Keystroke Anomaly Detection

Team 20

AGENDA

- ❑ Project Motivation
- ❑ Data
- ❑ Literature Review
- ❑ Proposed Method
- ❑ Experimental Results
- ❑ Conclusion and Future Work

PROJECT MOTIVATION

Anomaly detection based on keystroke dynamics

What?

- Behavioral biometric based on users' unique typing rhythms.
- After the registration process, system can authenticate individuals by matching the stored patterns.

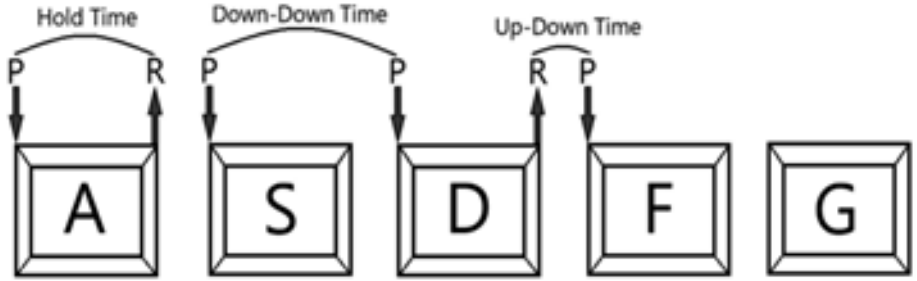
Why?

- Ease of use from the point of view of the developer and the end user.
- Easy compatibility with existing systems.
- Low cost with high accuracy.

DATA

Password: ***.tie5Roanl***

- Collected from 51 subjects over 400 times.

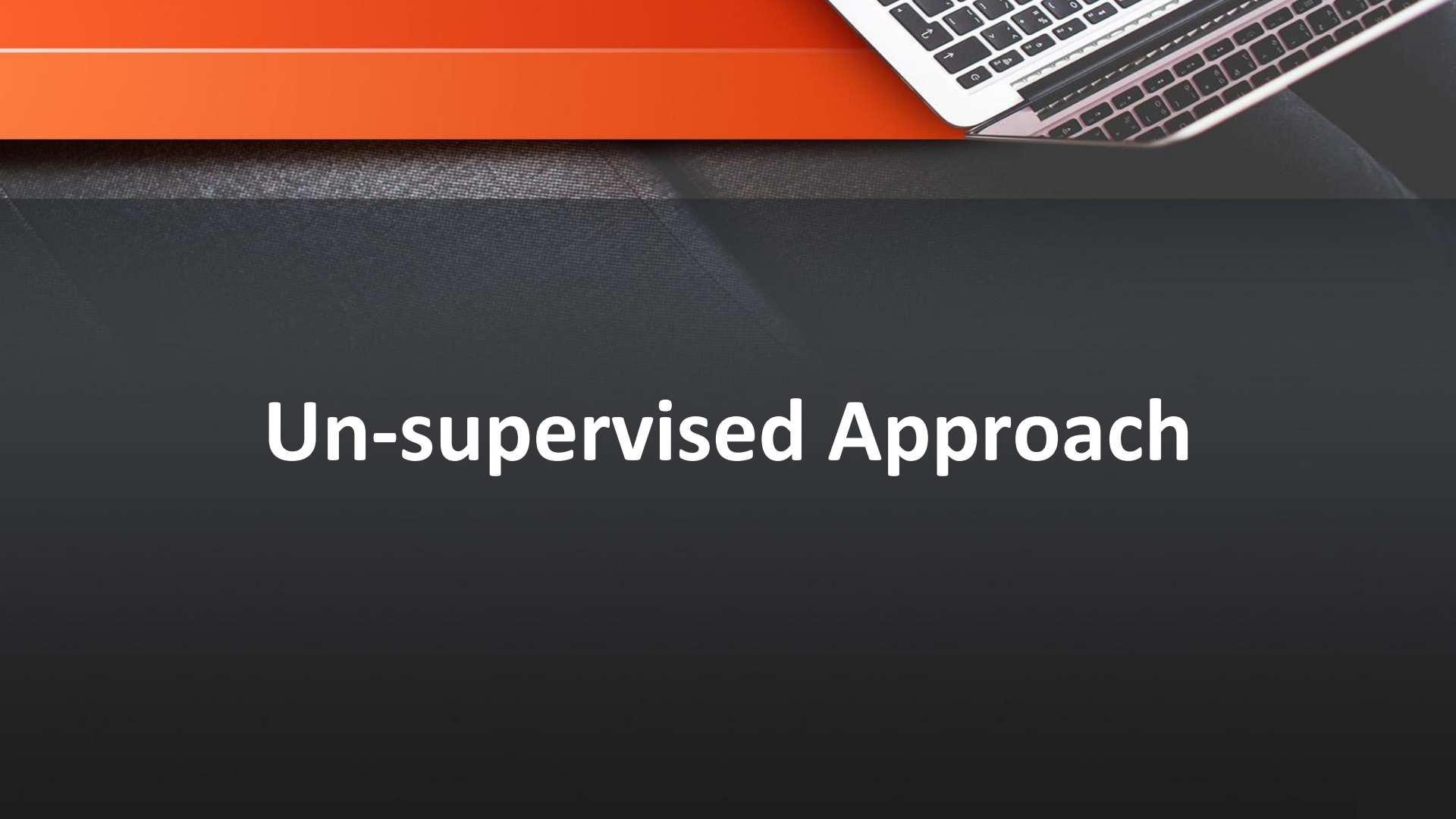


Source: A. M. Gedikli and M. Ö. Efe," A Simple Authentication Method with Multilayer Feedforward Neural Network Using Keystroke Dynamic", *Springer Nature Switzerland AG* 2020.

Feature	Description
Enter key	Timing for pressing enter
Keydown-Keydown	Timing of pressing consecutive keys
Keyup-Keydown	Timing of releasing one key and pressing the next key
Hold	Timing between pressing and releasing each key
Password attempts	Number of repetitions made until typing the password correctly
Password repetitions	Number of repetitions in typing the passwords that were used in the training phase

LITERATURE REVIEW

METHOD	ACCURACY	EER
Random Forest	-	0.3
MLP	-	0.543
feed-forward NN resilient backpropagation	94.7%	0.049
Deep Secure	93.59%	0.030
(RF, SVM, ANN)	-	0.720
Decision-level fusion	-	0



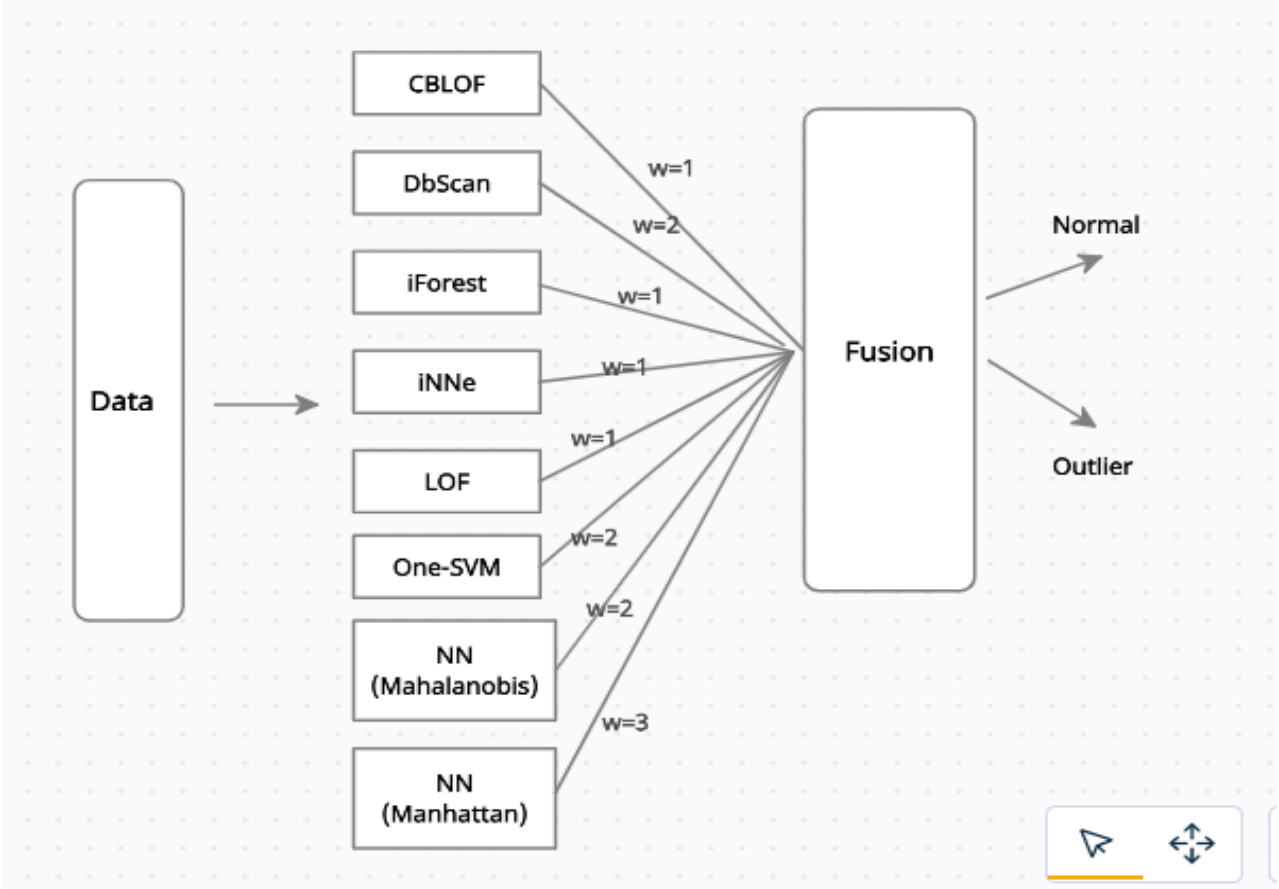
Un-supervised Approach

EXPERIMENTAL EVALUATION

- Data to be used for training and testing has 400 records (for each subject): 200 Normal (same subject) and 200 Imposter (different subjects).

- Testing data and evaluation metrics were fixed during the evaluation process.

DECISION-LEVEL FUSION

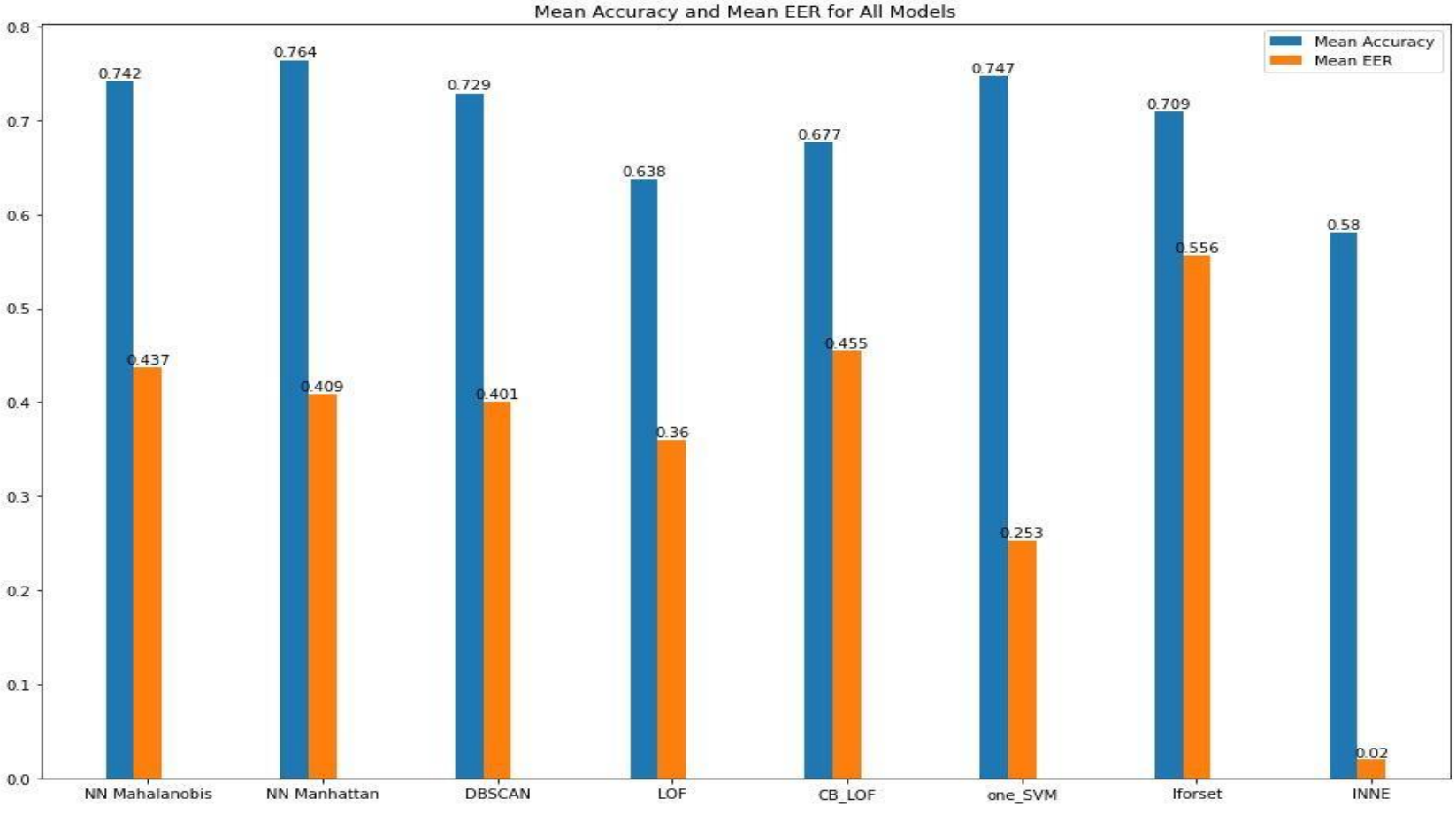


FUSION TECHNIQUES

The following fusion techniques were tested:

- Majority Voting
- Weighted Voting
- Weighted Anomaly Score

EXPERIMENTAL RESULTS



EXPERIMENTAL RESULTS

- Decision-level fusion has improved the individual performance of anomaly detection techniques
- The weighted average anomaly score anomaly detection technique has outperformed the others with a 79.7% accuracy following the unsupervised approach.

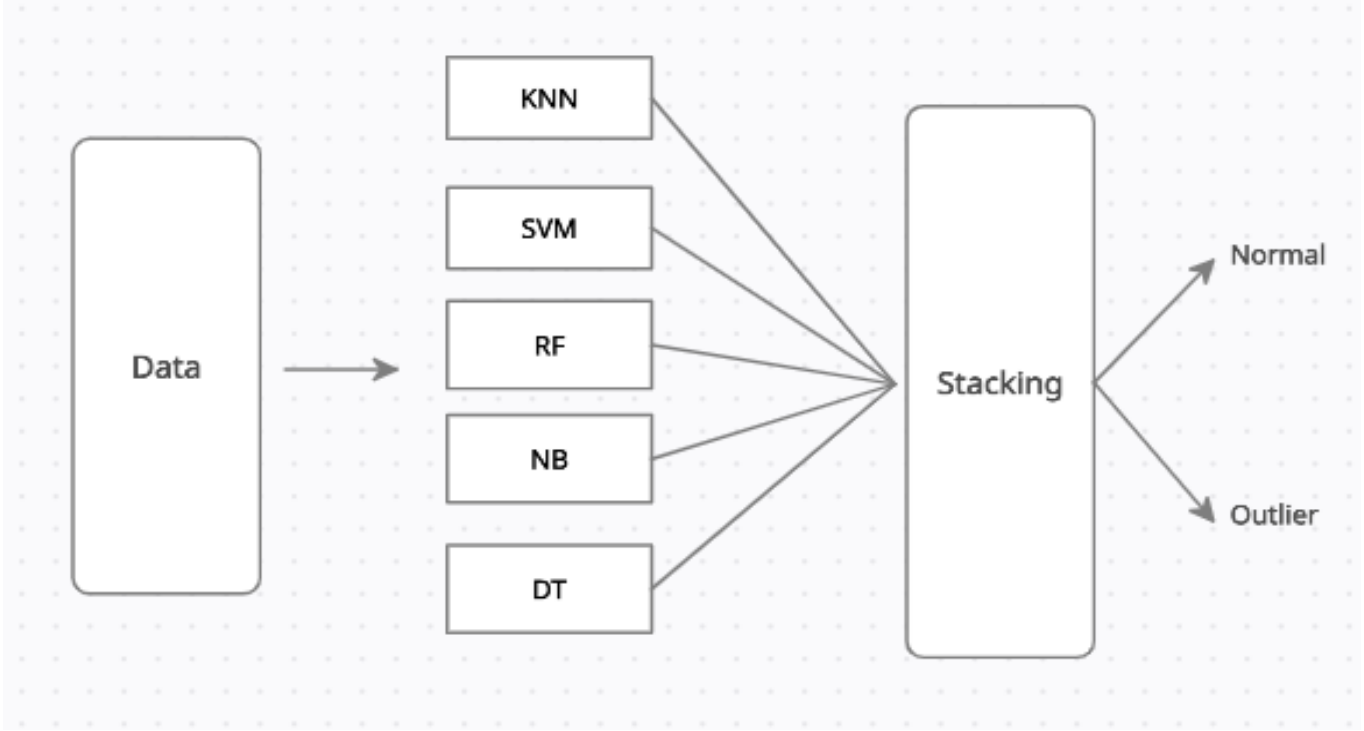
Method	Avg Accuracy	Avg EER
Majority Voting	70%	0.443
Weighted Voting	73%	0.42
Average weighted anomaly score	79.7%	0.31

Supervised Approach

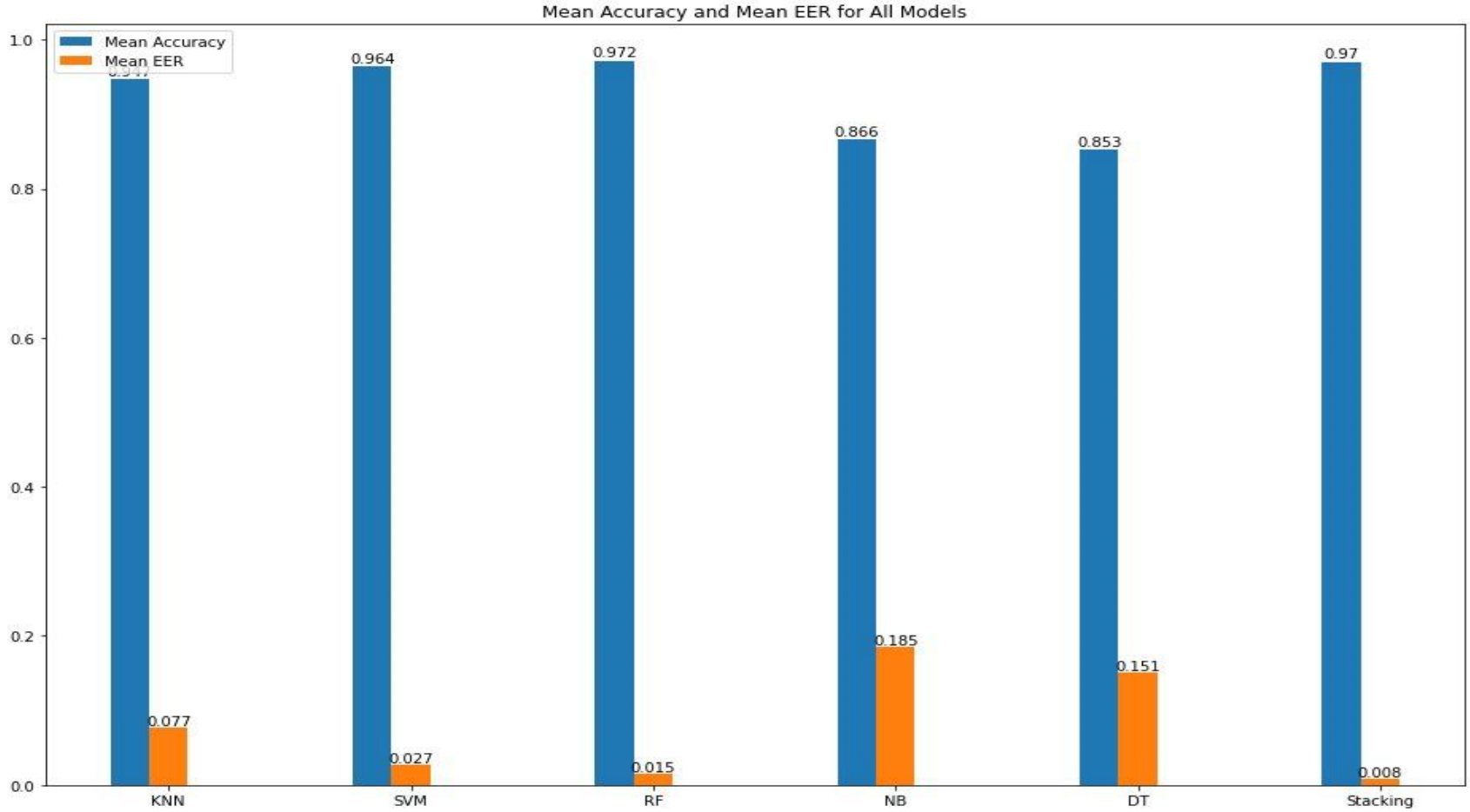
EXPERIMENTAL EVALUATION and Setup

- We select a subject considering it as a genuine user. We take other 50 subjects as impostors to that user's authentication.
- For each subject, we trained and tested the models on 400 records of the user as genuine user and 400 records of the other users as imposters.
- For each subject, we split the 800 records (400 genuine and 400 imposters) into 70% as a train and 30% as a test.

STACKING TECHNIQUE



EXPERIMENTAL RESULTS



Classification Conclusion

- In this approach we used the state-of-the-art techniques and used the stacking technique for all the models to enhance the accuracy.

- The stacking technique got 97% accuracy with least EER (0.00) which outperforms the previous state-of-the-art (94%).

CONCLUSION & FUTURE WORK

- Unsupervised approach is more common and realistic to detect anomaly based on keystroke dynamics. However, the supervised approach leads to more accurate results and outperforms the state-of-the-art techniques .

- More multivariate anomaly detection techniques, whether supervised, unsupervised, or semi-supervised, can be tested to further improve detection performance.

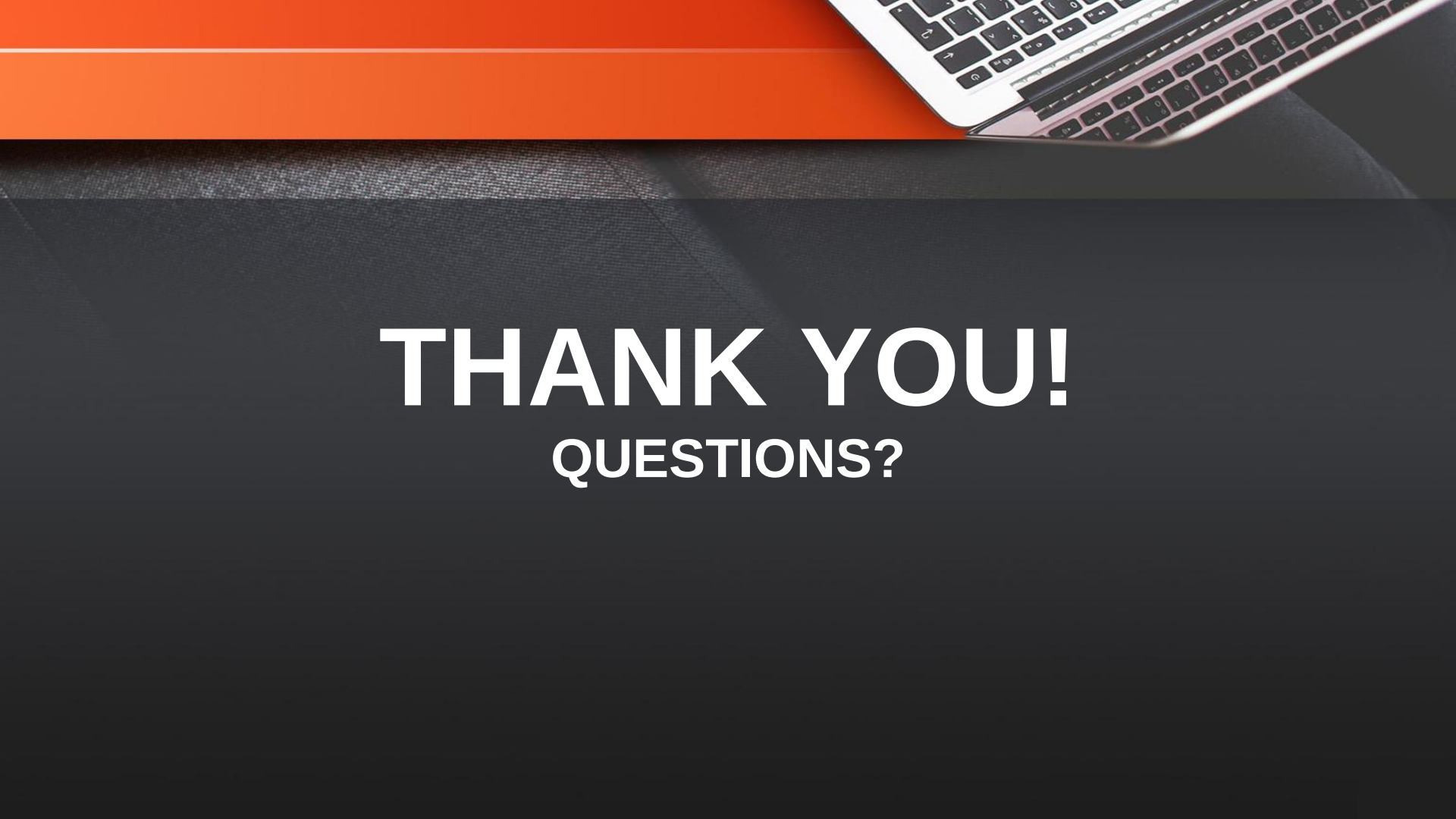
- In addition, tuning the hyperparameters of each technique to a wider range than the one already been implemented can further improve the results.

References

- A. M. Gedikli and M. Ö. Efe,” A Simple Authentication Method with Multilayer Feedforward Neural Network Using Keystroke Dynamic”, Springer Nature Switzerland AG 2020.
- Maheshwary, S., Ganguly, S., Pudi,”Deep Secure: A Fast and Simple Neural Network based approach for User Authentication and Identification via Keystroke Dynamics”.IWAISe, International Joint Conference on Artificial Intelligence (IJCAI) - 2017.
- Alsultan, Arwa, Kevin Warwick, and Hong Wei. "Improving the performance of free-text keystroke dynamics authentication by fusion." Applied Soft Computing 70 (2018): 1024-1033

References (continue)

- Huang, A., Gao, S., Chen, J., Xu, L. and Nathan, A., 2020. High security user authentication enabled by piezoelectric keystroke dynamics and machine learning. IEEE Sensors Journal, 20(21), pp.13037-13046.
- M. Antal and L. Z. Szabó, “An evaluation of one-class and two-class classification algorithms for keystroke dynamics authentication on mobile devices,” in 2015 20th International Conference on Control Systems and Computer Science. IEEE, 2015, pp. 343-350.
- A. Salem, D. Zaidan, A. Swidan, and R. Saifan, “Analysis of strong password using keystroke dynamics authentication in touch screen devices,” in 2016 Cybersecurity and Cyberforensics Conference (CCC). IEEE, 2016, pp. 15-21. .



THANK YOU!

QUESTIONS?