Contextual, Behavioral, and Biometric Signatures for Continuous Authentication

Kyle Quintal
School of Electrical Engineering and Computer Science, University of Ottawa

Burak Kantarci
School of Electrical Engineering and Computer Science, University of Ottawa

Melike Erol-Kantarci
School of Electrical Engineering and Computer Science, University of Ottawa

Andrew Malton
BlackBerry Limited

Andrew Walenstein
BlackBerry Limited

***Abstract*—Continuous authentication in the Mobile Internet of Things should be based as broadly as possible, since a wide range of factors continuously reveal unexpected correlations. Such factors may include captured events (e.g., password, fingerprint, application start and end, network connect, and disconnect), continuous time series (e.g., gesture, typing rate, accelerometer, GPS, ambient sound, light levels, and time-of-day), and derived behavioral features (e.g., user sociability, browser and application menus, application choice). All these factors have been shown to correlate with the actual user identity, often in surprising combinations. More and more sensors are being deployed in autonomous devices, smart environments and vehicles, enabling even further behavioral and contextual data to be analyzed. The pegs of this continuous authentication "big tent" are moving out further than ever before, bringing it closer to practical uses in our everyday lives.**

With the advances in next generation of communications and the Internet of Things (IoT), cybersecurity has evolved into a multidimensional problem. While encryption, access control, and defense against malicious behavior and malware are the major focus of traditional cybersecurity, identification, and authentication have introduced new objectives including continuity, nonintrusiveness, and convenience. Traditionally, authentication involves the verification of a user's identity on a particular system by means of

Digital Object Identifier 10.1109/MIC.2019.2941391
Date of publication 13 September 2019; date of current version 18 December 2019.

Published by the IEEE Computer Society

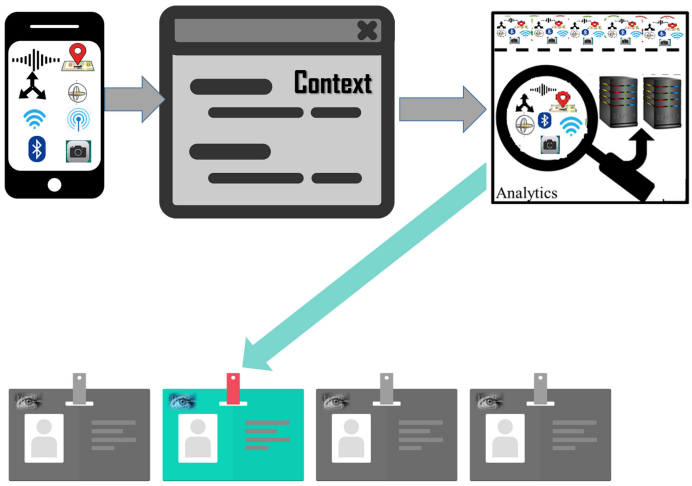

Figure 1. High-level presentation of context, behavior, and biometric-based authentication. The context is generated as a multisensor array by the user through various built-in sensors. Analytics engine runs real-time analytics solutions to classify the contextual pattern and make recommendation concerning the authenticity of a user.

passwords, cryptography and, more recently, biometrics. Upcoming transitions toward cloud, mobile edge, and fog systems, together with their integration with data science and signal processing techniques, have brought forward *behavioral signatures* as cost efficient, convenient, and complementary solutions to augment conventional authentication methods.[1] Using derived behavioral features such as user sociability, browser, and application menus, application choices for user identification is known as behaviometrics. Behaviometrics offer new opportunities in the recognition of behavioral and contextual patterns within different cyber domains, and has been identified as a strong candidate for implementation of continuous authentication in the presence of uncertainties concerning the user's identity.

Behavioral signatures of a user can be obtained from interaction patterns, habits, and routines of using mobile applications[1] as well as physical behavioral features, like gestural patterns.[2] Constructing behavioral signatures in various contexts can add support to continuous authentication by reducing the required reauthentication steps without triggering access control (password reauthentication) nor interfering with a user's regular usage patterns.

A minimal illustration of the use of context and behavioral signatures in user authentication is presented in Figure 1. Lower uncertainties, lower cost, less obtrusion, higher privacy preservation, and improved security are the main objectives in authentication. But how can contextual and behavioral signatures support continuous authentication of users with minimum uncertainties on authenticity? Alternatively, in a cyberspace where the number of connected devices is soon to pass the world population, how can the huge amount of data acquired from smart and personal devices (including wearables) be abstracted into identifiable behavioral signatures? Surely contextual and behavioral signatures cannot *replace* legacy authentication methods, but the first step is to model various contexts of a user's activity, and to define analytic models such as time series analysis or machine learning to authenticate users in the current or predicted environments.

In the IoT era, there exists a much larger scale of uniquely identifiable "things," not users, equipped with sensing and communication capabilities, which (like users) are subject to identity management. Continuous authentication, obtaining reliability through context and behavioral signatures, promises automated assistance for this problem of scale.

Different surveys on context-awareness have previously been published, such as by Huseynov and Seigneur,[3] where the authors focus on multifactor authentication methods, specifying how certain methods leverage a given context to provide heightened security or an improved user experience. A survey overviews different security schemes,[4] leveraging trust or context based-schemes for device authentication within ubiquitous settings.

This paper differs from previous studies in the multiple ways. The area of context-aware authentication is rapidly developing, and over the last few years, has made significant contributions to the literature, which are not covered in such papers. With these in mind, we focus on recent advances in context, biometric, and behavior-based authentication schemes and provide a comparative overview highlighting their respective pros and cons.

Generally, biometric studies require a high number of features, behaviometrics studies require rich and heterogeneous user participation, and context-based studies often have restrictions on data collection methods within their specific context. An elaborate comparison of challenges is provided in this paper to serve as a roadmap for readers interested in tackling the challenge of advancing the field of continuous authentication from feasibility to practicality.

FROM BIOMETRICS TO CONTEXTUAL AND BEHAVIORAL INFORMATION

Looking over the past half-century of biometric advancements, Jain *et al.* provide a rather complete analysis of the many decades of biometric identification methods.[5] Notably, three methods have found successful practical use: fingerprint recognition, facial recognition, and iris recognition. Each of these has been developed to track identification needs in the technological society. We can easily see these methods in use today: fingerprint authentication in mobile phones, face recognition embedded in social media, and iris scanners at many border crossings.

Although biometrics are becoming a more common method of identification, there still exists some limitations. It is not easy to make a distinct identification from a single sample of a biometric trait, because of noise and environmental variation. Persistence is another challenge: as a subject ages, some identifiable features change. Only recent machine learning methods have begun to address the aging of biometric data. Environmental conditions are not always pristine when extracting different traits. For instance, hats and/or glasses are not favorable when trying to identify someone using facial recognition. Finally, just like most authorization systems, biometrics methods are vulnerable to a number of security threats. These could include spoofing, replay attacks, man-in-the-middle, etc. However, these issues may be revisited in the near future, with the introduction of new sensing and computing platforms and advances in artificial intelligence.

Contextual data are increasingly recognized as a valuable supplement to established biometrics for authentication. A simple definition of *context* is the characteristics of a setting where an action is performed: for continuous authentication, this includes performed actions on networked devices. Those with daily routines move through different contexts, such as the laptop used in one's office, interactions with their mobile device while commuting, or even their browser activities during their lunch break. Each context has its own set of typical features, and contains characteristic information. For instance, a particular user always connects their laptop to a specific SSID when at work. The combination of this specific laptop on its specific network brings additional confidence that its user is the genuine owner. Such correlations suggest information to capture from the environment, to identify the context. In addition, recognizing which users and devices are habitually copresent suggests how context can be used to identify and authenticate users for an access control decision.

Although smart devices are increasingly present in our daily lives, their built-in sensors could provide much more contextual data, and they are at present underutilized for authentication purposes. In a system utilizing contextual and behavioral signature-based authentication, such multisensor devices would be used to construct and match *contextual signatures*: behavioral signatures correlated and coupled with context. A database of contextual patterns could then provide a contextual signature starting point, which could also be used by machine learning classifiers for training purposes. This way, future contextual signatures would undergo a classification process to find out whether a matching signature exists.

There already exist similar contextual recognition techniques. Machine learning has recently seen advancements in this field, as contextual and behavioral patterns of a user can be "learned" in this sense. Decisions can be made to authenticate users with high certainty, verifying their identity based on this information. It is also possible to "pair" entities together based on their context. This includes (but not limited to) pairing different devices together based on a shared secret (common key), pairing devices with their users based on similarity in features, or again to join a specific cluster of identified devices that share a common deviation in environmental change over time. In the following section, we focus on different domains of authentication, and their contributions to the overarching

challenge of continuous identity verification in the IoT era.

EXPANDING THE SCOPE OF AUTHENTICATION

The advances in data analytics and machine intelligence have led to innovative solutions in identification and authentication by mining and recognizing behavioral patterns and contextual properties. Such techniques call for effective solutions to cope with their variability over time and under different circumstances. These solutions should not be seen as replacements of conventional authentication techniques (biometric authentication) but, rather, as improvements.[6] Such improvements could render authentication mechanisms more convenient and less intrusive, while improving security. Unfortunately, many techniques have limiting challenges, which can reoccur in multiple domains. Such challenges are discussed in further detail within Section OPEN ISSUES AND CHALLENGES. The following sections discuss the current state of authentication methods, overview variations on current biometric methods, and demonstrate the potential of behavioral and context-based contributions in authentication.

Modern Authentication Techniques

Although there has been a wide range of new authentication methods recently, most of them still require some level of interaction with individuals. They often provide high security in a single or a few technological areas, but are almost never in all domains of IoT. Furthermore, with all this readily available data, innovations which depend on such rich information must be designed with ethical considerations.

An extensive survey was conducted[7], focusing on different social authentication applications. These applications were compared by their availability in local and online platforms, used features, task effectiveness, and potential threats. Three aspects were considered for scoring purposes: security, deployability, and usability. These metrics become critical as social authentication applications are emerging from so many domains, and their respective tradeoffs must also be considered. As an increasingly popular and time-consuming component of current and upcoming generations, social applications must consider those values in future context-aware mobile developments, as privacy, trust, identity, security deployability, and usability only become increasingly important considerations.

Adaptive Biometrics

Biometric authentication has now become one of the most successful methods of authentication. These techniques are also known to require low levels of interaction, limiting user intrusions. There have been solid and notable contributions to continuous authentication using adaptable biometric solutions, as seen below.

Multifactor authentication improves security, and multimodal biometric authentication, which is introduced by Huseynov and Seigneur,[3] improves the convenience-security tradeoff of such techniques. Furthermore, a new approach was introduced in cloud computing authentication systems,[8] where the authors analyze the association between features to focus on improving the user experience (UX). Particularly, their proposed algorithm considers the authentication habits of users, alongside time, device, and location. By using these features, the most historically adequate biometric method is presented to the user. The integration of behaviometrics in this study demonstrates the need to bridge the two domains in order to achieve efficient continuous authentication.

In a similar combinational model, Witte *et al.* introduced a context-aware mobile biometric technique, which authenticates with the power of machine learning.[8] More specifically, the authors combine users behavioral signatures alongside their biometric tendencies to learn which biometric method would be most effective in the given context. Unlike most mobile-based systems, the study stands out as a GPS-free solution. Since standard mobile anomaly detection systems often depend on location in large areas or without geographical limitations, this paper could provide valuable authentication improvements when localization is unavailable.

Continuous Behaviometrics

The concept of analyzing human behavior to determine one's authenticity has constantly

been gaining interest. The immense surge of available and heterogeneous data volumes in the past few years have led to reasonably accurate behavior analyses.

Different social networks continue to increase in popularity within the mobile domain. As such, the notion of sociability has become of interest.[1] Anjomshoa *et al.* introduce this notion by monitoring social networking behavior (i.e., social networking data usage, usage frequency, time spent on a particular social network application, etc.) to continuously verify users on their mobile devices. This continuous authentication method allows uninterrupted usage of mobile devices over 90% of the time. Not only did their results demonstrate convenience, but also were able to detect anomalous behavior with an accuracy of up to 97%. Sociability features extracted from a user's social context shows potential in improving system robustness and higher user comfort. The constant polling of social platform traffic enables the possibility of continuous authentication, although at a cost of higher computational requirement.

The study[9] leverages various mobile behavioral aspects: text input, application usage, browser history, and geographic data. The authors, despite their initial successful results, were able to introduce further improvements,[10] where they included input frequency (time-series) to improve their models. Using these behavioral patterns, they were able to authenticate with error rates as low as 1%. Indeed, the study only contained a limited set of features; even still, with low error rates, location can provide additional information when making authentication decisions. Despite the benefits of the proposed technique, battery consumption remains an issue for participants, as the constant polling of data across all components has a high resource demand.

Next, a similar system was proposed[11] to analyze users' behavioral patterns within their pervasive environments. Specifically, the system performed behavioral analysis to improve identity confidence and detect behavioral anomalies, using the following categories: 1) Operational context, which related to performed tasks, goals, and activities, 2) Interpersonal context, which denotes information portraying to relationships and communications within the users community and social applications, 3) Spatial context, which stands for data related to a participant's location and environmental properties. These features are combined to create what the authors call *Contextual Identity*. This identity is then learned using *k*-means clustering, and used to detect future behavior that is noncompliant with a user's *Contextual Identity*. This paper introduces the following question on behavioral signatures: even with the ability of identifying users based on previous context, what happens in the case of anomalies? Is the user simply entering a new context which should be learned (potentially with online learning), or should precautions be implemented to keep out malicious users? It becomes difficult to detect these differences under rapid context changes.

With the help of machine intelligence,Rauen *et al.*[2] appended their previous work on sociability analysis[1] to propose a dual authentication model. Bringing gesture patterns alongside social platform usage, Rauen *et al.* achieved near perfect authentication with 99.65% accuracy. Not only those results came out of their study; anomaly detection was again successfully achieved, with error rates under 3%. Their gesture model consisted of analyzing and associating different swiping behaviors to mobile users (such as single and double tap, tap and hold, fling, and scroll). This study is yet another example of how behavior patterns can lead to successful authentication techniques.

Context-Based Authentication

As environments are in constant flux, the resulting change in context also holds valuable information. Additional patterns tend to emerge, with potential corresponding identity associations, which are discussed below, in varying areas of IoT.

An important question is raised,[12] where the authors investigate how continuous authentication could be achieved on devices with no user interface. For example, smart watches and other body-area network sensors may not be equipped with keyboards or touchscreens, thus, limiting authentication methods. Using the interdependence of Apple products, the authors performed a case study to analyze participants' gait, echocardiogram signals, among other health metrics. Their top participants were able to achieve

authentication rates around 90%. However, their results require sensors to be in close proximity (within a six meters radius), and could only authenticate a particular selected user, and not all. As concluded by the authors, the higher the pool of features within this context, the further the analysis can be pursued for continuous authentication.

Looking toward a military environment, many applications could benefit from contextual extraction and analysis. A conceptual study presented by Castiglione *et al.* report of many available biometric features within a military setting.[13] Sensors located on soldiers, weapons, and vehicles can all provide additional sensory information, which allows the extraction of valuable insights in military situations. Such information includes both static (heart-rate) and dynamic (gestures, facial expressions) sensory data, alongside environmental metrics (e.g., operative conditions, environmental conditions, active sensors, subject motion). Notably, these features provide sufficient information for the identification of a soldier's health status. In Internet of Military Things, having such a wide variety and density of dynamic sensors results in large volumes of valuable information, which requires larger memory space. As a recurring theme, many context extraction techniques face computational limitations.

In a vehicular environment, driving efficiency, safety, and convenience are all desired outcomes. These considerations[14] propose a verification system in vehicular platoon admission, which relies on vehicular context. More specifically, road and traffic conditions are extracted to verify and identify a vehicle requesting to join a moving vehicular cluster. Such road properties are combined with environmental readings to determine the authenticity of the admitting vehicle. Their proposed system also considers an attacker model, as malicious entry to the platoon could cause tremendous physical and financial damage. Performance results demonstrate accurate admissions of around 91% when within the same lane, and 82% when crossing multiple lanes. The overwhelming details and complexities in such a domain produces many difficult and unexpected challenges. Thus, authentication is a concept not only relevant to human context, but also worth investigation within the domain of autonomous vehicles and IoT.

Miettinen *et al.* use context itself as an authentication factor by inspecting the surroundings of a device's sensory readings.[15] More specifically, two mobile devices that obtain similar environmental sensory readings are able to authenticate themselves within a given space. This becomes possible when devices have sufficiently similar entropy readings from the environment. Specifically, their entropy calculations combine readings of ambient noise levels with environmental readings in different environments (e.g., office and home). The authors conclude that only with enough time to analyze the entropy of the environment, contextual authentication is possible. The combination of such features leads to high computational complexity, which revokes the application in real-time scenarios. Nonetheless, adaptable authentication rules become an interesting concept when you consider the constant change of context in our lives; using ambient noise for such adaptability demonstrates significant potential.

A context-aware framework called SmartAuth was developed by Preuveneers *et al.* as a continuous authentication system[16] for intelligent devices. Suggested as a zero-interaction authentication scheme, SmartAuth extracts features from both the client (system language, color depth, screen resolution, timezone, platform, plugins) and server side (IP range, headers, time of access, geolocation) to authenticate users using machine learning (Hoeffding trees). Evidently, results improved as the number of successful interactions rose, increasing the correlation between identity with specific features. In other words, the higher the interaction count, the easier it became to authenticate users. In the previous mobile studies, geolocation was the most important feature, and although it remains important, case-by-case analysis is required to select the most important feature given a particular context.

OPEN ISSUES AND CHALLENGES

Currently, the most robust approach in solving uniqueness in authentication is the application of biometrics. Despite its robustness, it does require a minimal amount of user interaction, and certain

Table 1. Scope of authentication techniques.

Source	Authentication Domain	Domain Feature(s)	Authentication Method(s)	Advantages/Disadvantages
[17]	Adaptive Biometrics	MFA-MB Biometric preferences Location	SVM's by extension	⇑ Continuously improving UX ⇑ High circumvention with biometrics ⇓ Computation time not considered ⇓ Acceptability case-dependent
[8]	Adaptive Biometrics	Location , Light Accelerometer, Calls Battery, Microphone	SVM's	⇑ Persistent results despite high entropy ⇑ Distinct profiles ⇓ Malicious attempts not considered ⇓ Feature weights are device-dependent
[11]	Behaviometrics	Phone calls Personal schedule GPS Application usage	k-means clustering	⇑ High confidence rate ⇑ Clear behavior profiles ⇓ Unknown behavior in dense user space ⇓ Unknown contribution per feature
[1]	Behaviometrics	Social interactions Social applications	SVM's DBSCAN	⇑ FRR $< 10\%$ ⇑ 90% Continuous Authentication ⇑ 97% Anomalous detection ⇓ Limited data-set size ⇓ Homogeneous participants ⇓ Dependent on active users
[10]	Behaviometrics	Stylometry, apps, browser and GPS	SVMs Fusion-decision model	⇑ Large and heterogeneous dataset ⇑ Decreasing EER over time ⇓ Homogeneous participants ⇓ Battery intensive ⇓ Dependent on active users
[2]	Behaviometrics	Gesture Patterns	Random Forest Classifier SVM's DBSCAN	⇑ High Accuracy with dual-model ⇑ Low FAR-FRR rates with dual-model ⇓ Limited data-set ⇓ Homogeneous participants ⇓ Dependent on dual-model
[15]	Context-based	Ambient Noise levels	Similarity of fingerprint quantization model	⇑ Low FAR-FRR rates ⇑ Minimizes authentication attempts ⇓ Requires low entropy environment ⇓ Results require long fingerprints ⇓ Limited data-set
[18]	Context-based	Health metrics	NA	⇑ Resilient against cyberattacks ⇑ Low authentication time ⇓ No Learning/Reasoning model ⇓ Dependant on 5G
[12]	Context-based	Gait ECG + CSI signals	NA	⇑ No additional sensors required ⇑ Up to 93% recognition accuracy ⇓ Strict environmental limitations ⇓ Not suitable for sensitive tasks
[13]	Context-based	Equipment Sensors Soldier Biometrics Vehicle Metrics	NA	⇑ Wide feature-set extraction ⇑ Provide strategical military advantages ⇓ Requires Edge-computing ⇓ Limited by high data traffic
[14]	Context-based	Road and traffic conditions	Fingerprint similarity using fuzzy commitment scheme	⇑ 92% similarity in same lane ⇑ 81% similarity in multi-lane ⇓ High risk requires low uncertainty ⇓ Requires robust defense against attacks
[16]	Context-based	Fingerprints Client details Server details	Hoeffding Trees	⇑ 99% accuracy after learning ⇑ Minimal performance overhead ⇑ Improved UX from passwords ⇓ Results provided from simulations ⇓ Limited to OpenAM platform

biometric sensors (e.g., fingerprint scanner) do require higher processing power. Their effectiveness is however deemed an acceptable tradeoff, as seen in their deployments into many digital markets. A similar pattern of even less intrusive techniques is now emerging with continuous context-based authentication. In the previous sections, different techniques were discussed in authenticating users or devices in independent studies. An extensive comparison of such techniques is seen in Table 1, where the feasibility of each technique is only relevant within its particular study. These nonintrusive techniques are now assisting authentication decisions, but further improvements are required for a more widespread nonintrusive application of continuous authentication. Included in this section are common challenges found across the presented studies which limit the application of continuous authentication nowadays.

Data Collection

In any particular context, obtaining a precise, accurate, and ubiquitous dataset is quite desirable. However, real-world applications often introduce technical challenges; in research practice, obtaining a large pool of heterogeneous participants is not a common occurrence.[1] In fact, even in a simulated setting, behavioral patterns are often based on statistical models derived

from a few representative participants.[16] The resulting dataset is thus often limited in volume and/or heterogeneity. Also, participants have no incentives when installing external tools on their devices,[19] which causes the data frequency also to be limited.

Since many devices have significantly improved in computing specifications over the past few years, extracting contextual information can be a regular task for modern devices, but quite challenging for others. For instance, certain applications require constant environment polling to minimize errors and increase convenience.[10] Furthermore, memory limitations are also a concern when extracting data from a wide variety of nondedicated sensors.[13] A potential solution for this issue could be edge computing, also pointed out by Castiglione,[13] since edge nodes could include additional dedicated sensors, decreasing the memory requirements on such nondedicated sensors. The resulting high data traffic produced with edge computing would unfortunately require the upgrade of existing infrastructures, alongside the application of intelligent data filtering and throttling strategies.

Sensor readings often introduces small but significant errors, which inject noisy data patterns. This phenomenon spread across multiple devices, compromises the needed accuracy for sufficient results in highly sensitive and/or concurrent tasks.[12] Therefore, suggested improvements which obtained results from smaller data volumes must ensure considerations of noisy data when scaling their applications.

Selection of optimal features is another challenging issue concerning data collection. When there is a wide variety of available features, additional analysis is required to distinguish the contextual value provided with each feature. Especially within the domain of biometrics, the best features fluctuate between personas and context.[5]

Within the reviewed papers, many pairing techniques use similarities in context within their decision models. As such, there is direct dependence on copresent devices when extracting context which becomes challenging in lower device-dense environments.[20] To the contrary, in highly dense environments, authentication becomes increasingly feasible, but at the expense of needed considerations of attack threats. This point was addressed by Mansour *et al.*,[17] where brute force intrusions were nullified by increasing the guessing complexities of identifiers. However, this is but one of the many threats that could potentially rise from a highly dense environment.

Selection and Iteration of Methodologies

Selection of an optimal biometric method was investigated in Mansour *et al.*,[17] with the sole objective of improving user experience (UX). The question of optimality here then falters if other aspects are considered, such as resource allocation, direct biometric availability, or even biometric success rate.[17] Larger volumes of extracted features translate into higher data variety which could then open a vast pool of identification methods. For instance, when extracting and learning behaviometrics,[1] one could simultaneously explore the devices noise levels,[15] and use additional sensors[8] to make a combined or iterative decision. Even once authenticated, the confidence of authenticity may have its limits. By potentially solving the complexity issue found in Mansour *et al.*,[17] a continuous monitoring of environmental sensors could provide higher data confidence, translating into higher authentication confidence. As additional data becomes available, iterations among different techniques could lead to further promising results.

Influence of Hidden Context

The presented social authentication solutions[12] extract contextual features from a limited set of applications, but it is possible others may be overlooked (i.e., hidden context). Therefore, mining individual social contexts is of paramount importance in a continuously evolving social trending community.[7] Moreover, further analysis could be done on offline social factors (e.g., cultural backgrounds, beliefs, and prior experiences). Such hidden features could bring additional value on identification and authentication techniques, if extracted with correct privacy and ethical considerations.

Lack of Labeled Malicious Behavior

Secure authentication schemes must consider attacker models and risk analysis against

malicious users. Unfortunately, it remains an issue to be able to label such behavior, and even more to simulate it. For instance, it was noted[8] that within a GPS-central solution, estimating malicious behavior and considering anomalies require historical data that is labeled as such, which is not always obtainable. Similarly, tracking sociability rates and gestures within a smart mobile devices for authentication contains its own challenges, since spoofing patterns must also be labeled up front.[2] This concept is not only an issue in the authentication domain, but across many areas in the literature.

Confidence Levels in Critical Applications

Certain situations with higher risk and strict requirements necessitate higher confidence levels for real-time applications. As seen in Han *et al.*,[14] vehicular verification is one such example. Admission to vehicular clusters requires robust defenses and near perfect confidence scores, as malicious entry could be detrimental to the safety of the passengers and corresponding environment.[14] For such critical applications, convenience and minimal user intrusion should not have higher priorities than security, and applications should be surgical in their use of contextual details.

Privacy

Privacy of individuals is a reoccurring and increasing concern as data science advances are made: how can privacy concerns be addressed during extraction of contextual information? Not only privacy, but also user trust and identity are crucial components requiring transparent solutions. As such, proven methods, guarantees, and incentives need to be implemented for users to willingly participate[19] in providing context-aware data for context-aware improvements and solutions.

As explained by Niemi,[19] although certain properties may be extractable, the reasoning behind such data extraction may not always align with the users' interests. Many third-parties would be interested in obtaining this information for different applications, e.g., advertisement. Considering the wide array of sensors available on mobile phones, such information will grow in value in the upcoming years. However, different strategies exist which can improve users' privacy, protect their identity, and gain their trust, as suggested by the authors. As pointed out by Niemi,[19] the following five strategies can be considered: 1) *Privacy-triggered networking:* delay network communications until an appropriate privacy level is achieved (using predefined metrics), 2) *Privacy-preserving schedule:* use distributed computing and cryptography while keeping a private schedule, 3) *Pseudonyms:* constantly change pseudonyms which represent location and identity to confuse potential eavesdroppers, 4) *Usage Control:* Service providers must increase transparency on information use, 5) Context-aware policy management: adjustment of access control can enhance privacy by increasing authentication mechanisms in unsafe contexts or decreasing them in familiar contexts. These are the exact requirements for realistic deployment of context-aware authentication techniques; not many users willingly reveal their information, and there are few incentives for participation.

SUMMARY AND CONCLUDING REMARKS

Extraction and analysis of context and behavior-based features can result in expanding the scope of authentication techniques. With the correct adaptive selection of techniques, continuous authentication can improve our daily lives. Recognition of such details is the initial step in providing additional insights to current authentication methods. All this untapped data potential can be leveraged to increase user security, privacy, convenience, minimize risk, and progressively reduce uncertainty on the verified identity of the device owner. As multiple studies provide methodologies and results, which could definitely improve existing authentication methods, there are also many newly introduced challenges that need to be addressed. From contextual and behavioral analysis to extracting properties about any given context, a new variety and quantity of features is now available and can empower modern authentication techniques. With the resolution of their many challenges, continuous authentication is a goal which aims at little intrusive maneuvers with enhanced security while allowing users to use technologies to the maximum of their efficiency.

ACKNOWLEDGMENT

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada DISCOVERY and NSERC ENGAGE programs.

REFERENCES

1. F. Anjomshoa, M. Aloqaily, B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Social behaviometrics for personalized devices in the internet of things era," *IEEE Access*, vol. 5, pp. 12 199–12 213, 2017.
2. Z. Rauen, F. Anjomshoa, and B. Kantarci, "Gesture and sociability-based continuous authentication on smart mobile devices," in *Proc. 16th ACM Int. Symp. Mobility Manage. Wireless Access*, Oct. 2018, pp. 51–58.
3. E. Huseynov and J.-M. Seigneur, "Chapter 50—Context-aware multifactor authentication survey," in *Computer and Information Security Handbook - Third Edition*, J. R. Vacca, Ed. Boston, MA, USA: Morgan Kaufmann, 2017, pp. 715–726.
4. G. Jagadamba and B. S. Babu, "Adaptive security schemes based on context and trust for ubiquitous computing environment: A comprehensive survey," *Indian J. Sci. Technol.*, vol. 9, no. 48, 2017. doi: 10.17485/ijst/2016/v9i48/89396.
5. A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, vol. 79, pp. 80–105, 2016.
6. V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 49–61, Jul. 2016.
7. N. Alomar, M. Alsaleh, and A. Alarifi, "Social authentication applications, attacks, defense strategies and future research directions: A systematic review," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 2, pp. 1080–1111, Apr.–Jun. 2017.
8. H. Witte, C. Rathgeb, and C. Busch, "Context-aware mobile biometric authentication based on support vector machines," in *Proc. Fourth Int. Conf. Emerg. Secur. Technologies*, Sep. 2013, pp. 29–32.
9. R. R. Tenney and N. R. Sandell, "Detection with distributed sensors," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-17, no. 4, pp. 501–510, Jul. 1981.
10. L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location," *IEEE Syst. J.*, vol. 11, no. 2, pp. 513–521, Jun. 2017.
11. J. C. D. Lima, C. C. Rocha, I. Augustin, and M. A. R. Dantas, "A context-aware recommendation system to behavioral based authentication in mobile and pervasive environments," in *Proc. IFIP 9th Int. Conf. Embedded Ubiquitous Comput.*, Oct. 2011, pp. 312–319.
12. M. Shahzad and M. P. Singh, "Continuous authentication and authorization for the Internet of Things," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 86–90, Mar. 2017.
13. A. Castiglione, K. R. Choo, M. Nappi, and S. Ricciardi, "Context aware ubiquitous biometrics in edge of military things," *IEEE Cloud Comput.*, vol. 4, no. 6, pp. 16–20, Nov. 2017.
14. J. Han, M. Harishankar, X. Wang, A. J. Chung, and P. Tague, "Convoy: Physical context verification for vehicle platoon admission," in *Proc. 18th Int. Workshop Mobile Comput. Syst. Appl.*, 2017, pp. 73–78.
15. M. Miettinen, T. D. Nguyen, A.-R. Sadeghi, and N. Asokan, "Revisiting context-based authentication in IoT," in *Proc. 55th Annu. Des. Autom. Conf.*, 2018, pp. 32:1–32:6.
16. D. Preuveneers and W. Joosen, "Smartauth: Dynamic context fingerprinting for continuous user authentication," in *Proc. 30th Annu. ACM Symp. Appl. Comput.*, 2015, pp. 2185–2191.
17. A. Mansour, M. Sadik, E. Sabir, and M. Azmi, "A context-aware multimodal biometric authentication for cloud-empowered systems," in *Proc. Int. Conf. Wireless Netw. Mobile Commun.*, Oct. 2016, pp. 278–285.
18. F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial internet of things (IIOT) healthcare applications," *IEEE Trans. Ind. Inform.*, vol. 14, no. 6, pp. 2736–2744, Jun. 2018.
19. V. Niemi, "Privacy, identity and trust in context-aware mobile services," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Nov. 2011, pp. 9–10.
20. M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, "Context-based zero-interaction pairing and key evolution for advanced personal devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 880–891.

Kyle Quintal is a master's candidate at the School of Electrical Engineering and Computer Science, University of Ottawa, where he also received the bachelor's degree in software engineering. He is a member of the Networked Systems and Communications Research Laboratory and the Next-Generation Communications and Computing Networks Laboratory. His research focus is on context-awareness and continuous authentication within different domains of cybersecurity. His

interests expand to other projects regarding mobile crowdsensing and adversarial machine learning as well. He is currently finishing a specialization in the new Applied Artificial Intelligence Master's program at University of Ottawa. He is a student member of IEEE. Contact him at kquin039@uottawa.ca

Burak Kantarci is an Associate Professor with the School of Electrical Engineering and Computer Science, University of Ottawa. From 2014 to 2016, he was an assistant professor at the ECE Department, Clarkson University, where he currently holds a courtesy professor appointment. He received the M.Sc. and Ph.D. degrees in computer engineering from Istanbul Technical University, in 2005 and 2009, respectively. During his Ph.D. thesis, he studied as a Visiting Scholar with the University of Ottawa from 2007 to 2008. He has coauthored more than 160 papers in established journals and conferences, and contributed to 13 book chapters. He has served as the Technical Program Co-Chair of 15 international conferences/symposia/workshops. He has been the PI/co-PI of several federally/provincially funded research projects supported by Natural Sciences and Engineering Research Council of Canada, U.S. National Science Foundation, Ontario Centres of Excellence and MITACS (Canada). He is an editor of the IEEE Communications Surveys and Tutorials and an area editor of IEEE Transactions on Green Communications and Networking, an Associate Editor of IEEE Networking Letters, and Associate Editor for Elsevier Vehicular Communications. He serves as the Chair of the IEEE Communication Systems Integration and Modeling Technical Committee. He is a senior member of the IEEE and a Distinguished Speaker of the ACM. Contact him at burak.kantarci@uottawa.ca.

Melike Erol-Kantarci is an Associate Professor at the School of Electrical Engineering and Computer Science, University of Ottawa. She is the founding director of the Networked Systems and Communications Research Laboratory. She is also a courtesy Assistant Professor at the Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, USA, where she was a tenure-track Assistant Professor prior to joining University of Ottawa. She received the Ph.D. and M.Sc. degrees in computer engineering from Istanbul Technical University. During her Ph.D. studies, she was a Fulbright visiting researcher at the Computer Science Department, University of California Los Angeles. She has more than 100 peer-reviewed publications which have been cited over 4000 times and she has an h-index of 32. She has received the IEEE Communication Society Best Tutorial Paper Award and the Best Editor Award of the IEEE Multimedia Communications Technical Committee in 2017. She is the co-editor of two books: "Smart Grid: Networking, Data Management, and Business Models" and "Transportation and Power Grid in Smart Cities: Communication Networks and Services" published by CRC Press and Wiley, respectively. She has delivered seven tutorials and more than 30 invited talks around the globe. She is an Editor of the IEEE Communications Letters and IEEE Access. She has acted as the general chair or technical program chair for many international conferences and workshops. She is currently the Chair of Green Smart Grid Communications special interest group of IEEE Technical Committee on Green Communications and Computing. Her main research interests include AI-enabled wireless networks, 5G and beyond, smart grid, electric vehicles, and Internet of Things. She is a senior member of the IEEE. Contact her at melike.erolkantarci@uottawa.ca.

Andrew Malton is a Research Scientist at BlackBerry. He has held faculty positions at the University of Waterloo and at Queen's University, and industrial research positions in a number of companies in automated software engineering and security. He received the Ph.D. degree from the University of Toronto in 1990. Contact him at amalton@blackberry.com.

Andrew Walenstein is a Director of Security R&D within the Advanced Technology Development Labs Division of BlackBerry. He leads the advanced research and university partnerships program at BlackBerry, which engages with academics to joint forces in solving problems in privacy, security, and safety. He received the Ph.D. degree from Simon Fraser University, and is a member of the IEEE. Contact him at awalenstein@blackberry.com.