Continuous User Identity Verification via Mouse Gesture Dynamics

[1]Prasanna Kumawat, [2]P.N.Kalavadekar

[1] P.G. Student, Department of Computer Engineering, SRES, COE Kopargaon, Maharashtra, India
[2]P.G Coordinator, Department of Computer Engineering, SRES, COE Kopargaon, Maharashtra, India

Abstract: **Most Of The Authentication Systems Use Alphanumeric Characters In Their Password, But Their System Fails From Several Attacks Such As Brute Force Attack, Guessing, Social Engineering Etc. Though The Biometric Technology Which Is Available Today Produces High Accurate Processing, It Needs Additional Or Special Purpose Hardware And Large Processing Time To Achieve It. The Advanced Biometric Technique Which Analyzes The Behavior Characteristic Of The User Called Behavior Biometrics .The Behavior Biometric Technique Implements Using Mouse Dynamics That Analyze And Extract The Characteristics Movement Of The User, When He Interacts With The Computer. This Extracted Information Is Later Used for the Authentication Purpose .The Existing Systems Achieve Better Work Well In Continuous Authentication.**

Keywords: **Behavioral Biometrics, Biometric Authentication, Computer Security, Identity Verification, Mouse Dynamics, Anonymous Password Feature.**

I. INTRODUCTION

The primary focus of designing the biometric system is to provide the very accurate authentication .In the last two decades, with the rapid development in the computerized services like online banking, trading and many others, the number of hacking and identity theft incidents are increasing enormously. Token based authentication is simple but not foolproof. To overcome the problem with token based authentication system, Biometric systems were emerged. But biometric properties cannot be kept secret due to many factors. This limits the scope of biometrics in day-to-day life. Another reason for limited usage of biometric system is the reliance on special purpose devices for biometric data collection and verification.

Hence it developing a prototype for new category of behavioral biometrics that is gaining great attention in recent days is Mouse gesture dynamics. Mouse dynamics deals with extracting the features related to the mouse movements and analyzing them to extract a signature, which is unique for every individual and can be used to discriminate different individuals. The aim of mouse dynamics biometric technology is its ability to continuously monitor the legal and illegal users based on their usage of a computer system. This is referred to as continuous authentication. Continuous authentication is very useful for continuous monitoring applications such as intrusion detection. This paper first identifies the user movements or characteristics when the user interacts with the mouse, results in the generation of mouse gestures and checks every time when the user make session and provides authentication to the users. The mouse gestures are drowned in unistroke.

A mouse gesture results from the combination of computer mouse movements and clicks in a way that the software recognizes as a specific command. Biometrics refers to the identification of humans by their characteristics or traits. Biometric identifiers are characterized as physiological and behavioral characteristics. A physiological biometrics is related to voice, DNA, hand prints. A behavioral biometrics is related to the behavior of the persons. A biometric system involves 2 phases, enrollment phase and verification phase. In the enrollment phase, user will draw a set of gestures several times on a computer monitor using mouse. The features are extracted from the captured data, analyze them and train the neural network that is later used for identification. In the verification phase, the user will be asked to replicate a subset of gestures drawn during the enrollment phase for authentication.

Mouse gesture dynamics deals with biometric authentication. The mouse gesture dynamics uses a hidden Markova model for classification. In the existing graphical password schemes, the user is not only expected to memorize and remember the graphical passwords, the user has to hide the passwords during the login process to avoid surfing attacks. The mouse dynamics pro- posed schemes depends on the user biometric information and the user need not to memorize the gestures. There are only two mouse dynamics based biometric systems techniques available for static authentication due to the complexity or challenges. One of the methods proposed by Syukri etal uses the signature drawn by the user as input during the static authentication process. The other method proposed by Revett etal uses mouse lock method for static authentication. In the proposed approach, the user draws the gesture at login time which are collected and analyzed for authentication purpose. Existing gestures based authentication systems uses other input devices such as stylus but in this, mouse is used as input device for capturing the gestures.

II. RELATED WORK

A new biometric technology based on mouse dynamics 2007[1] paper introduces a new form of behavioural biometrics based on mouse dynamics which can be used in different security applications. It develop a technique that can be used to model the behavioural characteristics from the captured data using artificial neural networks. In addition, it present an architecture and implementation for the detector, which cover all the phases of the biometric data how including the detection process.

Random forests, Machine Learning 2001[2] which are a combination of tree predictors such that each tree depends on the values of a random vector sampled independently and with the same distribution for all trees in the forest. The generalization error for forests converges as to a limit as the number of trees in the forest becomes large. The generalization error of a forest of tree classifiers depends on the strength of the individual trees in the forest and the correlation between them. Multimodal person recognition for human vehicle interaction 2006[3] present an overview of multimodal in-vehicle person recognition technologies. It demonstrates, through a discussion of proposed framework, that the levels of accuracy required for person recognition can be achieved by fusing multiple modalities. It discusses techniques and prominent research reports, and it presents the results of two case studies they conducted. The sidebar, Solutions for In-Vehicle Person Recognition, discusses related work.

Performance of biometric quality measures 2007[4] paper documents a methods for the quantitative evaluation of systems that produce a scalar summary of a biometric samples quality. They are motivated by a need to test claims that quality measures are predictive of matching performance. They regard a quality measurement algorithm as a black box that converts an input sample to an output scalar. It evaluates it by quantifying the association between those values and observed matching results. The advance detection error trade-off and error versus reject characteristics as metrics for the comparative evaluation of sample quality measurement algorithms. It proceed with a definition of sample quality, a description of the operational use of quality measures. Identification of humans using gait 2004[5] paper propose a view-based approach to recognize humans from their gait. Two different image features have been considered: the width of the outer contour of the finalized silhouette of the walking person and the entire binary silhouette itself. To obtain the observation vector from the image features, it employ two different methods. First method is FED and second method is HMM.

Personal identification using multibiometrics rank-level fusion 2011[6] paper investigates a new approach for the personal recognition using rank-level combination of multiple biometrics representations. There has been very little effort to study rank-level fusion approaches for multibiometrics combination and none using multiple palm print representations. NABS: novel approaches for biometric systems 2011[7] paper, deal with some core issues related to the design of these systems and propose a novel modular framework, namely, novel approaches for biometric systems (NABS) that have implemented to address them. NABS proposal encompasses two possible architectures based on the comparative speeds of the involved biometrics.

III. CONTINUOUS USER IDENTITY VERIFICATION VIA MOUSE GESTURE DYNAMICS

The Fig.1 depicts the typical architecture of a behavioral biometrics user verification system. Such systems include the following components:

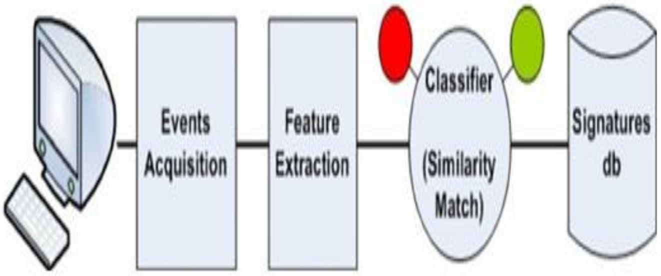


Fig.1 A General Block Diagram of Proposed System.

- **Feature acquisition-** Captures the events generated by the various input devices used for the interaction (e.g. keyboard, mouse) via their drivers.
- **Feature extraction-** Constructs a signature which characterizes the behavioral biometrics of the user.
- **Classifier-** Consists of an inducer (e.g. Support Vector Machines, Artificial Neural Networks, etc.) that is used to build the user verification model by training on past behavior, often given by samples. During verification, the induced model is used to classify new samples acquired from the user.
- **Signature Database-** A database of behavioral signatures that were used to train the model. Upon entry of a username, the signature of the user is retrieved for the verification process.

IV. MATHEMATICAL MODEL

- **Input Set:**

From the above definition, we get the input set(I), which contains input as Mouse Events.

There are seven inputs denoted by set I= (I1, I2, I3, I4, I5, I6, I7)

I1= Left Click Event.

I2= Right Click Event.

I3= Drag and Drop.

I4= Double Click

I5= Mouse Move and Left or Right Click Action.

I6= Mouse Move and Double Click Action.

I7= Mouse Move and Drag and Drop Action.

- **Process Set:**

Consider a set of processes which are used in this system.

P1: Event Acquisition () In this process, events are captured by acquisition module and passed it to feature extractor.

P2: Feature Extractor () In this process, the output of P1, is input for P2. Then, from the captured events feature extractor extracts feature and transform into actions.

P3: Classifier () In this process, the output of P2, is input for P3. Then, classifier categorizes the different actions and stores in signature database according to action type.

P4: Verification () In this process, the identity of user is verified.

- **Output Set:**

There are two output sets,

The first is, intermediate output set is denoted by (IO = IO1, IO2, IO3).

IO1 = Output of P1 (Acquired events) which is input for P2.

IO2 = Output of P2 (Extracted features) which is input for P3.

IO3 = Output of P3 (signature database).

The second is final output set is denoted by (O = O1).

O1 = Whether user is Authenticated or non-authenticated user.

- **Venn Diagram:**

Venn diagram shows the relation between different inputs, processes, intermediate output and output.

Input I is given to process P1, then, intermediate outputs are generated IO1, IO2 & IO3 which are given as input to process P2, P3 & P4 respectively.

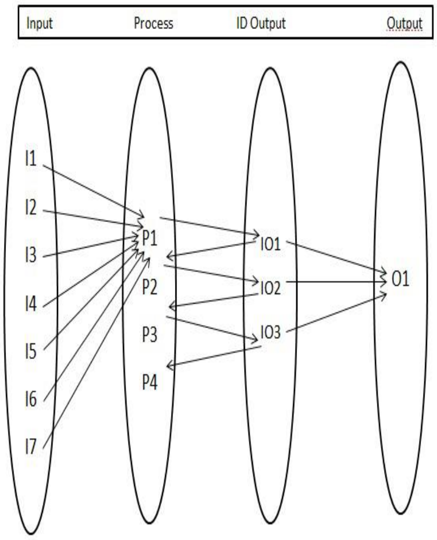


Fig.2 Venn Diagram

- **Process State Diagram:**

Here, process p1, p2, p3 and process P4 are denoted by q1, q2, q3 and q4 respectively.

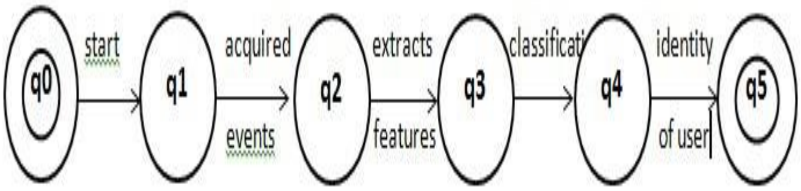


Fig.3 Process State Diagram

- **Time Complexity:**

The total time complexity (T) can be calculated by summing the separate time complexities of all three processes i.e. q1, q2, q3, q4, & q5. Time complexity of process q4 is O(nlsnA) Where n_ls represents number of samples in learning set. n_A represents number of attributes in node.

Therefore, the total time complexity is, T = O(n2)

Here, Process q1,q2,q3,q4 & q5 contains time complexity O(n2), where n represents number of mouse moves. Therefore, final time complexity of each process is O(n2).

V. EXPERIMENTAL RESULTS

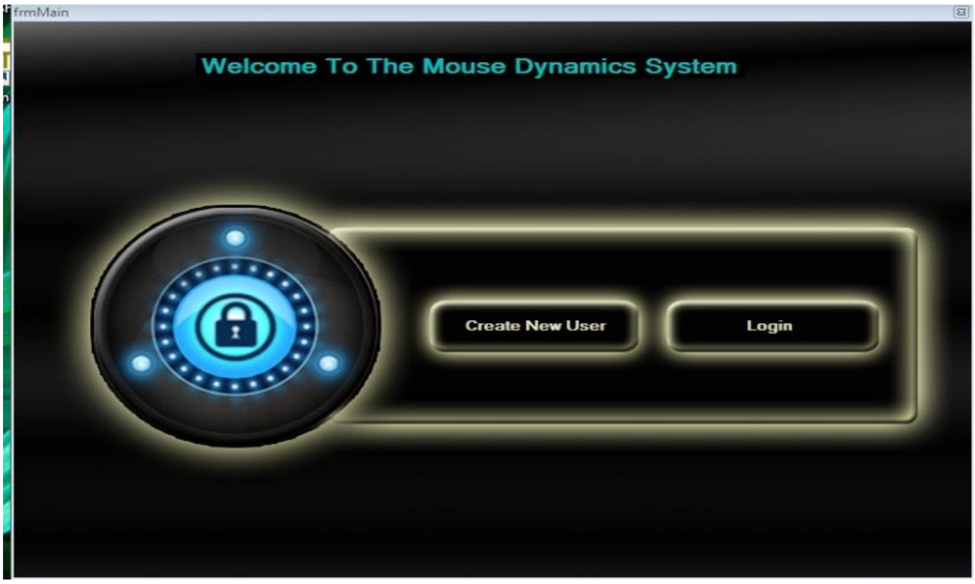
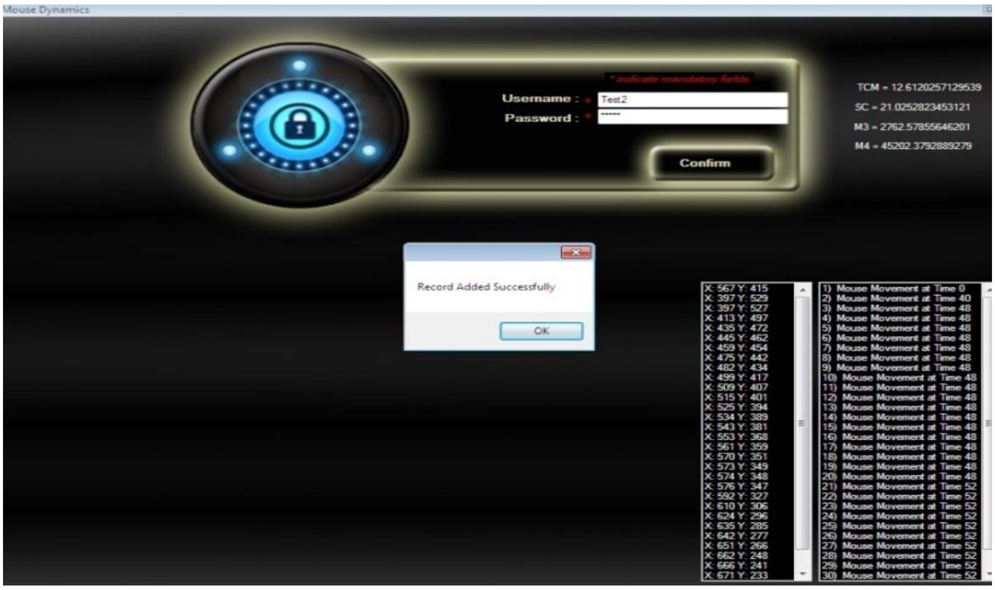


Fig.4 Main Login Form of the system.

Fig. 4 shows Main login form of the system which consist of two button one is for New user creation and another one is for logged into the system.



Username : * Test2
Password : * ******

TCM = 12.6120257129539
SC = 21.0252823453121
M3 = 2762.57855646201
M4 = 45202.3792889279

Record Added Successfully

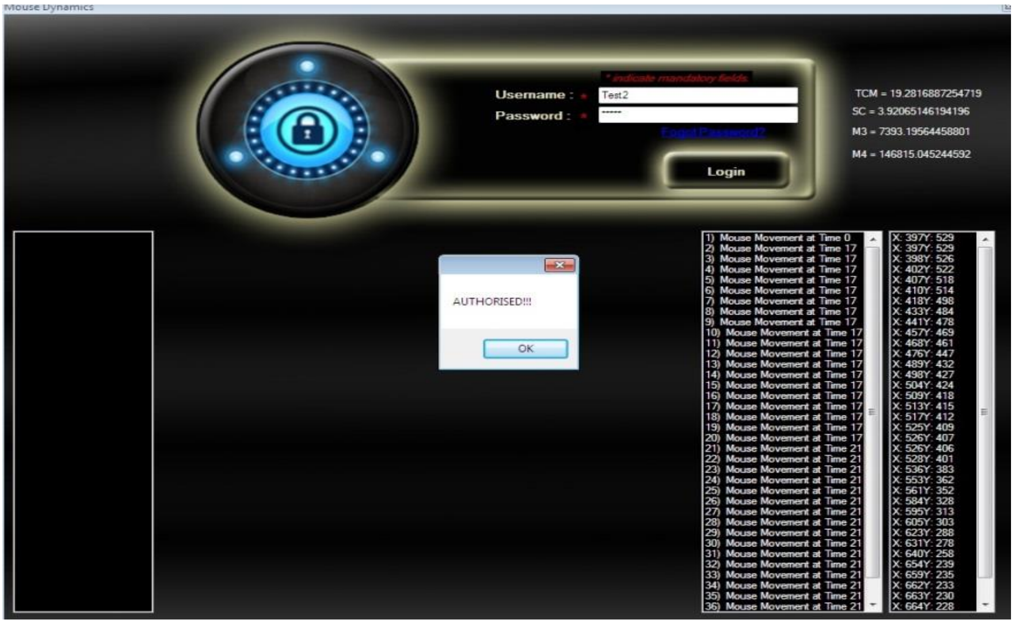
```
X: 567 Y: 415
X: 397 Y: 529
X: 397 Y: 527
X: 413 Y: 497
X: 435 Y: 472
X: 445 Y: 462
X: 459 Y: 454
X: 475 Y: 442
X: 482 Y: 434
X: 499 Y: 417
X: 509 Y: 407
X: 515 Y: 401
X: 525 Y: 394
X: 534 Y: 389
X: 543 Y: 381
X: 553 Y: 368
X: 561 Y: 359
X: 570 Y: 351
X: 573 Y: 349
X: 574 Y: 348
X: 576 Y: 347
X: 592 Y: 327
X: 610 Y: 306
X: 624 Y: 296
X: 635 Y: 285
X: 642 Y: 277
X: 651 Y: 266
X: 662 Y: 248
X: 666 Y: 241
X: 671 Y: 233
```

```
1) Mouse Movement at Time 0
2) Mouse Movement at Time 40
3) Mouse Movement at Time 48
4) Mouse Movement at Time 48
5) Mouse Movement at Time 48
6) Mouse Movement at Time 48
7) Mouse Movement at Time 48
8) Mouse Movement at Time 48
9) Mouse Movement at Time 48
10) Mouse Movement at Time 48
11) Mouse Movement at Time 48
12) Mouse Movement at Time 48
13) Mouse Movement at Time 48
14) Mouse Movement at Time 48
15) Mouse Movement at Time 48
16) Mouse Movement at Time 48
17) Mouse Movement at Time 48
18) Mouse Movement at Time 48
19) Mouse Movement at Time 48
20) Mouse Movement at Time 48
21) Mouse Movement at Time 52
22) Mouse Movement at Time 52
23) Mouse Movement at Time 52
24) Mouse Movement at Time 52
25) Mouse Movement at Time 52
26) Mouse Movement at Time 52
27) Mouse Movement at Time 52
28) Mouse Movement at Time 52
29) Mouse Movement at Time 52
30) Mouse Movement at Time 52
```

Fig.5 Learning Phase of the system.

Fig. 5 shows Learning Phase of the system. In this phase we create a new user and record his/her mouse gesture dynamics and stored in database which will be useful for further verification process.

Fig. 6 shows verification phase of the system. In this system actual verification of user is done by using his/her mouse gesture dynamics. During verification user enter his mouse gesture dynamics which will be compared with database. From that user identity is verified.



* indicate mandatory fields.
Username : * Test2
Password : * ******

```
TCM = 19.2816887254719
SC = 3.92065146194196
M3 = 7393.19564458801
M4 = 146815.045244592
```

AUTHORISED!!!

```
1)  Mouse Movement at Time 0     X: 397Y: 529
2)  Mouse Movement at Time 17    X: 397Y: 529
3)  Mouse Movement at Time 17    X: 398Y: 526
4)  Mouse Movement at Time 17    X: 402Y: 522
5)  Mouse Movement at Time 17    X: 407Y: 518
6)  Mouse Movement at Time 17    X: 410Y: 514
7)  Mouse Movement at Time 17    X: 418Y: 498
8)  Mouse Movement at Time 17    X: 433Y: 484
9)  Mouse Movement at Time 17    X: 441Y: 478
10)  Mouse Movement at Time 17   X: 457Y: 469
11)  Mouse Movement at Time 17   X: 468Y: 461
12)  Mouse Movement at Time 17   X: 476Y: 447
13)  Mouse Movement at Time 17   X: 489Y: 432
14)  Mouse Movement at Time 17   X: 498Y: 427
15)  Mouse Movement at Time 17   X: 504Y: 424
16)  Mouse Movement at Time 17   X: 509Y: 418
17)  Mouse Movement at Time 17   X: 513Y: 415
18)  Mouse Movement at Time 17   X: 517Y: 412
19)  Mouse Movement at Time 17   X: 525Y: 409
20)  Mouse Movement at Time 17   X: 526Y: 407
21)  Mouse Movement at Time 21   X: 526Y: 406
22)  Mouse Movement at Time 21   X: 528Y: 401
23)  Mouse Movement at Time 21   X: 536Y: 383
24)  Mouse Movement at Time 21   X: 553Y: 362
25)  Mouse Movement at Time 21   X: 561Y: 352
26)  Mouse Movement at Time 21   X: 584Y: 328
27)  Mouse Movement at Time 21   X: 595Y: 313
28)  Mouse Movement at Time 21   X: 605Y: 303
29)  Mouse Movement at Time 21   X: 623Y: 288
30)  Mouse Movement at Time 21   X: 631Y: 278
31)  Mouse Movement at Time 21   X: 640Y: 258
32)  Mouse Movement at Time 21   X: 654Y: 239
33)  Mouse Movement at Time 21   X: 659Y: 235
34)  Mouse Movement at Time 21   X: 662Y: 233
35)  Mouse Movement at Time 21   X: 663Y: 230
36)  Mouse Movement at Time 21   X: 664Y: 228
```

Fig.6 Verification Phase of the system.

VI. ACKNOWLEDGMENT

I take this opportunity to express my profound gratitude and ineptness to my guide and PG Co-ordinator Prof. P.N. Kalavadekar, for his personal involvement and constructive criticism provided beyond technical guidance and model direction, important input and consistent consolation all through the span of the venture. His important recommendations were of huge help all through my undertaking work. His insightful feedback kept me attempting to make this venture in a greatly improved manner. Working under him was a greatly learned experience for me.. He has been keen enough for providing me with the invaluable suggestions from time to time. Above all, his keen interest in the project helped me to come out with the best.

VII. CONCLUSION

A novel method for user verification based on mouse activity was introduced in this paper. Common mouse events performed in a GUI environment by the user were collected and a hierarchy of mouse actions was defined based on the raw events. In order to characterize each action, features were extracted. New features were introduced in addition to features. A two-layer verification system was proposed. The system employs a multi-class classifier in its first layer and a decision module in the second one in order to verify the identity of a user.

The proposed method was evaluated using a dataset that was collected from a variety of users and hardware configurations. Furthermore, evaluation showed a significant improvement in the verification accuracy when using the newly introduced features.

REFERENCES

[1] A.A.E. Ahmed, I. Traore, "A new biometric technology based on mouse dynamics", IEEE Transactions on Dependable and Secure Computing (2007)165-179.

[2] L. Breiman, "Random forests", Machine Learning (2001) 5-32.

[3] E. Erzin, Y. Yemez, A.M. Tekalp, A. Eril, H. Erdogan, H. Abut, "Multimodal person recognition for human vehicle interaction", IEEE MultiMedia (2006) 18-31.

[4] P. Grother, E. Tabassi, "Performance of biometric quality measures", IEEE Transactions on Pattern Analysis and Machine Intelligence (2007) 531-543.

[5] Kale, A. Sundaresan, A.N. Rajagopalan, N. Cuntoor, A. Roychowdhury, V. Kruger, R. Chellappa, "Identification of humans using gait", IEEE Transactions on Image Processing (2004) 1163-1173.

[6] A.Kumar, S. Shekhar, "Personal identi_cation using multibiometrics rank-level fusion", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews (2011) 743-752.

[7] M. De Marsico, M. Nappi, D. Riccio, G. Tortora, "NABS: novel approaches for biometric systems", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews (2011) 481-493.

[8] B J Gorad, D.V Kodavade, "User Identity Verification Using Mouse Signature", IOSR Journal of Computer Engineering (2013) 33-36.

[9] Peter Ordal, David Ganzhorn, David Lu, Warren Fong, "`Continuous Identity Verification through Keyboard Biometrics"', Department Of Computer Science (2005) 20-24.

[10] D. Shanmugapriya, G. Padmavathi, "`A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges"', IJCSIS (2009) 115-119.