International Journal of Computer Applications Technology and Research
Volume 4– Issue 4, 253 - 257, 2015, ISSN:- 2319–8656

Online Signature Authentication by Using Mouse Behavior

Jitender Kumar
Bharath University
Chennai ,India

S Goutham
Bharath University
Chennai,India

Amitabh Kumar
Bharath University
Chennai, India

Abstract: Several large-scale parole leakages exposed users to associate unprecedented risk of speech act and abuse of their data. associate inadequacy of password-based authentication mechanisms is turning into a serious concern for the complete data society. carries with it 3 major modules: (1) Mouse–Behavior dynamics Capture, (2) Feature Construction, and (3) coaching or Classification. the primary module serves to make a taking mouse behavior user signs. The second module is employed to extract holistic and procedural options to characterize mouse behavior and to map the raw options into distance-based options by exploitation numerous distance metrics. The third module, within the coaching section, applies neural network on the distance-based feature vectors to reckon the predominant feature elements, then builds the user's profile employing a one-class classifier. within the classification section, it determines the user's identity exploitation the trained classifier within the distance-based feature exploitation NN. A four Digit OTP is generated to the user's email ID. The user are going to be giving the '2' digit OTP and therefore the server are going to be giving balance '2' digit OTP. Users '2' digit OTP is verified by the server and contrariwise.
Keywords: mouse behaviour signatures; Biometric authentication; Verification; Template; String matching; Feature detection

1 INTRODUCTION

The quest for a reliable and convenient security mechanism to authenticate a computer user has existed since the inadequacy of conventional password mechanism was realized, first by the security community, and then gradually by the public.[3] As data are moved from traditional localized computing environments to the new Cloud Computing paradigm (e.g., Box.net and Drop box), the need for better authentication has become more pressing.[1]

Recently, several large-scale password leakages exposed users to an unprecedented risk of disclosure and abuse of their information. These incidents seriously shook public confidence in the security of the current information infrastructure; the inadequacy of password-based authentication mechanisms is becoming a major concern for the entire information society. Of various potential solutions to this problem, Mouse dynamics measures and assesses a user's mouse-behavior characteristics for use as a biometric.[2]

Compared with other biometrics such as face, fingerprint and voice, mouse dynamics is less intrusive, and requires no specialized hardware to capture biometric information. Hence it is suitable for the current Internet environment. When a user tries to log into a computer system, mouse dynamics only requires her to provide the login name and to perform a certain sequence of mouse operations. Extracted behavioral features, based on mouse movements and clicks, are compared to a legitimate user's profile.[4] A match authenticates the user; otherwise her access is denied. Furthermore, a user's mouse-behavior characteristics can be continually analyzed during her subsequent usage of a computer system for identity monitoring or intrusion detection.

2. EXISTING SYSTEM

In the existing system, there many password leakages exposed users to an unprecedented risk of disclosure and misuse their information. These types of password-based authentication mechanisms is becoming a major concern for varieties of Security based applications.[8] Also some attacks namely called, password guessing attacking has become more concern for the users, while accessing the some of the sensitive application like Bank transaction, Train Booking and Online Shopping.[6]

3. PROPOSED SYSTEM

We are implementing the proposed System which is consisting of three major modules: (1) signature dynamics, (2) fluctuate data define , and (3) design to different pattern **.** In the First Module, we'll create a user defining data, and to capture and information data. The second module is used to extract holistic and procedural features to characterize mouse behavior and to map the raw data manipulate by the user by using various distance metrics. The third module, in the defining the different section, applies on taking assign vectors to compute the predominant feature components, and then builds the user's profile using .

4. ARCHITECTURE DIAGRAM

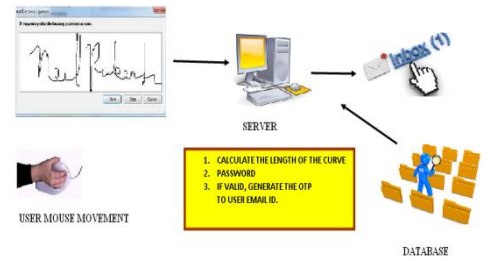

Fig 1. Architecture diagram

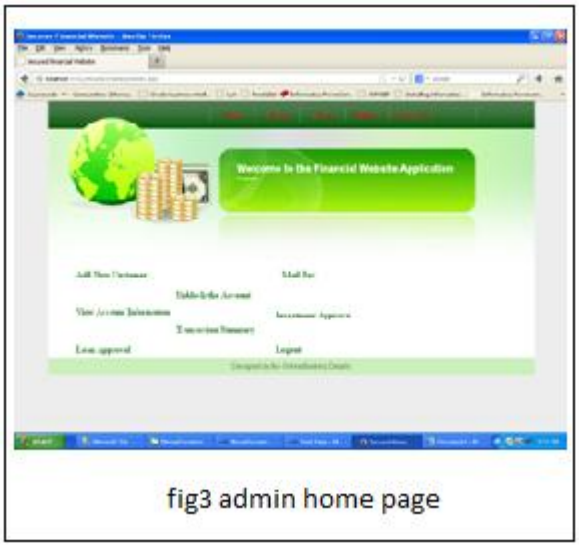

fig3 admin home page

5. MODULES

5.1 CLIENT OF THE NETWORK:

In this module we are implementing the Client interface by which the Client can interact with the Application. To access the Application, the Client want to the register their details with Application Server. They have to provide their information . This information will stored in the database of the Application Server. The User is allowed to the access the application only by their provided Interface.

5.2 SERVER:

The Server will monitor the entire User's information in their database and verify the if required. Also the Server will store the entire User's information in their database. Also the server localize itself. It be the data load in its database. they access the Application. So that the server are to taking by the user guide to server loaded data.

fig 2 admin login

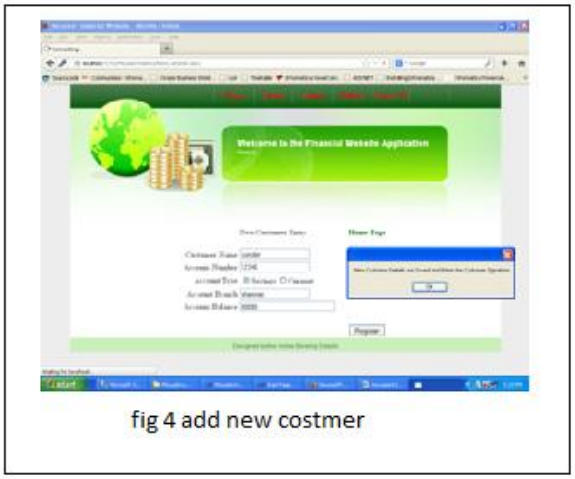

fig 4 add new costmer

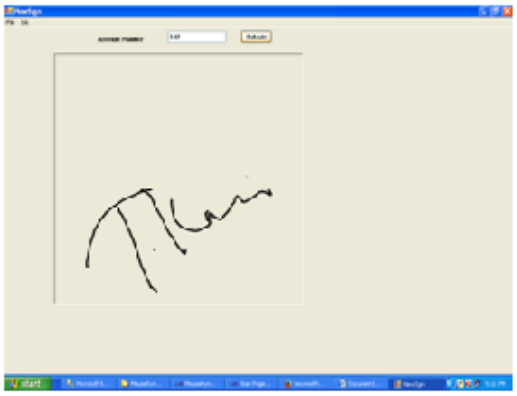

fig 5 costmer sign

fig 7 new user sign

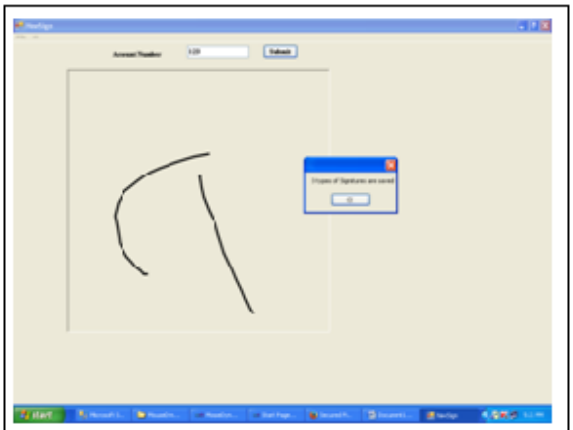

fig 6sign data to server

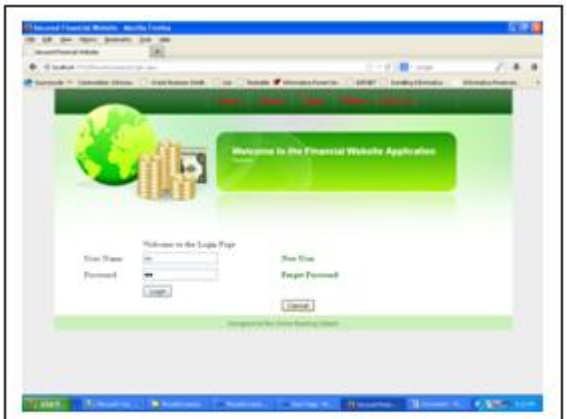

fig 8 user log in

5.3 LEARNING PHASE:

In this phase, the we'll train the system according to identify the User's Signature by using the following modules. (1) signature dynamics, (2) fluctuate data define , and (3) design to different pattern.. The first module serves to create a mouse-operation task, and to capture and user defining data. The second module is used to extract holistic and procedural features to characterize mouse behavior and to map the raw features into distance-based features by using various distance metrics. The third module, in the designing different phase, applies neural network on the data set to vectors compute.

5.4 VERIFICATON PHASE:

In the Verification Phase, the Server will verify the User when they are login into their account. The Servera will provided by the User while login with the Signature provided by the User when they provided during the Training Phase. If the signature is not matched, then the Server will not allow the User to access their account.

fig 9 verification sign

Fig9User authecate

fig10 verifigning user

5.5 CHECK MAIL/OTP VERIFICATION:

Once the User provided their signature correctly, the Server will generate the Session Key using Secure Random Number generation algorithm and send it to the User Email id. Once the User received their session key in their Email id, they have to provide the first '2' digits of the session key and the server will verify the next '2' digits of the session key. Once the Session key is verified by the Server, the User is allowed to access their account.

fig 11token verification

fig 12 user defing

6. CONCLUSION

Mouse dynamics is a newly emerging behavioral biometric, which offers a capability for identifying computer users on the basis of extracting and analyzing mouse click and movement features when users are interacting with a graphical user interface. Many prior studies have demonstrated that mouse dynamics has a rich potential as a biometric for user authentication. In this study, we highlighted the challenges faced by mouse-dynamics-based user authentication, and we developed a simple and efficient approach that can perform the user authentication task in a short time while maintaining high accuracy. Holistic features and procedural features are extracted from the fixed mouse-operation task to accurately characterize a user's unique behavior data. Then distance-based feature construction and parametric eigenspace transformation are applied to obtain the predominant feature components for efficiently representing the original mouse feature space. Finally, a one-class classification technique is used for performing the user authentication task.

7. ACKNOWLEDGMENT

We would like to express our sincere gratitude to our respected Chancellor Dr.J.SUNDEEP AANAND and Managing Director Dr.SWETHA AANAND for their valuable support and encouragement in technological upgrades and novel projects.

We take great pleasure in expressing our sincere thanks to our Pro-chancellor Dr.K.P.THOOYAMANI for backing us in this project. We take great pleasure in expressing our sincere thanks to our Vice-chancellor Dr.M.PONNAVAIKO for backing us in this project.

We thank our Dean Engineering Dr.J.HAMEED HUSSAIN , for providing sufficient facilities for the completion of this project.

We express our sincere thanks to our Dean-Research Dr.KATHIR VISWALINGAM and our Dean-CSE Dr.A.KUMARAVEL and Head of the Department Dr.K.P.KALIYAMURTHIE and Project Co-ordinator Dr.C.NALINI for their kind permission to carry out this project

8. REFERENCES

[1] A. A. E. Ahmed and I. Traore, "Anomaly intrusion detection based on biometrics," in *Proc. IEEE Information Assurance Workshop*, West Point, NY, 2005, pp. 452–453.

[2] Ahmed, A A E & Traore .I (2005) detection computer instruction using behavior biometric proc of 3rd ann conf on privacy security and trust Canada(pp91-98)

[3] Ahn,L v. Blum, M & Langford. J(2004)how lazy cryptography do Al communication of the ACM 47(2),56-60 doi 10 1109/TDSC 2007,70207

[4] Y. Aksari and H. Artuner, "Active authentication by mouse movements," in *Proc. 24th Int. Symp. Computer and Information Science*, Guzelyurt, 2009, pp. 571–574.

[5] S. Bengio and J. Mariethoz, "A statistical significance test for person authentication," in *Proc. Speaker and Language Recognition Workshop*, Toledo, Spain, 2004, pp. 237–244.

[6] D. J. Berndt and J. Clifford, "Using dynamic time warping to find patterns in time series," in *Proc. Advance in Knowledge Discovery in Database: Papers From the 1994 AAAI Workshop*, Jul. 1994, pp. 359–37.

[7] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys*, vol. 44, no. 4, 2012, to be published.

[8] P. Bours and C. J. Fullu, "A login system using mouse dynamics," in *Proc. 5th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing*, Kyoto, Japan, 2009, pp. 1072–1077.