ISSN:0975-9646

Continuous User Authentication Using Keystroke Dynamics

M.Pavithra[1], K.B.Sri Sathya [2]

U.G. Student, Department of Information Technology,
Vivekanandha College Of Engineering For Women,
Tiruchegode, Tamilnadu, India[1]

Assistant Professor, Department of Information Technology,
Vivekanandha College Of Engineering For Women,
Tiruchengode,Tamilnadu, India[2]

Abstract **Behavioural biometric is related to what a person does, or how the person uses the body. Keystroke dynamics (or typing rhythms) is an innovative behavioural biometric technique, refers to a user's habitual typing characteristics. These typing characteristics are believed to be unique among large populations. Keystroke dynamics allows for the design of more robust authentication systems than traditional password. Keystroke dynamics involves three phases namely enrollment phase, verification phase and identification phase. The enrollment phase allows the user to register independently. The verification phase matches the probe sequence with the already stored template in the gallery. The identification phase makes the accessed user as an authenticated user only if the template matches with the reference template otherwise the user gets exit. The user will be accessed only if keystroke timing is matched with the reference templates stored in the database. Accessed user will become the authenticated user.**

Keywords: Keystroke dynamics, Behavioral biometrics, Typing behavior.

1. INTRODUCTION

A biometric is a feature measured from the human body that is distinguishing enough to be used for user authentication. Biometrics include: fingerprints, eye (iris and retina), face, hand, voice, and signature, as well as other biometrics such as gait and smell. A biometrical system is a pattern recognition system that establishes the authenticity either specific physiological characteristics (some particular structural characteristics such as hand size or iris format and colour) or behavioural characteristics (some particular behavioural characteristic such as typing speed or writing pressure) inherent to a user".. Among them one of the techniques is one-shot user authentication but it provide authentication only at the login time. It doesn't suit well at all times. In order to overcome this disadvantage in providing authentication,

One of the popular alternative is to provide continuous authentication from the time of login till logout using biometrics technique. Biometrics generally refers to the identification of human by their physiological characteristics (eg: face, finger prints) and their behavioural characteristics (eg: gait, keystroke dynamics (KD), mouse dynamics (MD)). Generally a single user can communicate with a system using n number of ways. Prior works found many ways to provide continuous user authentication using some input devices (eg: Keyboard, mouse,…) In that mouse dynamics involves fingerprints embedded on the mouse will assume the identity with respect to the finger position. Both KD and MD takes few more minutes to provide continuous and reliable authentication. There exist a chance of an imposter entry at the time of delay.

Due to some problem exist in providing continuous authentication.our paper proposing a new approach of fusing typing behaviour with keystroke dynamics to provide continuous authentication by Short verification time and real-time efficiency. At first we allow the user to type for a while and using some input devices like webcam we monitor the hand movement of the user with respect to the position of the hand and then the database get collected and stored in gallery. In the next stage, if the user gets login means the continuous authentication gets started, the typing probe sequence will be compared with the gallery and as a result of comparison a mean value is found using some graph analysis, in order to match threshold value which is closer to the calculated threshold the user can access.

2. PROPOSED SYSTEM

There are two stages to distinguish between genuine and impostor user.

- Enrollment Stage
- Authentication Stage

At the enrollment stage user sign up their login details such as user name and password which is retyped for several times . The system takes the user dynamic keystrokes ten times for each enrollment, extracts the features, then collected features are stored in the gallery as frames.(i.e) The reference template is stored in a database(gallery). At the authentication stage, the user enters the login details to be matched with user's reference template which is already stored in the database. This phase consists of collecting user dynamic keystrokes, feature extraction, and feature matching with reference template in a database(i.e) the current probe sequence gets compared with the stored gallery sequence. At last the verification process yields two kinds of action: accepted or rejected user access. Dynamic or continuous monitoring of the interaction of users while accessing highly restricted documents or executing tasks in

environments where the user must be alert at all times (for example: Air traffic control), is a ideal scenario for the application of a keystroke authentication system. Keystroke dynamics may be used to detect uncharacteristic typing rhythm (brought on by drowsiness, fatigue etc.) in the user and notify third parties.

The features are extracted from the user's keystroke for formation of template and later for verification. Two features were extracted during the keystroke: keystroke duration and keystroke latency. Keystroke duration is the interval of time that a key is pressed and liberated. Keystroke latency is the interval of time the pressed of between two consecutive keys interval of time to liberate a key and press the key successor, which is known as flight time, dwell time.

- Flight time- The time take between releasing the key and pressing the next key.
- Dwell time-The time taken to press a key.

The extracted features: keystroke duration (duration) e keystroke latency (interval) of the word " Some features for validation and evaluations are Key Stroke Duration, Key Press and Key Release interval, Speed of Typing, The Keystroke Duration is just composed by positive whole values, however, The Keystroke Duration is just composed by positive whole values, however, and the Keystroke Latency can contain positive values as negative. The negative value happens when the user before of liberate the key press the key successor. This usually happens with users that it possesses practice of typing. The Classifier is responsible for deciding the authentication.The user gets accepted or rejected, based on Criterion of Separation (Threshold).The Classifier verifies the similarity between the pattern to be verified and the template of the prototypes, using the Distance Pattern between the vector of feature of the pattern and the prototype.

SCREEN SHOT 1: KEYSTROKE DURATION

System flow diagram and our proposed algorithm are given in Section II,III. Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusion.

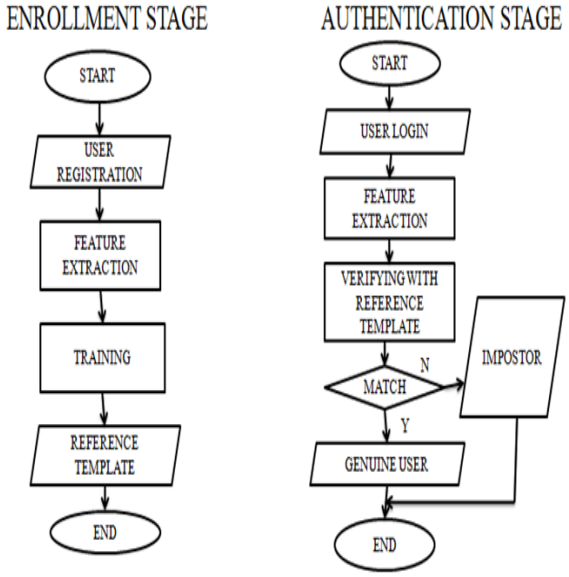

FIG 1: SYSTEM FLOW DIAGRAM

2.1Proposed algorithm

A. Bayesian classification

In case of continuous user authentication there exist feature extraction by fusing keystroke dynamics with typing behaviour. Webcam continuously monitors the user typing manner and identify finger location with respect to the key location..

SCREEN SHOT 2. FEATURE EXTRACTION OF USER

The user hand movements gets extracted using bayesian classification algorithm.In bayesian classification there exist probabilistic learning, incrementalprobabilistic prediction and standard.Statistical method is an method for feature extraction.

This method will verify the user based on statistical data such as mean and standard deviation. After the user feature gets extracted it is stored in the gallery as a prototype sets. For authenticating the user the probe sequence is compared with the gallery sequence and as a result of comparison a mean value is found using bayesian classification algorithm.

$$Stat_{score} = 1/n \sum^{n}_{i=1} e^{-(ti-\mu i)/\sigma i}$$

Where ti is the test feature,

μi and σi are mean and standard deviation of the referance template , "e" is a constant.

STEP 1: . PP (Press-Press) or DD (down-down) or digraph1: time between one key press and the next keypress (P2-P1).

STEP 2: PR (Press-Release) or DU (down-up) or duration: the length of key press (R1-P1).

STEP 3: RP (release-press) or UD (Up-down) or latency: time between key release and the next keypress (P2-R1)

STEP 4: RR (release-release) or UU (up-up) or digraph2: time between key release and the next keyrelease (R2-R1).

STEP 5: The extracted features gives the threshold value.

B- MCMC-Markov chain monte carlo Algorithm

Method for identifying the authenticated user

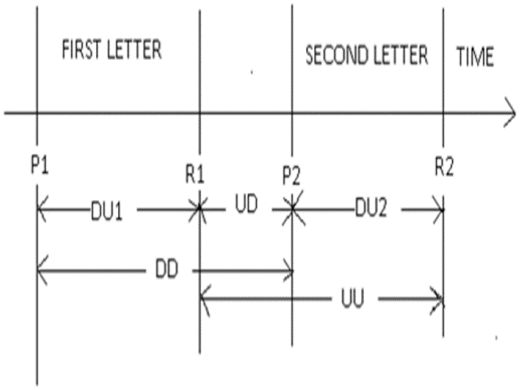

FIG 2: FEATURES OF DYNAMIC KEYSTROKE

$$\text{Final}_{\text{score}} = \sum(Wi * \text{score}^{i})$$

Where Σwi=1 and scorei is the score of i-th method used. Local threshold used in verification system is threshold value between the input data and the model. One way to estimate the value of local threshold is by using the genuine user data, impostor data or a combination of both . If the result of feature matching score < threshold, then the user is identified as an impostor, otherwise the user is identified as an actual user.
The equation used to determine the local threshold value is

$$\Theta = \mu user - \alpha , \sigma user$$

Where Θ - local threshold,
μuser - mean score from user enrollment,
α- a constant factor obtained from the experiment.

Monte Carlo techniques with special emphasis on Markov Chain Monte Carlo (MCMC). Since the latter needs Markov chains with state space that is R or Rd and most researches on Markov chains do not discuss such chains, we have included a short chain process that gives basic definitions and results in this case. Suppose X is a random variable (with known distribution, say with density f) and we are interested in computing the expected value

$$E[g(X)] = \int g(x)\, f(x)dx$$

For a given function g. If the functions f, g are such that the integral in (1) cannot be computed explicitly (as a formula for the indefinite integral may not be available in closed form) then we can do as follows.
Assuming that we can generate a random sample from the distribution of X, generate a random sample of size n: x1, x2 . . . xn, from this distribution and compute. The negative value happens when the user before of liberate the key press the key successor. This usually happens with users that it possesses practice of typing. The Classifier is responsible for deciding the authentication.The user gets accepted or rejected, based on Criterion of Separation (Threshold).The Classifier verifies the similarity between the pattern to be verified and the template of the prototypes, using the Distance Pattern between the vector of feature of the pattern and the prototype.

3. EXPERIMENTAL ANALYSIS

STEP 1: The classifier is responsible for the process of decision of the authentication.
STEP 2: Classifying accepts or it rejects the user, based on criterion of separation (Threshold).
STEP 3: The classifier verifies the similarity between the pattern and the template, using the distance pattern between the vector pattern and the prototype.
Keystroke dynamics has many applications in the computer security arena. One area where the use of a static approach to keystroke dynamics may be particularly appealing is in restricting root level access to the master server hosting a Kerberos key database. Any user accessing the server is prompted to type a few words or a pass phrase in conjunction with his/her username and password. Access is granted if his/her typing pattern matches within a reasonable threshold of the claimed identity. This safeguard is effective as there is usually no remote access allowed to the server, and the only entry point is via console login.
Alternatively, dynamic or continuous monitoring of the interaction of users while accessing highly restricted documents or executing tasks in environments where the user must be \alert" at all times (for example air traffic control), is an ideal scenario for the application of a keystroke authentication system. Keystroke dynamics may be used to detect uncharacteristic typing rhythm (Brought on by drowsiness, fatigue etc.) In the user and notify third parties.

TABLE 1

USER NAME	AVERAGE VALUE PROBE SEQUENCE (in Sec)	AVERAGE VALUE GALLERY (in Sec)	THRESHOLD VALUE	THRESHOLD ABOVE /BELOW	ACCESS /EXIT
SAM	5.01	4.05	4.53	A	E
TRUDY	3.20	3.15	3.21	CM	A
MAX	3.99	2.85	3.42	A	E
BILLY	2.83	2.00	2.41	B	E
JOHN	4.33	4.18	4.25	A	E

4. CONCLUSION

With the help of typing behaviour biometrics each and every individual user's identity can be continuously monitored with the help of web cam for providing continuous authentication. A multi – phase multi session and multi model (visual, audio, key-stroke timing can be collected here). When we leave our finger print when touching with our finger is called cognitive fingerprint, we will continue to enroll subjects in to unconstrainte typing speed we will perform keyboard based behaviour. In this mouse dynamics there are more limitations, in order to overcome this we are fusing the typing behaviour with keystroke dynamics. Finally this can be done during the registration phase then in the training phase users can be given with a static and free text paragraph to monitor their typing behaviour. The collected data are stored in the gallery. When the user gets login for the next time the current probe sequence gets compared with the stored gallery to fetch the common features. Then the accessed user will become an authenticated user only when the threshold value is obtained or else the user gets rejected.

REFERENCES

[1] Thomas J. Alexandre. Biometrics on smartcards: an approach to keyboard behavioral signature. In Second Smart Card Research & Advanced Applications Conference, 1996.

[2] Saleh Bleha, Charles Slivinsky, and Bassam Hussein. Computer-access security systems using keystroke dynamics. IEEE Transactions on Pattern Analysis and Machine Intelligence, PAMI-12(12):1217-1222, December 1990.

[3] Marcus Brown and Samuel Joe Rogers. User identification via keystroke characteristics of typed names using neural networks. International Journal of Man-Machine Studies, 39(6):999-1014, 1993.

[4] R. Chellappa, C. L. Wilson, and S. Sirohey. Human and machine recognition of human face images: A survey. In Proceeding of the IEEE, volume 83, pages 705-741, 1995.

[5] Edward Cureton. Factor analysis, an applied approach. Erlbaum Associates, Hillsdale, N.J., 1983.

[6] John G. Daugman. High confidence visual recognition of persons by a test of statistical independence. IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(11), November 1993.

[7] Geoger R. Doddington. Speaker recognition identifying people by their voices. Proceedings of the IEEE, 73(11):1651-1664, 1985.

[8] Richard Duda. Pattern classification and scene analysis. John Wiley & Sons, New York, 1973.

[9] R. Gaines, W. Lisowski, S. Press, and N. Shapiro. Authentication by keystroke timing: some preliminary results. Rand Report R-256-NSF. Rand Corporation,1980.

[10] Gentner. Keystroke timing in transcription typing. Aspects of skilled type writing, pages 95-120, 199