# A Proposal for Continuous and Silent User Authentication Through Mouse Dynamics and Explainable Deep Learning

*Giovanni Ciaramella* [1], Giacomo Iadarola [1], Fabio Martinelli [1], Francesco Mercaldo [1, 2], and Antonella Santone [2]

(1) Institute for Informatics and Telematics, National Research Council of Italy (CNR), Pisa, Italy | (2) University of Molise, Campobasso, Italy

## INTRODUCTION

The number of attacks on personal accounts has grown over time. Numerous user authentication techniques have been created throughout the years to avoid it.

Among these, there is biometric-based authentication. This type of technique exploits physical-biometric or behavior-biometric for user recognition.

For instance, touch dynamics, keyboard dynamics, and mouse dynamics belong to this second category.

## THE PROPOSAL

We experimented on the “Balabit Mouse Dynamics Challenge” dataset [1], which outlined some tasks, and the users logged to a remote server where they executed them, to collect the mouse interactions between users and the system.

The data were saved in CSV files with the following structure: **record timestamp** in second, **client timestamp** in second, the **current condition of the mouse buttons**, **additional information** about the current state of the mouse, and **x-y coordinate of the cursor on the screen**.

This process has been applied for every ten users, and at the end, each CSV file created was labeled as **legal behaviors** and **illegal behaviors**.

## DATASET COMPOSITION

For image generation, we developed a script that goes to insert the x and y coordinates for each file into each specific list, which takes the name of the action done by the user.

The coordinates represent the most significant data in a row.

After graph creation for each list, they are joined into a single image with a PNG extension.

After that, we divided them into two classes, such as legal behaviors (**1271** samples) and illegal behaviors (**405** samples).

We consider the **data augmentation technique**. Using this approach, we increased the number of components in our dataset to 8000 elements for each class.

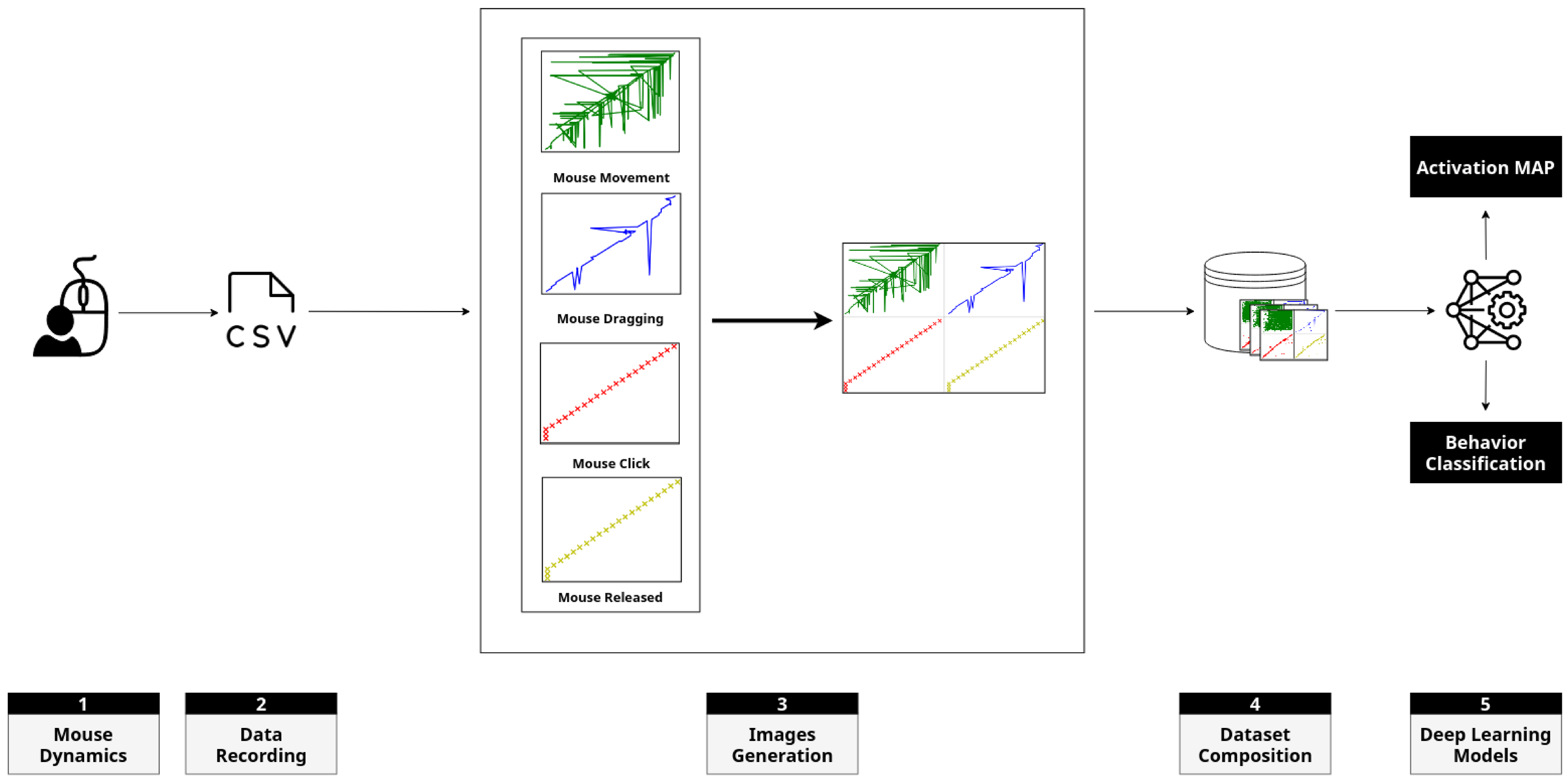


Figure 1 - The proposed method for continuous and silent user authentication.

## PRELIMINARY EVALUATION

We conducted a preliminary evaluation using the **VGG16 model** using the hyperparameters reported in Table 1, and we achieved the results reported in Table 2.

| Image Size | Batch Size | Epochs | Learning Rate |
|---|---|---|---|
| 150x3 | 64 | 20 | 0.0001 |

Table 1 – Hyperparameters used to conduct the preliminary evaluation.

| Loss | Precision | Accuracy | F-Measure | AUC |
|---|---|---|---|---|
| 0.428 | 0.902 | 0.902 | 0.902 | 0.953 |

Table 2 – Results obtained after the test session.

The class labeled illegal behaviors found **2179 true positives**, **2151 true negatives**, **249 false positives**, and **221 false negatives**. Results are displayed in Table 3.

| Loss | Precision | Accuracy | F-Measure | AUC |
|---|---|---|---|---|
| 0.897 | 0.902 | 0.902 | 0.902 | 0.902 |

Table 3 – Results obtained for “illegal behaviours” class

About the second class, labeled as legal behaviors the model retrieved **2151 true positives**, **2179 true negatives**, **221 false positives**, and **249 false negatives**. Results are shown in Table 4.

| Loss | Precision | Accuracy | F-Measure | AUC |
|---|---|---|---|---|
| 0.896 | 0.902 | 0.902 | 0.902 | 0.902 |

Table 4 – Results obtained for “legal behaviours” class

We proceeded to use the **Grad-CAM** to understand the reliability of classification and which areas of the image are useful for the prediction. An example of Grad-Cam is reported in Figure [2]

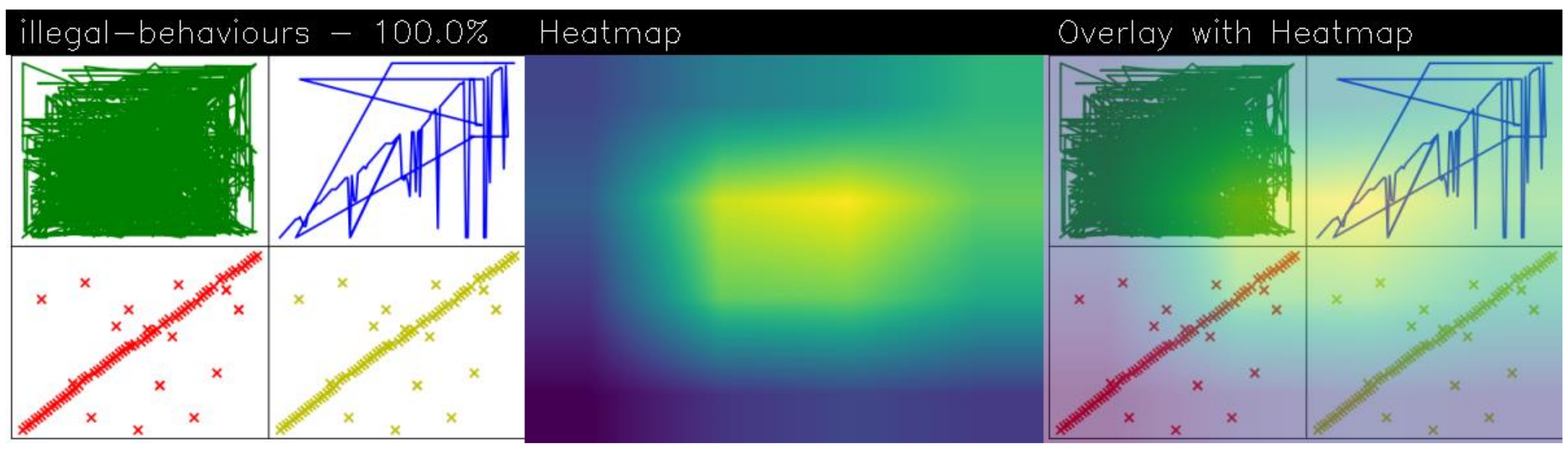


Figure 2 - The image belongs to the class illegal behaviours and was obtained after applying Grad-CAM

## FUTURE WORKS

In future studies, we would consider different models to improve the performances. Furthermore, we would consider more data for model training and evaluation.

## CONTACTS

g.ciaramella1@studenti.unimol.it, giacomo.iadarola@iit.cnr.it

fabio.martinelli@iit.cnr.it, francesco.mercaldo@unimol.it

francesco.mercaldo@iit.cnr.it, antonella.santone@unimol.it

## REFERENCES

[1] Fülöp, Á., Kovács, L., Kurics, T., Windhager-Pokol, E. (2016). Balabit Mouse Dynamics Challenge data set.

ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche