A Survey on Computational Intelligence Techniques in User Identity Management

Abhijit Kumar Nag
Department of Computer Information Systems, Texas A&M University-Central Texas
Killeen, TX 76549, USA

ABSTRACT

User identity is a critical part to secure the legitimate access of authentication to protect his personal sensitive information. In recent years, computational intelligence (CI) plays a significant role to innovate various authentication approaches to enhance this identity management. In this comprehensive survey paper, various computational identity verification techniques are discussed and how these techniques provide enhanced security in different levels are highlighted. Moreover, an empirical comparison of various authentication techniques is illustrated in this paper to reflect the overall current research directions in the areas of computational intelligence in the user identity management system.

Keywords: Cyber identity, Authentication factor, Continuous and Dynamic Authentication, Adaptive Authentication, biometrics.

1. INTRODUCTION

Authentication is a critical part of ensuring the identity of a legitimate user. During authentication, an individual's credential is validated with a specific computational technique to determine the association of the user with his/her claimed identity. A person's identity consists of several information in different layers. In physical identity, a person's real-world name works as the key information to verify. In addition, his friends and neighbors also serve as a form of shared identity, where his interests and society membership are considered as abstracted identity [1]. In the cyber domain, the digital identity consists of the username of that person to use any particular application or service. His connections will serve as a shared identity while his stated interest and online behavior serve as abstracted identity. These various layers of identity in cyber domain show the immense need for additional information about a user to identify correctly.

With the growth of online-based applications and services, it is required to verify the user's credentials digitally and allow users to access resources upon verification. In addition, the digital identity of a particular user should be interconnected so that various entities can communicate easily among them to identify the same user. Lastly, digital identity is required to be flexible to adapt to the nature of the online transaction and incorporate additional information of the user to prepare the rich profile of a legitimate user. All these characteristics reveal that a user's digital identity requires a good number of information to be processed in a strategic manner to provide access to any sensitive information.

To verify users' credentials in a robust way, a good number of research works have been done to build various CI systems. These systems capture various information (what you know, what you have, who you are, where you are, etc.) to create robust user credentials to allow legitimate access to digital resources. Password-based authentication is the most common and most vulnerable approach to identify users as of today. Some CI approaches are introduced to provide some complementary approaches to password-based authentication system for the secure and robust authentication process. Biometrics is widely used technique as an authentication factor. Various physiological and behavioral biometrics can be combined to create a user identity profile to verify users in various system settings. With the advent of smartphones and tablets, various sensors also play as passive authentication factors to identify a user in a given context. Researchers innovate ensemble methods based on CI to combine multiple authentication factors with building a robust and scalable user identity system.

In this survey paper, various authentication factors are illustrated and how their verification processes work to identify legitimate users. Continuous authentication, active authentication, and risk-based authentication are the emerging trends today that incorporate various machine learning techniques to assist in user identity management. The rest of the paper is designed in the following way. Section 2 discusses password-based systems and some complementary approaches to passwords. Section 3 highlights various continuous and active authentication systems that use extensive CI approaches to identify genuine users. Section 4 illustrates CI-based adaptive authentication techniques to identify users sensing the surrounding environments. Section 5 mentions the overall summary including future emerging trends of the user identity management system.

2. PASSWORD-BASED USER IDENTITY MANAGEMENT

Passwords are the most common and extensively used form of the authentication process. However, this is one of the most compromised authentication factors in the areas of user identity management. In 2018, 64% of breaches are related to identity theft where primary reason for this theft is password breaches[1]. To prevent various password-based attacks, a good number of hashing algorithms has been used. Most widely used hashing algorithms are SHA-1, SHA-2, SHA-3 along with random salt techniques [3-5]. These one-way hashing algorithms and salt provide additional layers of security against dictionary-based attacks or random table attacks. Bcrypt [6] is a popular password hashing algorithm that uses adaptive function over time to remain resilient to brute-force search attacks even with

[1] https://breachlevelindex.com/

increasing computational resources. Argon2 and PBKDF2 are also considered as a safe choice for hashing.

Graphical passwords are fallen under non-textual based passwords to reduce password fatigue of users. This user verification approach is proven useful for mobile devices where users can touch to authenticate themselves rather than typing long passwords. There are two categories of graphical passwords, namely recognition based and recall-based approaches. Some CI-based techniques are used to harden the graphical passwords. For example, Man et al. [7] proposed a shoulder-surfing resistant algorithm where a user selects several pictures as pass-objects. Each pass-object has many variants and each variant is assigned a unique code. Using CI approaches the authentication engine can quickly create several decoy images to challenge the user at any given time. "Passface" is another technique that give users a grid of images where they choose four images of human faces as their future password [8]. Various face analysis algorithms are designed to generate random faces from a diverse background and thereby making the authentication process less predictable by the attackers. More details of various graphical password-based approaches will be found in [9, 10]. There are some complementary approaches to passwords are existed in the literature that uses extensive CI approaches to design a robust authentication approach. The details of these approaches are described in the next subsections.

Negative Password-based Approach

One of the innovative approaches to mitigate password guessing attacks and side-channel attacks is known as a negative authentication approach [11, 12, 54]. In this approach, a negative password region is created from the positive password points and it is placed in the first layer of the password-based system. Both deterministic and non-deterministic mathematical models are developed to build a robust non-password region that complements the positive password space. To bring obfuscation to the attackers, some of non-password regions are not covered in the first layer. Hence, compromising the first layer (through guessing attack or side-channel attacks) will not disclose any sensitive information about the positive password space. In addition, due to computational power, the negative password space can quickly be generated and replaced in the first layer in a regular interval by network administration. This will eventually prohibit any types of password-based offline attacks. Another approach of non-password-based approach is to use an encrypted negative password to provide a secure authentication [13]. In this approach, the hashed password is passed through a prefix algorithm with permutation to create a negative database, and then the negative database is encrypted using a symmetric algorithm. These steps can successfully prevent lookup table attack and rainbow table attack. These computational approaches are designed to harden the password authentication process and strengthen the overall security of the user identity management.

Honeywords, Cracking-resistant password vaults, Bloom filter

Honeywords [14] is a popular complementary password-based approach, where multiple user credentials are stored for a single user. One of the credentials is genuine, and others are fake credentials. This approach can successfully detect any intrusion of the password database if any attacker uses fake credentials to login to a system. A computational algorithm is used to design look-alike decoy credentials per user in a given system. Honeyword based approach can prevent guessable passwords and block any illegitimate request.

Cracking-resistant password vaults are another CI-based complementary approach which is based on a secure encoding system [15, 16]. In general, password vaults are as vulnerable as regular password as it can be decrypted using a master password. Natural language encoders (NLE) [15] is a framework that permits the construction of password vaults in a different way such that if it is decrypted using a wrong master password, it will produce plausible looking decoy passwords. This approach uses Markov chain concept to represent the password strings.

Bloom filter [17] is another approach that uses a probabilistic data structure to determine whether an element belongs to a set or not. This approach can easily be adapted in password-based authentication scheme [18]. It uses a good number of hash functions and an access request is authenticated by these hash functions. This approach is computationally efficient compared to other complementary approaches and no false negative scenarios. A brief comparison among password complementary approaches is illustrated in Table 1.

Table 1: Comparison of various complementary password-based approaches.

Characteristics	Deterministic NAS Model	Bloom Filter	Honeywords
Approach	Implements Negative selection algorithm	Filter for Positive authentication	Extra false credentials
Space	Two-dimension grid space	*m* length string	*n* times false credentials
Password Mapping	One cell	*n* bit positions for *n* hashes	Not Applicable
No. of checks per access request	One check	*n* checks for *n* hash functions	Alarm raised if "*Honeyword*" is used
Information Utilization	Low	Low	Not Applicable
Hash Function used	One	*n* hash functions	Depends on the implementation
Complexity of Authentication	*O (n)*	*O(1)*	Not Applicable
False Positive Rate	Relatively Higher	Relatively Lower	Not Applicable
False Negative Rate	No False Negative	No False Negative	Chance of False Negative exists

3. CI-BASED CONTINUOUS AUTHENTICATION AND ACTIVE AUTHENTICATION APPROACHES

Multi-factor-based authentication is one of the best ways to validate a user's identity against fraud. With the increase of smart devices and mobile applications, it is always extremely difficult to keep user data secure in various operating environments. Hence, continuous verification of a user's identity is the optimal solution to provide seamless access to sensitive information. Active authentication [19] is another term used that facilitates user authentication using passwords,

biometrics, how a user behaves and surrounding contexts. One critical difference between a one-time authentication process is that it continuously captures users' data and calculates the user score. If the score is above the threshold value, it will continue as before. Otherwise, it prompts the user to verify his/her identity again. Depending on which authentication factors are measured to capture user data, various computational techniques are proposed to authenticate users in a real-time scenario. Most commonly, they are categorized as uni-modal and multi-model authentication approaches. A summary of the continuous authentication-based approaches is mentioned below.

Unimodal continuous authentication

Keystroke Dynamics

Keystroke dynamics is a widely used non-intrusive authentication metric. This trait is sometimes referred to as typing behavior. In mobile devices accelerometer, gyroscope and orientation sensors are used to capture a rich set of keystroke dynamics of a legitimate user. The standard sets of features are digraph latency; keystroke time, duration, pressure or force; keystroke interval; keystroke latency; digraph, duration time, and trigraph [20]. Text-independent keystroke features [21-24] are mostly used approach for continuous authentication in mobile devices. Each of these works collects a good keystroke dataset to run their proposed approaches. An approach that uses a virtual keyboard-based system [22] collect features from 315 mobile users. As keystroke captures a good number of features, feature subset selection is applied to select an optimized set of features [25, 26] to run various Machine learning algorithms.

Web browsing behavior

Due to an increase in smartphone usage, web browsing [27-30] has become an integral part of users and can be considered as a user identification factor. In general, a set of global and internal session features from a website are captured. Day-of-week and day-of-time distributions [27] are part of global session features. In the case of internal session features, pauses, burstiness, the time between revisits, and genres are considered. However, one drawback of this approach is the FAR (false acceptance rate), and FRR (false rejection rate) are varied significantly for a given user in various sessions. Hence, web browsing is sometimes used in conjunction with GPS location, application usage and stylometry [29]. In a research work mentioned in [28], n-gram models are used to capture user interactions with web-based software. These applications show that computational intelligence-based models are widely adopted to build a model for user authentication purposes.

Cognitive and Screen Fingerprint

Humans use language differently to express their views and hence, language fingerprint can be considered as a unique feature to each individual. In general, cognitive and linguistic features are collected from the keyboard and it is sometimes called stylometric features [30-32]. The accuracy using cognitive fingerprint-based approaches is 55.30% using 500 characters as input while accuracy increases to 63.98% considering 1000 characters [32]. Screen fingerprint [33-34] basically captures the cognitive abilities, motor limitations, subjective preferences, and work patterns of an individual. Both these fingerprints perform in a similar accuracy. To design a robust system, mouse movement, typing and scrolling are considered together to increase the overall accuracy of the system.

Face Recognition

Face recognition is widely used as a biometric approach and using a smartphone's front camera it is possible to use it as an authentication factor. Body localization [35] with face recognition provides a good computational model to have better accuracy to identify users. Another approach [36] uses ambient lighting conditions to detect partially cropped and occluded faces and develop a computational model to identify smartphone users. This model is tested with 50 users.

Phone movement and motion patterns

Smartphone's accelerometer sensor provides a good biometric of moving patterns of a user. Some of the significant features of moving patterns are—spectral energy, histogram, dynamic time warping distance, peak magnitude to RMS ratio, median frequency, the correlation between a pair of the signal, etc. These rich set of features are trained in various machine learning techniques (Logistic regression, neural network, SVM, random forest, etc.) to build a robust authentication approach [37]. A neural network-based approach [38] is also used to tune the temporal features to identify 1500 users in active biometric authentication. These approaches have average EER (Equal Error Rate) of 5.36% with 2.7% of standard deviation.

Multi-modal continuous authentication

Hand Movement, Orientation and Grasp (HMOG)

HMOG is considered as a new biometric trait that captures subtle micro-movement and orientation dynamics of legitimate users. In total it captures 96 features [39]. This CI-based technique performs 6.92% EER values while walking but 10.2% EER values while sitting. As smartphone users use the device while moving, this biometric is a good candidate to authenticate users on the go.

Keystroke and Mouse Movement, Application Usage, and System Footprint

BehavioSec [40-41] captures keystroke, mouse, application usage and system footprints to provide a robust form of the user verification process. It then developed a computational trust model to measure the trust value of the user's system at a given time. The trust value lies between 0 and 100. The system is started with a trust value of 100 and adaptively calculates the trust value of the system in real-time. In their proposed user study, it is found that using keystroke dynamics, correct users are not falsely rejected, and incorrect users are recognized after 38 interactions (between 20 and 25 keystrokes). Hence, multi-modal based CI models perform quicker than that of uni-modal based approaches.

Stylometry, Application Usage, Web Browsing, and GPS Location

In this type of multi-modal based system, data is collected from 200 participants for more than a 5-month period [42]. The features that are collected include typed texts, visited apps, navigated websites, location reported using GPS and Wi-Fi. Out of all these four authentication modalities, classifier fusion approach has been applied to achieve EER of 1% after 30 minutes. This multi-modal shows that using a hybrid ensemble classifier can increase the overall authentication performance to a significant level.

Gestures, Keystroke, Touch, and Body Movements
In this approach, an experiment is conducted with 74 participants for typing, 47 participants for swiping, and 11 participants for body movements [44]. To use the best set of features from these modalities, a fusion-based computational framework is designed that integrates different modalities in a context-aware fashion. It is found from the user study that body movements achieve the lowest FAR (3.2%) and FRR (3.2%) values. Another work uses smartphone accelerometer sensor-based context ware [45] authentication to actively verify mobile users.

Face detection, touch, and location
Face detection modality can be combined with touch and location data to provide a scalable active authentication mechanism. In [46], authors collected data over various age groups and different sessions over a period to generate a large dataset. This dataset lists a rich set of modality-specific information for every user which can be used in other research experiments.

Smartphone-based Multi-sensor Authentication
Smartphone sensors always capture information about a mobile user and can easily be integrated to verify user credentials in the background. It is found that the smartphone-based system using multiple sensors can create a user profile in 10 seconds and then detect an imposter in 20 seconds using the computational model [47]. Hence, real-time recognition of a human is possible with only smartphone embedded sensors [48].

Self-authenticable Wearable devices
Wearable devices now communicate among themselves and hence, to share information, it is an urgent need to verify their identities using mutual authentication approaches [49, 50]. Various surrounding factors along with device ID are used to provide a multi-layer authentication process. Recent Internet of Things (IoT) devices also require such authentication mechanism to verify user identity in a continuous manner.

4. CI-BASED ADAPTIVE MULTIFACTOR AUTHENTICATION TECHNIQUES

Adaptive Multi-factor authentication system (A-MFA) [51-53] is a novel concept that adopts computational intelligence techniques to validate users' sensing connecting devices, operating medium and surrounding conditions. This approach provides dynamicity in the multifactor authentication process. In general, many multifactor products use a fixed set of authentication factors to verify users. However, ideally, not all authentication factors are suitable in every environment setting. Hence, an adaptive selection strategy will be the best option to dynamically select the authentication factors. The authors in their proposed research presented a mathematical model to calculate the pair-wise trustworthy model for various combinations of devices and mediums. They incorporate the error rates to distinguish trustworthy values among various authentication factors. Then a multi-objective optimization model has been designed to choose the best set of authentication factors which has higher trustworthy values with a lesser number of authentication factors. In addition, the proposed computational model considers previously selected authentication factors so that there is no repetition of those factors. This innovative concept can prevent any attack that tries to record previous attempts and guess the next authentication attempts. This A-MFA is tested with a set of 50 users each trying to authenticate for five times. Moreover, to test the FAR of the framework, the proposed system is tested with 1000 invalid request to see how many will pass through the authentication process. The results are shown in Table 2 and Table 3.

Table 2:THE SUCCESSFUL ATTEMPTS FOR VALID USER DATA IN DIFFERENT SURROUNDING CONDITIONS FOR TWO FACTOR AND THREE FACTOR BASED ADAPTIVE MFA SYSTEM.

Surrounding conditions	Two-Factor of A-MFA	Three-Factor of A-MFA
Light and Noise are in the range	94%	93%
Light is in range	92%	90%
Noise is in range	90%	88%
None are in the range	86%	84%

Table 3: THE SUCCESSFUL ATTEMPTS FOR INVALID USER DATA IN DIFFERENT SURROUNDING CONDITIONS FOR TWO FACTOR AND THREE FACTOR BASED ADAPTIVE MFA SYSTEM.

Surrounding conditions	Two-Factor of A-MFA	Three-Factor of A-MFA
Light and Noise are in the range	0%	0%
Light is in range	0.5%	0%
Noise is in range	0.45%	0%
None are in range	3%	0%

From Table 2, it is noteworthy that the A-MFA approach works better when surrounding conditions are in favor, which is intuitive as surrounding conditions restrict the number of usable authentication factors. Table 3 shows that the A-MFA performs significantly better against illegitimate access requests in various surrounding conditions. This result shows how the proposed computational model outperforms in blocking invalid authentication requests.

A good number of MFA products also adopt the adaptive authentication concept and they vary their selection by user preference or system settings. In the majority of these solutions, a computation model is developed to choose the best set of authentication factors to authenticate users in real time.
A multi-level authentication mechanism is also another way of authenticating legitimate users with the help of contextual information and user experience [55]. Authors in [55] provide decision tree-based authentication approaches that keep balance between user satisfaction (related to Quality of Experience (QoE)) and obtained level of security (related to Quality of Protection (QoP)). The proposed approach is tested with the PIN, password and biometric-based authentication approaches in various environments (places), several device categories, different time periods and various service applications.
CI-based MFA solution is also used in vehicular integration as a large number of sensors are used in modern vehicles which can accurately identify the actual driver or owner of the vehicle [56]. The proposed approach integrates the password, PIN with biometrics-based sensors that are used in modern vehicles (speech recognition for voice commands, face detection,

fingerprint, etc.). Then based on their FAR and FRR values, an efficient Bayes estimator is designed to get the accept or reject decision. Such MFA based solution can easily be extended to verify passengers in any commercial airport. More forward-looking MFA solution can utilize the heart and brain [57, 58] of humans (in forms of ECG and EEG) to provide unique identification samples.

5. CONCLUSIONS

This survey paper provides an overview of current state-of-the-art CI-based techniques to facilitate user authentication as part of user identity management. Due to computational advancements in information processing and storage, user authentication process now checks the user's credentials against millions of existing credentials and provides a score that quantifies the authentication decision for a user. Computational Intelligence comes with a diverse set of techniques to combine various user information and provide a rich set of user credentials to authentication various services simultaneously. Due to recent trends of cyber-attacks and identity thefts, these CI techniques provide appropriate safeguards to verify users' credentials more precisely in a wide range of platforms (desktop-based, cloud-based, mobile-based solutions). It is anticipated that CI-based approaches will enhance the seamless experience of user identity management for autonomous entities, internet of things (IoT) devices. In addition, CI techniques are also adopted to authenticate over a GSM system using CL-PKC and providing a location-based service for road networks [59, 60]. Hence, computation intelligence-based methods will significantly benefit the contemporary emerging authentication technologies in coming years.

6. REFERENCES

[1] M. Rowe, "Identity: Physical, Cyber, Future," Invited talk on Physical-Cyber-Social Computing, October 2013.

[2] R. J. McWaters, "A Blueprint for Digital Identity- The Role of Financial Institutions in Building Digital Identity", August 2016. Url: http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[3] C De Canniere, C Rechberger / "Finding SHA-1 characteristics: General results and applications." In International Conference on the Theory and Application of Cryptology and Information Security, pp. 1-20. Springer, Berlin, Heidelberg, 2006.

[4] N. Sklavos, Nicolas, and K. Odysseas , "On the hardware implementations of the SHA-2 (256, 384, 512) hash functions." In Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on, vol. 5, pp. V-V. IEEE, 2003.

[5] S. Chang et al., "Third-round report of the SHA-3 cryptographic hash algorithm competition." NIST Interagency Report 7896 (2012).

[6] N. Provos, and D Mazieres. "A Future-Adaptable Password Scheme." In USENIX Annual Technical Conference, FREENIX Track, pp. 81-91. 1999.

[7] S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[8] T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.

[9] X Suo, Y Zhu, and G. Scott Owen. "Graphical passwords: A survey." In Computer security applications conference, 21st annual, pp. 10-pp. IEEE, 2005.

[10] D. Dasgupta, A Roy, and A K Nag. Advances in User Authentication. Springer International Publishing, 2017.

[11] D. Dasgupta et al. "G-NAS: A grid-based approach for negative authentication." In Computational Intelligence in Cyber Security (CICS), 2014 IEEE Symposium on, pp. 1-10. IEEE, 2014.

[12] D. Dasgupta et al. "Design and implementation of Negative Authentication System." International Journal of Information Security (2017): 1-26.

[13] W Luo, Wenjian, Y Hu, H Jiang, and J Wang. "Authentication by Encrypted Negative Password." IEEE Transactions on Information Forensics and Security (2018).

[14] 14. A Juels, and R. L. Rivest. "Honeywords: Making password-cracking detectable." In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pp. 145-160. ACM, 2013.

[15] R. Chatterjee, J Bonneau, A Juels, and T Ristenpart. "Cracking-resistant password vaults using natural language encoders." In2015 IEEE Symposium on Security and Privacy, pp. 481-498. IEEE, 2015.

[16] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh. Kamouflage: loss-resistant password management. In ESORICS, pages 286–302, 2010.

[17] S. Geravand, and M. Ahmadi. "Bloom filter applications in network security: A state-of-the-art survey." Computer Networks 57, no. 18 (2013): 4047-4064.

[18] E. Spafford. Observations on reusable password choices. In USENIX Security, 1992.

[19] R. P. Guidorizzi, "Security: Active authentication," IT Professional, vol. 15, no. 4, pp. 4–7, 2013.

[20] ML Ali, J V. Monaco, C. Tappert, and M Qiu. "Keystroke biometric systems for user authentication." Journal of Signal Processing Systems 86, no. 2-3 (2017): 175-190.

[21] Feng, Tao, Xi Zhao, Bogdan Carbunar, and Weidong Shi. "Continuous mobile authentication using virtual key typing biometrics." In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 1547-1552. IEEE, 2013.

[22] Gascon, Hugo, Sebastian Uellenbeck, Christopher Wolf, and Konrad Rieck. "Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior." In Sicherheit, pp. 1-12. 2014.

[23] J Kim, Junhong, H Kim, and P Kang. "Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection." Applied Soft Computing 62 (2018): 1077-1087.

[24] J Yadav, K Pandey, S Gupta, and R Sharma. "Keystroke dynamics based authentication using fuzzy logic." In 2017 Tenth International Conference on Contemporary Computing (IC3), pp. 1-6. IEEE, 2017.

[25] J. Yang, V. Honavar, Feature subset selection using a genetic algorithm, EEE Intelligent Systems and their Applications, 13 (1998), pp. 44-49.

[26] G.H. John, R. Kohavi, K. Pfleger, Irrelevant features and the subset selection problem, Machine Learning: Proceedings of the Eleventh International Conference, Morgan Kaufmann, San Francisco (1994) pp. 121–129.

[27] M Abramson, and DW. Aha. "User Authentication from Web Browsing Behavior." In FLAIRS conference, pp. 268-273. 2013.

[28] LC Leonard, "Web-Based Behavioral Modeling for Continuous User Authentication (CUA)." In Advances in Computers, vol. 105, pp. 1-44. Elsevier, 2017.

[29] L Fridman, S Weber, R Greenstadt, and M Kam. "Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location." IEEE Systems Journal 11, no. 2 (2017): 513-521.

[30] Juola, Patrick, John I. Noecker, Ariel Stolerman, Michael V. Ryan, Patrick Brennan, and Rachel Greenstadt. "Keyboard-behavior-based authentication." IT Professional 15, no. 4 (2013): 8-11.

[31] Pokhriyal, Neeti, Kshitij Tayal, Ifeoma Nwogu, and Venu Govindaraju. "Cognitive-Biometric Recognition From Language Usage: A Feasibility Study." IEEE Transactions on Information Forensics and Security 12, no. 1 (2017): 134-143.

[32] SMA Husain, and MA Abel. "Systems and methods for using cognitive fingerprints." U.S. Patent 9,578,053, issued February 21, 2017.

[33] ME Fathy, VM. Patel, T Yeh, Y Zhang, R Chellappa, and LS. Davis. "Screen-based active user authentication." Pattern Recognition Letters 42 (2014): 122-127.

[34] Patel, Vishal M., Teng-Hao Yeh, Mohammed E. Fathy, Yangmuzi Zhang, Yan Chen, Rama Chellappa, and Lisa Davis. "Screen fingerprints: a novel modality for active authentication." IT Professional 15, no. 4 (2013): 38-42

[35] Niinuma, Koichiro, and Anil K. Jain. "Continuous user authentication using temporal information." In Biometric Technology for Human Identification VII, vol. 7667, p. 76670L. International Society for Optics and Photonics, 2010.

[36] Mahbub, Upal, Vishal M. Patel, Deepak Chandra, Brandon Barbello, and Rama Chellappa. "Partial face detection for continuous authentication." In Image Processing (ICIP), 2016 IEEE International Conference on, pp. 2991-2995. IEEE, 2016.

[37] Kumar, Rajesh, Partha Pratim Kundu, Diksha Shukla, and Vir V. Phoha. "Continuous User Authentication via Unlabeled Phone Movement Patterns." arXiv preprint arXiv:1708.04399 (2017).

[38] Neverova, Natalia, Christian Wolf, Griffin Lacey, Lex Fridman, Deepak Chandra, Brandon Barbello, and Graham Taylor. "Learning human identity from motion patterns." IEEE Access 4 (2016): 1810-1820.

[39] Sitova, Zdenka, Jaroslav Sedenka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, and Kiran Balagani. "HMOG: A new biometric modality for continuous authentication of smartphone users." arXiv preprint arXiv 1501 (2015).

[40] Deutschmann, Ingo, Peder Nordström, and Linus Nilsson. "Continuous authentication using behavioral biometrics." IT Professional 15, no. 4 (2013): 12-15.

[41] Upadhyaya, Shambhu J. "Continuous Authentication Using Behavioral Biometrics." In IWSPA@ CODASPY, p. 29. 2017.

[42] Li, Fudong, Nathan Clarke, Maria Papadaki, and Paul Dowland. "Active authentication for mobile devices utilising behaviour profiling." International journal of information security 13, no. 3 (2014): 229-244.

[43] Spooren, Jan, Davy Preuveneers, and Wouter Joosen. "Leveraging battery usage from mobile devices for active authentication." Mobile Information Systems 2017 (2017).

[44] O'Neal, Mike, Kiran Balagani, Vir Phoha, Andrew Rosenberg, Abdul Serwadda, and Md E. Karim. Context-Aware Active Authentication using Touch Gestures, Typing Patterns and Body Movement. No. AFRL-RI-RS-TR-2016-076. LOUISIANA TECH UNIVERSITY Ruston United States, 2016.

[45] Primo, Abena, Vir V. Phoha, Rajesh Kumar, and Abdul Serwadda. "Context-aware active authentication using smartphone accelerometer measurements." In Computer Vision and Pattern Recognition Workshops (CVPRW), 2014 IEEE Conference on, pp. 98-105. IEEE, 2014.

[46] Mahbub, Upal, Sayantan Sarkar, Vishal M. Patel, and Rama Chellappa. "Active user authentication for smartphones: A challenge data set and benchmark results." In Biometrics Theory, Applications and Systems (BTAS), 2016 IEEE 8th International Conference on, pp. 1-8. IEEE, 2016.

[47] Lee, Wei-Han, and Ruby B. Lee. "Multi-sensor authentication to improve smartphone security." In Information Systems Security and Privacy (ICISSP), 2015 International Conference on, pp. 1-11. IEEE, 2015.

[48] Xia, Qishou, Xiaoling Yin, Juan He, and Feng Chen. "Real-Time Recognition of Human Daily Motion with Smartphone Sensor." International Journal of Performability Engineering 14, no. 4 (2018): 593.

[49] Diez, Fidel Paniagua, Diego Suarez Touceda, Jose Maria Sierra Camara, and Sherali Zeadally. "Toward self-authenticable wearable devices." IEEE Wireless Communications 22, no. 1 (2015): 36-43.

[50] Eya, Nnabuike, Trust T. Mapoka, Simon J. Shepherd, Raed A. Abd-Alhameed, Issa T. Elfergani, and Jonathan Rodriguez. "Secure Mutual Self-Authenticable Mechanism for Wearable Devices." (2016).

[51] AK Nag, A Roy, and D Dasgupta. "An adaptive approach towards the selection of multi-factor authentication." In Computational intelligence, 2015 IEEE symposium series on, pp. 463-472. IEEE, 2015.

[52] AK Nag, D Dasgupta, and K Deb. "An adaptive approach for active multi-factor authentication." In 9th annual symposium on information assurance (ASIA14), p. 39. 2014.

[53] D Dasgupta, AK Nag, and A Roy. "Adaptive multi-factor authentication system", Utility Patent no. 9912657, 2018.

[54] D Dasgupta, A Roy and A Nag. "Negative Authentication Systems" in Advances in User Authentication, p. 85-145, 2017.

[55] Sepczuk, Mariusz, and Zbigniew Kotulski. "A new risk-based authentication management model oriented on user's experience." Computers & Security 73 (2018): 17-33.

[56] Ometov, Aleksandr, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. "Multi-Factor Authentication: A Survey." Cryptography 2, no. 1 (2018): 1.

[57] Weiner, S. The Future of Biometrics Could Be Your Heart. 2017. Available online: http://www.popularmechanics.com/technology/security/a28443/biometric-heart-scanner/ (accessed on July 10, 2019).

[58] Barkadehi, Mohammadreza Hazhirpasand, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi, and Sarminah Samad. "Authentication systems: A literature review and classification." Telematics and Informatics (2018).

[59] I Memon et al. Design and implementation to authentication over a GSM system using certificate-less public key cryptography (CL-PKC). Wireless personal communications, 79(1), pp.661-686 (2014).

[60] I Memon et al. Efficient user based authentication protocol for location based services discovery over road networks. Wireless Personal Communications, 95(4), pp.3713-3732 (2017).