Team No.

TONGMYONG UNIVERSITY

전공연구형_Capstone Design 신청서

과제명	국문	SSL 인증서와 전자서명을 이용한 계약서 작성 웹 개발					
	영문	Development of Web for Contract Writing Using SSL Certificates and Electronic Signatures					
과제팀명		거짓말탐지기					
참여학과		정보보호학과	교과목명	DID 인증 기술 _Capstone Design			
지도교수		성명			소속(학과)		
		신 승 수			정보보호학과		
참여 학생	구분	소속학과(전공)	학번	학년	성명	연락처	이메일
	팀장	정보보호학과	17학번	3	최 * *	010-8006-****	tree4843@gmail.com
	팀원	정보보호학과	18학번	3	진 * *	010-8684-****	lst9123@naver.com
		정보보호학과	20학번	3	조 * *	010-2951-****	dmslrhdwn2@gmail.com
		정보보호학과	18학번	3	김 * *	010-4303-****	say11995@naver.com
수행기간		2022년 9월 ~ 2022년 12월					
유형선택		☐ 기업성장형 ☐ 사회기여형 ☐ 창업연계형					
구분 / 지원금액		■ 전공연구형		☐ 과제창출형_C유형 (예산 300,000원)			
				■ 학술연구형_D유형 (예산 200,000원)			

동명대학교 현장실습지원센터 규정에 의거, 캡스톤디자인 과제를 성실하게 수행하고자 본 과제 신청서를 제출합니다.

붙임 : 과제 제안서 1부

2022. 9. 14.

신청인(대표학생) : 최 * * (인)

과제지도교수 : 신 승 수 (인)

동명대학교 현장실습지원센터장 귀하

Capstone Design 과제 제안서

1. 과제 선정 배경 및 과제 수행 목적

개인 사업장 및 소규모 회사에서 흔히 사용되는 계약서(근로계약서, 비밀 유지계약서 등)는 종이 서류를 통해 많이 작성된다. 이러한 경우 분실 및 수정의 우려가 있고 서명자가 추후 해당 계약서를 부인하는 등 다양한 문제점들이 발생할 수 있다. ICT 산업이 고도화되고 보안의 중요성이 올라가는 현시점에서 다양한 단점을 안고 있는 종이 계약서를 대체할 수 있는 전자서명 계약서를 제안한다. 해당 아이디어는 SSL 인증서를 통한 기밀성 보장과 전자서명을 통한 무결성, 인증, 부인방지를 보장하여 플랫폼에서 간편하고 체계적으로 계약서를 작성 및 보관할 수 있도록 한다.

2. 과제 수행 방법

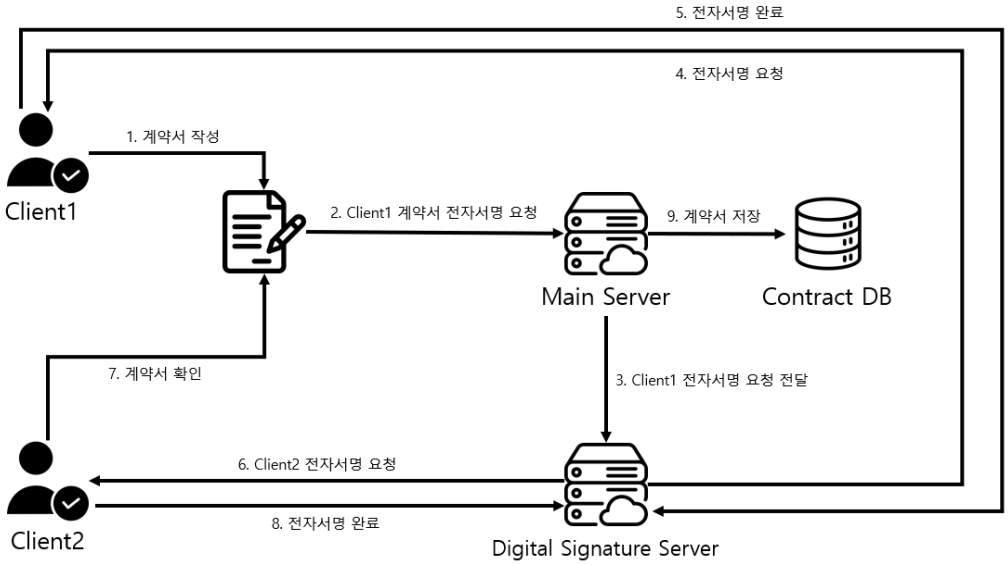
계약서 작성 시 전자서명을 이용하여 무결성, 인증, 부인방지를 충족하고, SSL을 이용하여 기밀성까지 제공하는 것이 목표이다.

(1) User ID, ID, Password, 이름 등의 회원 정보를 관리할 데이터베이스와 계약서의 고유 번호, 계약서 명, 계약서 참여자 등 계약서와 관련된 정보를 저장할 데이터베이스를 제작한다. 본 데이터베이스는 ORACLE 사의 MySQL을 사용하여 구축한다.

(2) 가상환경에서 리눅스를 통해 회원가입, 로그인, 계약서 생성 요청 등을 수행할 웹 운영 관리 서버와 전자서명 요청 확인, 대상자에게 전자서명 요청 및 전달, 전자서명 알고리즘을 수행하고 결과를 전달할 전자서명 작동 서버를 구축한다. 서버별 올바른 정책을 적용하여 접근성을 높이고 보안을 강화하여 안전한 서버 환경을 구축한다. 본 서버는 Virtual Box에서 CentOS 7.9와 Apache를 이용하여 구현한다.

(3) 국내에서 전자서명 표준으로 사용하고 있는 방식인 KCDSA 암호알고리즘을 이용하여 임의의 길이를 갖는 메시지 정보에 대해 부가형 전자서명을 생성하고 검증할 수 있도록 구현한다.

(4) 해당 프로토콜은 웹을 통하여 기능을 제공한다. 로그인, 회원가입, 전자서명 요청 등의 이벤트를 구현하여 회원 등록 및 관리, 계약서 작성에 용이성을 더하고 계약서에 대한 기밀성을 보장하기 위해 보안 소켓 계층(Secure Sockets Layer)을 적용하여 안전성을 포함한다. Microsoft사의 VisualStudio code에서 HTML5, CSS, Java-Script를 이용해 웹 구현 후 서버와 연동한다.



[그림] Service Flow

(1) 로그인을 완료한 Client1은 웹을 이용하여 계약서를 작성한다.
(2) Client1은 내용 기입을 완료한 후 계약서 전자서명을 요청한다. 이때 Client1 신원 정보, Client2(수신자)의 정보를 함께 보낸다.
(3) Main Server는 전자서명 요청을 받아 인가된 Client임을 확인한 후 Digital Signature Server로 전달한다.
(4) Digital Signature Server는 Client1에게 전자서명을 요청한다.
(5) 요청을 받은 Client1은 전자서명을 완료한 후 Digital Signature Server로 전달한다.
(6) Client1의 전자서명 결과를 확인한 후 Client2에게 전자서명을 요청한다. 이때 계약서 열람 권한을 부여한다.
(7) Client2는 계약서 열람 권한을 통해 계약서의 내용을 확인한다.
(8) Client2는 전자서명을 완료하고 Digital Signature Server로 전달한다.
(9) Digital Signature Server는 Client2와 Client1의 전자서명 결과를 Main Server로 전달한다. Main Server는 정상적인 계약서로 판단하여 Contract DB에 저장하게 된다.

3. 결과물에 대한 기대효과 및 활용방안

해당 전자서명 계약서 방식이 사회에 도입된다면 기존의 종이 계약서 방식에서 발생하는 계약서 보관, 훼손, 법적 효력 등의 다양한 문제점들을 해결할 수 있을 것이다.

또한 이 방식이 사회에 도입되고 많은 사람들이 활발하게 이용한다면 기존에 국내에서 개발된 전자서명인 KCDSA나 EC-KCDSA보다 효율적이고 안전한 전자서명을 만들기 위한 노력이 활발하게 이루어질 것이다. 이용자가 많은 플랫폼에 적용된다면 많은 사람들이 간편하게 계약서 작성 및 보관이 가능할 것이다. 또한 전자서명 계약서 특성상 복잡한 메커니즘을 요구하지 않아 HW나 SW 관리 측면에서도 효율적일 것이다.

계약서가 음식점, 회사 등 다양한 곳에서 쓰이는 만큼 국내를 벗어나 해외 시장에서도 충분히 적용이 가능할 것이고 서버, DB 관리자 및 전자서명 분야의 인재 양성과 고용 창출 또한 가능 할 것이다.

4. 수행 일정

주요내용	추진일정									소요 기간(월)
	03	04	05	06	07	08	09	10	11	
관련 이론 습득										*2주일*
자료 수집										*1개월*
전자서명 오픈소스 적용										2주일
서버 구축 및 DB 연동										1개월
사설 SSL 인증서 적용										2주일
웹 UI 구현 및 Event 적용										2개월
발표 자료 생성										2주일

5. 팀원별 역할

No.	성 명	담당 및 수행업무
1	**최 * ***	**팀원 Task 분배, Web 개발, 발표 자료 생성**
2	**진 * ***	**서버 구축, 전자서명 코드 개발**
3	**조 * ***	**자료 Search, Web 개발**
4	**김 * ***	**DB 구축, 서버 구축**

6. 소요 예산

구분	용도 (과제수행과의 연관성)	품목	규격	단위	수량	단가	금액 (원)
재료비							
그 외	용도 (과제수행의 연관성 기술)			산출 내역			금액 (원)
회의비	과제 수행 팀원과의 회의 진행			주 1회 한정			200,000원 (5000원 * 4명 * 10회)
합 계				200,000원			