Egérdinamika alapú felhasználó azonosítás mély neurális hálók segítségével

User authentication based on mouse dynamics using deep neural network

FEJÉR Norbert, ANTAL Margit

Sapientia EMTE, Műszaki és Humántudományok kar, Marosvásárhely
fejer.norbert@student.ms.sapientia.ro, manyi@ms.sapientia.ro

Abstract

Time series can be found in almost all areas that require human cognitive processes, therefore many of their real-life applications are known. Segmenting and classifying these types of time series is one of the most challenging tasks in the field of data mining. In the majority of cases these are extremely domain specific, so very often they claim the work of a data scientist with many years of experience. Nowadays, artificial intelligence based researches are constantly moving forward at very fast pace. Deep neural networks show an effective way of solving analytically difficult problems, therefore they can be applied on time series classification.

This research deals with mouse dynamics based user authentication, using deep neural networks. To approach the state-of-the-art performance in this field, we analyzed several types of convolutional neural networks. The effect of different preprocessing methods, as well as the effect of different amount of training data on the performance of the proposed architectures were evaluated. Since training DNN models requires a lot of data, we used transfer learning. The measurements were performed using the publicly available SapiMouse dataset, collected with our own web based application. ResNet provided the best performance. Using this type of architecture we achieved 0.86 AUC based on 3 seconds of mouse movement data. Increasing the amount of data to 12 seconds resulted in 0.92 AUC on the same dataset.

Keywords: *mouse dynamics, representation learning, convolutional neural networks.*

Kivonat

Az idősorok majdnem minden olyan területen fellelhetők, amelyek emberi kognitív folyamatot igényelnek, ezért számos valós életbeli alkalmazásuk ismert. Az ilyen típusú adatok szegmentálása és osztályozása a legnagyobb kihívást jelentő feladatok közé tartozik az adatbányászat témakörében. A legtöbb esetben rendkívül doménspecifikusak, így nagyon sokszor egy többéves tapasztalattal rendelkező adatmérnök munkáját igénylik. Napjainkban a gépi tanulás alapú mesterséges intelligencia egyre nagyobb teret hódít. A mély neurális háló modellek analitikusan nem megoldható probléma esetében is hatékony megoldást jelentenek, így használatuk elterjedt idősoros feladatok alkalmazására is.

Kutatásunkban egérdinamika alapú viselkedési biometria segítségével történő felhasználó azonosítást végeztünk. Többféle konvolúciós neuronhálóval kísérleteztünk és megvizsgáltuk a nyers adatok előfeldolgozásának a modellek tanítására gyakorolt hatását, illetve az azonosítási rendszer teljesítményét a tanítási adatmennyiség függvényében. Mivel a mély hálós modellek megfelelő tanításához igencsak nagy mennyiségű adat szükséges, ezért tudástranszfert alkalmaztunk. A méréseket a publikusan elérhető, saját gyűjtésű SapiMouse adathalmazzal végeztük. A legjobban teljesítő neuronháló architektúrának a ResNet bizonyult, amely az adathalmaz felhasználóira mérve 0.86 AUC értéket eredményezett 3 másodpercnyi egérmozgási adat alapján. A kapott teljesítmény tovább növelhető nagyobb mennyiségű adat felhasználásával. 12 másodpercnyi egérmozgási adat alapján 0.92 AUC értéket kapunk.

Kulcsszavak: *egérdinamika, reprezentáció tanulás, konvolúciós neuronhálók.*

1. Bevezetés

Napjaink rohamosan fejlődő digitális társadalmában a biztonság egy kulcsfontosságú szerepet játszik. A felhasználók adatainak illetéktelen kezekbe kerülése jelentős negatív következményekkel járhat. Mivel a hitelesítéséhez használt adatok számos módon veszélyeztetettek, ezért egy megbízható hitelesítés elvégzéséhez szükségünk van további módszerek alkalmazására [1].

Számos biometrikus hitelesítést ismerünk, ilyen például az ujjlenyomat, retina vagy arc alapú azonosítást. Ezek hátránya, hogy egyfajta tudatos erőfeszítést igényelnek, ugyanakkor egy szesszió alatt csak egyszer használatosak. A viselkedési biometria lehetővé teszi a felhasználók folyamatos hitelesítését. [2]. Lényegük, hogy a háttérben folyamatosan vizsgáljuk a felhasználó hitelességét, arra alapozva, hogy miként használja az adott perifériás eszközét. A felhasználó azon szokását, hogy hogyan használja az egerét, egérdinamikának nevezzük.

Habár a felhasználótól történő adatgyűjtés igen is fontos a hitelesítés szempontjából, az hogy az adott felhasználó éppen milyen feladatot végez, a viselkedési biometriát használó rendszerek esetében nem bír jelentőséggel. Az ilyen adatok könnyen alkalmazhatók mesterséges intelligenciát ötvözve, amelyek segítségével a felhasználó identitása pontosan megmondható. Egérdinamika esetében csak az egérrel való interakciót vizsgáljuk.

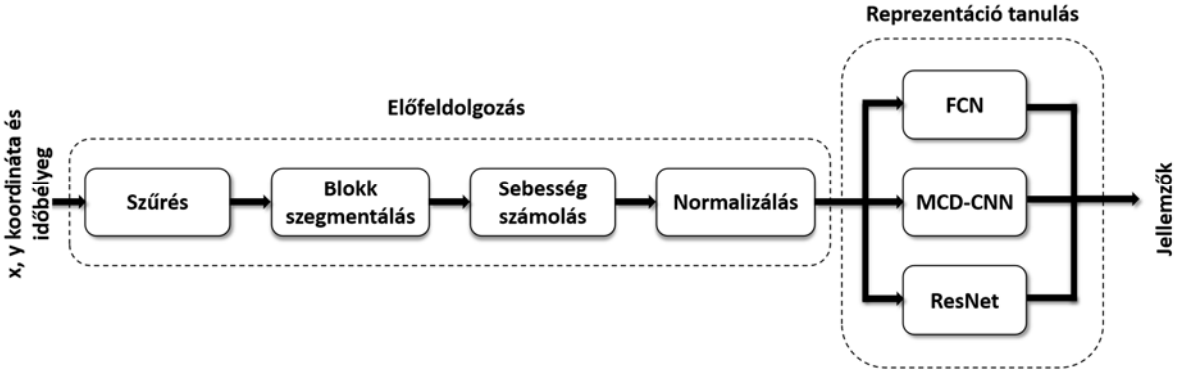
A fiziológiai biometrián alapuló azonosítás a gyakorlatban sokkal pontosabb, mint a viselkedési biometrián alapuló azonosítás, viszont ezek általában költségesek és egy speciális hardver meglétét is feltételezik [3]. Ezzel ellentétben az egérdinamikán alapuló felhasználó azonosítás azon kívül, hogy nem gyűjt érzékeny adatokat, nem igényel speciális hardver eszközt sem.

Több kutatás foglalkozott már egérdinamika alapú felhasználó azonosítással. A legtöbb tanulmányban a hitelesítéshez használt jellemzőket a nyers idősorokból statisztikai megfigyelések alapján nyerik ki [2, 4], emellett számos új kutatás világít rá a neurális hálók alkalmazásának hatékonyságára is [3]. Hasonló módszereket alkalmazva mi is tanítottunk konvolúciós neuronhálókat, az eredményeket is publikáltuk [5]. Idősorok feldolgozására az egydimenziós konvolúciós neuronhálók (1D-CNN) alkalmasnak bizonyultak a jelfeldolgozásból is ismert szűrők alkalmazása végett. Nagy előnyük, hogy a szűrő paramétereit a neuronháló automatikusan tanulja meg, így ezek egy sokkal finomabb hangolást eredményeznek a manuális konfigurálással szemben.

2. A megoldandó probléma definiálása

Kutatásunk célja egy megbízható, egérdinamikán alapuló hitelesítő rendszer létrehozása a jellemzők idősorokból történő automatikus kinyerésével majd ezek egyosztályos osztályozókkal történő osztályozásával. A munkánk így két különálló részre osztható fel:

1. Nyers idősorokból történő minőségi jellemzők kinyerése, melyek segítségével a későbbiek során a felhasználó egyértelműen azonosítható.
2. Felhasználók azonosítása a kinyert jellemzők segítségével.

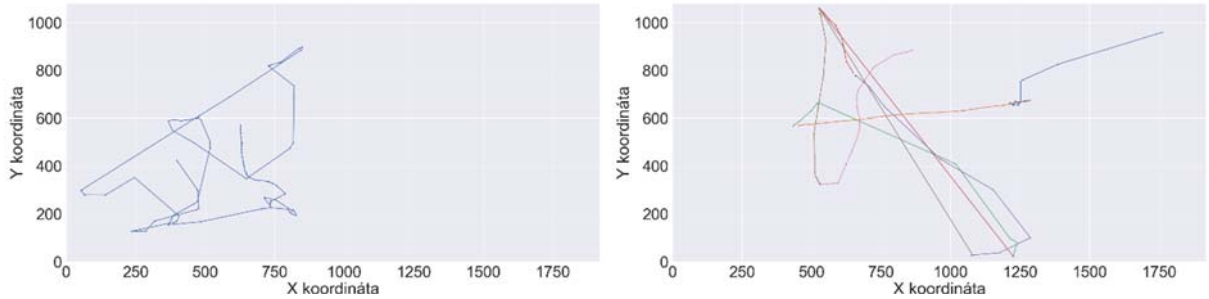


1. ábra. *Jellemzőkinyerés nyers idősorokból*

Az 1. ábra hűen tükrözi a jellemző kinyerés folyamatát. A kezdeti, nyers adatokon előfeldolgozást végzünk, majd ezeket az előfeldolgozott adatokat fogjuk használni a mély neuronhálók bemeneteként. A kiválasztott háló tanítási folyamatát reprezentáció tanulásnak nevezzük.

3. Adatanalízis és az adatok előfeldolgozása

Kutatásunkat a nyers adatok analízisével kezdtük. Mivel egérmozgást mintavételezett nyers adathalmaz állt rendelkezésünkre, első lépésben ezeknek a nyers adatoknak a kapcsolatát vizsgáltuk. Méréseink során a vertikális és horizontális irányú koordinátákat, illetve a mintavételezés során rögzített időbélyegeket használtuk fel.



2. ábra. *Folytonos és nem folytonos egérmozgást tartalmazó blokkok*

A nyers adathalmazunk rengeteg zajt tartalmazott, ezeket különböző módszerek szerint kezeltük. A 2. ábra 128 darab egymást követő egéresemény x és y koordinátáját illusztrálja. Ezeket blokkoknak nevezzük és ez lesz a feldolgozás alapegysége. Az ábra bal részén egy olyan folytonos egérmozgást láthatunk, ahol nem történt megállás a mozgások között, míg a jobb részén a különböző színnel jelölt görbék a mozgásban fellelhető szakadásokat reprezentálják. A folytonos mozgást tartalmazó blokkot kompaktnak, míg a megállásokat tartalmazót töredezettnek nevezzük. Ezek az esetünkben irreleváns adatnak számítanak, hisz nincs elégséges összefüggő adatpont, amelyre alapozva egy reprezentáció megtanulható lenne. A töredezett darabokat kétféleképpen kezeljük. Az első esetben csak azokat a blokkokat tartjuk meg, ahol van legalább 128 darab folytonos adatpont, a töredezett darabokat pedig eldobjuk. A másik esetben a töredezett blokkokat is felhasználjuk, ekkor viszont a tört részekből annyi darabot fűzünk össze, amennyiből egy 128-as méretű kompakt blokk alkotható.

Az adathalmazban szereplő egéreseményeket szekvenciákra szegmentáltuk. Egy szekvencia akkor ért véget, amikor két egymásutáni egéresemény időbélyegének különbsége átlépett egy küszöbértéket. Ezeket a szekvenciákat tovább szegmentáltuk előre meghatározott, konstans méretű blokkokra. Ez esetünkben 128 egéreseményt jelentett. A blokk ideális méretének meghatározása empirikusan történt a rendszer pontosságának vizsgálatával különböző blokkméretek függvényében a Balabit [6] adathalmaz összes felhasználójára nézve. Ezzel a feldolgozási módszerrel nem kellett foglalkoznunk az egérmozgások végének detektálásával.

Az így előkészített nyers adatok sajnos önmagukban nem szolgáltattak megfelelő tulajdonságokat a felhasználók hitelesítéshez. Ezért módosításokat kellett az adatokon végrehajtanunk, ahhoz hogy a számunkra releváns és későbbiekben felhasználható jellemzők kinyerhetők legyenek neurális modelljeink alkalmazásával. Annak érdekében, hogy transzláció invariáns egér pozíció szekvenciákat tudjunk kinyerni vertikális és horizontális irányú sebességekkel dolgozunk az abszolút pozíció koordináták helyett. Az így kapott sebességek Gauss-eloszlást mutattak. Ezt a tulajdonságot figyelembe véve az adathalmazunkat standardizáltuk. Mivel az általunk használt nyers adatok tulajdonságaikban nem tértek el egymástól, az adatok normalizálására nem lett volna szükségünk. Ennek ellenére a konvolúciós neuronhálók alkalmazásakor használt aktivációs függvények, mint például a sigmoid vagy a softmax, megkövetelik az adatok bizonyos egységes skálára normalizálást. Ezen felül fontos szempont volt a bemenő adataink egy adott intervallumon belüli tartása, így elkerültük a modell súlyainak nagy értékeit, és egy hatékonyabb tanítási folyamatot eredményezhetünk.

4. Reprezentáció tanulás

A nyers idősorokból történő automatikus jellemzőkinyerés folyamatát nevezzük reprezentáció tanulásnak. A reprezentáció tanulás lényege, hogy az előfeldolgozás során kinyert nyers adatokat a modelljeinknek átadva olyan kimeneti paramétereket (úgynevezett jellemzőket) szolgáltatnak, amelyek egyértelműen elkülöníthetővé teszik a kiválasztott felhasználó egérmozgását más felhasználókétól.

Az egérdinamikán alapuló biometrikus hitelesítési rendszerekben a konvolúciós hálók már bizonyították alkalmasságukat, ahogyan azt a [7], illetve [3]-es cikkben is láthattuk. A természetes nyelvfeldolgozásra előszeretettel használt 1D-CNN egy kitűnő alternatívát szolgáltat bármilyen típusú idősor vagy temporális modell feldolgozására. Kutatásunkban három különböző 1D-CNN modell architektúrát használtunk idősorokból való jellemzőkinyerésre. Választásunkat Fawaz és tsai. publikációjában [8] megjelölt mérési eredményekre alapoztuk. Méréseink során a három legjobban teljesítő architektúra a következő volt:

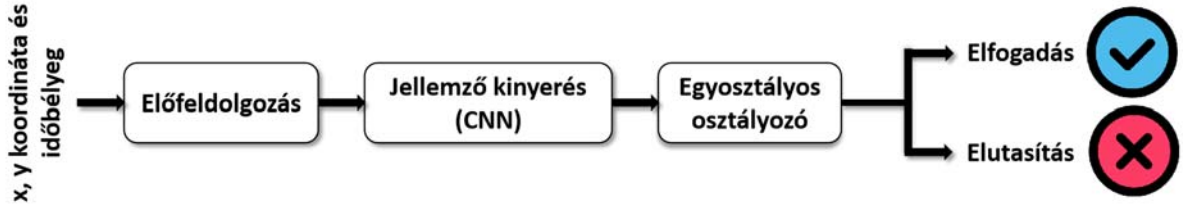
1. **ResNet** (Residual Neural Network)
2. **MCD-CNN** (Multi Channel Deep Convolutional Neural Network)
3. **FCN** (Fully Convolutional Neural Network)

Az előfeldolgozás folyamán kapott nyers adatokat a konvolúciós hálók bemeneteként megadva olyan jellemzőket tudtunk kinyerni, melyek segítségével a felhasználók hitelesítése egyértelműen megtörténhet. A hálók kimenete 60 különböző jellemzőt szolgáltat minden egyes bemeneti blokk esetén.

5. A felhasználók hitelesítése

Az egyosztályos osztályozó algoritmusok jól használhatók bináris osztályozásra olyan esetben, ahol a különböző osztályok eloszlása igencsak aszimmetrikus. Habár nem erre a feladatra tervezték őket, de kiválóan működnek olyan helyzetben is, ahol az adathalmaz kiegyensúlyozatlan vagy nem áll rendelkezésre koherens struktúra felügyelt tanítás alkalmazására. Az egyosztályos osztályozók lényege, hogy a modell tanítását csak pozitív adatokkal végezzük. Az új, eddig még nem látott adat pozitív vagy negatív osztályba tartozását egy score és egy küszöbérték segítségével állapítjuk meg.

A 3. ábra szemlélteti a hitelesítés folyamatát egyosztályos osztályozókat alkalmazva. Az előfeldolgozás lépéseit az 1. ábrán már ismertettük. Az előfeldolgozott adatblokkból a reprezentáció tanulásra betanított neuronháló segítségével jellemzőket nyerünk ki, amelyekkel egy egyosztályos osztályozót tanítunk be. A betanított egyosztályos osztályozó már használható hitelesítésre.



3. ábra. *Felhasználó hitelesítése egyosztályos osztályozóval*

Az egyosztályos osztályozók természetüknek köszönhetően alkalmazhatóak olyan esetben, amikor a pozitív osztály kevés mintaszámot tartalmaz, vagy a negatív osztályból nem áll rendelkezésünkre adat [9].

Egyosztályos osztályozóként a tartóvektor gépek egyosztályos változatát használtuk (One Class Support Vector Machine).

6. Mérési protokoll

A mérésekhez két adathalmazt használtunk: a DFL [10] és a SapiMouse [11] publikusan elérhető adathalmazokat. A DFL adathalmazt használtuk a reprezentáció tanuláshoz, ezekkel az adatokkal tanítottuk be a jellemzőkinyerésre használt konvolúciós neuronhálókat. A SapiMouse adathalmazon végeztük a felhasználó hitelesítési méréseinket.

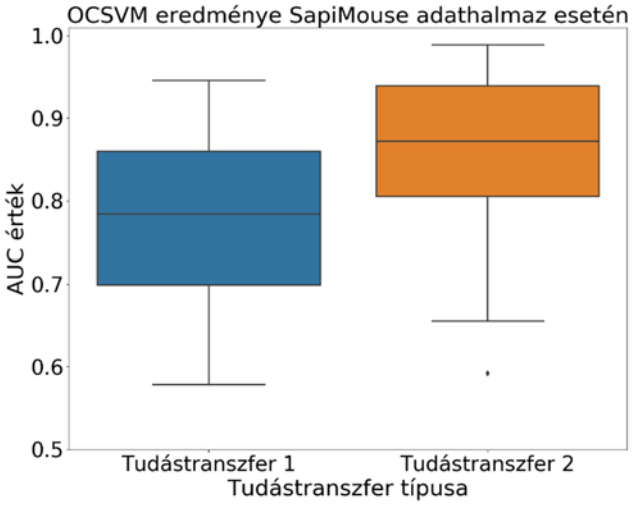
A mély neurális hálók megfelelő tanításához nagymennyiségű adatra van szükségünk. Mivel a SapiMouse adathalmaz nem tartalmaz elegendő mennyiségű adatot éppen ezért a reprezentáció tanulást tudástranszfer segítségével valósítottuk meg. Kétféle tudástranszfert alkalmaztunk:

1. Az első esetben (*tudástranszfer 1*) betanítottuk a ResNet modellünket a DFL adathalmazon, majd a betanított modell segítségével a SapiMouse adathalmaz utolsó 40 felhasználójának 3 perces szesszióiból jellemzőket nyertünk ki. A kinyert jellemzőkkel az egyosztályos OCSVM modellt tanítottuk be, illetve ennek kiértékelésére az 1 perces szessziókat használtuk fel.
2. A második esetben (*tudástranszfer 2*) a DFL adathalmazra betanított ResNet modellünket a SapiMouse adathalmaz első 43 felhasználójától származó adatokkal finomhangoltuk. A modell finomhangolásához az 1 és 3 perces szessziókat egyaránt felhasználtuk. Az így finomhangolt modell segítségével nyertük ki a maradék 40 felhasználó 3 perces adataiból a jellemzőket, amelyeket szintén OCSVM modellel tanítottunk. Az eredmények kiértékeléséhez itt is a felhasználók 1 perces szesszióiból kinyert jellemzőkkel dolgoztunk.

A méréseket megismételtük az FCN és az MCD-CNN modellekre is. Mivel a legjobban a ResNet modell teljesített, ezért csak az ezzel a modellel kapott mérési eredményeket ismertetjük.

7. Mérési eredmények

A 4. ábrán a kétféle tudástranszferrel végzett mérési eredményeket szemléltettük az adathalmaz utolsó 40 felhasználójára. A tanító adathalmazhoz 55, míg a tesztelő adathalmaz előállításához 15 blokkot használtunk. Láthatjuk, hogy a ResNet modellt finomhangolva a SapiMouse adathalmazra az eredmények megközelítőleg 10%-os javulást mutatnak. Tudástranszfer 1 esetén 0.77 AUC (Area Under the ROC Curve), míg Tudástranszfer 2 esetén 0.86 AUC értéket kaptunk.



4. ábra. *OCSVM modell eredménye a SapiMouse adathalmaz utolsó 40 felhasználójának tesztelése során*

Fontos kiemelnünk, hogy a fent látható eredmények egyetlen egy blokk alapján történő döntéshozatalt szemléltetnek. Abban az esetben, ha a több blokk alapján hozzuk meg a döntésünket, az az eredményeinek pontosabbak lesznek. 5 blokk aggregálásával *Tudástranszfer 1* esetén 0.92 AUC értéket kapunk.

8. Következtetések

Kutatásunk bizonyítja az egérdinamikán alapuló felhasználó-hitelesítés mély neurális hálók alkalmazásával történő hatékonyságát. A jellemzőkinyerés folyamata nagymértékben megkönnyíthető mély neurális hálók alkalmazásával, így a kézi jellemzőkinyerésre nincs szükségünk. Három különböző architektúrájú 1D-CNN háló segítségével végeztünk jellemzőkinyerést, majd ezek alapján felhasználó hitelesítést.

Méréseinket a saját webalkalmazásunk [12] segítségével gyűjtött SapiMouse adathalmazon végeztük. A dolgozatban szemléltetett minden mérési eredmény reprodukálható a GitHub-on [13] közzétett kód segítségével.

Az egéreseményeket különböző fix méretű blokkokra osztottuk fel és azt tapasztaltuk, hogy 128 darab egéreseményt tartalmazó blokkméret volt a legmegfelelőbb. A felhasználók hitelesítésére egyosztályos osztályozókat alkalmaztunk.

Egyosztályos osztályozásra OCSVM modellt használtunk, amely a SapiMouse adathalmaz felhasználóira 0.86 AUC értéket eredményezett. Ezt egyetlen blokk kiértékelésével kaptuk, ami megközelítőleg 3 másodpercnyi egérmozgási adatnak felel meg. Több blokk aggregálásával pontosabb hitelesítés végezhető. 15 másodpercnyi egérmozgási adat alapján 0.92 AUC értékre javultak az eredmények.

Köszönetnyilvánítás

A publikáció elkészítését az *Accenture Industrial Software Solutions* cég támogatta.

Hivatkozások

[1] ENSTRÖM, Olof. Authentication Using Deep Learning on User Generated Mouse Movement Images. Master's thesis. 2019.

[2] ANTAL, Margit; EGYED-ZSIGMOND, Elöd. Intrusion detection using mouse dynamics. IET Biometrics, 2019, 8.5: 285-294.

[3] CHONG, Penny; ELOVICI, Yuval; BINDER, Alexander. User Authentication Based on Mouse Dynamics Using Deep Neural Networks: A Comprehensive Study. IEEE Transactions on Information Forensics and Security, 2019, 15: 1086-1101.

[4] AHMED, Ahmed Awad E.; TRAORE, Issa. A new biometric technology based on mouse dynamics. IEEE Transactions on dependable and secure computing, 2007, 4.3: 165-179.

[5] ANTAL Margit; FEJÉR Norbert. Mouse Dynamics based User Recognition using Deep Learning. In: Acta Univ. Sapientiae, Informatica, 12, 1 (2020) 39−50.

[6] A. Fülöp, L. Kovács, T. Kurics, and E. Windhager-Pokol. (2016). Balabit Mouse Dynamics Challenge data set, [Online]. Available: https://github.com/balabit/MouseDynamics-Challenge.

[7] CHONG, Penny, et al. Mouse authentication without the temporal aspect–what does a 2d-cnn learn?. In: 2018 IEEE Security and Privacy Workshops (SPW). IEEE, 2018. p. 15-21.

[8] FAWAZ, Hassan Ismail, et al. Deep learning for time series classification: a review. Data Mining and Knowledge Discovery, 2019, 33.4: 917-963.

[9] MANEVITZ, Larry M.; YOUSEF, Malik. One-class SVMs for document classification. Journal of machine Learning research, 2001, 2.Dec: 139-154.

[10] ANTAL, Margit; DENES-FAZAKAS, Lehel. User Verification Based on Mouse Dynamics: a Comparison of Public Data Sets. In: 2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI). IEEE, 2019. p. 143-148.

[11] https://drive.google.com/file/d/1gvTUgLlEOY2QmUUgSVqrk2J07t8u5Hf-/view

[12] https://mousedynamicsdatalogger.netlify.app/

[13] https://github.com/norbertFejer/AFE_Project