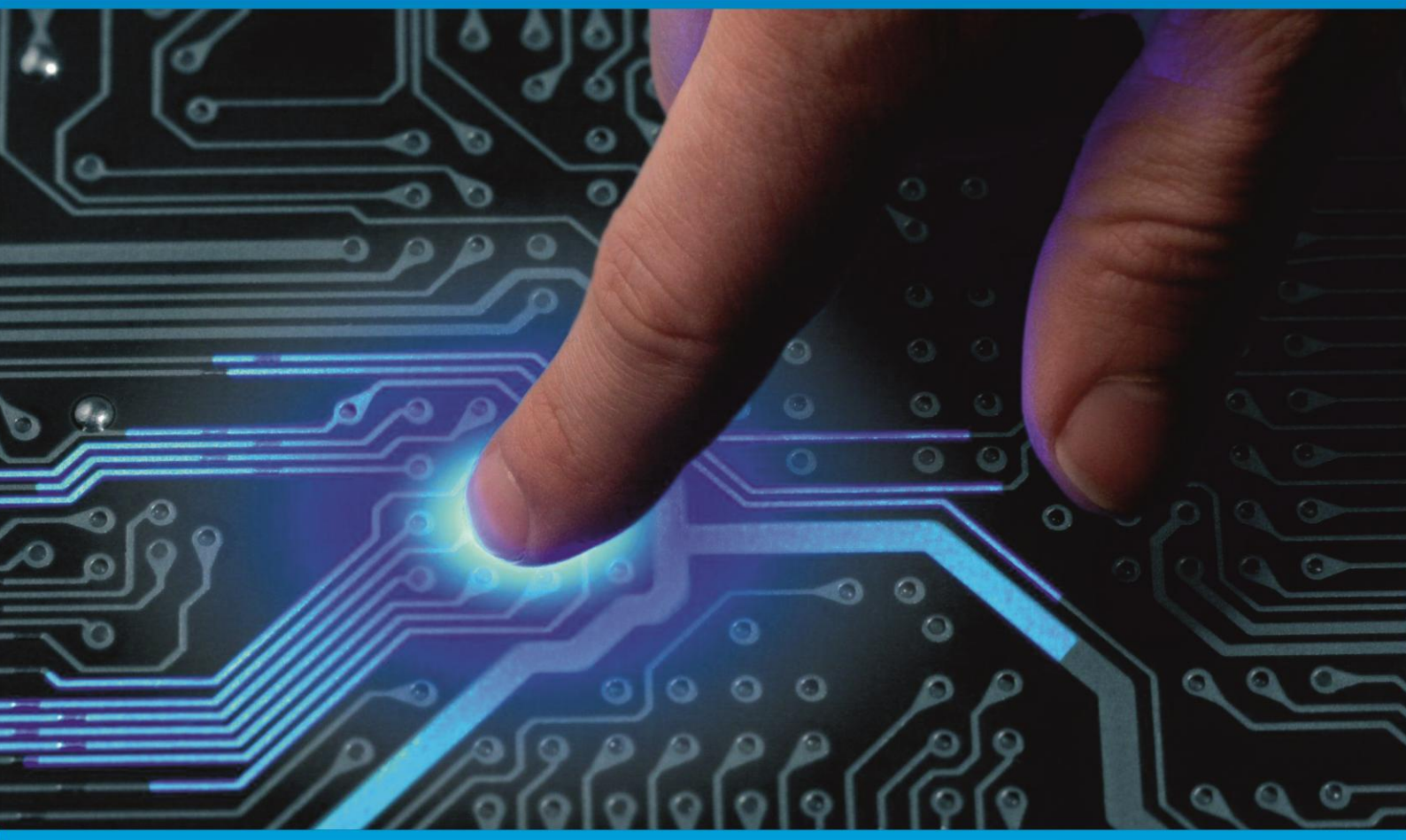
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 7, July 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007047 |

Authentication Using Keystroke Biometrics

N. Thanuja, Aashutosh Kumar Jha, Mohammad Ashhar , Mohit Chanani, Pashupati Rai

Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru, India

ABSTRACT: Behavioural biometrics measure behavioural tendencies that identify a person, like keyboard typing (dynamics), mouse movement, handwritten signature and so on. While this kind of authentication does not require any extra hardware, it has a lower adoption rate compared to physical biometrics mainly because of the variability of human body and mind over time. However, a big benefit of behavioural biometrics is that authentication can occur. actively throughout a user's session. This prevents cases when the user session is hijacked after the initial logon. Keystroke dynamics is a behavioral measurement and it utilizes the manner and rhythm in which each individual types. The approaches in keystroke dynamics can be categorized by the selection of features and the classification methods employed.

KEYWORDS: Authentication; Behavioural; Biometrics; Keystroke Dynamic;

I. INTRODUCTION

Keystroke biometric systems measure typing characteristics believed to be unique to an individual and difficult to duplicate Although most of the systems developed have been experimental in nature, there is a commercial product, BioPassword, currently used for hardening passwords (short input) in existing computer security schemes.

The keystroke biometric is appealing for several reasons. First, it is not intrusive and computer users type frequently for both work and pleasure. Second, it is inexpensive since the only hardware required is a computer with keyboard.

Our research focused on utilizing user keystroke biometrics to add second factor authentication to a system. Keystroke biometrics involves collecting a user's keystrokes and then extracting a typing behavior template from their keystrokes. There are several types of user biometrics each with their own downfalls and benefits which must be considered in the design of an authentication system. For example, consider the available hardware on a mobile system such as a finger print scanner, front facing camera and a software keyboard and how you can use the available hardware for authentication. First the finger print scanner can allow a user to authenticate with a biometric fingerprint, secondly, the user can use the front facing camera to authenticate with their face or iris via biometric and lastly, the user can authenticate with the keyboard by: entering their username and password and using their biometric keystrokes. Overall, the available hardware on a computing device will influence the type(s) of authentication that a system can use without having to add on extra hardware. This is the motivation behind using keystroke biometrics as most computing systems already have a keyboard and no extra peripherals or other hardware needs to be integrated into the system.

II. RELATED WORK

In [1] paper the authors Garciaproposeda method for conducting online handwritten signature verification. The co-occurrence matrix and local binary pattern are analyzed and used as features. The methods proposed in this work for improving the performance of on-line signature verification are based on the combination of LSTM and GRU RNNs with a Siamese architecture.]. In [2] paper the authorsdesigned Speaker Identification system. Speaker Identification (SI) is the task of establishing identity of an individual based on his/her voice characteristics.]. In [3] paper the authors proposed a DHGA-net architecture consisting of two major components: a spatio-temporal feature extraction backbone, and a Temporal-Identity-Extrating module (TIE).We design a spatio-temporal feature extraction backbone based on 3D convolution layers to extract spatio-temporal features of dynamic hand gesture videos. In [4] paper the author Proposed a consistent and efficient method for the identification of biometrics using the iris recognition in view of the fact that it has richness in texture information.[5] In this paper the authors proposes an innovative and scalable approach to exact multi-pattern matching of nucleotide sequences by harnessing the massively parallel computing power found in commodity graphical processing units. Their approach places careful consideration on preprocessing of DNA datasets and runtime performance, while exploiting the full capabilities of the heterogeneous platform it runs on.

[6] In this paper the authorspointed out that Face recognition has been one of the most important topics in the biometrics in the past several years. There have been many approaches proposed for this topic. In general, the research of face recognition is focused on verifying or identifying a face from its image.After being aligned the ROI images were transformed to gray images and used to generate the MHIs. The MHIs and the features extracted from gray images were resized into vectors and normalized and fused together as features. It therefore used this kind of features to

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007047 |

feed a DBN (7-layer deep learning neural network) to recognize faces. The count of input units of the whole network was 20000 and the count of output units was 100.[7] In this paper the author Rahul Thakran proposed authentication scheme that is an amalgamation of different authentication schemes altogether. It combines both recalls based (textual) and recognition based (graphical) passwords so that multifactor and a multi password authentication known as 3D password could be generated.Here, a new virtual environment is introduced which is termed as 3D virtual environment where a user can navigate and move in that environment to create a password based on both the schemes. In the proposed system, the biometric scheme has not been included because of some potent drawbacks like shoulder surfing attacks, venerability, increase in the cost of scheme and hardware parts needed.

III. PROPOSED ALGORITHM

The standard approach in a keystroke dynamics-based verification is using anomaly detectors.We will develop a keylogger which will be used to extract keystroke data(up-up time, up-down time, Down-down time, down-up time). The approach we presented here is different as it uses a binary classifier (recurrent neural net-works). Data from the genuine user are positive and from the other people – negative.

Due to assumed sequence nature of input data we have decided to use recurrent neural networks. These networks naturally operate on sequences. Plain recurrent neural net- works are very simple (compared to other neural network architectures) models. They differ from feed forward net- works in the way of processing input – here it is processed in a step-by-step manner. At step t the network receives xt as input and having knowledge about state from last step ht−1 it computes its output according to the formulas (1) and (2). Whh, Wxh and Why are matrices of network parameters.

$$h_t = \tanh(W_{hh} \cdot h_{t-1} + W_{xh} \cdot x_t) \quad (1)$$

$$y = W_{hy} \cdot h_t \quad (2)$$

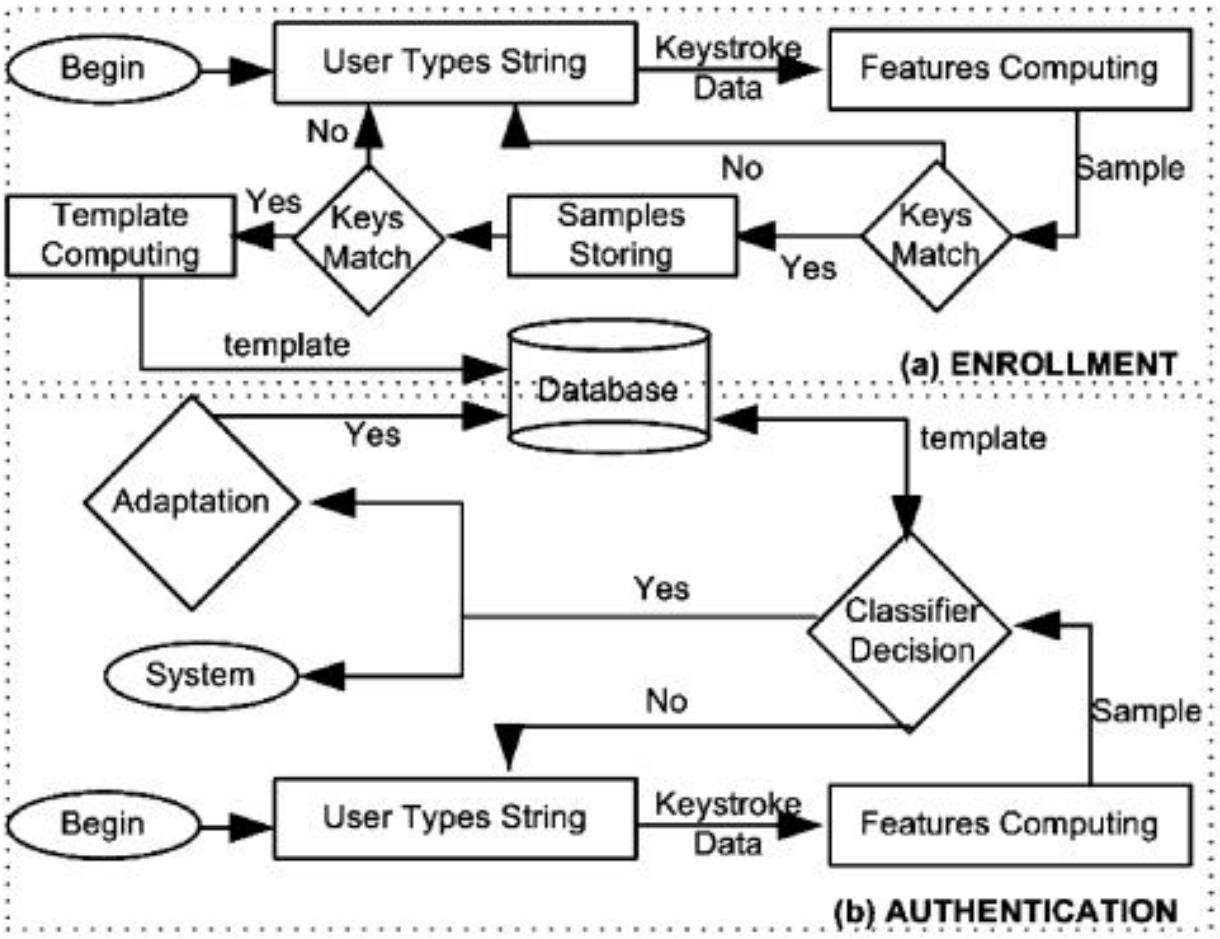


Fig. 1 System Architecture

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007047 |

IV. PSEUDO CODE

Model Training:

```
model_training(CMU_loc):
Data←pd.readcsv(CMU_loc)
Data←feature_extract(data)
for model in model:
m=model()
m.fit(data)
m.test()
Print(confusion(m))
save(m)
```

Recogniser:

```
Recogniser(username):
model←load("best_model",loc)
pos_data,neg_data←data.split(username)
EER←model.predict(pos_data,neg_data)
If(0.15<EER<0.04):
        redirect('/homepage','GET')
Else
        redirect('/login','GET')
```

.

V. RESULTS

The following graphs draws a comparison between different machine learing model which we tested to get the best accuracy for authentication using Keystroke Biometric

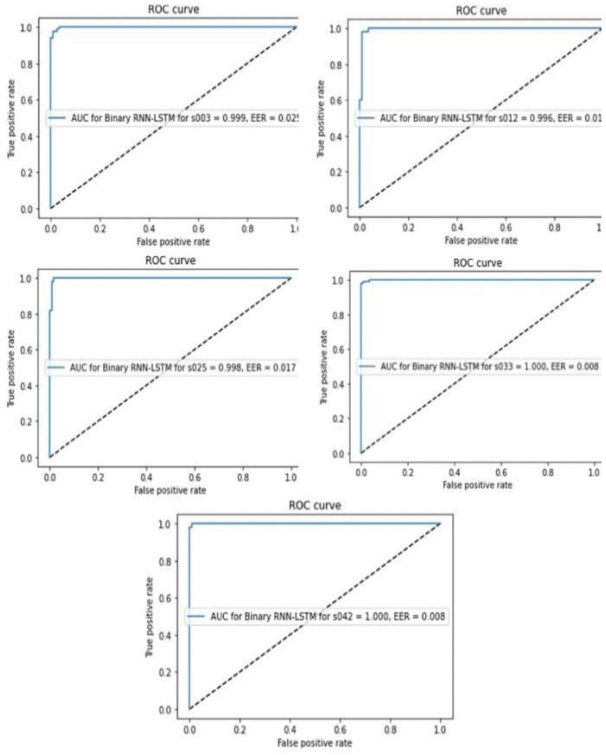


Fig. 2 ROC curves for 5 subject of Binary LSTM RNN

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007047 |

Table 1- EER values of 5 subject under Binary LSTM RNN

Subject	EER	AUC	Accuracy
s003	0.025	0.995	97.89%
s012	0.017	0.996	97.92%
s025	0.017	0.998	98.75%
s033	0.008	1.000	98.95%
s042	0.008	1.000	99.58%

A receiver operating characteristic curve, or ROC curve, is a graphical plot that illustrates the diagnostic ability of a binary classifier system as its discrimination threshold is varied.

To draw a ROC curve, only the true positive rate (TPR) and false positive rate (FPR) are needed (as functions of some classifier parameter). The TPR defines how many correct positive results occur among all positive samples available during the test. FPR, on the other hand, defines how many incorrect positive results occur among all negative samples available during the test.

VI. APPLICATIONS

- Keystroke dynamics can be used for authentication, then it is used mostly together with user ID / password credentials as a form of two-factor authentication.
- This system can be used for behavioral analysis as well.
- Keystroke event can be measured up to milliseconds precision by software Thus, it is impractical to replicate one’ s keystroke pattern at such high resolution without enormous amounts of effort.
- Keystroke dynamics biometrics offer a way to continuously validate the legitimate identity of a user.

VII. CONCLUSION AND FUTURE WORK

Technology has advanced vastly since keystroke dynamics was used as a reliable method for authenticating the users. Now keystroke dynamics is used on mobile phones and PDA’s which are web-enabled. The scope of using keystroke dynamics has spread far and wide spanning across different areas of applications. Both the statistical and Neural Networks techniques have been widely used by the researchers. Keystroke Dynamics can also be used to find the age and gender of the users. These soft features for example can then be used across web-based applications, which aim in understanding the buying behavior of the patrons. This system aims to provide a cheap and better alternative to biometric authentication using keylogger data and Statically Based learning methods.In future rather than using it only for two factor authentication, we can use it to continuously monitor user while he/she is using the system and raise a flag in case of non-privileged user accessing the system.Further this system can lso be used to coduct sentiment analysis of its users.

REFERENCES

1. Ruben Vera-Rodriguez; Julian Fierrez; Javier Ortega-Garcia – Exploring Recurrent Neural Networks for On-Line Handwritten Signature Biometrics, 2018.
2. BidhanBarai, Debayan Das, Nibaran Das, Subhadip Basu, MitaNasipuri– Closed-Set Text-Independent Automatic Speaker Recognition System Using VQ/GMM, 2018.
3. Chang Liu, Yulin Yang, Xingyan Liu– Dynamic-Hand-Gesture Authentication Dataset, 2021.
4. Dua, M., Gupta, R., Khari, M., and Crespo, R. G. – Biometric iris recognition using radial basis function neural network, 2019.
5. Kennedy Okokpujie, Samuel John – Fingerprint Biometric Authentication Based Point of Sale Terminal, 2018.
6. CiprianPungila, Viorel Negru– Towards real-time DNA biometrics using GPU-accelerated processing, 2020.
7. Haider Mehraj, Ajaz Hussain Mir– Person identification using fusion of deep net facial features, 2020.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007047 |

8. Dr. Arjun V. Mane, Dr. V. T. Humbe, Shriram D. Raut– Development of Biometric Palm Vein Trait Based Person Recognition System, 2017.
9. Rahul Thakran – 3D Password- A Desirable Unification of Pre-Existing Authentication Techniques, 2021.
10. S. R. Nirmala and Jarina B. Mazumdar– Retina Based Biometrics Authentication System, 2018.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details