

졸업 프로젝트 SE 1주차 보고서

201604142 박종혁

1. 문제정의서

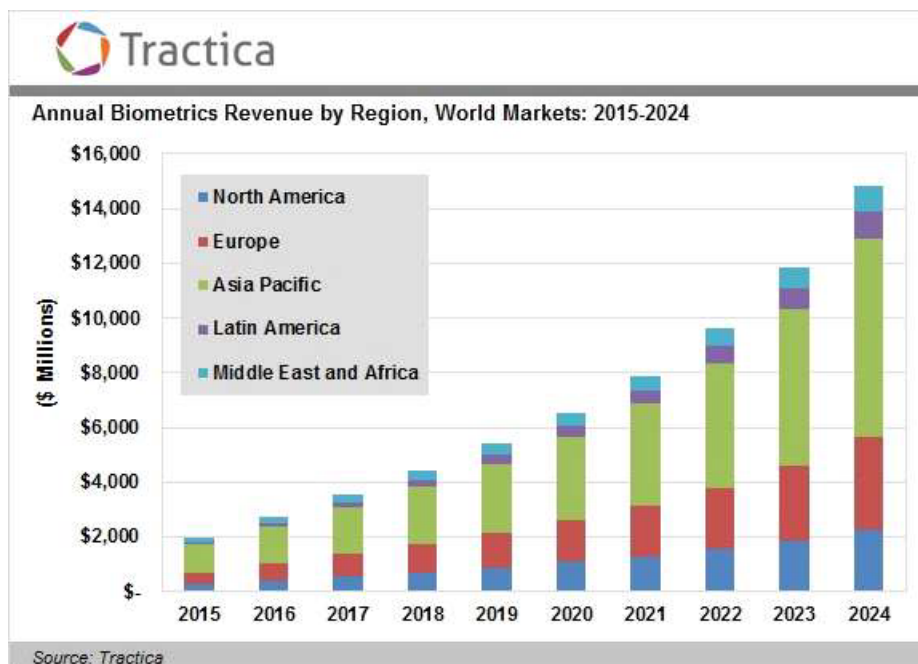
1. 연구의 필요성

1. 국내·외 연구현황, 문제점

IOT 시대의 도래로 인해 보안에 대한 중요성이 더욱 커진 현재에는 기존의 비밀번호 인증 방식의 보안에 관한 문제점의 보완책이 나타나고 있으며 이런 보완책을 '2차 인증'이라 한다. 이는 1차 인증은 비밀번호 인증 방식을 그대로 채택하지만 2차 인증을 통해 1차 인증의 보안의 불완전함을 보완하겠다는 것이다. 그러한 2차 인증 시스템 중에서도 최근 연구가 활발한 분야는 생체인식(biometrics) 분야이다.

현재 생체 인식 분야는 기존 대비 우수한 보안성과 편의성을 바탕으로 금융, 통신, 보안, 자동차, 의료 분야에서 본인인증 수단으로 광범위하게 적용중이다.

또한 미국 IT시장 연구기관 Tractica에 따르면 글로벌 생체 인식 시장은 2024년에 대략 150억의 시장 가치를 지닐 것으로 전망되며 특히 아시아 지역이 비중을 가장 많이 차지하고 있다.



출처: Tractica('15.5.6)

현대의 컴퓨터 시스템의 대표적인 인증 방식은 사용자의 아이디와 비밀번호 문자열을 확인한 후 일치하면 접속이 허가되고 일치하지 않으면 접속이 허가 되지 않는 방식이다. 이러한 비밀번호 기반 사용자 인증은 보안을 위해 사용자가 자주 비밀번호를 변경하고 웹사이트마다 서로 다르면서도 복잡한 비밀번호를 사용해야 한다. 하지만 사람들은 복잡한 많은 비밀번호를 기억할 수 없고 자신의 편의를 위해 주기적으로 비밀번호를 변경하는 것을 하지 않게 되어 간단한 비밀번호를 많은 웹사이트에서 동일하게 계속 사용하는 현상이 일어난다.

이러한 문제점을 해결하기 위해 생체 기반 인증이 등장하였다. 생체 기반 인증은 지문, 홍채, 동공 등 개인이 유전적으로 타고나는 생리학적 인증과 음성 또는 키스트로크 다이내믹스와 같이 행위를 통해 나타나는 행동 기반 인증으로 나뉘어 진다. 생리학적 인증은 한 번 사용자 정보가 유출되면 사용자가 정보 변경을 하기 매우 어렵다는 특성 때문에 정보에 대한 엄격한 저장 이 요구되며 추가적인 하드웨어 또한 필요하다는 단점이 존재한다.

반면 행동 기반 인증 중에서도 키스트로크 다이내믹스는 추가적인 하드웨어 없이도 전통적인 인증 방식인 아이디와 비밀번호 기반 인증 시스템에 자연스럽게 접목될 수 있다는 장점이 있다. 보안적 측면에서도 키스트로크 다이내믹스는 아이디와 비밀번호의 유출 문제에도 강하다는 장점을 가지고 있다. 따라서 본 연구에서는 위 문단에서 상술한 장점들을 지닌 키스트로크 다이내믹스를 이용한 사용자 인증 및 보안 방법을 개발하고자 한다.

2. 필요성 및 중요성

키스트로크 다이내믹스에 대한 논문은 국내외에 꾸준히 있었고 외국에서는 몇몇 솔루션들이 개발 중이거나 이미 개발되었지만 국내에서는 개발된 솔루션은 보이지 않는다. 또한 전술된 대로 생체 인식 시장 규모가 2024년에는 150억 달러가 될 전망인데 이는 무척이나 커다란 수치이다. 이런 점들을 고려할 때 국내에서의 키스트로크 다이내믹스 시장은 아직 형성되지 않았지만 천문학적인 규모의 시장을 형성할 것으로 보이며 본 연구를 통해 이런 시장 형성에 기여할 수 있기를 기대한다.

2.

2. 연구의 목표 및 내용

본 연구에서는 사용자의 키보드 패턴을 이용한 키스트로크 다이나믹스를 통해 사용자 인증을 하여 비밀번호 기반 인증에 대한 보안을 강화하고자 한다. 이를 위한 적용 가능한 방식은 크게 두 가지가 있다.

먼저 고정된 길이의 문자열을 가지고 사용자 인증을 하는 것이다. 예를 들어 사용자가 회원가입 시 자신의 비밀번호 패턴도 같이 전송하면 나중에 사용자가 로그인 시 자동으로 키스트로크 다이나믹스가 적용되어 사용자를 접속시킬 것인 것 판단하게 된다. 하지만 이런 방식은 일단 한번 사용자가 인증되면 다른 사용자가 인증된 사용자의 시스템을 이용하는 것을 막을 수 없다는 문제점이 생긴다.

이런 문제점을 해결하기 위해 가변적 길이의 문자열을 가지고 사용자 인증을 할 수 있다. 이런 방식을 채택하면 사용자의 키보드 패턴을 지속적으로 감시할 수 있기에 인증된 사용자의 키보드 패턴인지 아니면 다른 사용자의 키보드 패턴인지를 판단해 낼 수 있다.

따라서 위와 같은 장점을 고려하여 본 연구에서는 가변적 길이의 문자열에 대한 키스트로크 다이나믹스를 통한 사용자 인증 및 보안 방법을 개발하고자 한다.

3. 연구의 추진전략 및 방법

기계 학습에 대한 개략적인 이해를 바탕으로 하여 키스트로크 다이나믹스 관련 논문들을 공부한다. 공부한 내용을 바탕으로 하여 파이썬으로 모델을 구현해 본다.

실험 참여자를 모집하여 참가자마다 다양한 문자열을 입력 받아 데이터를 수집하고, 통계를 내어 분석하고, 데이터를 바탕으로 구현한 모델을 평가하여 개선하는 것을 반복한다

4. 연구 팀의 구성 및 과제 추진 일정

구성원

박종혁 - 실험 진행 및 프로젝트 팀장

김주성 - 소프트웨어 구현 및 알고리즘 설계

김신원 - 데이터 분석

김종훈 - 프로그램 테스트

일정

1학기 소프트웨어 구현 및 데이터 분석

4월 - 디자인 스프린트 진행, UI 설계

5월 - 소프트웨어 개발

6월 - 알고리즘 설계 및 구현

2학기 실험 참가자 모집 및 진행

데이터 분석 및 구현 모델 개선

- 참고문헌(Reference)

자유로운 문자열의 키스트로크 다이내믹스와 일범주 분류기를 활용한 사용자 인증

사용자 인증 및 계정공유 탐지를 위한 개인 키스트로크 모델에 대한 연구

자유로운 문자열의 키스트로크 다이내믹스를 활용한 사용자 인증 연구

2. 요구사항 명세서

Table of Contents

1. Introduction	1
1.1. Purpose	1
1.2. Scope	1
1.3. Definitions, acronyms, and abbreviations	1
1.4. References	1

<u>2. External Interface Requirements</u>	<u>2</u>
<u>2.1. 사용자 인터페이스 (User Interface)</u>	<u>2</u>
<u>2.2. 하드웨어 인터페이스 (Hardware Interface)</u>	<u>2</u>
<u>2.3. 소프트웨어 인터페이스 (Software Interface)</u>	<u>2</u>
<u>2.4. 통신 인터페이스 (Communication Interface)</u>	<u>2</u>
<u>3. System Features</u>	<u>3</u>
<u>3.1. 시스템 기능 1 (System Feature 1)</u>	<u>3</u>
<u>3.1.1. 설명 및 우선순위 (Description and Priority)</u>	<u>3</u>
<u>3.1.2. 기능 요구사항 (Functional Requirements)</u>	<u>3</u>
<u>3.2. 시스템 기능 2 (System Feature 2)</u>	<u>3</u>
<u>3.2.1. 설명 및 우선순위 (Description and Priority)</u>	<u>3</u>
<u>3.2.2. 기능 요구사항 (Functional Requirements)</u>	<u>3</u>
<u>4. Other Nonfunctional Requirements</u>	<u>4</u>
<u>4.1. 성능 요구 (Performance Requirements)</u>	<u>4</u>
<u>4.2. 안전 요구 (Safety Requirements)</u>	<u>4</u>
<u>4.3. 보안 요구 (Security Requirements)</u>	<u>4</u>
<u>4.4. 소프트웨어 품질 속성 (Software Quality Attributes)</u>	<u>5</u>
<u>5. Other Requirements</u>	<u>6</u>
<u>5.1. H/W 제약 조건</u>	<u>6</u>
<u>5.2. 자원, 인력에 대한 제약 조건</u>	<u>6</u>
<u>6. 부록</u>	<u>7</u>

1. Introduction

1.1. Purpose

이 문서는 생체 인증 기술 중 키스트로크 다이내믹스를 기반으로 한 사용자 인증이 적용된 소프트웨어에 대해 키스트로크 다이내믹스를 사용할 것으로 기대되는 사용자에게 설명하고자 하는 목적이다.

1.2. Scope

키스트로크 다이내믹스를 기반으로 한 인증이 적용된 소프트웨어는 기존의 비밀번호 기반 인증 방식에 더해 추가적으로 사용자의 키보드 입력 패턴을 통해 인증한다. 이를 통해 비밀번호만을 이용한 인증에서의 보안 취약성을 보완할 수 있고 추가적인 하드웨어 없이 소프트웨어적으로 가능한 인증 방식이기에 다른 생체 인증 기술보다 저렴하다는 이점도 가진다.

1.3. Definitions, acronyms, and abbreviations

생체 인증(Biometrics) : 생체 인증(Biometrics)은 하나 이상의 고유한 신체적, 행동적 형질에 기반하여 사람을 인식하는 방식을 두루 가리킨다.

키스트로크 다이내믹스(Keystroke Dynamics) : 키스트로크 다이내믹스(keystroke dynamics)는 키보드에서 타이핑(typing)하는 리듬과 방법에 기반하여 사용자를 확인하는 방법이다.

DB : 데이터베이스(영어: database, DB)는 여러 사람이 공유하여 사용할 목적으로 체계화해 통합, 관리하는 데이터의 집합이다.[1] 작성된 목록으로써 여러 응용 시스템들의 통합된 정보들을 저장하여 운영할 수 있는 공용 데이터들의 묶음이다.

FAR : 오인식률(FAR:False acceptance rate): 본인의 것이 아닌 생체인식 정보를 본인의 것으로 잘못 판단할 확률을 의미한다.

FRR : 오거부률(FRR:False Rejection Rate): 본인의 생체정보를 본인이 아닌 것으로 잘못 판단할 확률을 말한다.

1.4. References.

위키백과

사용자 인증 및 계정공유 탐지를 위한 개인 키스트로크 모델에 대한 연구

2. External Interface Requirements

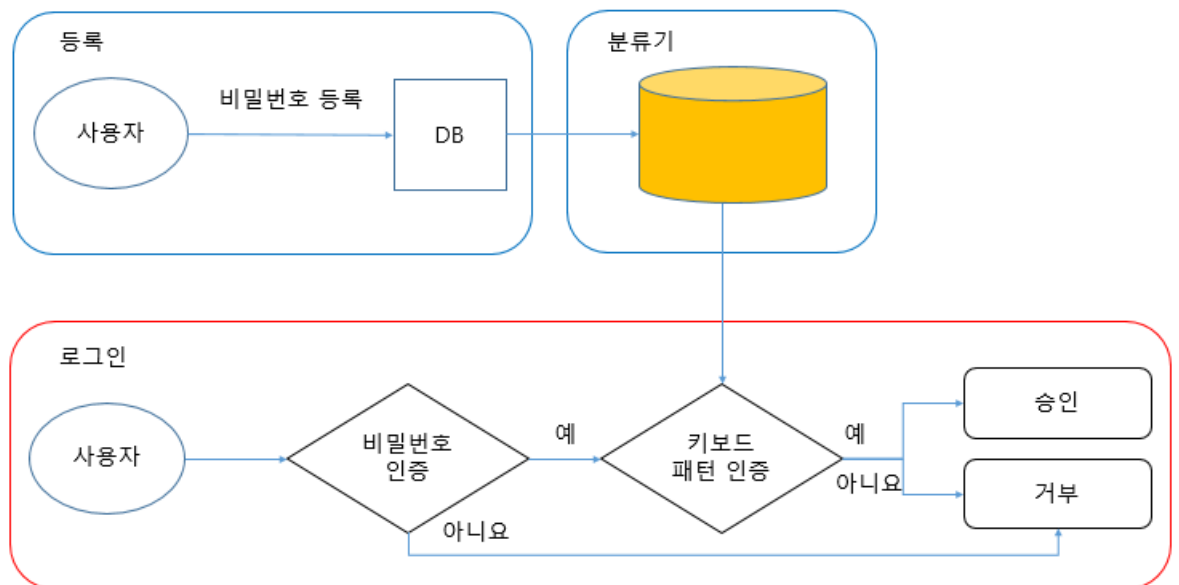
1.5. 사용자 인터페이스 (User Interface)

1. 키스트로크 다이내믹스 기능 사용 여부 표시
2. 사용자의 키보드 입력 패턴 일치 율 표시 및 로그인 성공하기 위한 키보드 입력 패턴 일치 율 기준 표시

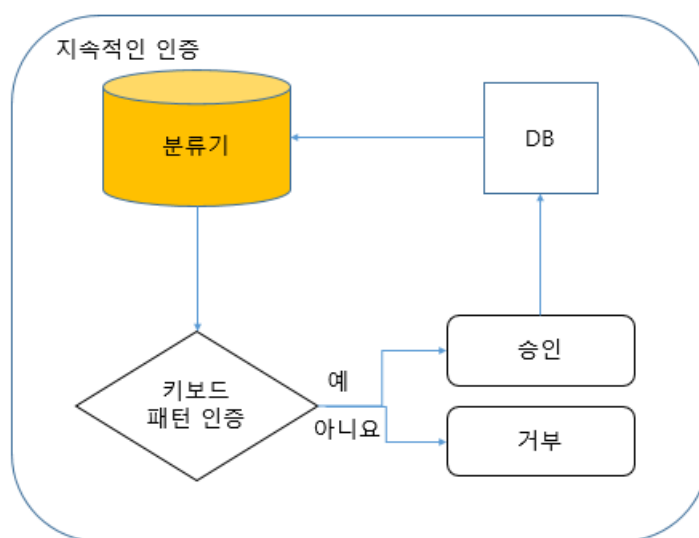
1.6. 하드웨어 인터페이스 (Hardware Interface)

해당 없음.

1.7. 소프트웨어 인터페이스 (Software Interface)



[그림 1] 고정 길이 문자열 기반 키스트로크 다이내믹스



[그림 2] 가변 길이 문자열 기반 키스트로크 다이내믹스

1.8. 통신 인터페이스 (Communication Interface)

해당 없음.

3. System Features

1.9. 시스템 기능 1 (System Feature 1)

1.1.1. 설명 및 우선순위 (Description and Priority)

사용자는 키스트로크 다이내믹스 인증 기법이 적용된 특정 시스템의 DB에 아이디, 비밀번호, 키보드 입력 패턴을 등록한다.

우선순위 : 높음

1.1.2. 기능 요구사항 (Functional Requirements)

요구사항 분류	기능
요구사항 번호	SFR-001
요구사항 명칭	사용자 등록
요구사항 정의	사용자를 시스템에 등록하는 기능

상세설명	세부	- 아이디, 비밀번호, 키보드 입력 패턴 등의 사용자 정보를 시스템의 DB에 저장
	내용	- 필수 정보인 아이디, 비밀번호, 키보드 입력 패턴을 입력하지 않은 경우 오류 메시지 출력
산출 정보		회원정보가 갱신된 DB
관련 요구 사항		

1.10. 시스템 기능 2 (System Feature 2)

1.1.3. 설명 및 우선순위 (Description and Priority)

사용자는 키스트로크 다이내믹스 인증 기법이 적용된 특정 시스템에 대한 접속이 허가되거나 거부된다.

우선순위 : 높음

1.1.4. 기능 요구사항 (Functional Requirements)

요구사항 분류	기능	
요구사항 번호	SFR-002	
요구사항 명칭	사용자 로그인	
요구사항 상세설명	정의	사용자 로그인 시 시스템은 사용자의 접속의 허가 여부를 판별하는 기능
	세부 내용	<ul style="list-style-type: none"> - 사용자가 1차 인증인 비밀번호 기반 인증에서 실패하면 로그인 실패 메시지 출력 - 사용자가 1차 인증을 통과하면 시스템은 2차 인증을 시도 - 2차 인증은 키보드 입력 패턴 기반 인증으로 분류기에서 1차 인증에서의 키보드 입력 패턴이 DB에서 등록된 사용자의 키보드 입력 패턴과 얼마나 일치하는지 확인. - 일치율이 정해진 기준으로 높으면 로그인 성공 메시지를 출력하고 그렇지 않으면 로그인 실패 메시지를 출력.
산출 정보		로그인 성공/실패 메시지

관련 요구 사항	SFR-001
----------	---------

1.11. 시스템 기능 3 (System Feature 3)

1.1.5. 설명 및 우선순위 (Description and Priority)

사용자나 관리자는 키보드 입력 패턴을 관리할 수 있다.

우선순위 : 높음

1.1.6. 기능 요구사항 (Functional Requirements)

요구사항 분류		기능
요구사항 번호		SFR-003
요구사항 명칭		키보드 입력 패턴 관리
요구사항 상세설명	정의	회원의 키보드 입력 패턴을 관리하는 기능
	세부 내용	<ul style="list-style-type: none">- 사용자는 자신의 키보드 입력 패턴을 추가 및 삭제할 수 있다.- 관리자는 회원의 비정상적인 키보드 입력 패턴을 삭제할 수 있다.- 키보드 입력 패턴 추가 시 일정 기간 동안 키보드 입력이 없으면 키보드 입력 패턴 추가 실패 메시지 출력
	산출 정보	키보드 입력 패턴 추가 또는 삭제 성공/실패 메시지
	관련 요구 사항	SFR-001, SFR-002

4. Other Nonfunctional Requirements

1.12. 성능 요구 (Performance Requirements)

요구사항 분류	성능
요구사항 번호	PER-001
요구사항 명칭	로그인 승인 여부 판단 시간
요구사항 상세설명	정의 로그인 승인 여부 판단 시간 목표 정의
세부 내용	- 사용자가 로그인 성공/실패 메시지를 정보 입력 후 5초 이내에 제시
산출정보	
관련 요구사항	SFR-002

1.13. 안전 요구 (Safety Requirements)

해당 없음.

1.14. 보안 요구 (Security Requirements).

요구사항 분류	보안 요구사항
요구사항 번호	SER-002
요구사항 명칭	DB 보안
요구사항 상세설명	정의 DB 저장 요건
세부 내용	- DB에서 사용자의 아이디, 비밀번호, 키보드 입력 패턴이 동시에 탈취되지 않도록 주의한다.
산출정보	
관련 요구사항	SFR-001

요구사항 분류		보안 요구사항	
요구사항 번호		SER-003	
요구사항 명칭		사용자 로그인 인증 보안	
요구사항 상세설명	정의	사용자 로그인 FAR, FRR 목표 비율 정의	
	세부 내용	- FAR은 5% 이하, FRR은 10% 이하를 목표로 잡는다.	
산출정보			
관련 요구사항		SFR-002	

1.15. 소프트웨어 품질 속성 (Software Quality Attributes)

요구사항 분류		품질	
요구사항 번호		QUR-001	
요구사항 명칭		정확성(correctness)	
요구사항 상세설명	정의	정확성 개념 정의	
	세부 내용	<ul style="list-style-type: none">- 시스템은 사용자 등록 시 사용자의 정보를 정확하게 DB에 저장하여야 한다.- 시스템은 사용자 로그인 시 사용자의 키보드 입력 패턴이 DB에 저장된 키보드 입력 패턴과의 일치 율이 정해진 기준보다 높으면 성공 낮으면 실패 메시지를 출력해야 한다.- 시스템은 사용자나 관리자의 요청에 따라 키보드 입력 패턴을 추가 삭제할 수 있어야 한다.	
	산출정보		
	관련 요구사항	SFR-001, SFR-002, SFR-003	

요구사항 분류		품질
요구사항 번호		QUR-002
요구사항 명칭		신뢰성(reliability)
요구사항 상세설명	정의	신뢰성 개념 정의
	세부 내용	<ul style="list-style-type: none">- 시스템은 모든 사용자에게 동일한 입력과 결과가 주어져야 함- 시스템의 사용자 로그인 판단 기준이 일정해야 함- 시스템의 모든 메시지는 5초 이내에 사용자에게 제시되어야 함
산출정보		
관련 요구사항		

5. Other Requirements

1.16. H/W 제약 조건

해당 없음.

1.17. 자원, 인력에 대한 제약 조건

해당 없음.

3. 유스케이스

Table of Contents

<u>1. Introduction</u>	<u>1</u>
<u>1.1. Objective</u>	<u>1</u>
<u>2. Usecase Diagram</u>	<u>2</u>
<u>2.1. 설정 Diagram</u>	<u>2</u>
<u>3. Usecase Specification</u>	<u>3</u>
<u>3.1. 회원 가입</u>	<u>3</u>
<u>3.2. 프로필 사진 설정</u>	<u>3</u>

1. Introduction

1.1. Objective

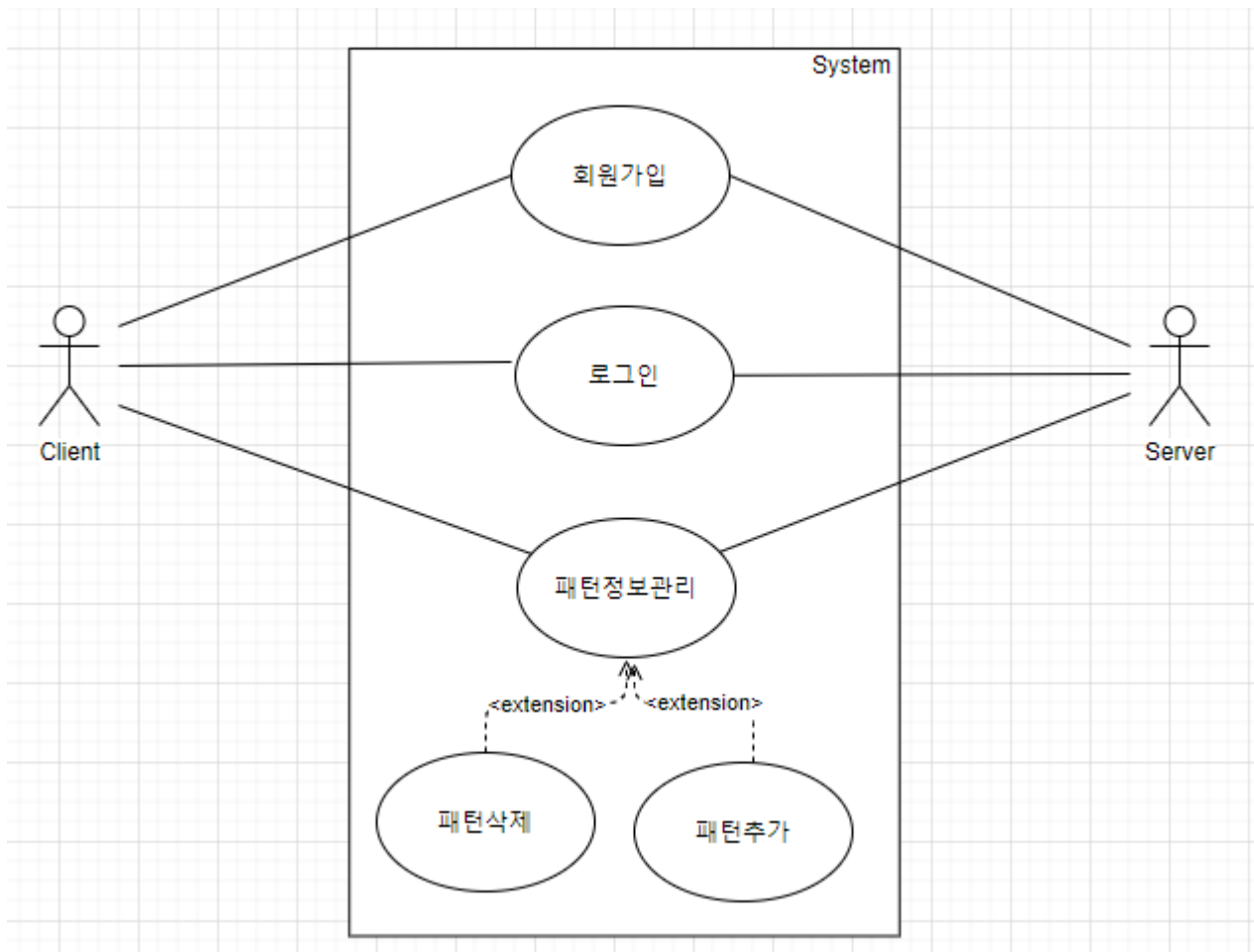
이 문서는 키보드 입력 패턴을 이용한 사용자 인증 및 보안을 수행하는 인증 프로그램의 기능을 명세하고 있다.

2. Usecase Diagram

1.2. 설정 Diagram

키보드 입력 패턴을 이용한 인증 및 보안 프로그램에서 전체시스템에 대한 유스케이스 다이어그램은 다음과 같다.

그림 1. 전체시스템에 대한 유스케이스 다이어그램



3. Usecase Specification

1.3. 회원 가입

Usecase 이름	회원 가입
ID	1
간략 설명	사용자가 시스템을 사용하기 위한 일련의 회원 가입 절차에 대해 명세한다.
Actor	Client(Initiator), Server
Pre-Conditions	-
Main Flow	1) 사용자는 아이디, 비밀번호, 키보드 입력 패턴을 입력한다. 2) 서버 DB 내에 사용자의 정보가 정상적으로 저장되면 회원 가입 성공 메시지를 출력한다.
Post-Conditions	- 사용자는 회원으로 등록된다.
Alternative Flow	1-1) 사용자는 회원 가입 시 이메일 또는 휴대폰 번호를 입력할 수 있다. 2-1) 필수 입력 정보인 아이디, 비밀번호, 키보드 입력 패턴이 입력되지 않아 필수 정보 입력 필요 메시지를 출력한다.

1.4. 사용자 로그인

Usecase 이름	사용자 로그인
ID	2

간략 설명	사용자가 시스템을 사용하기 위한 일련의 로그인 과정을 명세한다.
Actor	Client(Initiator), Server
Pre-Conditions	-
Main Flow	<p>1) 사용자는 로그인 입력 정보를 입력한다.</p> <p>2) 서버는 1차적으로 사용자가 입력한 아이디와 비밀번호를 확인해서 DB에 존재하는지 확인한다.</p> <p>3) 사용자가 존재하는 것으로 확인되어 서버는 2차 인증을 시작한다.</p> <p>4) 서버는 분류기에서 DB에 등록된 키보드 입력 패턴과 입력한 키보드 입력 패턴 일치 율을 확인한다.</p> <p>서버는 사용자의 입력 패턴이 일정 기준이 넘었음을 확인하고 로그인 성공 메시지를 출력한다.</p>
Post-Conditions	- 사용자는 로그인 성공을 한다.
Alternative Flow	<p>1-1) 사용자는 자신의 이메일 주소나 휴대폰 번호로 로그인 할 수 있다.</p> <p>2-1) 아이디 또는 비밀번호가 DB에 존재하지 않아 서버는 로그인 실패 메시지를 출력한다.</p> <p>4-1) 일치 율이 기준을 넘지 않아 서버는 로그인 실패 메시지를 출력한다.</p>

1.5. 키보드 입력 패턴 관리

Usecase 이름	키보드 입력 패턴 관리
------------	--------------

ID	3
간략 설명	사용자나 관리자가 키보드 입력 패턴 관리 과정을 명세한다.
Actor	Client(Initiator), Server
Pre-Conditions	- 사용자는 회원이어야 한다.
Main Flow	1) 사용자는 자신의 키보드 입력 패턴을 추가 및 삭제하고 관리자는 회원의 키보드 입력 패턴을 삭제한다. 2) 서버는 사용자나 관리자의 요청을 받아 DB에서 요청에 해당하는 키보드 입력 패턴을 추가하거나 삭제한다.
Post-Conditions	- DB에서 키보드 입력 패턴이 추가되거나 삭제된다.
Alternative Flow	