

Frictionless Authentication Systems: Emerging Trends, Research Challenges and Opportunities

Tim Van hamme, Vera Rimmer,
Davy Preuveneers, and Wouter Joosen

imec-DistriNet KU Leuven
Celestijnenlaan 200A, B-3001 Leuven, Belgium
Email: {firstname.lastname}@cs.kuleuven.be

Mustafa A. Mustafa, Aysajan Abidin,
and Enrique Argones Rúa

imec-COSIC KU Leuven
Kasteelpark Arenberg 10, B-3001 Leuven, Belgium
Email: {firstname.lastname}@esat.kuleuven.be

Abstract—Authentication and authorization are critical security layers to protect a wide range of online systems, services and content. However, the increased prevalence of wearable and mobile devices, the expectations of a frictionless experience and the diverse user environments will challenge the way users are authenticated. Consumers demand secure and privacy-aware access from any device, whenever and wherever they are, without any obstacles. This paper reviews emerging trends and challenges with frictionless authentication systems and identifies opportunities for further research related to the enrollment of users, the usability of authentication schemes, as well as security and privacy trade-offs of mobile and wearable continuous authentication systems.

Keywords—Frictionless authentication; Biometrics; Security; Privacy; Usability.

I. INTRODUCTION

Nowadays, the ubiquitous nature of mobile and wearable devices has allowed users to access a multitude of new applications, services and content. More and more personal related information is stored on (or accessed via) personal devices such as smart phones, which enhances users' experience and convenience, and creates new opportunities for both, consumers and service providers. However, such access of multitude applications via personal devices also brings new challenges for service providers that must now secure access from a wide variety of devices [1]. Moreover, there is a continuous growth of mobile malware and other mobile security threats. Thus, it is important these mobile devices to be equipped with reliable means of authentication and authorization.

However, usually, these mobile and wearable devices have limited computational and interaction capabilities. Furthermore, because these devices are small, light, and easy to carry, there is also an associated risk in that they are susceptible to loss and theft, and easier to break. The use of context information (such as the user's current location, his typical behavior, etc.) may also trigger privacy concerns. Moreover, due to the increased prevalence of wearable and mobile applications, users nowadays expect a frictionless customer experience, making minimum effort. Taking into account these characteristics, the way users are authenticated and granted access to a wide range of online services and content becomes more challenging.

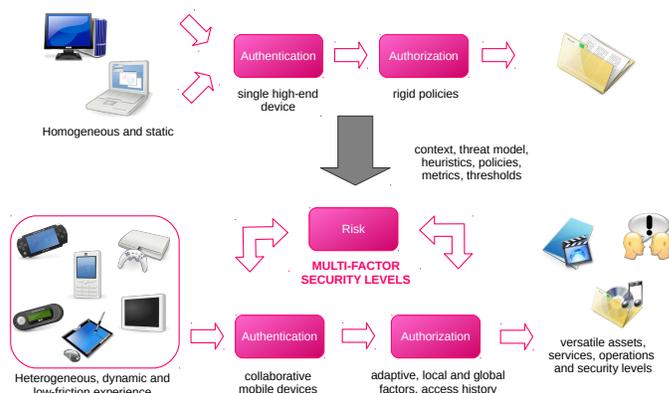


Figure 1. Collaborative, frictionless and adaptive multi-factor authentication with many mobile devices.

Ideally, users' devices will jointly and continuously operate in the background to establish the identity of the individual by continuously monitoring the context and detecting unusual deviations, as depicted in Figure 1. The advantage is that this will move the verification of the additional factors away from the user, making it transparent, and thereby greatly improving the convenience for the user, but posing important privacy challenges when sensitive context information is used, the addressing of which is an important aspect. The objective of pursuing a collaborative multi-device approach is that it can be less vulnerable against malicious users or unauthorized access after theft or loss of a device. Systems that support such user experience are called frictionless authentication systems [2].

In this paper we provide an overview of the emerging trends, research challenges and opportunities in such frictionless authentication systems that allow users to authenticate themselves using their devices to service providers without intentionally performing any specific authentication-related actions, such as entering a password.

The rest of this paper is structured as follows. In Section II, we review the current state of practice in mobile and multi-factor authentication, as well as risk-adaptive solutions. Emerging trends on collaborative and behavioral are highlighted in Section III. Section IV reviews challenges and opportunities for further research. We conclude the paper in Section V.

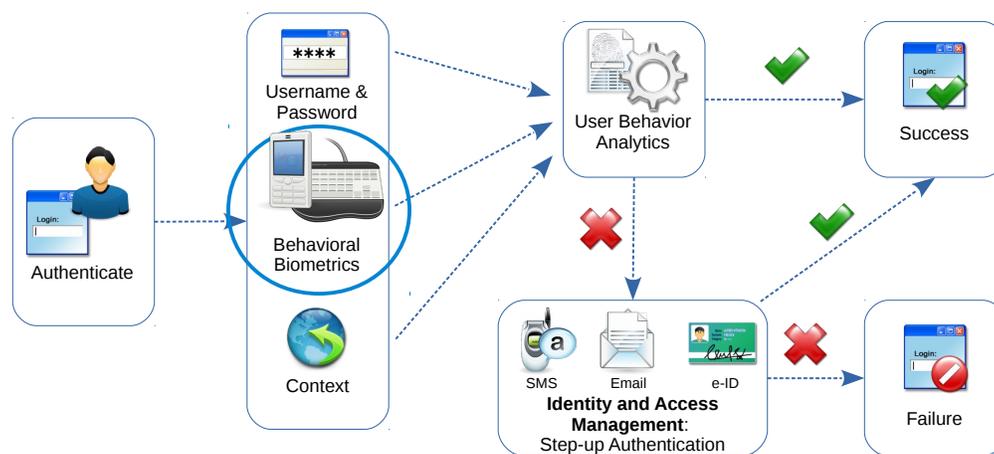


Figure 2. Risk-adaptive step-up authentication leveraging context and behaviometrics adopted within contemporary Identity and Access Management systems.

II. STATE-OF-PRACTICE IN AUTHENTICATION

Before highlighting emerging trends in frictionless authentication systems, we will briefly review current best practices and the state-of-the-art in multi-factor authentication.

A. Mobile and Multi-Factor Authentication

Weak passwords are a major cause of data and security breaches [3]. With dictionary attacks and optimized password cracking tools, users with simple or short (i.e., less than 8 characters) passwords are easy prey, especially if they use the same password for various services. Additionally, complex passwords are difficult to enter on mobile and wearable devices. This illustrates the generally acknowledged conception that passwords are problematic. Therefore, efforts are ongoing to replace password-based authentication with better alternatives [4]–[7]. With multi-factor authentication, users authenticate with a combination of authentication factors, i.e., knowledge, intrinsic (biometrics) and possession. Biometric factors like speaker recognition, fingerprints, iris or retina scans cannot be forgotten, but may require expensive equipment to implement. Furthermore, such solutions require storing biometric templates, which can also be compromised and which are often cumbersome to revoke.

An interesting alternative to multi-factor mobile authentication is the Pico, a concept introduced by Stajano [8]. The Pico is a dedicated hardware token to authenticate the user to a myriad of remote servers; it is designed to be very secure while remaining quasi-effortless for users. The authentication process is based on the use of public-key cryptography and certificates, making common attacks on passwords (such as sniffing, phishing, guessing, and social engineering) impossible. Although being an interesting proposal, an actual implementation is currently lacking.

Leveraging on these recent initiatives, dynamic, multi-factor, collaborative and context-based authentication could further improve the current state-of-the-art on mobile authentication, finding an optimal balance between cost, user-convenience and security and privacy. Early work in this direction was presented in [9] in which the authors presented SmartAuth, a scalable context-aware authentication framework built on top of OpenAM, a state-of-practice Identity and

Access Management (IAM) suite (see Figure 2). It uses adaptive and dynamic context fingerprinting based on Hoeffding trees [10] to continuously ascertain the authenticity of a user's identity.

However, existing solutions that exploit context information often depend on a single device. Especially for mobile devices, a simple device or browser fingerprint is hardly unique and can easily be intercepted and spoofed by an attacker [11].

B. Risk-based Access Control and Enabling Technologies

Authentication is a basic building block of practically all business models. As mobile devices and wearables continue to proliferate and become part of the user's expanded computing environment - fundamentally changing the way people access services and content - there is an associated security risk in that these devices are susceptible to loss and theft because they are small, light, and easy to carry.

The latest trend in access control models is Risk-Adaptive Access Control (RADAC) where access decisions depend on dynamic risk assessments. There is a large body of knowledge on this topic in the scientific literature [12]–[19], and risk-based authentication and access controls are being adopted in contemporary identity and access management solutions, such as SecureAuth IdP 8.0, RSA SecurID Risk-Based Authentication, CA Technologies and ForgeRock's OpenAM 14. Contextual information (device fingerprints, user location, time zone, IP address, time of day and other parameters) is used to evaluate the risk of users attempting to access a resource, but the approach is often based on weighted score functions or meaningless user-defined risk thresholds.

III. EMERGING TRENDS

In this section we provide an overview of the emerging trends in collaborative authentication and behaviometrics.

A. Collaborative Authentication

Authentication means solely based on possession factors bear the risk that the unique possession factor could be lost or stolen, hence compromising the security of the authentication system. Combining these schemes with other authentication factors, such as passwords or PINs, could improve the security,

but at the cost of user-friendliness. Furthermore, one still needs to take into account the typical attacks on knowledge-based authentication factors, such as PIN guessing or phishing attacks. An interesting alternative are collaborative authentication schemes, where multiple devices jointly authenticate to a remote server or within a device-to-device setting. To limit the cost, the combination of wearables and the user's smartphone would be preferred. Such collaborative authentication schemes overcome the security problems of using a single possession factor during the authentication process as an adversary would have to steal multiple wearables to successfully impersonate a user, while still offering user-friendliness. Moreover, by using wearables the user is carrying anyhow, one avoids the need of employing external hardware authentication tokens, which could be quite costly.

The concept of collaborative authentication is to transform a challenge-response protocol with a single prover and verifier, to a challenge-response protocol with multiple collaborating provers and a single verifier. To mitigate the threat of wearables being stolen or lost, and the fact that the set of wearables is dynamic (the user is not always carrying the same set of wearables), threshold-based cryptography is used. The aim of threshold cryptography is to protect a key by sharing it amongst a number of entities in such a way that only a subset of minimal size, namely a threshold $t + 1$, can use the key. No information about the key can be learnt from t or less shares. Shamir [20] was the first to introduce this concept of secret sharing. Feldman [21] extended this concept by introducing verifiable secret sharing. Pedersen [22] then used this idea to construct the first Distributed Key Generation (DKG) protocol. Shoup [23] showed how signature schemes such as RSA could be transformed into a threshold-based variant.

To increase the resilience in a threshold-based authentication scheme, the number of devices included in the threshold scheme should be maximized. Therefore, Simoens et al. [24] presented a new DKG protocol and demonstrated how this allows wearables not capable of securely storing secret shares to be incorporated. Peeters et al. [25] used this idea to propose a threshold-based distance bounding protocol. A gap that remains to be filled is a threshold-based mobile authentication scheme, where the secret keying material is distributed among a set of personal wearables. For recent developments in continuous authentication, we refer the reader to [26].

B. Biometrics

A recent trend in the area of continuous authentication is the use of biometrics. DARPA hosted the Active Authentication program [27] in which various kinds of behavioral biometrics, i.e., metrics that measure human behavior to recognize or verify the identity of a person, are investigated. Several studies have investigated the application of using biometrics in order to provide an authentication method that is (a) *continuous*, during an entire user session, and (b) *non-intrusive*, since the normal user interaction with the system is analyzed. It has been demonstrated that a user identity can be recognized and verified by means of several biometrics, such as keystroke dynamics, mouse movements (together with display resolution) [28], gait analysis [29], CPU and RAM usage [30], accelerometer [31] and battery fingerprints of mobile devices [32], stylometry [33], web browsing behavior [34], etc.

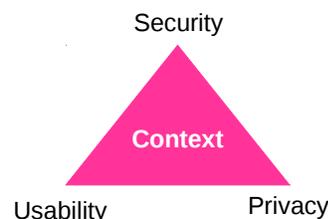


Figure 3. Security, privacy and usability trade-offs in frictionless authentication.

An overview of techniques can be found in these works [35]–[37] and survey [38]. A key challenge will be to investigate which combination of biometrics will deliver a sufficient low number of false positives (mistakenly granted access = security concern) and false negatives (mistakenly denied access = user experience concern) such that the risk is acceptable given the circumstances.

IV. CHALLENGES AND OPPORTUNITIES

A frictionless authentication system is a complex system, involving multiple devices and sensors that interact with each other. This complexity makes such systems also a very flexible kind of authentication system. Nonetheless, several challenges and research opportunities remain. Authentication systems are usually characterized by the following interacting dimensions (see Figure 3):

- *Security*, which refers to how difficult it is for an impostor to be falsely authenticated.
- *Usability*, which describes how easy and convenient it is for genuine users to be authenticated.
- *Privacy*, which describes how any private information about the user being used are securely stored and/or processed by the system.

Security and usability are usually a trade-off in most authentication systems. For instance, False Acceptance and False Rejection Rates (FAR and FRR, respectively) are usually depicted in a ROC curve in biometric systems, and the lower the FAR is the higher the FRR is, where FAR is related to security, and FRR is related to usability. Hence, authentication systems are characterized by a specific security-usability trade-off. Regarding privacy, it can be also related to the security and usability of an authentication system. For instance, biometric systems based on protected templates, with a superior privacy protection when compared to their unprotected counterparts, usually provide an inferior set of working points regarding usability and security. In addition, the disclosure of a biometric template can lead to a security problem, unless appropriate revocation mechanisms are incorporated.

Active authentication systems involve multiple devices and sensors that interact with each other. This complexity also makes a frictionless authentication system a very flexible and powerful kind of system, which can be dynamically adapted to different usage scenarios, security-usability trade-offs, and overcome situations in which other types of authentication mechanisms would normally fail. In what follows, we expose different challenges and opportunities related to these three dimensions, *security*, *usability* and *privacy*, and specific to frictionless authentication systems

A. Security

Regarding security, active authentication systems based on multiple biometrics and/or biometrics can provide increased security, since they are intrinsically multi-factor, and each employed behavioural modality makes them more difficult to spoof. However, the authentication decision will be based on the outcome of the classification and/or clustering algorithms. Such algorithms are usually not 100% accurate [38], and in some cases the templates must be retrained by discarding old data to account for changes in the user's behaviour. This creates an opportunity for an attacker to impersonate a legitimate user by manipulating input data to compromise the learning process (i.e., a poisoning attack).

A specific security concern in continuous authentication systems is related to the enrollment. The enrollment phase establishes the identity of the subject within the authentication systems. Typically, this is based on credentials or certificates. However, with behavioral and context-dependent authentication, the enrollment phase becomes far more challenging, especially when using a collaborative authentication relying on multiple mobile and wearable devices. In the case of other biometrics, this can be done by ensuring the identity of the user during the enrollment phase by other means. However, since the enrollment in biometrics is done in an uncontrolled environment, the enrollment can also pose a threat to security, since it may be easier to inject artificial data to the system. Furthermore, behavioral authentication systems relying on machine learning methods require a time-consuming training step on an individual basis before they become effective.

B. Usability

Regarding usability, the frictionless nature of continuous authentication makes these systems one of the most convenient and easy to use modalities, since the user does not even need to learn how to use the authentication system, and the authentication process is transparent, potentially providing a smooth user experience. Furthermore, the availability of different sensors and modalities opens the opportunity to provide a very flexible authentication mechanism, where the system can implement different security/usability trade-offs for controlling the access to different functionalities or services. However, this also poses a challenge regarding the design of template protection techniques, since this flexibility may increase significantly the complexity of the system.

C. Privacy

Another key challenge with frictionless authentication systems is addressing the privacy concerns which arise when user behaviour analytics on sensitive data is used to continuously authenticate against online services. *Honest but curious* service providers can use the keystrokes – collected for behavioral authentication purposes – to reconstruct the original text typed by the users. In addition, accelerometer data could be used by the same kind of adversary to reconstruct the whole history of a user's location. Furthermore, continuous authentication can also use physiological biometric measurements, whose implications regarding privacy are well known. Hence, employing the adequate biometric template protection mechanisms and appropriately imposing data minimality principles in the system design is even more important in continuous authentication.

V. CONCLUSIONS

There is a continuous quest for stronger authentication systems that at the same time offer a frictionless experience towards users of mobile and wearable devices. Context and behavioral information are nowadays being adopted in the enterprise marketplace as part of an adaptive authentication strategy that better serves the needs of the mobile consumer in diverse situational circumstances. However, irrespective of the technological advances to have multiple mobile and wearable devices collaborate to authenticate a user, the adoption of frictionless authentication will only be successful when the right balance between usability, security and privacy can be found that meets the demands of a diverse set of users.

ACKNOWLEDGEMENTS

This work was partially supported by the Research Council KU Leuven: C16/15/058. In addition, it was also funded by FWO through SBO SPITE S002417N and imec through ICON DiskMan. DiskMan is a project realized in collaboration with imec. Project partners are Sony, IS4U and Televic Conference, with project support from VLAIO (Flanders Innovation and Entrepreneurship).

REFERENCES

- [1] S. Sagioglu and D. Sinanc, "Big data: A review," in International Conference on Collaboration Technologies and Systems (CTS 2013), May 2013, pp. 42–47.
- [2] M. A. Mustafa, A. Abidin, and E. Argones Rúa, "Frictionless authentication system: Security & privacy analysis and potential solutions," in the 11-th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2017). IARIA, 2017.
- [3] M. Jakobsson and M. Dhiman, *The Benefits of Understanding Passwords*. New York, NY: Springer New York, 2013, pp. 5–24.
- [4] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino, "Privacy preserving multi-factor authentication with biometrics," in Proceedings of the Second ACM Workshop on Digital Identity Management, ser. DIM '06. New York, NY, USA: ACM, 2006, pp. 63–72.
- [5] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proceedings of the IEEE Symposium on Security and Privacy, ser. SP '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 553–567.
- [6] E. Grosse and M. Upadhyay, "Authentication at scale," *IEEE Security Privacy*, vol. 11, no. 1, Jan 2013, pp. 15–22.
- [7] R. P. Guidorizzi, "Security: Active authentication," *IT Professional*, vol. 15, no. 4, July 2013, pp. 4–7.
- [8] F. Stajano, *Pico: No More Passwords!*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 49–81.
- [9] D. Preuveneers and W. Joosen, "Smartauth: Dynamic context fingerprinting for continuous user authentication," in Proceedings of the 30th Annual ACM Symposium on Applied Computing, ser. SAC '15. New York, NY, USA: ACM, 2015, pp. 2185–2191.
- [10] P. Domingos and G. Hulten, "Mining high-speed data streams," in Proceedings of the Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ser. KDD '00, 2000, pp. 71–80.
- [11] J. Spooen, D. Preuveneers, and W. Joosen, "Mobile device fingerprinting considered harmful for risk-based authentication," in Proceedings of the Eighth European Workshop on System Security, ser. EuroSec '15. New York, NY, USA: ACM, 2015, pp. 1–6.
- [12] J. Li, Y. Bai, and N. Zaman, "A fuzzy modeling approach for risk-based access control in ehealth cloud," in 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, July 2013, pp. 17–23.
- [13] I. Molloy, L. Dickens, C. Morisset, P.-C. Cheng, J. Lobo, and A. Russo, "Risk-based security decisions under uncertainty," in Proceedings of the Second ACM Conference on Data and Application Security and Privacy, ser. CODASPY '12. New York, NY, USA: ACM, 2012, pp. 157–168.

- [14] R. A. Shaikh, K. Adi, and L. Logrippo, "Dynamic risk-based decision methods for access control systems," *Computers and Security*, vol. 31, no. 4, 2012, pp. 447 – 464.
- [15] Q. Ni, E. Bertino, and J. Lobo, "Risk-based access control systems built on fuzzy inferences," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 250–260.
- [16] D. R. d. Santos, C. M. Westphall, and C. B. Westphall, "A dynamic risk-based access control architecture for cloud computing," in *2014 IEEE Network Operations and Management Symposium (NOMS)*, May 2014, pp. 1–9.
- [17] "An adaptive risk management and access control framework to mitigate insider threats," *Computers and Security*, vol. 39, 2013, pp. 237 – 254. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167404813001119>
- [18] H. Khambhammettu, S. Boulares, K. Adi, and L. Logrippo, "A framework for risk assessment in access control systems," *Computers & Security*, vol. 39, 2013, pp. 86 – 103.
- [19] S. Kandala, R. Sandhu, and V. Bhamidipati, "An attribute based framework for risk-adaptive access control models," in *6th International Conference on Availability, Reliability and Security*, Aug 2011, pp. 236–241.
- [20] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, 1979, pp. 612–613.
- [21] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *SFCS '87*, ser. SFCS '87, 1987, pp. 427–438.
- [22] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *CRYPTO'91*, ser. LNCS, vol. 576. Springer, 1992, p. 129140.
- [23] V. Shoup, "Practical threshold signatures," in *Advances in Cryptology–EUROCRYPT 2000*. Springer, 2000, pp. 207–220.
- [24] K. Simoens, R. Peeters, and B. Preneel, "Increased resilience in threshold cryptography: Sharing a secret with devices that cannot store shares," in *International Conference on Pairing-Based Cryptography*, ser. LNCS, vol. 6487. Springer, 2010, pp. 116–135.
- [25] R. Peeters, D. Singelee, and B. Preneel, "Toward more secure and reliable access control," *IEEE Pervasive Computing*, vol. 11, no. 3, 2012, pp. 76–83.
- [26] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," *IEEE Signal Processing Magazine*, vol. 33, no. 4, 2016, pp. 49–61.
- [27] R. P. Guidorizzi, "Security: active authentication," *IT Professional*, vol. 15, no. 4, 2013, pp. 4–7.
- [28] P. X. de Oliveira, V. Channarayappa, E. O'Donnell, B. Sinha, A. Vadakkencherry, T. Londhe, U. Gatkal, N. Bakelman, J. V. Monaco, and C. C. Tappert, "Mouse movement biometric system," *Proc. CSIS Research Day*, 2013.
- [29] T. V. hamme, D. Preuveneers, and W. Joosen, "Improving resilience of behaviorometric based continuous authentication with multiple accelerometers," in *Data and Applications Security and Privacy XXXI - 31st Annual IFIP WG 11.3 Conference, DBSec 2017*, Philadelphia, PA, USA, July 19-21, 2017, *Proceedings*, 2017, pp. 473–485.
- [30] I. Deutschmann, P. Nordström, and L. Nilsson, "Continuous authentication using behavioral biometrics," *IT Professional*, vol. 15, no. 4, 2013, pp. 12–15.
- [31] T. van Goethem, W. Scheepers, D. Preuveneers, and W. Joosen, "Accelerometer-based device fingerprinting for multi-factor mobile authentication," in *Engineering Secure Software and Systems - 8th International Symposium, ESSoS 2016*, London, UK, April 6-8, 2016. *Proceedings*, 2016, pp. 106–121.
- [32] J. Spooren, D. Preuveneers, and W. Joosen, "Leveraging battery usage from mobile devices for active authentication," *Mobile Information Systems*, vol. 2017, 2017, pp. 1 367 064:1–1 367 064:14.
- [33] K. Calix, M. Connors, D. Levy, H. Manzar, G. McCabe, and S. Westcott, "Stylometry for e-mail author identification and authentication," *Proceedings of CSIS Research Day*, Pace University, 2008, pp. 1048–1054.
- [34] M. Abramson and D. W. Aha, "User authentication from web browsing behavior," *DTIC Document*, Tech. Rep., 2013.
- [35] M. Karman, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Applied Soft Computing*, vol. 11, no. 2, 2011, pp. 1565 – 1573.
- [36] I. Deutschmann, P. Nordström, and L. Nilsson, "Continuous authentication using behavioral biometrics," *IT Professional*, vol. 15, no. 4, July 2013, pp. 12–15.
- [37] H. Saevanee, N. L. Clarke, and S. M. Furnell, *Multi-modal Behavioural Biometric Authentication for Mobile Devices*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 465–474.
- [38] L. Wang, *Behavioral Biometrics for Human Identification: Intelligent Applications*. IGI Global, 2009.