

- NRMS은 사용자 정보와 인증키 정보, API과싱 정보, 통계정보를 관리하며, 보고서 성과물과 등록현황 정보, 구축현황 정보, 구축통계 정보, 라이브러리 서비스, ASP서비스를 연구 관리 대표 기관과 사업관리/발주기관, 성과물등록기관에 제공하고 앞의 기관들이 보고서를 등록 하면 보고서 원문정보와 메타정보를 등록함.
- 우리나라의 어문 저작물에 대한 보안은 크게 문서 보안과 위변조 방지, 화면 보안, 개인정보 보호 등으로 나누어 질 수 있음. 국내에서는 마크애니, 파수닷컴, 씨케이앤비 등이 관련 기술을 보유하고 있는 것으로 파악됨.
- 문서보안은 서버 보안이 기본 축을 이루고 있음. 문서 유통 시 불법적 유출 방지와 전사적 자료 유통 보안으로 중앙집중식 권한 설정과 사전/사후 보안 관리로 구분됨. 크게 암호화, 키관리, 정책관리, 권한제어, 인증 및 라이선스 등으로 구분되며, 불법복제 및 외부 유출 가능성을 원천적으로 차단하는 것이 기본 골격임.
- 국가 R&D 수행기관에서는 암호화된 문서에 대한 로그 기록 및 열람, 대량의 연구 문서들을 일괄 서버를 통해 암호화 할 수 있는 기술 등이 필요하며, 개발 되고 있는 상태임.
- 클라이언트 보안은 연구를 수행하는 연구자의 PC내에 문서가 생성되는 시점부터 강제적 또는 선택적으로 암호화를 적용시키거나 권한을 제한하여 권한이 있는 연구자만이 연구기간동안 연구내용을 열람하거나 출력 또는 편집이 가능한 것이 기본 축을 이루고 있음. 또한 문서내의 화면 캡처를 방지하거나 노트북, 메일, USB 등을 이용한 파일 유출 방지하고, 만약에 외부에 유출이 되었다면 추적 가능한 워터마킹 기술이 적용될 수 있음. 이외에도 연구자 웹 환경에 대한 보안 및 모바일에 대한 보안 등이 개발 되고 있는 상태임.
- 파일의 문서출력과 PC 화면 캡처를 통한 정보유출의 방지에는 워터마킹 기술, 문서 진위 및 위변조 방지를 위한 바코드 기술, 복사방지 코드 삽입하는 기술 등이 사용되고 있음.
- 위변조 방지를 위해서 패턴인식 방식의 화면캡처 방지나 마우스 및 키보드 제어 등의 기술이 사용되고 있음.
- 표절 기술에는 검색엔진을 기반으로 한 표절시스템이 한국저작권위원 및 특허청의 특허검색, 논문검색 등에서 개발된 상태임. 그러나 기존 기술 기반의 시스템으로는 대용량 연구보고서 표절 탐지 한계점이 있음. 특히, 외산 제품(글로벌 제품)의 한글 처리 및 속도에 한계성이 있음. 또한 영문이 아닌 한글 특성에 적합한 기술 개발이 필요하며, 고속검색 기술 엔진과 대용량 한글 문장 처리에 적합한 문장검색 기술 엔진이 요구됨.
- Open Source 기반 엔진으로서 기존의 기술 한계성 해소할 수 있으며, 의도적 표절(불법복제) 탐지 기술과 한글의 특성에 맞는 탐지 기술이 확보되어야 함.
- 이미지 파일에 저작권 정보를 보이지 않게 삽입하는 이미지 워터마킹 기술이 사용되고 있음.
- 워터마킹 기술은 이미지 내에 다양한 비트를 삽입하거나 코드를 삽입하는 기술이 사용되고