한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

사용자 입력 패턴 분석을 이용한 사용자 판별 방법 연구

박민수*, 박주민*, 김경헌O, 원유재*
O*충남대학교 컴퓨터공학과
e-mail: {deceglie92, dynamiseus}@gmail.com*, rudgjs0618@gmail.comO, yjwon@cnu.ac.kr*

User Identification Method Using Input Pattern Analysis

Minsoo Park*, Jumin Park*, Kyungheon KimO, Yoojae Won*
O*Dept. of Computer Science & Engineering, Chungnam National University

● 요 약 ●

본 논문에서는 사용자 입력패턴 분석을 통한 행위 기반 인증 방법을 제안한다. 이 알고리즘은 기기를 통해 들어온 사용자의 다양한 입력정보를 받아오고, 받아온 정보를 분석하여 사용자만의 고유한 정보를 추출한다. 이렇게 추출된 정보를 데이터베이스에 저장 후, 사용자에 대한 인증요청이 들어오면 입력 정보들과 저장된 입력정보의 일치여부에 따라 인증을 허용할지 결정한다. 이를 이용하면 사용자의 고유한 행위에 대한 정보를 가지고 인증을 진행하기 때문에, 사용자의 기억에 의존하지 않고 간단하게 인증 절차를 진행할 수 있다. 본 논문에서는 실험을 통해 모인 데이터를 분석하여 제안하는 인증 방법이 실질적으로 사용자 인증에 적용 될 수 있음을 보인다.

키워드: 패턴(Pattern), 행위(Behavior), 사용자 인증(User-Authentication)

I. Introduction

국내 인터넷과 스마트폰 보급률은 꾸준히 증가하였고, 이에 따라 인터넷 또는 웹서비스를 이용하는 사용자도 크게 증가하였다. 서비스를 사용하는 사용자가 증가함에 따라 서비스를 사용하고자 하는 사용자가 옳은 사용자인지 인증하는 과정은 매우 중요해졌다. 따라서 각종 인증 시스템이 등장하였고, 국내에서는 금융거래 시 공인인증서를 의무적으로 사용하도록 규정을 세워 사용자 인증에 신뢰성을 높였다.

그러나 2015년 3월 공인인증서 의무사용 규정이 폐지되었고, 이에 따라 다양한 보안 시스템에 대한 요구가 증가하고 있다. 이러한 흐름에 맞춰 최근에 핀테크 시장에서는 새로운 인증시스템이 등장하고 있다.

시장에 등장하고 있는 인증시스템 중 가장 주목받는 분야는 생체정보를 이용한 생체인증 분야이다. 기존에 사용하던 아이디와 패스워드를 이용한 인증의 경우, 서비스 제공자는 사용자가 사용할 아이디와 패스워드에 대해서 철저한 보안이 필요하고, 사용자 또한 보안 강화를 위해 복잡하고 어려운 패스워드를 이용하면서 주기적으로 변경을 요구하는 등 현실적인 어려움이 존재했다. 이에 비해 생체인식의 경우 인증에 사용자의 생체정보를 이용하는데, 생체정보는 사용자의 고유한 정보이기 때문에 앞서 아이디와 패스워드를 사용하였을 시 발생한 관리에 대한 현실적인 문제들이 발생하지 않으면서도 간단하게 인증할 수 있다는 장점이 있다.

본 논문에서는 최근의 추세를 반영하고, 별도의 생체인식 장치를 필요로 하지 않고 사용자가 디바이스의 입력장치를 사용할 때 발생하는 다양한 정보를 분석하여 인증에 사용하고자하는 행위 기반 인증을 제시하고자 한다. 이에 먼저 최근에 등장한 인증방식들에 대한 간단한 내용을 2장에서 소개할 예정이다. 3장에서는 본 논문에서 제안하고자 하는 인증방식을 기술한다. 4장은 결론으로 우리가 제시한 인증방식에 대한 실험을 통해 실질적으로 사용자 인증에 사용될 수 있을지 분석한다.

II. Related works

1. FIDO

FIDO는 Fast Identity Online의 약자로 지문, 홍채, 안면인식 등 생체인증을 접목한 사용자 인증 방식을 말한다.

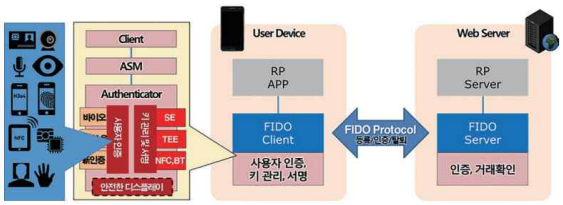

Fig. 1. FIDO Architecture

Fig 1은 FIDO 아키텍처이다. FIDO는 로컬 기기에 이미 탑재된 인증수단을 이용하여 로컬인증을 하고, 인증 사용자를 대신하여 FIDO 인증장치가 표준화된 단일 프로토콜을 이용하여 서버와 원격 인증을 하는 구조를 채택하고 있다. 따라서 서비스 기업은 다수의 인증 수단들을 하나의 인증 서버를 이용하여 제공할 수 있으며, 사용자는 본인에게 익숙한 장치를 이용하여 서비스를 제공받을 수 있다는 장점이 있다. 또한 사용자의 민감한 생체정보가 사용자 개인의 장치 내부에 존재하기 때문에 서버를 통해 생체정보가 유출 될 수 있는 문제를 근본적으로 해결하고 있다. 또한 사용자를 특정할 수 있는 식별정보가 포함되지 않도록 FIDO 프로토콜이 설계되어있기 때문에 대규모 DB유출이 발생해도 다른 사이트로 확산되는 것을 방지할 수 있다[1].

이런 FIDO 기술의 인증 방법의 편리성과 안정성 때문에 국내외 다양한 기업에서 FIDO 기술을 도입한 인증 서비스를 제공하고 있다. 국내에서는 대표적으로 삼성의 삼성페이와 NH농협, 하나은행 등 국내 대표적인 금융기업들이 FIDO기술을 도입하여 결제 서비스를 제공하고 있다[2].

2. 행위 기반 인증

행위 기반 인증은 개인의 고유한 행동 특성을 이용하여 개인을 식별하고 인증하는 기술로, 넓은 의미로 생체인증의 방식 중 하나이다. 행위 기반 인증의 종류로는 키 입력 패턴, 마우스 이동 패턴, 터치스크린 패턴, 자필 서명 검증, 화자 인증 및 음성 인식 등이 있다.

이러한 행위 기반 인증을 사용한 사례로는 국내의 스마트 사인과 해외의 Identity Provider, Behavioral Authentication 등의 기술들이 있다. 각각의 기술에 대해서 살펴보면, 먼저 스마트폰 및 태블릿의 터치패드에 사용자가 직접 수기서명을 입력함으로써 등록된 원본 정보와 실시간 입력 받은 정보를 비교해 본인 여부를 확인한다. 해외의 사용자의 키보드 입력과 마우스 이동행위를 분석한 뒤 사용자의 고유한 패턴을 생성하여 사용자 기기별로 고유한 행위기반 프로파일을 모델링하거나, 태블릿 기기에서 사용자의 스크롤 행위를 분석하여 사용자 인증에 적용한다. 또한 사용자가 입력하는 키보드 입력, 마우스 클릭 패턴 등의 패턴정보를 통합하여 사용자 인증에 사용하는 등 다양한 방식을 통해 연구가 활발히 진행되고 있다[3].

이처럼 다양한 행위기반 인증 기술을 도입한 사례들이 존재하고, 이 기술들 또한 앞에서 설명한 FIDO처럼 편의성과 보안성을 제공하고 있다. 이에 따라 본 논문에서는 행위 기반 인증 이용한 인증 방법을 제시하고자한다.

III. The Proposed Scheme

1. 연구 내용

본 논문에서는 PC환경의 마우스, 키보드, 모바일 환경의 터치화면을 이용한 행위 기반 인증 방식을 제공하고자 한다. 이때 우리가 판별에 입력장치별 사용할 인증 정보는 아래 Table 1에 나오는 정보들이다.

Table 1. Authentication information used for user identification per input device

	인증 정보
마우스	속도 낭비동선 방향성 변화도
키보드	키 값의 평균 입력시간 평균 입력 시간의 분산
터치스크린	패턴의 모양 걸린시간 시작점의 x, y좌표 끝점의 x, y좌표

먼저 PC 환경은 마우스의 동작 정보와 키보드의 입력정보를 이용하여 사용자 인증에 사용한다. 이때 사용하는 마우스 정보는 20ms 마다 들어오는 마우스의 x, y 좌표이다. 이렇게 들어온 좌표들을 통해 이전의 지점과의 거리를 구하고 구해진 거리를 이용하여 속도, 낭비동선, 방향성의 변화도를 구한다. 이들을 구하는 수식은 아래와 같다.

$$\text{속도} = \sum_{n=1}^{ListSize} (n-th\,node).dist / ListSize \quad (1)$$

$$\text{낭비동선} = \sum_{n=1}^{ListSize} (n-th\,node).dist - dist((front\,node).coordinate, (rear\,node).coordinate) \quad (2)$$

$$\text{방향성 변화도} = \sum_{n=1}^{ListSize-1} innerProduct(n-th\,node, next\,node) \quad (3)$$

수식(1)은 들어온 거리를 저장된 노드 리스트의 크기로 나누어 속도를 구한다. 수식(2)는 리스트의 첫 번째 노드와 마지막 노드간의 직선거리를 구하고 실제 측정된 거리를 구한 뒤 두 값의 차를 통해 낭비동선을 구한다. 수식(3)은 방향성의 변화도를 구하는 수식으로, 한 노드에서 인접한 노드까지의 내적을 구해서 계산한다. 이렇게 분석된 각각의 정보는 여러 번의 입력을 통해 최솟값과 최댓값을 가지게 되고 이것들을 임계값으로 사용하여 인증 시 값의 유효범위를 지정하게 된다. 이렇게 구해진 정보를 저장하고, 이후 사용자 입력이 들어왔을 때 들어온 정보가 저장된 유효범위 안에 존재한다면 인증에 성공하게 된다.

키보드 정보의 경우, 입력이 들어온 키 값과 키가 눌려져있는 시간을 이용한다. 이렇게 들어온 정보를 통해 각키의 평균과 분산을 구하는데 이를 구하는 수식은 아래와 같다.

$$\text{평균} = u = \frac{1}{N}\sum_{i=1}^{N} timeKeyStroke_i \quad (4)$$

$$\text{분산} = \frac{1}{N}\sum_{i=1}^{N} (timeKeyStroke_i - u)^2 \quad (5)$$

수식(4)는 키 입력 시간의 평균을 구하는 수식으로 해당하는 키가 입력된 모든 시간을 더한 뒤 입력 횟수만큼 나누어서 구한다. 수식(5)는 수식(4)를 통해 구해진 평균값과 각각의 입력시간에 대한 차를 모두 더하고, 이것을 입력 횟수만큼 나누어서 구한다. 이렇게 구해진 평균에 대해 분산만큼의 유효범위를 가지게 된다. 계산된 정보를 저장하고 이후 사용자 입력이 발생할 때 저장된 정보를 이용하여 유효범위 안에 입력정보가 존재한다면 인증에 성공하고 그렇지 않다면 실패한다.

마지막으로 터치화면의 경우 드래그 패턴을 인증수단에 사용하는데 이때 사용한 패턴의 모양, 패턴의 시작점의 좌표, 끝점의 좌표, 패턴을 그리는 데 걸린 시간이 인증에 이용된다. 각각의 정보는 수집단계 때 여러 번 반복을 통해 정보를 수집하게 되고 이렇게 수집된 정보들을 시작점과 끝점의 경우는 최솟값과 최댓값을 이용하여 유효범위를 저장하고, 걸린 시간의 경우 평균시간을 구한 뒤 평균 시간의 ±15%를 유효범위로 저장한다. 이렇게 저장된 정보를 바탕으로 사용자의 입력이 들어왔을 때 비교하고 비교 결과 유효범위 안에 입력정보가 존재한다면 인증에 성공한다.

2. 연구 결과

앞에서 소개한 방식을 적용하여 인증을 시도해 보았고, 먼저 터치화면에 적용한 방식에 대한 실험 결과는 아래 표와 같다.

Table 2. The number of successful authentication attempts for each user information

	실험자A	실험자B	실험자C
A의 정보	31/40	7/40	12/40
B의 정보	6/40	36/40	11/40
C의 정보	10/40	13/40	30/40

표에서 보는 것과 같이 저장된 정보와 일치하는 실험자가 인증을 시도했을 경우 75%이상의 높은 인증 성공률을 보였다. 저장된 정보와 일치하지 않는 실험자가 인증에 시도했을 경우 대부분 25%이하의 인증 성공률을 보인다. 실험을 통해 전반적으로 사용자를 판별하는데 사용할 수 있을 만큼에 결과를 보였으나 일치하지 않는 사용자에 대한 인증 성공률이 다소 높아 세부적인 조정이 필요한 것으로 판단된다.

이어서 아래의 표는 본 논문에서 제시한 키보드 입력을 통한 인증 방식을 적용하였을 때의 결과를 나타낸 표이다.

Table 3. Experimental results using authentication information of experimenter A

	실험자A	실험자B	실험자C
1회	91.3%	26.09%	4.35%
2회	100%	26.09%	17.39%
3회	82.61%	27.74%	34.74%
4회	82.61%	30.43%	13.04%
5회	86.96%	21.74%	21.74%

Table 4. Experimental results using authentication information of experimenter B

	실험자A	실험자B	실험자C
1회	39.13%	56.62%	30.43%
2회	39.13%	78.26%	39.13%
3회	34.78%	82.61%	34.78%
4회	26.09%	73.91%	43.78%
5회	43.48%	82.61%	43.48%

Table 5. Experimental results using authentication information of experimenter C

	실험자A	실험자B	실험자C
1회	17.34%	47.83%	78.26%
2회	21.74%	43.48%	69.57%
3회	21.74%	43.48%	82.61%
4회	26.06%	39.13%	86.96%
5회	21.74%	39.13%	65.22%

표에서 보는 것과 같이 저장된 정보와 일치하는 실험자가 키보드를 가지고 입력하였을 경우, 평균적으로 70%이상의 일치율을 보이고, 일치하지 않는 실험자는 평균적으로 30% 이하는 낮은 일치율을 보인다. 이에 따라 충분히 사용자를 구분하는 근거로 삼을 수 있을 것이라 판단된다.

마지막으로 아래의 Fig 2는 각각 길이가 4이고 6인 비밀번호를 마우스를 가지고 입력할 때 저장된 정보와 일치하는 사용자가 시도하였을 때의 일치율과 일치하지 않는 사용자가 시도하였을 때의 일치율을 보여주는 그래프이다.

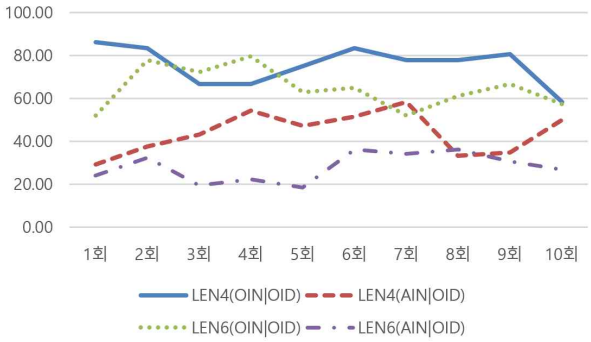

Fig. 2. Experimental results on authentication method using mouse

Fig 2에서 보이는 것과 같이 비밀번호가 길어질수록 저장된 정보와 입력된 정보의 일치율은 낮아지나 저장된 정보와 일치하는 실험자가 입력을 시도하였을 때의 일치율과 일치하지 않는 실험자가 입력을 시도하였을 때의 일치율의 차는 더 커지는 것을 볼 수 있다. 따라서 적당히 긴 비밀번호를 사용하면서 본 논문에서 제시하는 인증 방식을 적용한다면 충분히 사용자를 구분하는 근거로 사용될 수 있을 거라 판단된다.

IV. Conclusions

본 논문에서는 마우스, 키보드, 터치화면을 이용한 행위 기반 인증 방식을 제시하고 이 방식을 실질적인 사용자 인증에 적용 될 수 있는지 분석해 보았다. 각각의 환경에서 우리가 제시한 방식은 평균적으로 일치하는 사용자와 일치하지 않는 사용자를 뚜렷하게 구분해 낼 수 있었다. 따라서 본 논문에서 제시한 행위 기반 인증 방식이 사용자 판별의 근거가 될 수 있음을 보였다. 다만 마우스의 경우 각각의 경우마다 편차가 다소 존재하였고, 터치화면의 경우 오 인식률이 25%정도로 다소 높은 경향을 보였다. 이에 따라 각각의 방식을 단독적으로 사용하기에는 다소 무리가 있으나, 마우스는 키보드와 결합하여 마우스가 보이는 한계점을 보안하고, 터치화면의 경우 사용자 입력데이터에 대한 분석을 통해 앞에 제기한 한계점을 보안할 수 있는 방안이 있는지 조사하여 적용할 수 있다면 충분히 우리가 생각하는 보안효과를 거둘 수 있을 것이라고 판단된다. 이와 더불어 기존에 보편적으로 알려진 SVM(Support Vector Machine)이나 HMM(Hidden Markov Model)같은 알고리즘을 도입하여 적용하면 더 좋은 효과를 거둘 수 있을 것이라 판단된다.

Acknowledgment

This research was supported by the MISP(Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW) (R7115-16-1007) supervised by the IITP(Institute for Information & communications Technology Promotion)

References

[1] Soohyung Kim (2016). FIDO based PinTech authentication technology. The Jounal of The Koran Institute of Communioation Soienes, 33(2), 59-65.

[2] Seung-Hyun Kim, Jong-Hyuk Roh, Sung-Hoon Lee, Jin-Man Cho, Soohyung Kim, Seunghun Jin (2016). A trends of Fintech's security technology. Coomunications of the Korean Institute of Information Scientists and Engineers, 34(4), 20-24.

[3] Soohyung Kim, YeongSub Cho, DaeSeon Choi (2015). FinTech Era: Needs for the innovation of user authentication technology. Coomunications of the Korean Institute of Information Scientists and Engineers, 33(5), 17-22.