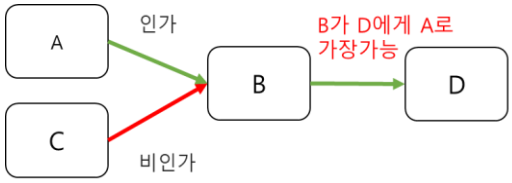
문 제	**6. 식별(Identification)과 인증(Authentication)에 대하여 다음을 설명하시오.** **가. 개인 식별과 사용자 인증의 정의 및 차이점** **나. 사용자 인증시 보안 요구사항** **다. 인증 방식에 따른 4 가지 유형 및 유형별 특징**
출 제 영 역	정보보안 / 난 이 도 ★★☆☆☆
출 제 배 경	- 정보보안의 개인 식별 방법과 사용자인증 방법의 개념적 이해도 파악 여부, 사용자 인증 위한 보안적 필요사항 및 인증 방식에 대한 이해도 파악
출 제 빈 도	120 회 정보관리기술사 (4 교시)
참 고 자 료	- 2022 년 정보보안기사 필기 교재 - https://peemangit.tistory.com/190
Keyword	- 자격증명, 권한, 식별, 인증, 인가, 책임추적성, 지식기반, 소유기반, 존재기반, 행위기반, ACL
풀 이	박영길(126 회 정보관리기술사)

1. 개인 식별과 사용자 인증의 정의 및 차이점

가. 개인 식별과 사용자 인증의 정의

구분	정의
개인 식별	사용자 개인이 시스템에게 자산의 신원정보(ID 등)를 제공하고 시스템이 신원정보가 맞는지 확인하는 행위
사용자 인증	사용자가 가지고 있는 지식, 소유, 존재, 행위등을 확인하여 현재 인증하고 있는 사용자의 신원 주장에 대해 정당한 권한을 가지고 있는 인가자 인지 확인하는 과정

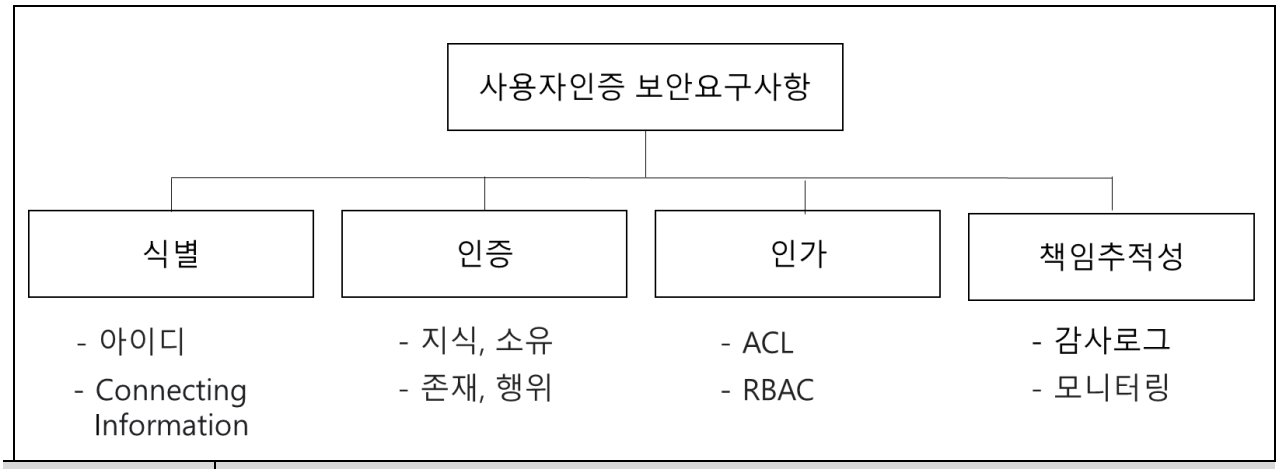
나. 개인 식별과 사용자 인증의 차이점

구분	개인 식별	사용자 인증
개념도		
설명	- A 는 B 에게 A 라고 확인가능 - C 가 B 에게 A 로 속이기 불가 - B 가 D 에게 A 라고 속이기 불가	- A 가 B 에게 A 라고 증명가능 - C 가 A 라고 속이기 불가 - B 가 D 에게 A 로 속이기 가능
인증방법	- 자격 증명 확인	- 권한 허가/거부
활용사례	- 비밀번호, 생체인증 - 일회용 핀 또는 앱	- 보안 팀에서 관리하는 인증 설정 사용

- 사용자 인증은 식별, 인증, 인가, 책임추적성의 보안 요구사항을 통해 사용자 인증을 수행함

2. 사용자 인증 보안 요구사항

가. 사용자 인증 보안 요구사항 유형



유형	설명
식별 (identification)	- 본인이 누구라는 것을 시스템에 밝히는 것 - 인증 서비스에 확인시키기 위해 정보를 공급하는 활동
인증 (authentication)	- 주체의 신원을 검증하기 위한 사용증명(verify)활동 - 본인임을 주장하는 사용자가, 본인임이 맞다고 시스템이 인증해 주는 것
인가 (authorization)	- 인증된 주체에게 접근을 허용하고 특정 업무를 수행할 권리를 부여하는 과정 - 주체에게 어떤 정보가 유용할지 여부와 관계가 있는 공인된 형식상의 접근수준
책임 추적성 (accountability)	- 시스템에 접근한 주체가 시스템에 어떤 행위를 하고 있는지를 기록 - 문제 발생시 원인 및 책임 소재를 명확하게 하기 위해 사용

- 사용자 인증은 식별을 통한 사용자 인증, 접근에 대한 인가 및 책임 추적성을 통해 사용자에 대한 접근통제 수행

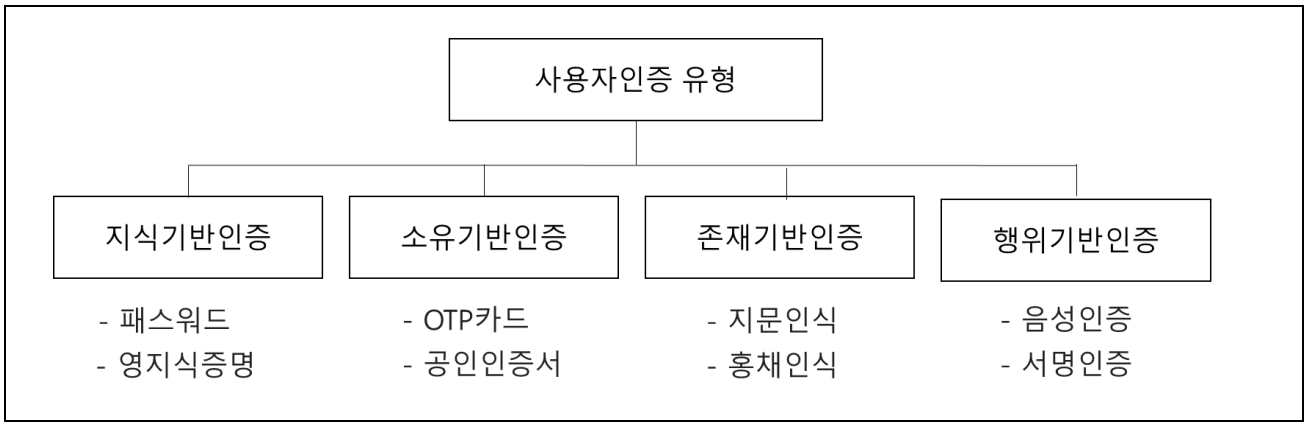
나. 사용자 인증 보안 요구사항별 기술요소 설명

요구사항	기술요소	설명
식별 (identification)	**- 아이디, 유저이름, 계좌번호**	- 사용자의 고유 식별 요소를 통해 사용자를 식별
	- CI (Connecting Information)	- 온라인에서 서로 다른 인터넷 업체 간 동일인을 식별하기 위해 사용되는 정보로 확인기관이 주민등록번호를 암호화하여 생성한 88byte 의 정보
인증 (authentication)	**- 지식기반인증, 소유기반인증, 존재기반인증, 행위기반인증**	- 정확한 식별을 위해 식별 정보에 개인이 아는 것, 개인이 가지고 있는 것, 개인 자체에 대한 정보를 함께 제공하여 주장하는 신원이 본인이라는 것을 증명
인가 (authorization)	**- ACL(Access Control List)**	- 액세스 목록을 통해 개체나 개체 속성에 적용되어 접근 권한을 부여하여 접근 권한 인가
	- MAC, DAC, RBAC	- 강제적 접근, 임의적 접근, 역할 기반 접근 권한을 통해 접근 권한 인가
책임 추적성 (accountability)	**- 감사 로그, 모니터링**	- 고유하게 식별된 주체의 행위를 기록하여, 주체가 실행한 행위에 대해 책임을 부여하는 것

- 사용자 인증의 유형에는 지식, 소유, 존재, 행위가 있으며 이 중 둘을 결합하여 사용하는 것을 Two Factor, 그 이상을 결합하여 사용하는 것을 Multi Factor 인증이라고 함

3. 인증 방식에 따른 4 가지 유형 및 유형별 특징

가. 인증 방식에 따른 4 가지 유형



- 사용자인증 4 가지 유형으로 지식기반인증, 소유기반인증, 존재기반인증, 행위기반인증 존재

나. 인증 방식 따른 유형별 특징 및 활용사례

인증유형	특징	활용사례
지식기반	- 주체가 알고 있는 것을 통해 인증 (What you know)	- 패스워드, 질문, 아이핀, 영지식 증명, 캡챠(CAPTCHA)
소유기반	- 주체가 가지고 있는 것을 통해 인증 (What you have)	- 토큰(Token), 스마트카드, 보안카드, OTP, 공인인증서, 운전면허증
존재기반	- 주체를 나타내는 특징을 기반으로 인증 (What you Are)	- 지문 인증, 홍채 인증, 망막 인증 DNA 인증 등
행위기반	- 주체가 하는 행동을 기반으로 인증 (What you do)	- 걸음걸이, 서명, 음성, 키 스트로크 다이내믹

- 사용자 인증 방식을 SSO 에 활용하여 한번의 시스템 인증으로 다양한 정보시스템에 재 인증 없이 접속 가능

4. 사용자 인증을 활용한 통합 인증 체계 (SSO, Single Sign On)

구분	SSO	EAM	IAM
개념	- 한 번의 시스템 인증을 통하여 접근하고자 하는 다양한 정보시스템에 재 인증 절차 없이 접근할 수 있도록 하는 통합 로그인 솔루션		
관련 기술	PKI, LDAP	PKI, LDAP, SSO, AC, 암호화	통합자원관리+프로비저닝
특징	- 하나의 계정으로 접근	- SSO+정책기반+접근제어	- 기업 업무 프로세스 근거 사용자 관리 및 접근제어

- SSO 외 티켓기반 사용자 인증 프로토콜인 커버로스, 커버로스의 약점 보완한 세사미, 사용자 인증 메시지 부인방지를 위한 메시지 출처 인증 기술 활용 가능

"끝"

기출풀이 의견

6. 개인 식별과 사용자 인증의 명확한 구분과, 사용자 인증 보안 요구사항, 4가지 유형을 명확하게 작성해주시면 좋겠습니다. 추가적으로 사용자 인증을 위한 기술요소들을 다양한 관점에서서 풍부하게 작성해 주시면 고득점 가능합니다.