Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm

Rohit A. Patil
Department of Electronics & Tele-Communication Engineering
K.I.T's College of Engineering, Kolhapur, Maharashtra, 416234, India

Amar L. Renke
Department of Electronics & Tele-Communication Engineering
K.I.T's College of Engineering, Kolhapur, Maharashtra, 416234, India

ABSTRACT

In this era computer security is an important issue now a days because these are used everywhere to store & process the sensitive data. Specially those used in e-banking, e-commerce, virtual offices, e-learning, distributed, computing & various services over the internet. Using Keystroke dynamics authentication technology can be secured by password from various attacks. This technique is based on human behavior to type their password. Here analysis is done using human behavior with their typing pattern. As keystroke dynamics does not require any hardware, no extra hardware is used. Only software based technology is required for password protection. The result provides emphasis with pleasure security that growing in demand in web-based application.

Keywords

Biometrics**,** Keystroke dynamics, typing, authentication & identification, feature.

1. INTRODUCTION

Whenever we login onto the computer systems the combination of username & password is required to authenticate the users. This ensures that the users have access to their own data. But there are some weakness of using this scheme like username is not a secret and an imposter who wants to imitate a user can simply guess a password. Also due to simplicity of passwords they are vulnerable to various social engineering attacks like phishing attacks, brute force attack etc.

Biometric authentication is the most secure and convenient authentication tool. It can't be borrowed; stolen, forgotten and forging one is practically not easy. Biometrics measure is individual physiological or behavioural characteristics to recognize their identity.

The security process uses three different types of authentication:

- Something you know password, Personal Identification Number, or piece of information.
- Something you have a card key number, smart card, or token
- Something you are as a biometric.

Common physical biometrics authentication include finger-prints; hand or palm geometry; and retina, IRIS, or facial recognition characteristics. Behavioral characters include signature, voice, typing rhythm, and speaking style of this class of biometrics, technologies for signature and voice are most developed. Mouse dynamics is also used for security purpose but recognize of keyboard activities is much more practical now a days. Keystroke dynamics is a behavioral biometric characteristic based on the assumption that different people type in a unique manner. Neurophysiologic factors make written signatures distinctive as per person. These factors are also expected to make typing characteristics unique as per person. The idea behind keystroke dynamics authentication appeared in the twentieth century when telegraph operators could authenticate each other based on their distinctive patterns when keying messages on telegraph lines. Keystroke dynamics is also known with as keyboard dynamics, keystroke analysis, typing biometrics and typing rhythms.

Although Physiological biometrics is considered to be more robust and secure, they are expensive to use because specialized hardware is needed to detect the features. On the other hand, behavioral characteristics are cheaper than physiological characteristics because additional hardware is not required. Thus behavioral characteristics are easy to reveal but hard to forge. Because of the variability over time, most of the biometric systems need to be designed to be more dynamic and accept some degree of instability.

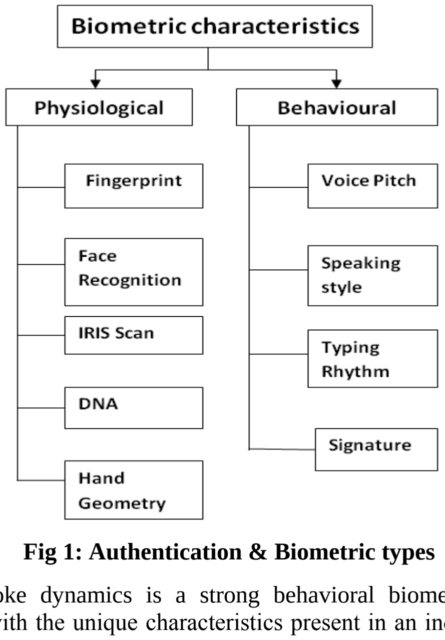


Fig 1: Authentication & Biometric types

Keystroke dynamics is a strong behavioral biometric that deals with the unique characteristics present in an individual' typing rhythm i.e. when each key was pressed and when it was released as a person types at computer keyboard. How we type on a keyboard is known as keystroke dynamics, which most often use timing information to decide who is typing. By measuring when a key is pressed and when it is released it is possible to detect pattern that can be used to authenticate the people. Authentication can be categorized into three main groups: something a person knows (Password, PIN), something a person possesses (e.g. token), and something you are (Biometric based authentication). The merit of using this behavioral biometrics is that no special equipment is required. It is user friendly, non-invasive and the typing rhythm of the person can't be lost or forgotten. If stolen or lost, the new one can be easily generated.

2. RELATED WORK

The use of keyboards to measure the keystroke dynamics of individuals for identification was first suggested by *Spillane,* R.J. *in* 1975. Keystroke dynamics deals with the unique characteristics that are present in an individual‘s typing rhythm i.e. when each key is pressed and released as a person types at computer keyboard.

Hosseinzadeh [2008, 14] proposed a novel up–up keystroke latency feature and compared its performance with existing features using a GMM based verification system. The results proved that the UUKL feature significantly outperformed the commonly used key hold-down time and down– down keystroke latency features. Balagani et al. [2011, 22] classified the keystroke feature vectors as homogeneous, heterogeneous or aggregate and concluded that a heterogeneous vector has higher discriminability than an aggregate vector, especially when the reference text is so short. However, the length of the text increases, the difference in the discriminability between the heterogeneous and aggregate vectors tends to decrease.

In order to authenticate a user's identity using behavioral biometrics Purgason [2012, 23] validated a method of collecting and analyzing behavioral biometric data. The method used the timing information (time to transition from one finger to another) while typing and feed forward neural network was used for the analysis purpose. Chang [2012, 24] used the keystroke features such as Dwell time, flight time & inter key time to generate a long-lived private key based on password keystroke features and neural networks. This key was generated dynamically rather than statically stored in a storage unit.

Schclar et. al [2012, 26] incorporated keystroke dwell time for user authentication based on the keystroke dynamics of the password entry. Rather than using the complete dataset for training only the keystroke dynamics of a small subset of users, referred to as representatives, was used along with the password entry keystroke dynamics of the examined user. By doing this the possibility of over fitting gets reduced, while allowing scalability to a high volume of users. Bours [2012, 28] measured mean and standard deviation of feature values such as key up, key down and latency to evaluate the performance of biometric authentication system.

Ahmed A. Ahmed [2013,31] presented a new approach for the free text analysis of keystrokes that combines the analysis of monographs and digraphs, and uses ANN to predict missing digraphs based on the relation between the monitored keystrokes. Rahman et. al [2013, 32] presented a Snoop-Forge-Replay attacks on continuous verification with keystrokes using key hold, key interval and key press latencies that synthesizes keystroke forgeries using timing information stolen from victim users.

Li F. et. al [2013, 33] described a continuation authentication technique for mobile devices utilizing behavior profiling. For this purpose a combination of rule based classifier, a dynamic profiling technique and a smoothing function was used. Wangsuk [2013, 34] showed how trajectory dissimilarity technique was used to verify user's typing behavior on a username as an additional authentication token. Hold time, inter key time and latency time were used as keystroke features for this purpose. Most of the pattern algorithms are probabilistic in nature. The probabilistic algorithms output a probability of the instance being described by the given label rather than simply output a "best" label. So some of the researchers used the probabilistic algorithms partially or completely to avoid the problem of error propagation by ignoring the outputs with low confidence values.

3. PROPOSED METHOD

Keystroke dynamics typically includes the analysis of characteristics such as duration of a key press or group of keys and the latency between consecutive keys i.e. time elapsed from one key to a subsequent key.

Generally all keystroke-dynamics evaluations involve (1) recruiting subjects for data collection & presenting them with a typing task, (2) recording keystroke-timing information, (3) feature extraction suitable for training and testing a classifier, (4) training the classifier using one portion of the typing data and (5) testing the classifier performance using another portion of typing data. Researchers make a lot of choices in each of the phase. In this research paper, some of different choices that researchers have made regarding each of the five evaluation steps noted above is described.

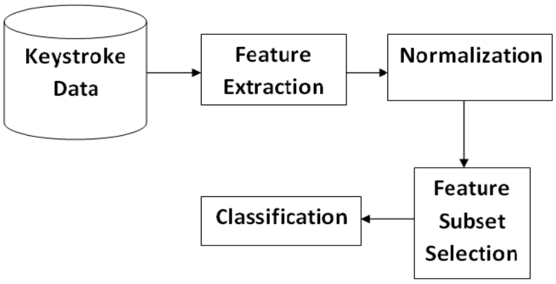


Fig 2: Steps involved in Key-rhythm Authentication

Before discussing the approaches taken by researchers in keystroke dynamics, the features that can be extracted from the typing data is described here. While typing, the computer can record the time at which key is pressed (dwell time), for how long the key is pressed and latency between consecutives keys i.e. time elapsed from one key to a subsequent key. The time measured between key up and the key down is called Flight time. Thus from the raw data, three timing features can be extracted are press-to-press (PP), release-to-release (RR) and release-to-press (RP).

Other timing information like time it takes to write a word, digraph (two letters) or tri-graph (three letters) can also be extracted. Diagraph comes under Press-to-Press category. Digraphs contain two consecutive keystrokes, whereas Tri-graphs contain three; this continues for any number of combinations, which creates n-graphs. Using this terminology, the word 'search' would have three digraphs ('se', 'ar', 'ch') and two tri-graphs ('sea', 'rch'). The recorded keystroke timing data is then processed to get the simple patterns derived from statistics of the features such as mean and standard deviations to complex pattern recognition algorithm to classify the typists. All these information can be stored while a user is typing the data. Figure 3 shows the definition of different parameters.

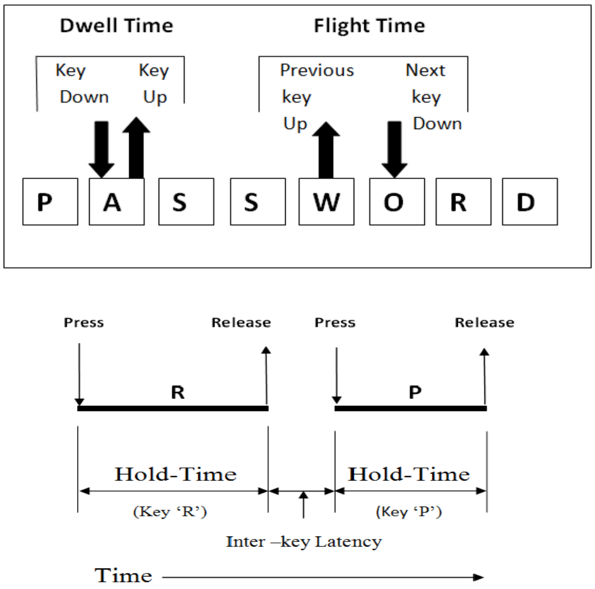


Fig 3: Dwell time, Flight time, Inter-key latency

3.1 Traditional Benchmarks or Matrices for Keystroke Dynamics

Many classifiers are available for Keystroke dynamics till date, so these models are validated based on security metrics like False Acceptance rate (FAR), False Rejection rate (FRR) and Equal error rate (EER).

1. FAR is the ratio of number of false matches divided by total number of fraud match attempts. Thus FAR gives the number of frauds or imposters who are inaccurately allowed as genuine users.

2. FRR is the ratio of number of false rejections divided by total number of genuine match attempts. Thus FRR gives the number of genuine users who are rejected from using the system. Higher FRR is preferred in high security systems.

3. EER is the ratio of FAR divided by FRR. Lower value of EER signifies a better system

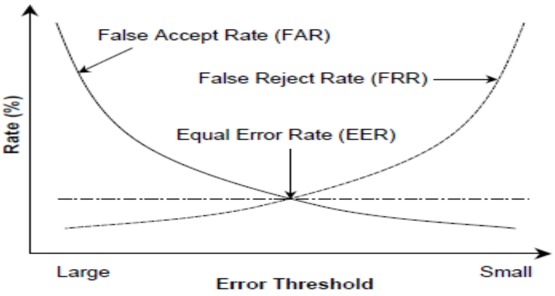


Fig 4: A general relationship between FAR, FRR &EER.

3.2 Feature Subset Selection

The next step where lots of research is going on is the Feature Subset Selection (FSS). Feature selection is a process that selects a subset of original features. FSS is very useful in data mining, machine learning because FSS reduces the number of features, removes the irrelevant, redundant and noisy data and thus speed up or improve the accuracy and results obtained from various algorithms. A typical FSS consists of 4 basic steps [1997, 2]. Subset generation procedure is a search procedure that produces candidate feature subsets for evaluation based on evaluation criterion [1998, 4]. An evaluation function is used to evaluate the subset under examination, stopping criterion is used to decide when to stop and validation procedure is used to check whether the subset is valid.

FSS algorithms are categorized into three categories and this categorization is done on the basis of different evaluation criteria namely (a) the filter model, (b) the wrapper model [1997, 2] and (c) hybrid model. In all the categories, algorithms can be further differentiated by how the space of feature subsets is explored and the exact nature of their evaluation function.

3.2.1. The Filter Model

It requires general characteristics of the data to evaluate and select the feature subsets without involving any learning algorithm. Sometimes, the right subset of features are not selected or filter method failed to select the right subset of features if the used criterion digress from the one used for training the learning machine. Another drawback of filter model is the filter approach is that it may also fail to find a feature subset that would jointly maximize the criterion, since most of the filters estimate the significance of each feature just by means of evaluating one feature at a time [2009, 13]. Thus, the performance of the learning models is degraded.

3.2.2. The Wrapper Model

It requires a learning algorithm and uses its execution as the evaluation criterion. By taking prediction accuracy into consideration, Wrappers model can reach better results than others. Unfortunately, Wrapper models are less general and are computationally expensive than filter model because they need more computational resources and use specific learning algorithm [1999, 5]. The main advantage of filter approach is that filters execute many times faster than wrappers, and therefore stand a much better prospect of scaling to databases with a large number of features than wrappers do. Filters also do not require re-execution for different learning algorithms. Thus Filters can provide the same benefits for learning as wrappers do.

3.2.3 The Hybrid Model

It takes the advantage of filter as well as wrapper model by exploiting their different evaluation criteria in different search stages. Some examples of the embedded methods are decision tree learners, such as ID3, C4.5, and SVM and so on. The hybrid methods are more efficient because they combine the advantages of wrapper and filter approach by keep away for retraining a predictor from scratch for every feature subset investigated. However, they are much complex and limited to a specific learning machine [2007, 12, 13]. ElAlami [2009, 16] used a filter model for feature subset selection based on GA and found that the dimensionality of 2 databases Monk1's database and Car Evaluation database has been reduced to 50% and 33% respectively.

Bermejo et. al [2011, 25] proposed a hybrid algorithm "GRASP" based on meta-heuristic. The main goal of using the hybrid approaches was to speed up the FSS process, by reducing the number of wrapper evaluations to carry out. Bidgoli [2012, 29] proposed a hybrid feature selection model that utilizes both the feature space and sample domain to improve the process of FS and uses a combination of Chi squared with consistency attribute evaluation methods to seek reliable features. The experiments showed that this hybrid FSS method outperforms other feature selection methods.

Bermejo et. Al [2014, 35] presented the incremental wrapper feature subset selection with Naïve Bayes classifier and found that their algorithm's performance is better than filter based FSS.

3.3 Classification

After the feature extraction and feature selection phase, the next phase is the classification phase where the matching between the template stored and sample provided during the session takes place. There are various methods used for classification. These classification algorithms are categorized into four major categories [2012, 27]: Statistical Algorithms, Artificial Neural Networks, Pattern Recognition and learning based algorithms, Search heuristics and combination of algorithms. In statistical approaches, the computation of mean, standard deviation of the features in the template is done. Distance techniques like Euclidean distance, weighted Euclidean distance, Manhattan distance etc. are used for comparing the training dataset with testing dataset. It is not necessary that the data collected for keystroke authentication and verification is linear, thus sometimes these linear statistical approaches do not provide good results. So, there is a need of some approaches that use probabilistic data rather than deterministic data. Also another statistical techniques like decision trees, Bayes classification (based on posterior probability) etc can be used for classification. Sheng et.al [2005, 9] uses Monte carlo approach for keystroke dynamics and thus achieved average false reject rate 9.62% and the average accept rate 0.88%. Another approach that is used for classification purpose is use of Artificial Neural Network. Chang [2012, 24] used ANN technique and keystroke features to dynamically generate a long-lived private key and found that rather if the password is revealed, the probability of exposing the private key is reduced. The advantage of this approach is that this approach can handle many parameters and thus giving good results.

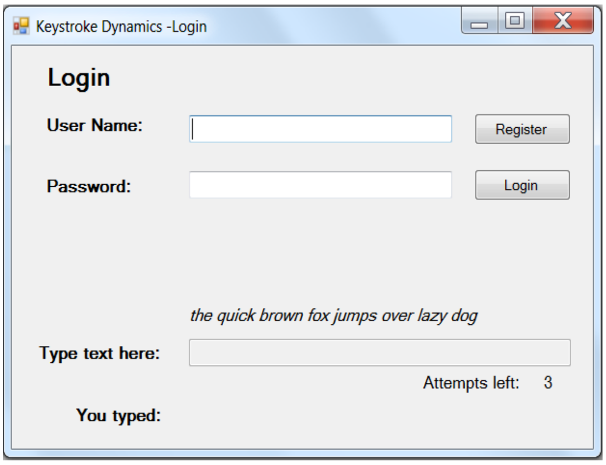
Pattern recognition is defined as an act of taking raw data (patterns, objects) and classifying them into different categories based on algorithms. Pattern recognition includes machine-learning algorithms, various classification techniques like Nearest Neighbor rule, Bayes classifier, and Support Vector machine, clustering techniques like Kmeans etc. Hyoung-joo Lee [2007, 26] used SVM and it has been observed that retraining improves the authentication performance and that learning vector quantization for novelty detection outperforms other widely used novelty detectors. Fourth approach generally includes evolutionary algorithms like genetic algorithm, Ant colony optimization, Particle swarm optimization etc. The advantage of using these evolutionary techniques is that they can handle large databases.

4. PROPOSED WORK

The proposed method is based on to calculate the pressing time, dwell time and total time of password. This work is analyzed on laptop keyboard. The statistical method is used to measure the mean time and average time. The Microsoft Visual Studio 2010 Ultimate IDE is an open-source integrated development environment. The Microsoft Visual Studio 2010 Ultimate IDE is written in VB C and exe.file runs everywhere including Windows, Mac OS, Linux, and Solaris.

4.1 Login Process

When a user starts the application, a Keystroke Dynamics-Login activity is launched where a registered user submits his User Name as well as Password if user name and password are matched then one message is displayed i.e. Hello User Name!..Next step is type the given statement or type the statement when you are typed at the time of registration for authenticates you. When user is not register can register him by clicking on Register button.



the quick brown fox jumps over lazy dog

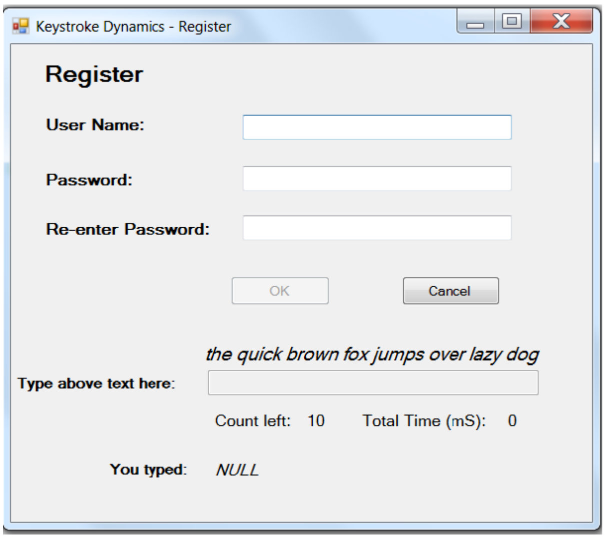
Attempts left: 3

Fig 5: Keystroke Dynamics Login Process

After entering the password and clicking on Login button, if the password is not found in the database an error message is displayed.

4.2 New User Registration

New user clicks on Register button, then registration activity is displayed where user is asked to enter User Name, Password and Re-enter Password if these two password and re-enter password are matched then Ok button is enabled otherwise disabled. When you are click on Ok button you should complete a task such as type a sentence given below 10 times for save data in data base see Figure. While the user is typing on keyboard for submitting a sample, factors like dwell time (time interval between consecutive key press and key release), flight time (time interval between consecutive key release and key press), total time and pressing time of characters key is calculated and When you are typed the sentence 10 times the values are stored in the respective rows. Every user is identified by typing the sentence at time of registration. Hence values calculate while typing the sentence is stored in database along with password, time interval calculated and timestamp.



the quick brown fox jumps over lazy dog

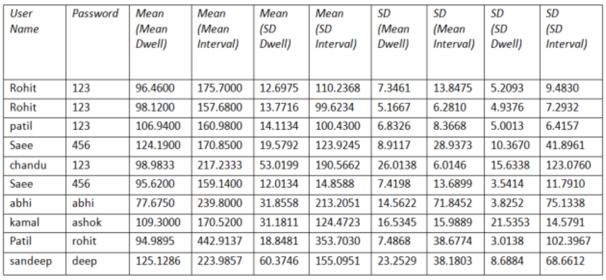
Count left: 10 Total Time (mS): 0

You typed: NULL

Fig 6: keystroke Dynamics Registration Process

4.3 Storage Database

Figure shows the image of the rows of the login name which will be used as an example for description. As from the image it can be seen that ten samples of the user with User name and password are present. Total time taken in milliseconds by the user to enter statement stored in database.



User Name	Password	Mean (Mean Dwell)	Mean (Mean Interval)	Mean (SD Dwell)	Mean (SD Interval)	SD (Mean Dwell)	SD (Mean Interval)	SD (SD Dwell)	SD (SD Interval)
Rohit	123	96.4600	175.7000	12.6975	110.2368	7.3461	13.8475	5.2093	9.4830
Rohit	123	98.1200	157.6800	13.7716	99.6234	5.1667	6.2810	4.9376	7.2932
patil	123	106.9400	160.9800	14.1134	100.4300	6.8326	8.3668	5.0013	6.4157
Saee	456	124.1900	170.8500	19.5792	123.9245	8.9117	28.9373	10.3670	41.8961
chandu	123	98.9833	217.2333	53.0199	190.5662	26.0138	6.0146	15.6338	123.0760
Saee	456	95.6200	159.1400	12.0134	14.8588	7.4198	13.6899	3.5414	11.7910
abhi	abhi	77.6750	239.8000	31.8558	213.2051	14.5622	71.8452	3.8252	75.1338
kamal	ashok	109.3000	170.5200	31.1811	124.4723	16.5345	15.9889	21.5353	14.5791
Patil	rohit	94.9895	442.9137	18.8481	353.7030	7.4868	38.6774	3.0138	102.3967
sandeep	deep	125.1286	223.9857	60.3746	155.0951	23.2529	38.1803	8.6884	68.6612

Fig 7: Keystroke Dynamics Database

4.4 Matching Process

Proposed algorithm finds the difference between actual value stored in database and current value of login user. Here, threshold value is assumed to compare with time. These threshold values increase the efficiency of result. This value is compared to the current time of login user if the value will be matched according to the threshold value the person is accepted or called authenticated user. This value will be changed according to analysis. Using this output FAR (False accept ratio) and FRR (false Reject Ratio) values are calculated.

5. APPLICATION AREA

Computer's security is very important issue as lots of transactions are done using computers. A smart card is required to gain access to a protected resource but a biometric security system requires physiological or behavioral characteristics to gain the access of the computer systems. Thus biometrics represents an additional level of security because it physically proves an individual's identity. Keystroke Dynamics is one of the behavioral biometrics that has been researched in past but it has not been applied yet much in security field. Due to static and dynamic categorization of keystroke dynamics, a wide variety of other applications can also benefit from such authentication schemes. Some of the application areas where KD could provide security are cyber security against online attacks, to prevent practice by impostors and to avoid the spyware attacks. KD systems are also used in time attendance system.

Trustable Keystroke-Based Authentication known as TOKEN [2010, 20] is used for Web-Based Applications on Smart phones. Establishment of the identity of a user requesting information via Smart phones is a prerequisite for secure systems in such scenarios. Keystroke-based user identification has been successfully deployed on production level mobile devices to ease the risks associated with new credentials based authentication mechanism.

Keystroke dynamics is also useful in providing the cloud security. For any application residing in the cloud, security is an important concern and within the scope of security, user authentication is a critical factor. Tera-data, Big-data etc. is most useful for organizations in terms of customers' security, relationship, and business intelligence. By applying keyboard based authentication their existing data safety mechanism becomes many times more secure and then only they can assure their customers that their data is well invested. Lots of commercial solutions have been developed which are offering authentication of user identity. Psylock is a German company that develops the security solutions based on keystroke dynamics for implementations on different platforms from MS Windows login, to web login, to Citrix and VPN integration.

BehavioSec is a Swedish company that develops IT security systems based on the integration of keystroke dynamics and mouse dynamics.

A Dutch company named ID Control also offers affordable authentication solutions, some of which use keystroke dynamics.

Scout Analytics also focuses on behavioral biometrics i.e. keystroke dynamics in detecting the clients and preventing the users from sharing account with multiple partners.

6. CONCLUSION & RECOMMENDATIONS

The paper emphasizes on the importance of keystroke dynamics for desktop, laptop etc. The implementation of keystroke dynamics on desktop is cost effective and compatible as integration of external hardware is not required. The conclusion of the paper is based on comparing the data stored of a user with the login input for authentication. Keystroke Dynamics is a two factor security biometric security, hence, for a successful login, firstly password should be known and secondly, typing rhythm should be match .In human behavior security system of any keypad requires making a programming. In another method of biometrics hardware is required but human behavior method we can generate a secure key to protect the password. This key is generating according to human behavior for e.g. when user give password he use his typing speed to fill the password. The key is generated by programming to calculate different times in millisecond. The main drawback of this project is different types of keyboard. But if more work is done on this project and find the solution for that and can be better advancement of this keystroke dynamics. If all keyboards of same style, same features are used then it gives better results.

As it is clear from the literature survey that there are certain features that are very useful. Thus future work is to find other features or combination of features that would be helpful in increasing accuracy of the biometric systems. One of the factors, which affect the performance, is effective size and the type of passwords. What could be the size and type of passwords is one of the area where more investigations are required, because the problem with large passwords is that they are difficult to remember and if shorter passwords are used then they can be stolen or recognized easily. We have mentioned 2 authentication approaches: Static and continuous. Which approach is better and the use of approach depends upon type of application. The raw user patterns contain noise and many outliers because of the user's typing inconsistencies, which accordingly could result in poor detection accuracy. Thus pre-processing is a necessary step in keystroke dynamics and must not be done manually.

The major problem in this field is lack of standardized protocol for keystroke system evaluation that would be helpful in providing accurate results and doing the comparisons. (Most of FAR, FRR, EER fields are not specified in table 1).The field of keystroke dynamics is still an emerging field, where most of the challenges need to be overcome in order for it to become an effective biometric.

7. REFERENCES

[1] B.Miller, "Vital signs of identity" IEEE spectrum, 1994, pp 22 30.

[2] M. Dash and H. Liu, "Feature Selection for Classification", inIntelligent Data Analysis 1, 1997, pp. 131-156.

[3] Ron Kohavi and George H. John, "Wrappers for Feature SubsetSelection", in Artificial Intelligence, 1997, pp. 273-324.

[4] Huan Liu and Hiroshi Motoda,"Feature Selection for Knowledge Discovery and Data Mining", Boston: Kluwer Academic, 1998.

[5] M. Hall, Correlation based feature selection for machine learning, Doctoral dissertation, University of Waikato, 1999.

[6] CENELEC. European Standard EN 50133-1: Alarm systems access ontrol systems for use in security applications. Part 1: System requirements. European Committee for Electro technical Standardization, 2002.

[7] Enzhe Yu and Sungzoon Cho, "Keystroke dynamics identity verification-its problems and practical solutions", in Computers & Security, vol 23, 2004, pp 428-440.

[8] Huan Liu and Lei Yu, "Toward Integrating Feature SelectionAlgorithms for Classification and Clustering" IEEE Transactions on knowledge and data engineering, vol. 17, no. 4, 2005, pp 491-502.

[9] Yong Sheng, Vir V. Phoha and Steven M. Rovnyak ," A Parallel Decision Tree-Based Method for User Authentication Based on Keystroke Patterns", IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics, vol. 35, No. 4, 2005, pp 826-833.

[10] William E. Burr, Donna F. Dodson and W. Timothy Polk, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology (NIST), 2006, pp 800-63.

[11] Lee Hyoung-joo and Cho Sungzoon ,"Retraining a keystrokedynamics-based authenticator with impostor patterns", in Computers & Security, vol 26 , 2007, pp 300-310.

[12] Ozge Uncu , I.B. Turksen, " A novel feature selection approach: Combining feature wrappers and filters", in Information Sciences 177, 2007, pp 449-466.

[13] Jinjie Huang, Yunze Cai and Xiaoming Xu, "A hybrid genetic algorithm for feature selection wrapper based on mutual information." In Pattern Recognition Letters 28, 2007, pp 1825–1844.

[14] Danoush Hosseinzadeh and Sridhar Krishnan," Gaussian Mixture Modeling of Keystroke Patterns for Biometric Applications", IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 38, no. 6, 2008,pp 816-826.

[15] K. Killourhy and R. Maxion ," The Effect of Clock Resolution on Keystroke Dynamics," in Recent Advances in Intrusion Detection, vol 5230 , 2008, pp 331–350.

[16] M.E ElAlami ,"A filter model for feature subset selection based on genetic algorithm", in Knowledge-Based Systems 22, 2009, pp 356–362.

[17] Marcus Karnan, M. Akila and A. Kalamani , " Feature subset selection in keystroke dynamics using ant colony optimization" in Journal of Engineering and Technology Research ,vol.1 (5), 2009, pp 072-080.

[18] Kevin S. Killourhy and Roy A. Maxion, "Comparing Anomaly Detectors for Keystroke Dynamics," Proceedings of the 39th Annual International Conference on Dependable Systems and Networks , pp 125- 134, 2009.

[19] P. Khanna and M. Sasikumar, " Recognising Emotions from Keyboard Stroke Pattern", International Journal of Computer Applications, vol 11(9), 2010.

[20] Mohammad Nauman and Tamleek Ali, "TOKEN: TrustableKeystroke-Based Authentication for Web-Based Applications onSmartphones," Springer-Verlag Berlin Heidelberg, 2010, pp 286-297.

[21] M. Karnan, M. Akila and N. Krishnaraj," Biometric personal Authentication using keystroke dynamics: A review,"in Applied Soft Computing , vol 11, 2011, pp 1565–1573.

[22] Kiran S. Balagani , Vir V. Phoha , Asok Ray and Shashi Phoha ," On the discriminability of keystroke feature vectors used in fixed text keystroke authentication", in Pattern Recognition Letters 32, 2011, pp 1070–1080.

[23] Benjamin Purgason and David Hibler, "Security through Behavioural Biometrics and Artificial Intelligence", Procedia Computer Science, vol 12, 2012, pp 398 – 403.

[24] Ting-Yi Chang, "Dynamically generate a long-lived private key based on password keystroke features and neural network," Information Sciences 211, pp 36–47, 2012.

[25] Pablo Bermejo, Jose A. Gamez and Jose M. Puerta , " A GRASPalgorithm for fast hybrid (filter-wrapper) feature subset selection in highdimensional datasets", in Pattern Recognition Letters, vol 32, 2011, pp 701–711.

[26] Alon Schclar, Lior Rokach, Adi Abramson, and Yuval Elovici , "User Authentication Based on Representative Users", IEEE Transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 42, no. 6,pp 1669-1678, 2012.

[27] Salil P. Banerjee, Damon L. Woodard, "Biometric Authentication and Identification using Keystroke Dynamics: A Survey", Journal of Pattern Recognition Research 7, pp 116-139, 2012.

[28] Patrick Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation", in Information SecurityTechnical Report 17, 2012, pp 36-43.

[29] Amir-Massoud Bidgoli, Mehdi Naseri Parsa, "A Hybrid Feature Selection by Resampling, Chi squared and Consistency Evaluation Techniques", World Academy of Science, Engineering and Technology, vol 6, 2012, pp 230-239.

[30] Salil P. Banerjee, Damon L. Woodard, "Biometric Authentication and Identification using Keystroke

Dynamics: A Survey", Journal of Pattern Recognition Research 7, pp 116-139, 2012.

[31] Ahmed A. Ahmed and Traore Issa, "Biometric Recognition Based on Free-Text Keystroke Dynamics", IEEE Transactions on cybernetics, 2013.

[32] Khandaker A. Rahman , Kiran S. Balagani , Vir V. Phoha ,"Snoop- Forge-Replay Attacks on Continuous verification with Keystrokes", IEEE Transactions on information forensics and security, vol. 8, no. 3, pp 528-541, 2013.

[33] Fudong Li, Nathan Clarke, Maria Papadaki and Paul Dowland, Active authentication for mobile devices utilizing behavior profiling," International Journal of information Security, Springer-Verlag Berlin Heidelberg, 2013.

[34] Kasem Wangsuk and Tanapat Anusas-amornkul," Trajectory Mining for Keystroke Dynamics Authentication.", in Procedia Computer Science 24, 2013, pp175 – 183.

[35] Pablo Bermejo, Jose A. Gamez and Jose M. Puerta, "Speeding up incremental wrapper feature subset selection with Naïve Bayes classifier," Knowledge-Based Systems 55, pp 140–147, 2014.