Vilniaus universitetas
Duomenų mokslo ir skaitmeninių technologijų institutas

Informatikos krypties doktorantų atestacinė konferencija
Veiklos ataskaita už 2021 m. spalio 1 d. – 2022 m. kovo 24 d.

ANOMALINIŲ ĮVYKIŲ IDENTIFIKAVIMAS IR JŲ UŽKARDYMAS KOMPIUTERIŲ TINKLUOSE TAIKANT MAŠININIO MOKYMOSI METODUS

dokt. Arnoldas BUDŽYS – Informatika N 009
Studijų metai: II
Darbo vadovas: dr. Viktor Medvedev
Doktorantūros pradžios ir pabaigos metai: 2020–2024

2021–2022 m.

STUDIJŲ PLANAS IR JO VYKDYMO SUVESTINĖ

Studijų metai	Egzaminai [1]		Dalyvavimas konferencijose [2]		Publikacijos [3]		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta	Būklė [4]
I (2020/2021)	1	1					
II (2021/2022)	**2**	**2**	**1**		**1**		
III (2022/2023)	1		1		1		
IV (2023/2024)			1		1		
Iš viso:	4	3	3		3		

2021–2022 m.

- **ATASKAITINIŲ METŲ DARBO PLANAS IR JO SUVESTINĖ**

Egzaminai		Dalyvavimas konferencijose		Publikacijos	
Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta
Fundamentalieji informatikos ir informatikos inžinerijos metodai	Išlaikytas				
Mašininis mokymasis	Išlaikytas				

2021–2022 m.

ATASKAITINIŲ METŲ DARBO PLANAS IR JO SUVESTINĖ

Dalyvavimas konferencijose		
Planas	Įvykdyta	Konferencijos tipas
Data Analysis Methods for Software Systems 2021 m. gruodžio 1–3 d., Druskininkai	User Behaviour Analysis Based on Similarity Measures to Detect Anomalies Data Analysis Methods for Software Systems 2021 m. gruodžio 1-3 d., Druskininkai Autoriai: Arnoldas Budžys, Viktor Medvedev, Olga Kurasova Įvertintas kaip geriausias posteris	Nacionalinė

Publikacijos			
Planas	Įvykdyta	Būklė	Publikacijos tipas
	Budžys, Arnoldas; Medvedev, Viktor; Kurasova, Olga. User behaviour analysis based on similarity measures to detect anomalies // DAMSS: 12th conference on data analysis methods for software systems, Druskininkai, Lithuania, December 2–4, 2021. Vilnius : Vilnius University Press, 2021. ISBN 9786090706732. eISBN 9786090706749. p. 8. DOI: 10.15388/DAMSS.12.2021.	Publikuota	Be cituojamumo rodiklio

Mokslinių tyrimų ir disertacijos rengimo planas:

2020–2021 m.

Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):

- **Disertacijos tyrimo objekto detalizavimas;**
- **Atlikti mašininio mokymosi metodų taikymo kompiuterių tinkluose analitinę apžvalgą;**
- **Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su įsilaužimų prevencija kompiuterių tinkluose taikant mašininio mokymosi metodus;**
- **Tyrimo tikslo suformavimas.**

Mokslinių tyrimų ir disertacijos rengimo planas:

2021–2022 m.

Mokslinio tyrimo vykdymas:

- **2.1. Tyrimo metodikos sudarymas:**
- **2.1.1. Tyrimo metodikos iškeltiems uždaviniams spręsti parinkimas;**
- **2.1.2. Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką.**
- **2.2. Teorinis tyrimas:**
- 2.2.1. Mašininio mokymosi metodų, naudojamų kompiuterių tinkluose įsilaužimų prevencijai, tyrimas.
- 2.2.2. Įsilaužimų prevencijos atpažinimo mašininio mokymosi metodo sukūrimas ir/ar testavimas.

Mokslinių tyrimų ir disertacijos rengimo planas:

2022–2023 m.

- **2.3. Empirinis tyrimas:**
- 2.3.1. Sudarytų metodų pritaikymas praktinių uždavinių sprendimui.
- 2.3.2. Gautų duomenų analizė, rezultatų apibendrinimas, išvadų parengimas.

Mokslinių tyrimų ir disertacijos rengimo planas:

2023–2024 m.

Atskirų daktaro disertacijos dalių (tyrimo metodikos, rezultatų, ginamų teiginių, išvadų, ir kt.) parengimas:

- 3.1. Tikslų, uždavinių, tyrimo metodikos, ginamųjų teiginių patikslinimas;
- 3.2. Analitinės disertacijos dalies parengimas;
- 3.3. Teorinės disertacijos dalies parengimas;
- 3.4. Eksperimentinės disertacijos dalies parengimas;
- 3.5. Bendrųjų išvadų formulavimas.

Mokslinių tyrimų ir disertacijos rengimo planas:

2024 m. birželio mėnesį

- Daktaro disertacijos parengimas ir svarstymas padalinyje

2024 m. rugsėjo mėnesį

- Daktaro disertacijos gynimas

Disertacijos tema, tyrimo objektai ir tikslas

Preliminari disertacijos tema:

- anomalinių įvykių identifikavimas ir jų užkardymas kompiuterių tinkluose taikant mašininio mokymosi metodus.

Tyrimo objektai:

- vartotojo sugeneruoti klaviatūros, pelės biometriniai duomenys, bei mašininio mokymosi metodų taikymas anomalinių įvykių identifikavimui ir neteisėtų veiksmų užkardymui.

Tikslas:

- pasiūlyti metodiką sistemos vartotojui autentifikuoti pagal jo biometrinius elgsenos duomenis siekiant užkardyti insaiderio veiklą bei apsaugoti sistemą nuo jo neteisėtų veiksmų.

Tyrimo uždaviniai

- Atlikti išsamią literatūros analitinę apžvalgą, siekiant identifikuoti tinkamus metodus anomalinių įvykių identifikavimui ir insaiderio užkardymui kompiuterių tinkluose;
- Atlikti skirtingų mašininio mokymosi metodų, skirtų anomalinių įvykių identifikavimui ir insaiderio užkardymui kompiuterių tinkluose, analizę ir tyrimą;
- Sukurti metodiką, apimančią mašininiu mokymusi grįstus algoritmus, sistemos vartotojui autentifikuoti pagal jo biometrinius elgsenos duomenis;
- Įvertinti sukurtos metodikos efektyvumą realaus laiko duomenims atliekant eksperimentinius tyrimus;
- Atlikti gautų rezultatų analizę: rezultatų apibendrinimas, išvadų parengimas.

Literatūros analitinės apžvalgos apibendrinimas

- Pastaraisiais metais biometrinis elgsenos autentifikavimas pagrįstas klavišų paspaudimu yra aktyvi tyrimų sritis dėl mažų sąnaudų ir paprasto integravimo su esamomis apsaugos sistemomis.
- Remiantis straipsnių apžvalga, kiekvieno vartotojo sudarytas klaviatūros bei pelės biometrinių duomenų profilis yra autentiškas ir negali būti atkartojamas.
- Vartotojo autentifikavimas naudojant klaviatūros biometrinius duomenis skirstomas į dvi kategorijas: pirminį (statinį) autentifikavimą (SA) ir nepertraukiamą autentifikavimą (NA).

Atlikta dalis teorinio tyrimo

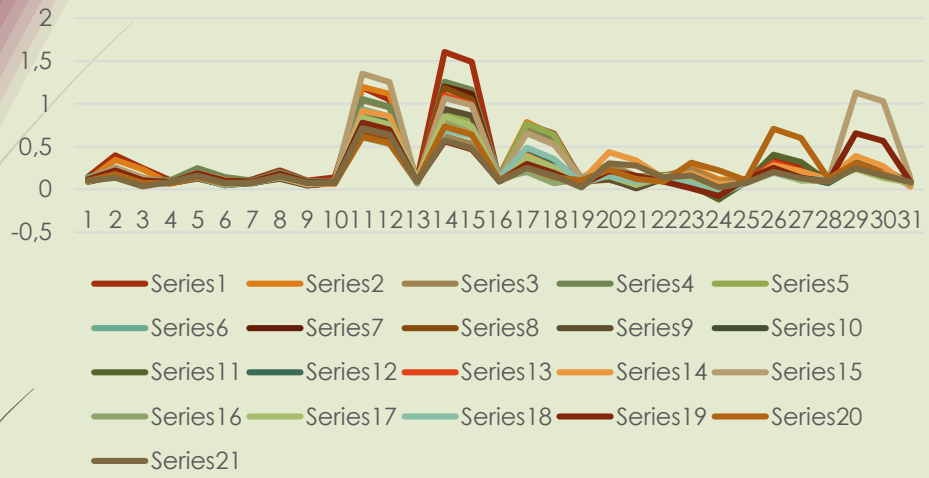
- Tarpusavyje palyginti vienuolika anomalijų aptikimo algoritmų identifikuotų literatūros analitinės apžvalgos metu (panašumo matai, klasikiniai metodai, pvz. SVM, K-vidurkio metodas, Euklidinis, Manheteno, Mahalanobio atstumas ir t. t.).
- Tyrimui atlikti buvo pasirinkta CMU duomenų aibė. Naudojant skirtingus duomenų pateikimo algoritmui variantus buvo apskaičiuotas ir pateiktas anomalijų aptikimo vidutinis klaidų rodiklis EER.
- Buvo atlikti tyrimai, siekiant nustatyti kuris anomalijų aptikimo metodas yra stabiliausias, keičiant apmokymo/testavimo parametrus, bei insaiderio pateikimo būdus (žr. 1b paveikslą). Rezultatai pateikti 2 paveiksle.

CMU duomenų aibė (slaptažodis .tie5Roanl)

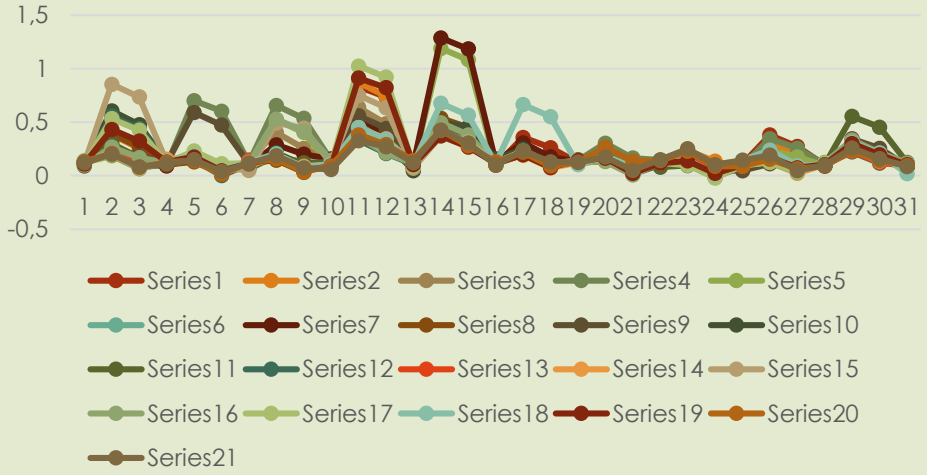
1	subject	H.period	DD.period	UD.period	H.t	DD.t.i	UD.t.i	H.i	DD.i.e	UD.i.e	H.e	DD.e.five	UD.e.five	H.five	DD.five.Sh	UD.five.Sh	H.Shift.r	DD.Shift.r	UD.Shift.r	H.o	DD.o.a	UD.o.a	H.a	DD.a.n	UD.a.n	H.n	DD.n.l	UD.n.l	H.l
2	s002	0.1491	0.3979	0.2488	0.1069	0.1674	0.0605	0.1169	0.2212	0.1043	0.1417	1.1885	1.0468	0.1146	1.6055	1.4909	0.1067	0.759	0.6523	0.1016	0.2136	0.112	0.1349	0.1484	0.0135	0.0932	0.3515	0.2583	0.1338
3	s002	0.1111	0.3451	0.234	0.0694	0.1283	0.0589	0.0908	0.1357	0.0449	0.0829	1.197	1.1141	0.0689	0.7822	0.7133	0.157	0.7877	0.6307	0.1066	0.1684	0.0618	0.1412	0.2558	0.1146	0.1146	0.2642	0.1496	0.0839
4	s002	0.1328	0.2072	0.0744	0.0731	0.1291	0.056	0.0821	0.1542	0.0721	0.0808	1.0408	0.96	0.0892	0.6203	0.5311	0.1454	0.7195	0.5741	0.1365	0.2931	0.1566	0.1621	0.2332	0.0711	0.1172	0.2705	0.1533	0.1085
5	s002	0.1291	0.2515	0.1224	0.1059	0.2495	0.1436	0.104	0.2038	0.0998	0.09	1.0556	0.9656	0.0913	1.2564	1.1651	0.1454	0.755	0.6096	0.0956	0.153	0.0574	0.1457	0.1629	0.0172	0.0866	0.2341	0.1475	0.0845
6	s002	0.1249	0.2317	0.1068	0.0895	0.1676	0.0781	0.0903	0.1589	0.0686	0.0805	0.8629	0.7824	0.0742	0.8955	0.8213	0.1243	0.7632	0.6389	0.043	0.1975	0.1545	0.1312	0.1582	0.027	0.0884	0.2517	0.1633	0.0903
7	s002	0.1394	0.2343	0.0949	0.0813	0.1299	0.0486	0.0744	0.1412	0.0668	0.0863	0.9373	0.851	0.0942	1.0896	0.9954	0.1681	0.3716	0.2035	0.1154	0.1287	0.0133	0.1272	0.1534	0.0262	0.0858	0.2528	0.167	0.0792
8	s002	0.1064	0.2069	0.1005	0.0866	0.1368	0.0502	0.08	0.1407	0.0607	0.0789	0.7967	0.7178	0.0855	1.2005	1.115	0.0948	0.3083	0.2135	0.1233	0.14	0.0167	0.1318	0.1204	-0.0114	0.0782	0.1999	0.1217	0.0879
9	s002	0.0929	0.181	0.0881	0.0818	0.1378	0.056	0.0747	0.1367	0.062	0.0776	0.6447	0.5671	0.1373	1.1876	1.0503	0.1059	0.3139	0.208	0.0903	0.1152	0.0249	0.1322	0.104	-0.0282	0.0821	0.2127	0.1306	0.1006
10	s002	0.0966	0.1797	0.0831	0.0771	0.1296	0.0525	0.0839	0.1425	0.0586	0.0755	0.7357	0.6602	0.08	0.9406	0.8606	0.1027	0.2257	0.123	0.1114	0.126	0.0146	0.1262	0.1403	0.0141	0.0787	0.2138	0.1351	0.0882
11	s002	0.1093	0.1807	0.0714	0.0731	0.1457	0.0726	0.0766	0.1241	0.0475	0.0813	0.755	0.6737	0.0826	0.8065	0.7239	0.1156	0.3117	0.1961	0.1119	0.1785	0.0666	0.1463	0.1162	-0.0301	0.1207	0.2281	0.1074	0.1204
12	s002	0.0887	0.166	0.0773	0.0876	0.156	0.0684	0.0839	0.1386	0.0547	0.0692	0.6927	0.6235	0.0824	0.8135	0.7311	0.1278	0.3157	0.1879	0.0948	0.1746	0.0798	0.1682	0.0502	-0.118	0.0866	0.4062	0.3196	0.0927
13	s002	0.0911	0.1525	0.0614	0.0824	0.1516	0.0692	0.0731	0.1391	0.066	0.0832	0.9155	0.8323	0.0713	0.7485	0.6772	0.1193	0.4426	0.3233	0.1103	0.2065	0.0962	0.1465	0.1492	0.0027	0.0758	0.2201	0.1443	0.0742
14	s002	0.1114	0.162	0.0506	0.09	0.1547	0.0647	0.0797	0.1349	0.0552	0.0708	0.7028	0.632	0.1051	1.0995	0.9944	0.1157	0.3474	0.2317	0.1164	0.1967	0.0803	0.1404	0.1581	0.0177	0.0942	0.3101	0.2159	0.1093

CMU duomenų aibė

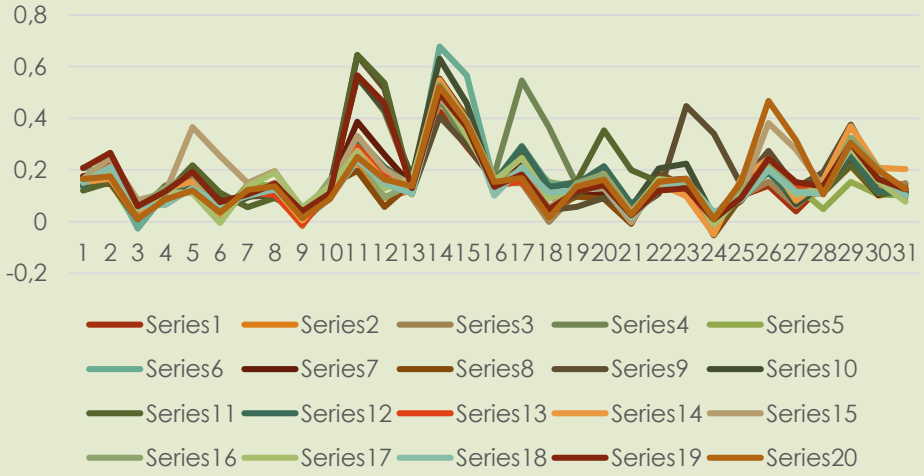
S002 pirmi 20 kartų



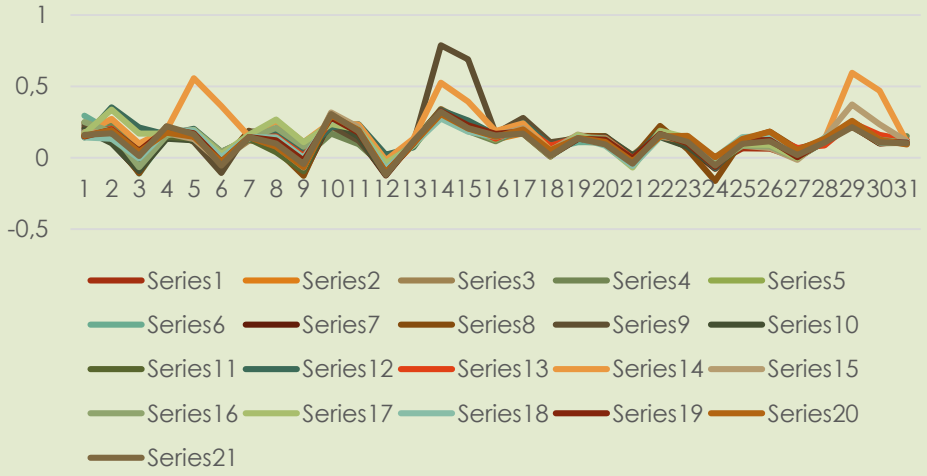
S003 pirmi 20 kartų



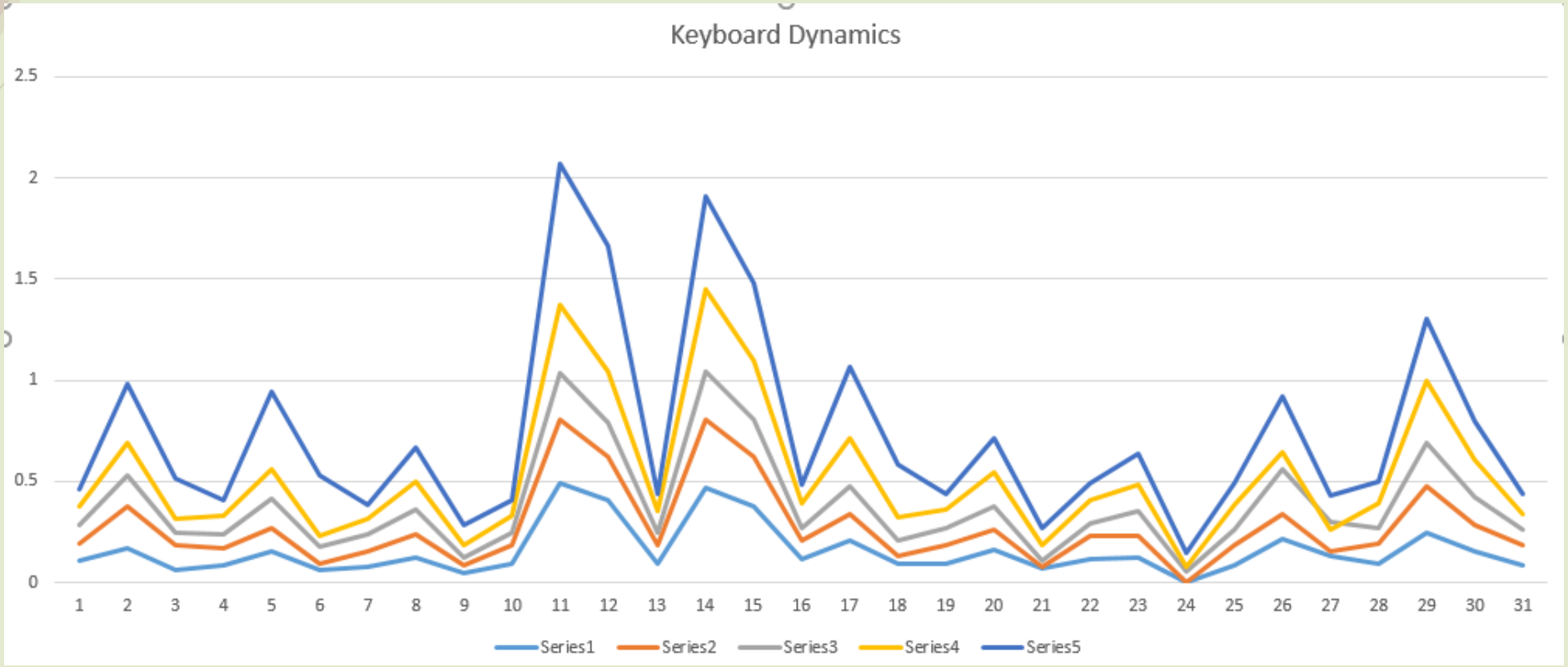
S002 paskutiniai 20 kartų

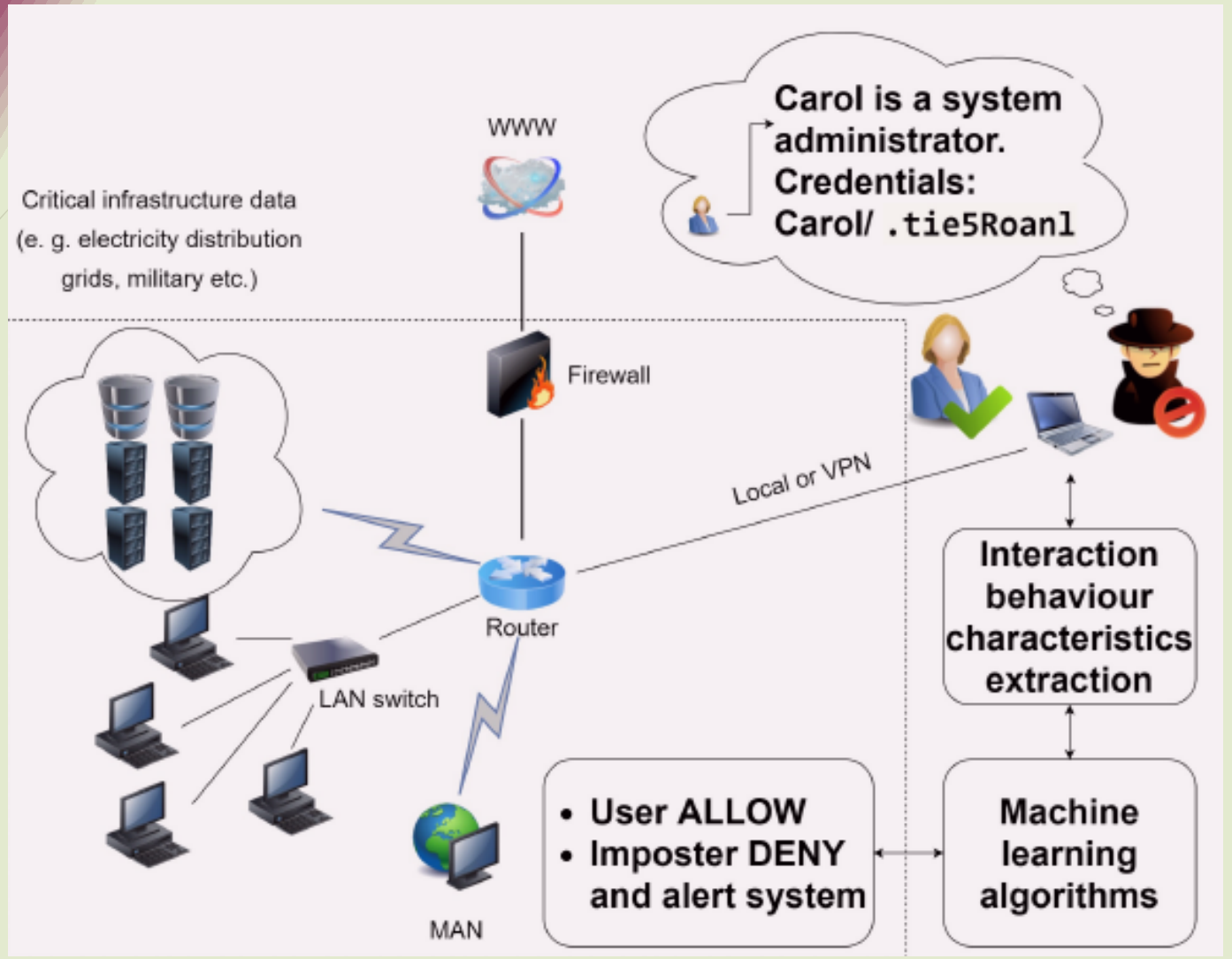


S003 paskutiniai 20 kartų

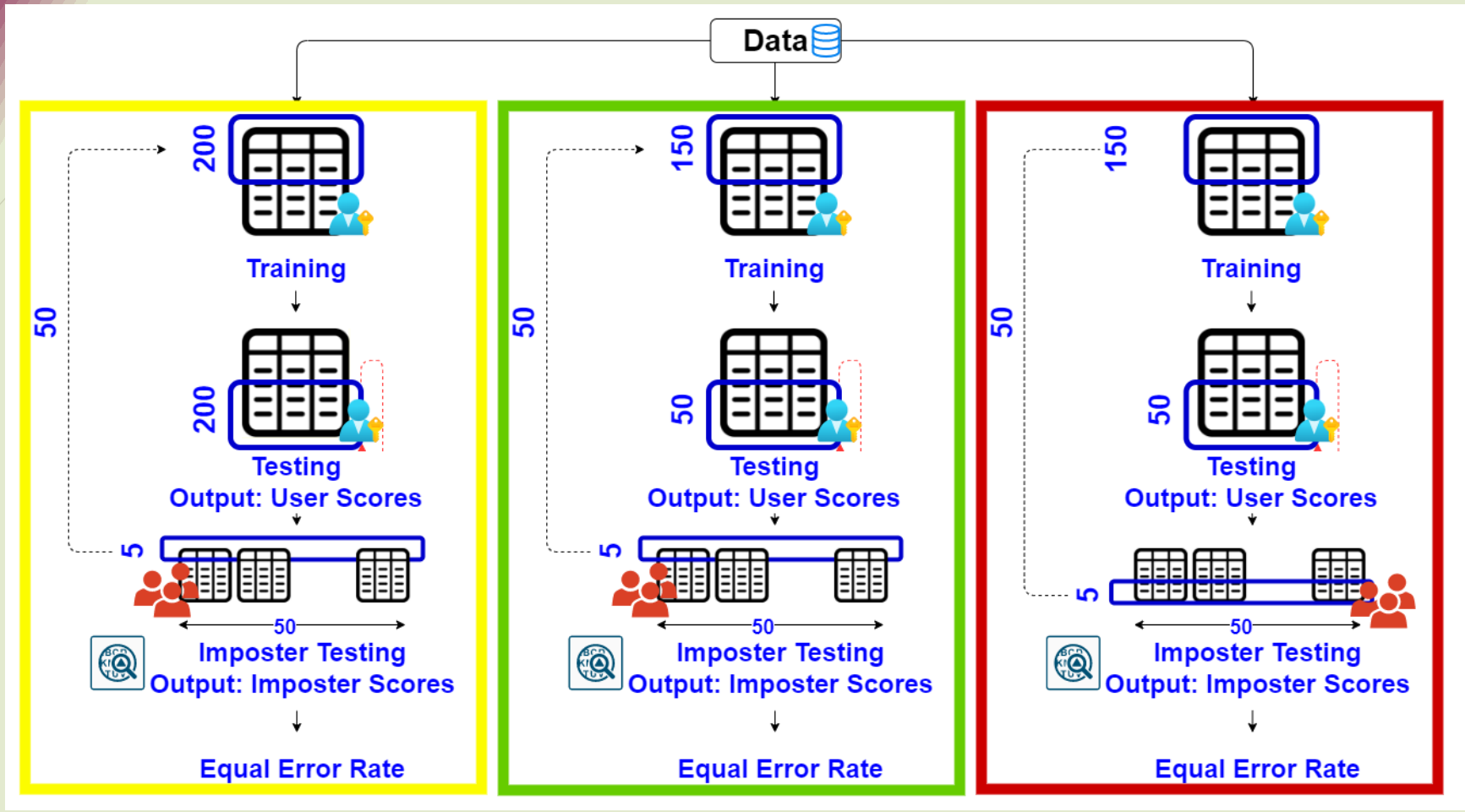


Penkių atsitiktinai parinktų vartotojų klaviatūros biometriniai duomenys





1a pav. Vartotojo biometrinės elgsenos identifikavimo schema



1b pav. Duomenų apmokymo bei testavimo strategijos anomalijų aptikimo metodų efektyvumui įvertinti

Atliktų eksperimentų rezultatai

Methods	Average-EER		
Nearest Neighbour (Mahalanobis)	0,3795	0,4548	0,5013
Euclidean	0,1693	0,1863	0,2346
Manhattan	0,1503	0,1622	0,2032
Manhattan (Scaled)	0,0945	0,0986	0,1291
Manhattan (Filtered)	0,1253	0,1399	0,1886
Mahalanobis	0,1596	0,1987	0,2338
Euclidean (Normed)	0,2107	0,2308	0,2483
Mahalanobis (Normed)	0,1996	0,2686	0,3083
Outlier (Counting)	0,1031	0,1060	0,1687
k Means	0,1533	0,1721	0,2238
SVM	0,1205	0,1077	0,1478

2 pav. Anomalijų aptikimo algoritmai

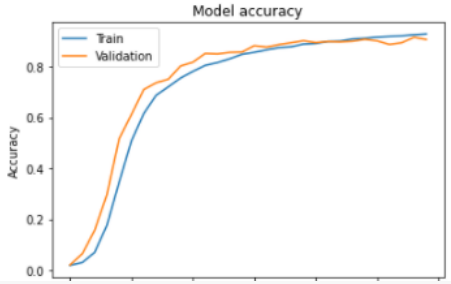
LSTM

```
[43] model = Sequential()
     model.add(LSTM(270, input_shape=(10,3), return_sequences='true', kernel_initializer=initializer, activation='tanh'))
     model.add(GaussianDropout(0.5))
     model.add(LSTM(270, return_sequences='true', activation='tanh'))
     model.add(GaussianDropout(0.5))
     model.add(LSTM(270, activation='tanh'))
     model.add(GaussianDropout(0.5))
     model.add(Dense(270, activation='tanh'))
     model.add(GaussianDropout(0.5))
     model.add(Dense(y_train.shape[1], activation='sigmoid'))
     model.compile(loss = 'BinaryCrossentropy', optimizer='adam',metrics = ['accuracy'])
     print(model.summary())
```

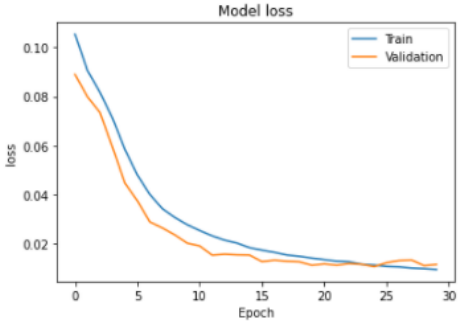
```
batch_size = 32
history=model.fit(X_train, y_train, epochs = 30, batch_size=batch_size, validation_split = 0.1, verbose = 1)

score,acc = model.evaluate(X_test, y_test, verbose = 1, batch_size = batch_size)
print("score: "+str(score)+" accuracy: "+str(acc))
```

```
Epoch 30/30
459/459 [==============================] - 13s 29ms/step - loss: 0.0096 - accuracy: 0.9279 - val_loss: 0.0116 - val_accuracy: 0.9062
128/128 [==============================] - 3s 11ms/step - loss: 0.0114 - accuracy: 0.9071
score: 0.011408143676817417 accuracy: 0.9071078300476074
```

```
plt.plot(history.history['accuracy'])
plt.plot(history.history['val_accuracy'])
plt.title('Model accuracy')
plt.ylabel('Accuracy')
plt.xlabel('Epoch')
plt.legend(['Train', 'Validation'], loc='upper left')
plt.show()
```

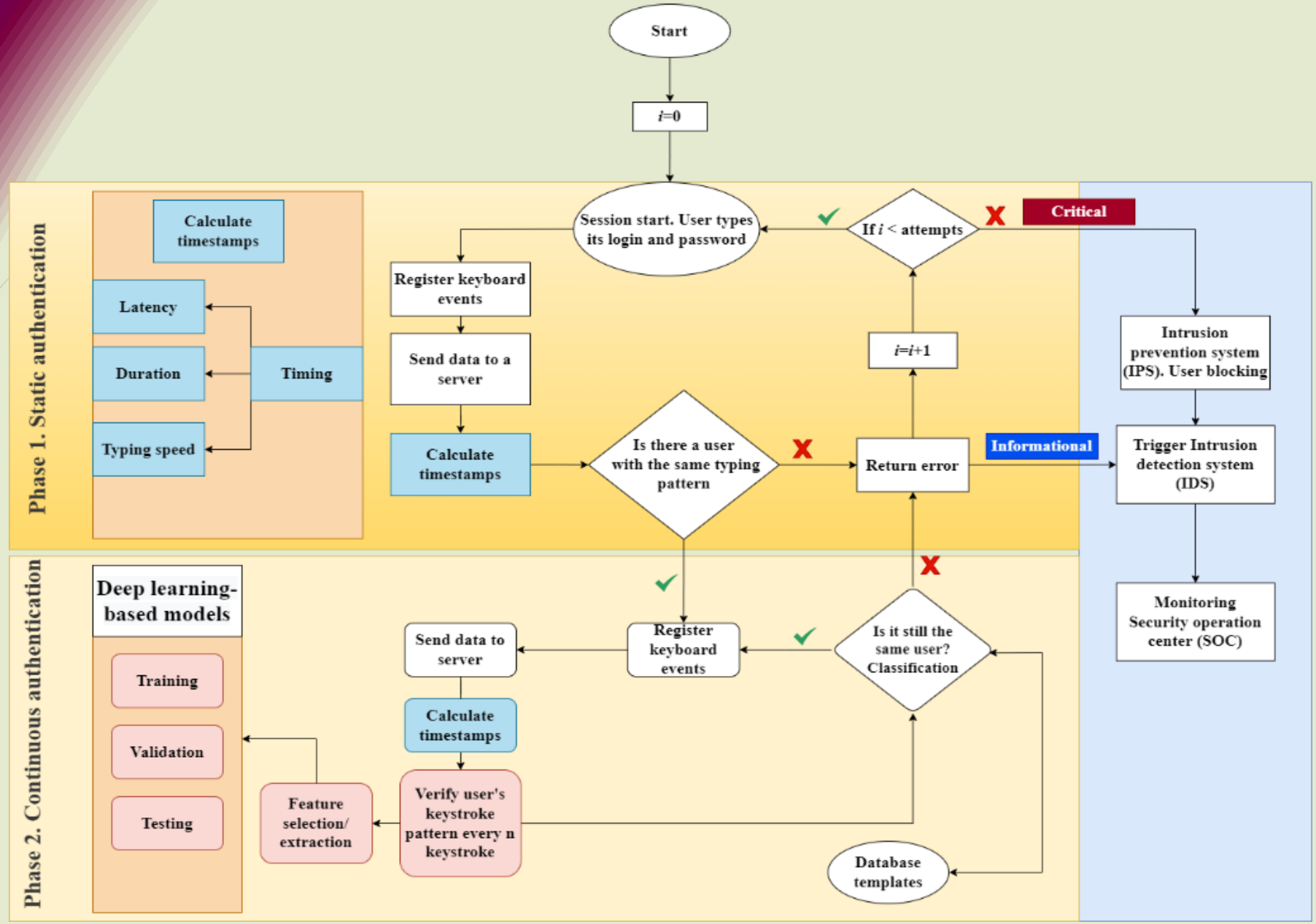



```
plt.plot(history.history['loss'])
plt.plot(history.history['val_loss'])
plt.title('Model loss')
plt.ylabel('loss')
plt.xlabel('Epoch')
plt.legend(['Train', 'Validation'], loc='upper right')
plt.show()
```



Siūloma metodika

- Sistemos vartotojui autentifikuojantis sistemoje yra tikrinamas jo įvesto slaptažodžio laiko žymos ir lyginamos su jau duomenų bazėje esančiu vartotojo šablonu.
- Prisijungus prie sistemos, vartotojo klaviatūros biometrika yra toliau stebima ir kaskart tikrinama ar pirminiame etape autentifikavęsis vartotojas toliau naudojasi sesija.
- Esant abejonėms, dirbtinis neuroninis tinklas inicijuoja sistemos užrakinimą ir vartotojas turi iš naujo autentifikuotis pirminiame (statiniame) etape (žr. 3 paveikslą).



3 pav. Vartotojo pirminio (statinio) ir nepertraukiamo autentifikavimo schema

Kito pusmečio darbo planas

- Išlaikyti egzaminą: „*Gilieji neuroniniai tinklai*“;
- Apžvalginio straipsnio rašymas (periodiniame recenzuojame mokslo žurnale arba konferencijų medžiagoje);
- Dalyvauti *„EURO2022“* konferencijoje, kuri vyks Suomijoje š. m. liepos 3–6 dienomis;
- Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką bei metodikos tobulinimas;
- Tinkamų metodų identifikavimas bei jų panaudojimo galimybių tyrimas tikslui pasiekti.

Ačiū už dėmesį

KLAUSIMAI?

arnoldas.budzys@mif.stud.vu.lt