Yusuf Korkmaz

UMID: 40883545

New User Log-in System

Cyber Security Project Report

Every webpage has a user log-in system. An example of the log-in system is shown at figure 1. If a username and its password match, the system allow to entire the account. If a user writes your username and password, the user can log-in to your account (*Select * from user_account where username = unameTextbox.getText() and password = passwordTextbox.getText()*). All the webpage uses this system. This system is not secure.

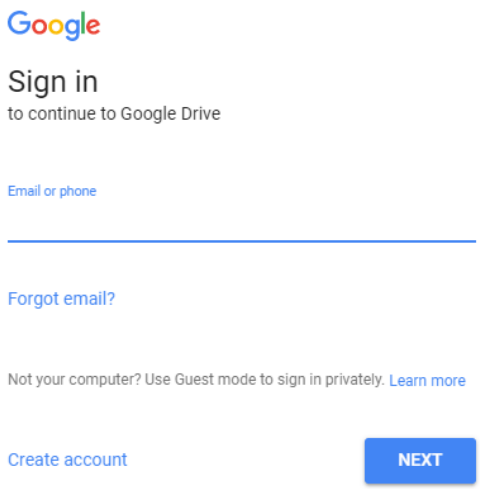

Figure 1: Google log-in system

Also, hackers can easily find our password using the brute force attack. Brute force attack systematically checks all possible passwords until the correct password is found by this method [1]. Because of this, we have some security measures. For instance, we try to create strong passwords like using characters and numbers or special characters or some verifications for proving we are owner of this account as text verifications. An example of text verification is shown at figure 2. Our accounts are very important in these days. Because they are like our identity. If a hacker reaches our account, the hacker can learn everything about us. The hacker can steal our identity and give big damage us. We should protect our accounts our information. That's why, we need more secure user log-in systems.

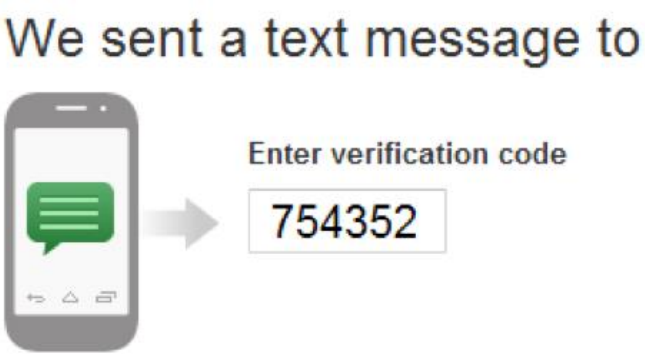

Figure 2: Text verification

I developed new user log-in system. The user log-in system is shown at figure 3. This system will protect us from bots which try to find our password. Also, this system will learn your usage pattern of keyboard and if this information and new input don't match, the system will not allow to log-in system. I used users' usage pattern of keyboard because it is unique for each person [2] like a finger print or DNA.

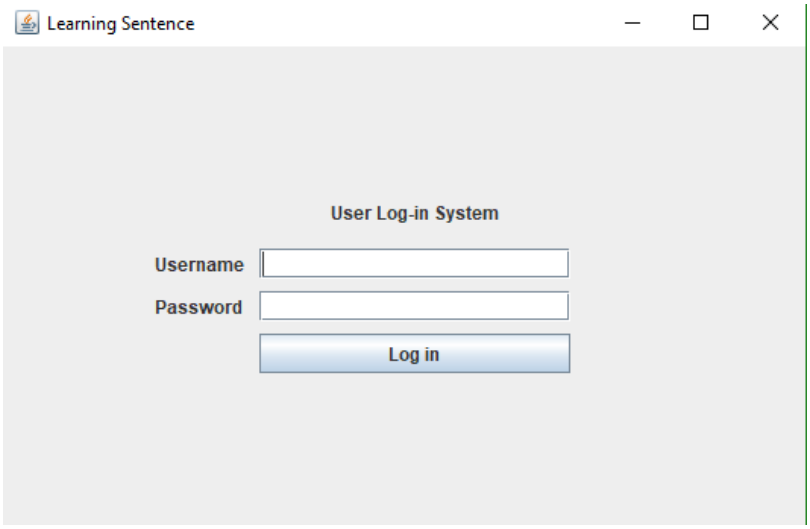

Figure 3:New user log-in system

How does this system work?

- This system takes several examples of writing password. An example is shown at figure 4.

```
c-y-25/y-b-73/b-e-113/e-r-76/r- -80/ -s-100/s-e-68/e-c-69/c-u-121/u-r-25/r-i-88/i-t-37/t-y-34/
c-y-116/y-b-68/b-e-73/e-r-6/r- -85/ -s-17/s-e-52/e-c-47/c-u-178/u-r-38/r-i-102/i-t-52/t-y-64/
c-y-10/y-b-61/b-e-93/e-r-53/r- -60/ -s-23/s-e-81/e-c-54/c-u-11/u-r-17/r-i-117/i-t-30/t-y-68/
c-y-79/y-b-67/b-e-88/e-r-36/r- -61/ -s-82/s-e-66/e-c-40/c-u-137/u-r-11/r-i-7/i-t-34/t-y-87/
c-y-32/y-b-70/b-e-121/e-r-49/r- -68/ -s-65/s-e-92/e-c-73/c-u-191/u-r-50/r-i-98/i-t-77/t-y-42/
c-y-106/y-b-51/b-e-84/e-r-65/r- -107/ -s-56/s-e-66/e-c-61/c-u-157/u-r-52/r-i-85/i-t-82/t-y-40/
```

Figure 4:Example of writing password

- The accuracy of recognizing the user will be higher when the system takes much data. Each time, the user log-in the system, it takes the new input and improves accuracy.
- When a user writes the password, the system takes the latency of between two keys. We can see the structure of the input in the figure 4, too.
- When a user clicks the “Log-in” button, the system takes the data and creates a single layer perceptron (SLP) (artificial neural network).
- For each entity, the system creates a neuron. This neuron has two keys information, latency, mean, standard deviation, weight. I would like to show these steps with one example. Let’s take “c-y”.

1. Calculate the mean using the data.

$$\text{Arithmetic mean}: \frac{25+116+10+79+35+106}{6} = 61.83$$

2. Calculate the standard deviation using the data and mean

$$Standard\ deviation: \sqrt{\frac{(61.83-25)^2+(61.83-116)^2 \ldots (61.83-106)^2}{6}} = 41.5$$

3. The system creates neuron of c-y with this information. This neuron is shown at figure 5.

Figure 5: The neuron of c-y

- The system follows these steps for each entity and creates the single layer perceptron. This perceptron is shown at figure 6.

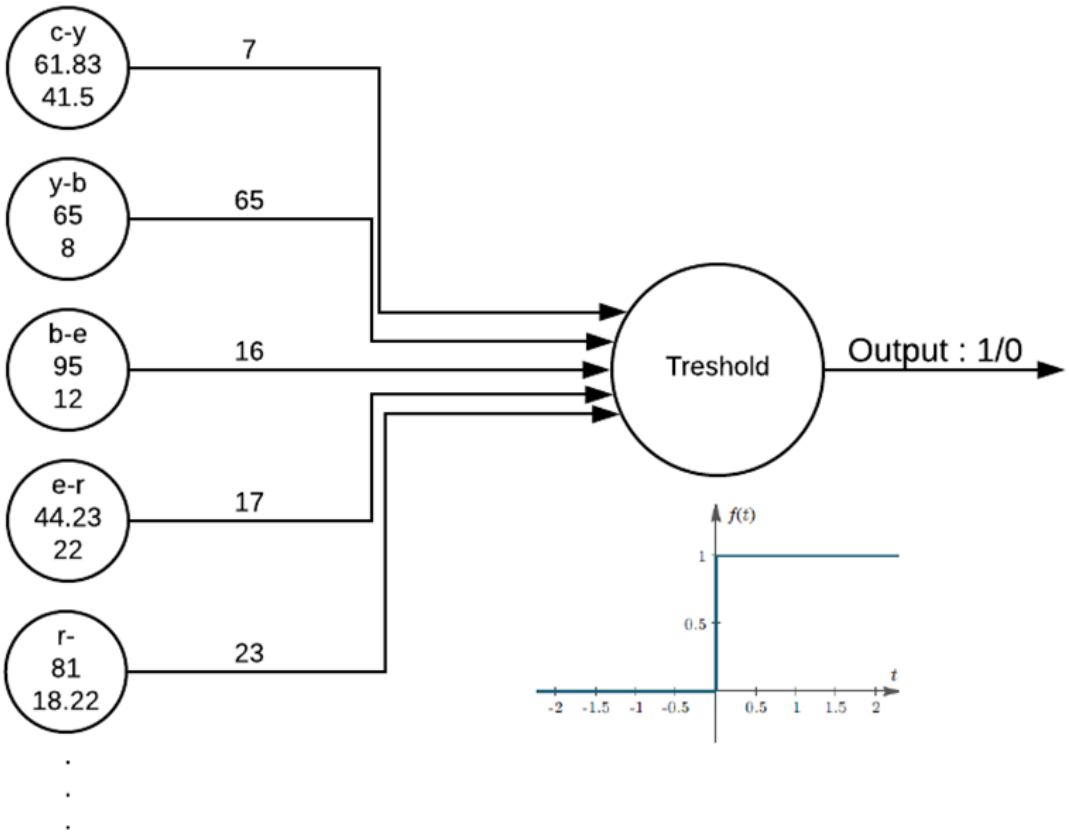

Figure 6: The single layer perceptron

- The system looks at each usage pattern to set weights of the neurons. If data's latency is so similar, its neuron's weight greater than others. Because it's mean is that this entity is important for recognizing user.
- The system gives each data to SLP and collects to threshold.
- The system takes the mean of thresholds.
- If the new input's threshold greater than system's threshold, the user is allowed to log-in the account.

Successful and unsuccessful examples of the system are shown at figure 7 and figure 8.

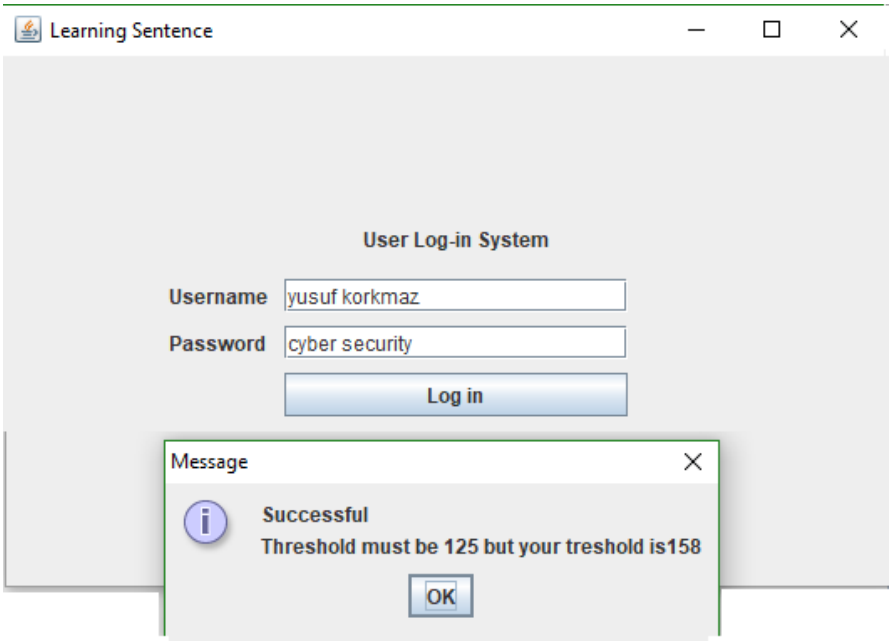

Figure 7:A successful typing

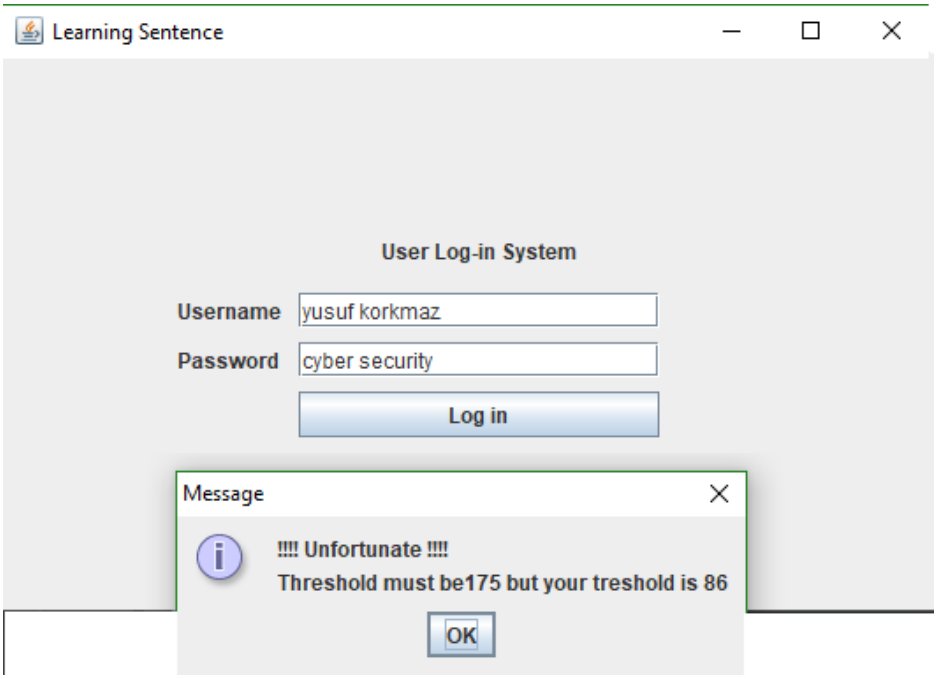

Figure 8: An unsuccessful typing

This system has many advantages and disadvantages. First, I would like to mention advantages.

1. This system is more secure than traditional user log-in system. It doesn't allow to log-in system when a user writes correct username and password. It wants much more than this.
2. If someone uses brute force attack to find correct password, it will not work with this system. Because this system needs typing. All entities time will be 0 and the system will understand this is a bot and if the bot finds the correct password, the system will not allow to log-in account. The bot will not find the correct password.
3. This system works with milliseconds and a user can't imitate another user.
4. One of the best advantages is that, if a user does same mistake every time when the user types his/her password but we can't see it in the password, the system will give a weight for this mistake too and it will wait to do this mistake again. If a user doesn't do same mistake, the user's usage pattern's threshold will be lower than the system's threshold. The user can't log-in the account.

On the other hand, this system has same disadvantages, too. For example;

1. Devices to devices usage patter of keyboard is changeable. It does not just depend on the devices. It can change with your comfortableness or your emotion.
2. The system accuracy is not well. It is because of some algorithms. I need to improve them. For example, I need to change arithmetic means to k-means algorithm.
3. You can't log-in every time when you type your password. Maybe, I should change the structure of the system, too. You can log-in the account 6 out of 10 times.

As a conclusion, it is fascinating to think that a system will an ability to recognize you. Also, I just would like to create a security layer for computers or webpages not just for log-in systems. When a person starts to use the keyboard for anything or anywhere computer will detect to user and the computer will lock itself unless the user is not the real user. In addition, I should improve the accuracy. With better accuracy, this system can be very useful.

REFERENCES

[1] McClure, S., Scambray, J., Kurtz, G., & Kurtz. (2009). Hacking exposed: network security secrets and solutions.

[2] Krátky, P., & Chudá, D. (2018). Recognition of web users with the aid of biometric user model. *Journal of Intelligent Information Systems*, 1-26.