Indian Journal of Science and Technology, Vol 9(6), DOI: 10.17485/ijst/2016/v9i6/82084, February 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Keystroke Dynamics for Mobile Phones: A Survey

Baljit Singh Saini[1,2]*, Navdeep Kaur[1] and Kamaljit Singh Bhatia[3]

[1]CSE, Sri Guru Granth Sahib World University, Fatehgarh Sahib - 140407, Punjab, India; drnavdeep.iitr@gmail.com
[2]CSE, Lovely Professional University, Phagwara - 144411, Punjab, India; baljitsaini28@gmail.com
[3]ECE, Sri Guru Granth Sahib World University, Fatehgarh Sahib-140407, Punjab, India;kamalbhatia.er@gmail.com

Abstract

Biometric is the science of authenticating a user based on his physical or behavioral attributes. Keystroke dynamics is behavioral study which analyses the typing rhythm of the user. We adopted a systematic procedure for studying the state of the art in keystroke dynamics in mobile phones. We analyzed the features extracted, the classification techniques, the input text, length of the input text, number of users, hardware used and the results that each study got. We included research articles that focused on keystroke dynamics for mobile devices only. It was found that majority of the research used latency as the prominent feature. Hold time and pressure are also used in combination with latency to get improved results. The most popular classification techniques are either statistical or neural network based, although it is difficult to say which is better since the users, testing conditions and features used are different in all researches. Also the number of users that are used for taking the input are generally less than 100 which is not a good representation sample. The application of this technique is very cost effective as it does not require any extra hardware. Hence there is a need to share the datasets by researchers and develop a standard against which every researcher can compare his results. Also the environment in which the tests are performed should be uncontrolled which will give results that are more realistic and close to real deployment environment.

Keywords: Keystroke Dynamics, Mobile, Survey

1. Introduction

Authentication is the process to verify, that a person is what he claims to be. A user can be verified in one of the following ways[1]:

Password: Something a user knows like a password or a PIN

Token: Something a user has like smart card

Biometric attribute: Something you are. Biometric attribute can be of two types-physical(retina scan, finger scan etc) and behavioural(signature, keystroke dynamics etc)

Whereas identification is ability of the system to correctly identify a person from a list of possible users. In this the system accumulates information about the subject and tries to associate it with one of the possible users based on a matching technique.

With more and more diversified use of cell phones[2], they are being used for online-banking, shopping and payments nowadays. There are more than 900 million mobile phone users in India alone[3]. Thus restricting access to our mobile phones is of utmost priority. For this a mobile phone user usually uses a 4-digit number (PIN) or a secret drawing pattern. Both these techniques can be easily compromised by shoulder surfing and systematic trial and error attacks.

Biometric authentication tools like fingerprint scan which are deployed on laptops or PCs have not been deployed on mobile phones yet because this will increase the cost of the phones. This calls for a cost effective solution which has been proposed through the use of keystroke dynamics. Since then a lot of work has been done on keystroke dynamics for hard keyboards deployed with PCs or laptops and in the recent years with the increased use of mobile phones researchers have also focused on analysing keystroke dynamics for mobile phones. A few survey papers[4–9] on keystroke dynamics has been published in the recent years with focus on physical

*Author for correspondence

keyboards. However, in our paper we have focused on research papers published on use of keystroke dynamics on mobile devices thus justifying our effort in this regard. Our paper lists all the research papers published in this regard including those published in lesser known journals or conferences till date.

2. Keystroke Dynamics

Keystroke dynamics is a behavioural biometric which identifies users based on their typing rhythm. The rhythm of every user is identified by extracting features like key hold time, latency (defined later on) etc. identifying a user based on typing goes back to the days of World War II where the operators identified each other by "fist of the sender"[10]. Keystroke dynamics has obvious advantages like:

1. No extra hardware is required
2. No extra effort. Typing is what a user will obviously do
3. Continuous authentication can be done for the entire session till the user is typing

Use of keystroke dynamics in mobile phones offers some advantages over hard keyboards used in PCs:

1. Use of two thumbs or one index finger only. While typing on hard keyboards we use all our fingers but while using mobile we normally use one index finger (right/left hand) or both our thumbs.
2. The variation in the typing pattern is less in different positions that we might take during typing e.g. typing message on mobile while sitting or while lying on bed will alter the pattern less as we can handle the mobile in almost the same manner in both the situations. But this is not the case with hard keyboards.

The keystroke biometric system works as depicted in Figure 1.

2.1 User Input

The first step in this system is to acquire user input. The input can be of two types – static or dynamic. Static text means that the user will enter a predefined text whereas in dynamic text he/she can enter any text. For example, password is an example of static text. The user enters the same password while enrolment phase and during

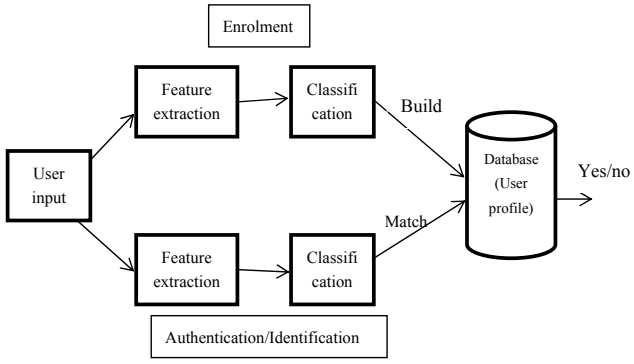

Figure 1. Biometric System.

authentication phase. But in dynamic text the user may enter different text during authentication phase than that entered during enrolment phase. He may enter different text each time in different authentication phases. During enrolment phase features are extracted carefully between various possibilities and are matched with the common features extracted during authentication phase. For example, suppose during enrolment phase user typed "hello there" and di-graph is calculated. During authentication phase the user types "this hero". Now the digraph for "th", "he" and "er" are matched.

The analysis of keystroke dynamics can be of two types – static or continuous[11]. In static analysis the user is authenticated on once during logging time. In continuous analysis the user typing pattern is monitored for the entire duration for which the user is logged in. This is beneficial in those situations where a user might be forced to log in and then the system is taken over by an intruder who then tries to steal secret information. With continuous authentication the intruder will be identified as unauthorized user and corrective measures can be taken as prescribed.

The typing environment plays an important role in user determination. In physical keyboards with change in keyboard the typing pattern of the user may differ. But this is not the case with soft keyboards in touch screen devices. But with change in mobile phone or the type of screen or the sensitivity of the screen the typing behavior varies. Hence the researchers can adopt two variations during data collection – controlled environment or uncontrolled environment. In controlled environment all the subjects are provided with the same input device. The data collected in this case may not be actual representation of the real data under actual conditions. In uncontrolled environment the researcher has no control

over how a subject provides the data. Here an application may be installed on user mobile and the user can type the data according to his convenience. Another important thing that some of the researchers[12–14] considered was whether text correction was allowed or not. Since pressing backspace will change some features and the user profile may differ.

2.2 Features

During typing the system can record which key was pressed, the time at which the key was pressed and the time at which the key was released. This is done for each key pressed and some features are extracted on their basis as shown in Figure 2.

Latency is the most commonly used feature in keystroke dynamics. Latency can be defined as – press-to-press, release-to-release and release-to-press latency[15]. Trojahn M and Ortmeier F[16] observed that using press-to-press latency (or digraph) gave better results. Giuffrida et al.[17] has used N-graph as a feature. Hold time is the time for which the key was being pressed. Other features like pressure[18,19] with which the key is being pressed and size[20,21] i.e. the amount of screen that is touched by the user while typing were analyzed. Giuffrida et al.[17] used features available with android phones like accelerometer and gyroscope apart from traditional keystroke features and got an FAR of 0.08%. Jeanjaitrong and Bhattarakosol[22] used a very different feature of calculating the distance between the two button presses. Error rate i.e. number of times backspace is pressed was considered by Zahid et al.[23] which is ignored by all other researchers and not considered as legitimate input. Various kinds of touch inputs like average touch movement speed per direction (8 directions), fraction of touch movements per direction (8 directions), average single-touch time, average multi-touch time, number of touch movements per session, number of single-touch events per session and number of multi-touch events per session were analyzed by Meng et al.[24]

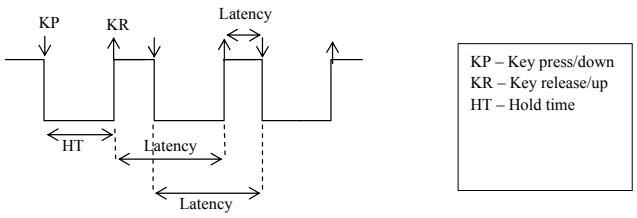

Figure 2. Keystroke Features.

2.3 Performance Evaluation

After acquiring the features, a profile is built for every user during enrolment phase. Then during authentication, the features are again extracted and biometric is built. This biometric is then compared with the existing profile using a matching algorithm.

Three important error rates are used to measure the performance of a keystroke dynamic system. False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (ERR).

FAR is the percentage of intruders who are allowed as genuine users.

$$FAR = \frac{Number\ of\ wrong\ acceptances}{Total\ number\ of\ intruder\ attempts\ made} * 100$$

FRR is the percentage of genuine users considered as intruders and rejected by the system.

$$FRR = \frac{Number\ of\ wrong\ rejections}{Total\ number\ of\ genuine\ attempts\ made} * 100$$

ERR is the value at which FAR and FRR are equal.

For identification systems accuracy is the measure of performance.

2.4 Classification

Classification aims at identifying the class to which a pattern belongs. During enrolment phase a profile is built for each user and later when the user wants to log in a temporary profile is built and matched with the existing one to authenticate the user. Various classification techniques have been used ranging from statistical methods to pattern recognition. In the following section the major classification methods used are being discussed.

2.4.1 Statistical Method

Simple methods like mean and standard deviation are used to build templates and for comparison hypothesis tests like t-test or distance measures like Euclidean or Manhattan distance are used. De Mendizabal-Vazquez et al.[21] achieved an EER of 20% using Euclidean distance while Dhage et al.[25] achieved an EER of 0.806 using mean and standard deviation. Chang et al.[19] achieved the best EER of 6.9% using mean and standard deviation.

2.4.2 Neural Network

Neural networks constitute a family of statistical learning algorithms motivated from the central nervous system

of the animals. They are used to approximate functions that depend on huge amount of inputs. The learning in neural networks can be supervised or unsupervised learning. The algorithms that that fall in this category and those used for keystroke dynamics are BPNN,[5] RBFN,[24] PNN,[18] FF-MLP[26]. Meng et al.[24] used different algorithms like Decision tree (J48), Naive Bayes, Kstar, Radial Basis Function Network (RBFN) and Back Propagation Neural Network (BPNN) and achieved the best FAR of 7.08% and FRR of 8.34% using RBFN. Results using neural networks have been promising what they are slow during enrolment as well as authentication phase

2.4.3 Pattern Recognition

Goal of pattern recognition is to classify objects into different classes. Different pattern recognition techniques have been proposed and analyzed. Saevanee and Bhattarakosol[18] used kNN to analyse inter key time, pressure and hold time and got an ERR of 1%. Antal et al.[14] experimented using Naïve Bayes, Bayesian network, J48, kNN, SVM, Random forest, MLP and achieved 93.04% accuracy with Random Forest.

2.4.4 Other Techniques

Clarke & Furnell[26] used a neural hybrid model combining GRNN, RBF, FF MLP and got an EER of 8.5%. Hwang et al.[30] used the concept of artificial rhythm with cues to analyze hold time and latency and the results were positive with 4% EER.

Table 1 and Table 2 describe all the major work done by researchers on mobile devices for authentication/identification using keystroke dynamics. The summary has been fit into two separate tables in order to accommodate all the data.

3. Performance Related Issues

Saevanee and Bhatarakosol[18] found out that finger pressure acts as the best indicator to identify users as compared to hold time and latency. Results of Chang et al.[19] and Tasai

Table 1. Summary of features, classification, input time, input length and results

Study	Features	Classification	IT	IL	Results (in %)			
					EER	FAR	FRR	Accuracy
Dhage et al.[25]	HT,di-graphs	Mean and SD	String	10	.806			
De Mendizabal-Vazquez et al.[21]	pressure, size, latency, linear, angular acceleration	PCA and LD	PIN	4				90
Chang et al.[19]	Latency	Mean and SD	Graphical Password		12.2	11.22	12.2	
Chang et al.[19]	Pressure	Mean and SD	Graphical Password		14.6	14.54	14.6	
Chang et al.[19]	Latency, pressure	Mean and SD	Graphical Password		6.9	6.92	6.8	
Campisi et al.[31]	Latency	Mean and SD	Six different passwords	10	13			
Maiorana et al.[13]	Latency	Distance	Alphabets	10				
Huang et al.[32]	Latency, HT	Mean	abertay2011	11		7.5	5	
Tasai et al.[20]	HT/latency	Statistical	PIN	4	11.72	11.72	11.6	
Tasai et al.[20]	Time, pressure	Statistical			8.4	8.32	8.4	
Tasai et al.[20]	Time, size	Statistical			11.14	11.14	11	
Tasai et al.[20]	Time, pressure, size	Statistical			10	9.78	10	
Buchoux & Clarke[29]	Latency	Statistical	PIN			53.13	20.63	
Buchoux & Clarke[29]	Latency	Statistical	Alphanumeric			20	2.5	

(*Continued*)

Clarke et al.[26]	HT	FF-MLP	--	--	18			
Trojahn & Ortmeier[16]	Digraph, pressure, size	J48,Kstar, MLP, RBFN, BN and NB	Any	11		2.03	2.67[!]	
Trojahn & Ortmeier[16]	x, y coordinates, pressure, size	J48,Kstar, MLP, RBFN, BN and NB	password	8		11	16	
Meng et al[24].	Touch inputs	J48, NB, Kstar, RBFN and BPNN.	--	--		7.08[&]	8.34[&]	
Meng et al.[24]	Touch inputs	PSO-RBFN	--	--		2.5	3.34	
Saevanee & Bhattarakosol[18]	Latency	PNN	Phone number	10				90
Saevanee & Bhattarakosol[18]	Pressure	PNN			1			
Karatzouni & Clarke[28]	Latency	FF-MLP	--	--	12.2	15.8	9.1	
Karatzouni & Clarke[28]	HT	FF-MLP	--	--	36.8	34.2	36.8	
Karnan & Krishnaraj[5]	HT, latency, digraph	BPNN	--	10				94.8
Jeanjaitrong & Bhattarakosol[22]	HT, latency, latency ratio, distance between buttons	BN	Graphical	4		.02	.178	82.18
Zahid et al.[23]	HT, digraph, error rate	Fuzzy	--	--		2	0	
Clarke & Furnell[29]	Latency, HT	GRNN, RBF, FF MLP	Numbers	4	8.5[%]			
Clarke & Furnell[29]	Latency, HT	GRNN, RBF, FF MLP	Numbers	11	4.9			
Clarke & Furnell[29]	Latency, HT	GRNN, RBF, FF MLP	Numbers	Any	17.6			
Saevanee & Bhatarakosol[18]	Pressure, latency, HT	Knn	Numbers	10	1			
Trojahn et al.[12]	HT, Digraph, pressure, size	Statistical classifier using k-means	--	17		4.19	4.59	
Hwang et al.[30]	HT, latency	Artificial rhythm with cues	PIN	4	4			
Hwang et al.[30]	HT, latency	Natural rhythm without cues	PIN	4	13			
Antal et al.[14]	HT, latency, pressure, size	NB, BN, J48, KNN, SVM, RF, MLP	.tie5Roanl	10				93.04[$]
Sen & Muralidharan[27]	Pressure, HT	K*, MLP, J48, NB	Numbers (1,5,9,3)	4		14.1[#]	14.06[#]	
Giuffrida et al.[17]	accelerometer, gyroscope,	one-class SVM, NB, kNN, and the "mean algorithm".	internet and satellite	--	0.08[@]			
Giuffrida et al.[17]	n-graph				4.97			

IL – input length, IT – input text, HT – hold time,

SD-standard deviation, PCA-Principal Components Analysis, LDA-Linear Discriminant Analysis, %FF-MLP - Feed forward-MLP, #MLP - Multilayer Perceptron, &RBFN-Radial Basis Function Network, BN-Bayesian Network, NB-Naive Bayes, BPNN-Back Propagation Neural Network, PSO-Particle Swarm Optimization, PNN-Probabilistic Neural Network, GRNN-Generalized Regression Neural Network, RBF-Radial Basis Function, SVM-Support Vector Machine, $RF-Random Forest,@kNN-k-nearest neighbour, !J48

Table 2. Summary of typing correction, number of users, samples and mobile devices used

Study	Typing corrections	Users	Samples	Mobile
Dhage et al.[25]	--	--	--	Sony xperia M
De Mendizabal-Vazquez et al.[21]	--	80	3346	
Chang et al.[19]	--	100	5500	Motorola Milestone, HTC Desire HD and Viewsonic Viewpad
Campisi et al.[31]	Not allowed	30	3600	Nokia 6680
Maiorana et al.[13]	Not allowed	40	4800	
Huang et al.[32]	--	40	240	
Tasai et al.[20]	--	100	--	Motorola Milestone
Buchoux and Clarke[29]	--	16	480	SPV C600
Clarke et al.[26]	--	30	900	
Trojahn and Ortmeier[16]	--	18,16	180,128	HTC desire, HTC desire HD
Meng et al.[24]	--	20	120	Google/HTC Nexus One
Saevanee and Bhattarakosol[18]	--	10	300	Notebook touch pad
Karatzouni and Clarke[28]	--	50	--	XDA IIs
Karnan & Krishnaraj[5]	--	25	1250	--
Jeanjaitrong and Bhattarakosol[22]	--	10	1000	Iphone
Zahid et al.[23]	--	25	--	Nokia N, E and 6xxx series
Clarke and Furnell[29]	Not allowed	32	960	Nokia 5110
Saevanee and Bhatarakosol[18]	--	10	300	Synaptic Touchpad
Trojahn et al.[12]	Not allowed	152	1520	Samsung Galaxy Nexus
Hwang et al.[30]	--	25	--	SAMSUNG SCH-V740
Antal et al.[14]	Not allowed	42	2142	Nexus 7 Tablet, Mobil LG Optimus L7 II P710 device
Sen and Muralidharan[27]	--	10	1000	HTC Nexus-One
Giuffrida et al.[17]	--	20	800	Samsung Nexus S

et al.[20], show that combining time features with pressure gives better results as compared to considering them separately. Campisi et al.[31] observed from experiments that with increase in number of acquisitions during enrolment phase the EER decreases. Clarke and Furnell[26] came to the conclusion that keystroke dynamics is not a suitable method for those users whose typing pattern changes with variations in handset interactions and those who do not use mobiles regularly. Buchoux and Clarke[29] observed that statistical classifiers can be used on real devices as they showed low processing requirements. They also observed that the length of the input is also important and that 4-digit PINs are too short for practical use. Giuffrida et al.[17] observed that sensor based features yielded better results as compared to traditional keystroke dynamics features (i.e. 0.08% EER vs. 4.97% EER). Hwang et al.[30] is of the view that the users that are selected for data collection should be more diverse as diverse users may show diverse usage patterns.

Machine learning methods focus on detection performance only while ignoring robustness. They must also understand the practical point of view i.e. the amount of knowledge or computational power that an attacker needs to break through[33].

Since while using mobile users normally use index finger or one thumb or two thumbs only so the variation in typing patterns is limited as compared to hard keyboards. Also the variation in pattern will be minimum in

situations like when a user is using mobile while sitting or lying on bed but the pattern may significantly vary while is user is walking and typing.

4. Conclusion

In this paper we have tried to present a comprehensive survey of work done on keystroke dynamics in the field of mobile phones in the past decade. But there are some open challenges which are still to be addressed.

The variation in the typing pattern of the users under different situations can lead to different typing patterns and thus this issue needs to be taken care of while designing an authentication system for keystroke dynamics. No study has compared and analyzed the variations in typing patterns of users in various situations while typing e.g. while the user is sitting, standing, walking or lying down etc. Also the emotional state of the user will play a significant role in the typing behavior.

Another area of research in use of keystroke dynamics for mobile phones yet to be explored is continuous authentication wherein the user is authenticated throughout the period that he is logged in.

Research on optimum password length, type and minimum number of samples required, need to be conducted so that a user profile can be built as quickly as possible.

Keystroke dynamics is still in its early stages in the field of mobile devices and a lot of research needs to be done to make it an effective biometric.

5. References

1. Wood HM. The use of passwords for controlled access to computer resources. NBS Special Publication: US Department of Commerce; 1977.
2. Chang JM, Fang C, Ho K, Kelly N et al. Capturing cognitive fingerprints from keystroke dynamics. IT Professional. 2013; 15(4):24–28.
3. Roushan R, Mehta M, Chandani A. Study of mobile marketing communication in India. Indian Journal of Science and Technology. 2015 Mar; 8(6):125–31. DOI: 10.17485/ijst/2015/v8iS6/71216.
4. Crawford H. Keystroke dynamics: characteristics and opportunities. Eighth Annual International Conference on Privacy Security and Trust(PST); Ottawa: ON; 2010. p. 205–12.
5. Karnan M, Akila M, Krishnaraj N. Biometric personal authentication using keystroke dynamics: A review. Applied Soft Computing. 2011; 11(2):1564–73
6. Shanmugapriya D, Padmavathi G. A survey of biometric keystroke dynamics: Approaches, security and challenges. International Journal of Computer Science and Security. 2009; 5(1):115–19.
7. Banerjee SP, Woodard D. Biometric authentication and identification using keystroke dynamics: a survey. Journal of Pattern Recognition Research. 2012; 7(1):116–39
8. Pisani PH, Lorena AC. A systematic review on keystroke dynamics. Journal of Brazilian Computer Socienty. 2013; 19(4):573–87.
9. Bhatt S, Santhanam T. Keystroke dynamics for biometric authentication - a survey. 2013. International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME); Salem; 2013. p. 17–23.
10. Miller B. Vital signs of identity. IEEE Spectrum. 1994; 31(2):22–30.
11. Menshawy D El, Mokhtar HMO, Hegazy O. For continuous authentication biometrics : a brief overview. 2014:415–24.
12. Trojahn M, Arndt F, Ortmeier F. Authentication with Keystroke dynamics on touchscreen keypads-effect of different n-graph combinations. Third International Conference on Mobile Services, Resources and Users(MOBILITY); 2013. p. 114–19.
13. Maiorana E, Campisi P, González-Carballo N, Neri A. Keystroke dynamics authentication for mobile phones. Proceedings 2011 ACM Symposium on Applied Computing SAC' 11; 2011. p. 21–6.
14. Antal M, Szabó L, László I. Keystroke dynamics on android platform. 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014; Tirgu Mures; Romania; 2014. p. 9–10
15. Balagani KS, Phoha VV, Ray A, Phoha S. On the discriminability of keystroke feature vectors used in fixed text keystroke authentication. Pattern Recognition Letters. 2011; 32(7):1070–80.
16. Trojahn M, Ortmeier F. Toward mobile authentication with keystroke dynamics on mobile phones and tablets. Proceedings - 27th International Conference on Advanced Information Networks Applications Workshops(WAINA); Barcelona; 2013. p. 697–702.
17. Giuffrida C, Majdanik K, Conti M, Bos H. I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. Detection of Intrusions and Malware, and Vulnerability Assesment. 2014; 8550:92–111.
18. Saevanee H, Bhattarakosol P. Authenticating user using keystroke dynamics and finger pressure. 2009 6th IEEE Consumer Communications and Networking Conference; 2009. p. 1–2.
19. Chang T-Y, Tsai C-J, Lin J-H. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. Journal of Systems Software. 2012; 85(5):1157–65.

20. Tasia CJ, Chang TY, Cheng PC, Lin JH. Two novel biometric features in keystroke dynamics authentication systems for touch screen devices. Security and Communication Networks. 2014; 7(4):750–58
21. De Mendizabal-Vazquez I, De-Santos-sierra D, Guerra-casanova J, Carmen S. Supervised classification methods applied to keystroke dynamics through mobile devices. International Carnahan Conference on Security Technology (ICCST); 2014. p. 1–6.
22. Jeanjaitrong N, Bhattarakosol P. Feasibility study on authentication based keystroke dynamic over touch-screen devices. 2013 13th International Symposium on Communications and Information Technologies; Surat: Thani; 2013. p. 238–42.
23. Zahid S, Shahzad M, Khayam SA, Farooq M. Keystroke-based user identification on smart phones. Recent Advances in Intrusion Detection, Springer: Berlin Heidelberg; 2009.
24. Meng Y, Wong DS, Schlegel R. Touch gestures based biometric authentication scheme for touchscreen mobile phones. Information Security and Cryptology; Berlin: Heidelberg; 2013..
25. Dhage S, Kundra P, Kanchan A, Kap P. Mobile authentication using keystroke dynamics. International Conference on Communication, Information & Computing Technology; Mumbai, (ICCICT'15); 2015. p. 15–95.
26. Clarke NL, Furnell SM. Authenticating mobile phone users using keystroke analysis. International Journal of Information Security. 2007; 6(1):1–14.
27. Sen S, Muralidharan K. Putting 'pressure'on mobile authentication. Seventh International Conference on Mobile Computing and Ubiquitous Networking (ICMU); Singapore; 2014. p. 56–61.
28. Karatzouni S, Clarke N. Keystroke analysis for thumb-based keyboards on mobile devices. IFIP International Federation for Information Processing, New approaches for Security, Privacy and Trust in Complex Environments; Boston; 2007. p. 253–63
29. Buchoux A, Clarke NL. Deployment of keystroke analysis on a smartphone. Australian Information Security Management Conference; 2008. p. 48.
30. Hwang SS, Lee HJ, Cho S. Improving authentication accuracy using artificial rhythms and cues for keystroke dynamics-based authentication. Expert Systems with Applications. 2009; 36(7):10649–56.
31. Campisi P, Maiorana E, Lo Bosco M, Neri A. User authentication using keystroke dynamics for cellular phones. Signal Processing, IET. 2009; 3(4):333–41.
32. Huang X, Lund G, Sapeluk A. Development of a typing behaviour recognition mechanism on android. 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); Liverpool; 2012. p. 1342–7.
33. Sensarma D, Sensarma S. A Survey on different graph based anomaly detection techniques. Indian Journal of Science and Technology. 2015; 8(31):1–7. DOI: 10.17485/ijst/2015/v8i1/75197.