A Survey of Behavioural Authentication in Internet of Things Ecosystems

Ahmad Charba
achar238@uottawa.ca
University of Ottawa
Canada

ABSTRACT

The prevalence of IoT devices creates new avenues to authenticate and identify users using their behaviour as a key. Recent works have shown the vast array of potential input devices that may allow to authenticate user seamlessly, without the requirement for additional effort from the part of the users. This paper summarizes the present context of behaviour based authentication for IoT by studying the background of the different aspects that allow this field to exist, surveying the recent proposals related to this field and analyzing the ideas contained within them, and by describing the future landscape of this domain based on the knowledge gained. Proposal making use of various behaviours, such as gait, gesture and voice, have shown promising results. Classifiers of various types are being used and assessed for their performance for authentication using these behaviours, with SVM and derivatives of decision trees having generally good results when compared to other general-purpose algorithms. Challenges were found in various aspects of the field. Computational and network requirements are often too high with commonly used algorithms, the lack of guidelines leads to difficulties when comparing proposals, a lack of understanding of attacks makes it difficult to know if they are truly secure, and privacy can be endangered if better lightweight schemes to protect the data aren't put in place.

KEYWORDS

IoT, Authentication, Authorization, Machine learning, Behaviour-based, Biometrics

1 INTRODUCTION

Internet of Things is on the rise, and with it many technologies are gaining new capabilities and added connectivity. This gives rise to new challenges when it comes to privacy and security, such as securing access to smart things, protecting the data they hold, and making sure information isn't leaked during communications. This implies the need for authentication of users for personal devices, as well as identification of users for shared IoT device.

Currently most, if not all, authentication schemes are knowledge-based (passwords, pins; what the person knows) or make use of physiological biometrics (face, iris; what the person is). However, because of their heterogeneous nature, IoT devices don't always find a suitable authentication method from those that are currently used for other types of devices. For instance, entering a password in a voice controlled device leaks said password to eavesdroppers, and using facial recognition or a touchscreen password in a door lock will require the user to remove facial coverings or gloves, which would be inconvenient and sometimes dangerous in a cold climate.

On the other hand, the prevalence of IoT devices creates new avenues to authenticate and identify users, as they integrate sensors beyond those that were already used for this purpose in the past. Behavioural biometrics (keystroke patterns, gait; what the person does [20]) has been studied for its potential to authenticate users to mobile phones [8] and computers, and previous constraints due to a lack of sensory data can be overcome by this new input source from IoT objects. Sensors such as microphones in smart locks [6], accelerometers in smart watches [1] or force sensors in smart socks [5] can be used to identify users by the way they speak, move or walk, opening the door to using behavioural data to authenticate users seamlessly and securely.

In recent years, multiple authors have proposed schemes that employ these new sensors in IoT devices to authenticate and identify people from their biometrics. The goal may be 1) to authenticate the user to the device holding the sensor, 2) to authenticate the user to an external device (such as their door lock), or 3) to authenticate the user to a cloud server [7]. This survey will focus on proposals that cater to the second category, where a user will use a smart device's sensors to authenticate themselves on an external, local device using behavioural biometrics.

2 OUTLINE

This paper is structured in the following manner:

- In section 3, background information relation to machine learning, behavioural biometrics, continuous authentication and performance metrics will be give.
- In section 4, threats related to behaviour-based authentication will be explained, along with attacks that it may be subject to.
- In section 5, a survey of existing works will be done. Various proposed schemes will be compared, and their specificity will be discussed.
- In section 6, future works, areas that need improvement will be noted and discussed.
- In section 7, closing thoughts will be given about the state of behavioural authentication.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
Carleton Univerity, April 10 2023, Ottawa, Ontario, Canada
© 2023 Copyright held by the owner/author(s).
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

3 BACKGROUND

3.1 Machine Learning

Machine learning is the use of computer algorithms that automatically improve over time [33]. This field has been extremely active in recent years, with many real-world applications such as chatbots and computer vision being accessible to the public, causing widespread disruption in sectors ranging from education [34] to the military [35].

Machine learning models are numerous, but some come up more often than others due to their power and/or low computing cost. This second requirement is even more important in the context of IoT, as devices are numerous and have limited computing power when compared to other types of hardware [36]. This issue is sometimes circumvented by delegating the training and classification of data to external devices, such as cloud servers [9]. However, issues of data size and transmission speed still stand in that case, in addition to the privacy threats involved.

3.1.1 Machine Learning Models. Machine learning is a branch of AI that uses data and algorithms to have computers to learn from experience and improve their performance over time. Machine learning can be applied to many domains, such as computer vision, natural language processing, speech recognition, etc. Machine learning can be done using different methods, such as supervised learning, unsupervised learning, and deep learning.

A supervised machine learning model will be trained on labelled data, as opposed to an unsupervised model, which is trained on data without labels.

Many algorithms are used for machine learning. Some which have been used in the papers surveyed include:

- Support Vector Machines, a supervised algorithm that finds an optimized hyperplane through regression that separates the data points into different classes [48].
- A decision tree is a model that consists of nodes that represent tests, and outcomes represented by branches. A final decision is taken based on the result of multiple nodes in the tree.
- Random forest, a supervised machine learning algorithm that combines multiple decision trees to more accurately categorize data.
- Hidden Markov model, a statistical model which has been found to be effective at voice recognition [46].
- Neural Networks, a type of ML algorithm where neurons/processing units, which take inputs and activate using an activation function, are used in a network. The processing units' activation affect the activation probability of the ones linked to it [44].
- Recurrent Neural Networks, a type of neural network where neurons are able to send feedback to each other, beyond their activation functions being each other's inputs [43].

3.2 Pre-Processing

In order to maximize the accuracy of a machine learning model, it is often required to turn data into features usable by machine learning models. Raw data often has issues that will degrade the model, such as missing values, having redundant data and the data being noisy [37]. Taking the right pre-processing steps can increase a model's accuracy, decrease the amount of processing power required and lower biases [39].

Here are some common data pre-processing actions that can be taken:

- Scaling: changing the range of the raw data, and moving the data points in this new range.
- Threshold based de-noising: the use of a threshold to determine if a certain wave is noise/clipped in order to have cleaner data.
- Fast Fourier Transform: a preprocessing method to efficiently calculate discrete Fourier transforms. It is often used in signal processing [47].
- Moving average filter: taking the average on the n closest points as the new data point [4].
- Auto-encoding: the use of an unsupervised machine learning model that is trained to output its input. The intuition behind this method is that this initial pre-processing layer will turn the low-level raw data into higher level data, reducing noise[38].

3.3 Behavioural Biometrics

3.3.1 Biometrics. Biometrics is the recognition of individuals through their biological and behavioural characteristics by a digital system. Biological biometrics relate to the way a person is. Biological traits that have been used in practice for identification include the Face, fingerprints, iris, hand veins among others. By sensing features of these traits, we are able to differentiate individuals in an automated and secure manner[21].

3.3.2 Behavioural Biometrics. Behavioural traits on the other hand relate to the way a person acts. Commonly studied examples of this may include gait (the unique way in which a person walks), keystroke pattern (the unique way in which a person types), or handwriting. These traits can often, similarly to some biological biometrics, be used in human to human identification; a person can, for instance, recognize their friends and family by the sound of their footsteps and their gait [22]. Computers are able to do the same: by extracting features from the behavioural traits of a person, as detected by an input device such as a camera or accelerate, a trained machine learning model is able to classify individuals. This can be used for authentication.

Authentication on biometric traits is not subject to certain attacks that a knowledge-based scheme is subject to. Firstly, they are not easy to forge; copying someone's face or way of walking is more challenging than copying their password [23]. They also avoid the risk of being lost or forgotten [25]. Shoulder surfing attacks are also not an issue as opposed to PINs and patterns [26]. These differences will be further discussed in section 4.

3.4 Continuous Authentication

Continuous Authentication is the idea of continuously monitoring a device to determine if the user or device is legitimate at a given point in time. It is usually thought of as a complement to static authentication [27]. It consists of the analysis of a user's interactions with the device to build a behaviour using machine learning (enrolment phase) [29], and checks continuously for anomalies in

		Actual Values	
		Positive Authorized User	Negative Unauthorized User
Predicted Values	Positive Accepted Access	True Positive (TP) or True Acceptance (TA)	False Positive (FP) or False Acceptance (FA)
	Negative Rejected Access	False Negative (FN) or False Rejection (FR)	True Negative (TN) or True Rejection (TR)

Table 1: Confusion matrix in the context of authentication. True Acceptance occurs when an authorized user would have their access accepted; False Rejection occurs when an authorized user would have their access rejected; False Acceptance occurs when an unauthorized user would have their access accepted; True Rejection occurs when an unauthorized user would have their access rejected.

the behaviour. There are various schemes proposed for determining whether or not the user should be authenticated again (continuous authentication phase). Some examples are:

- Maintaining a "trust value" representing the confidence that a user is the one that's authorized; this trust value will increase or decrease based on whether or not the model classifies the behaviour as normal [28] [16]. It can then be used to decide, based on a threshold, if the user needs to prove their identity.
- Keeping track of the number of consecutive classifications, and if t consecutive classifications by the model are abnormal, the user will need to prove their identity [29].
- Calculating the likelihood ratio of a series of classifications, considering the FAR and FRR. If the ratio is beneath a certain threshold, the user is deemed unauthorized [32].

Continuous Authentication can be done with regards to a user's actions, such as determining that an authorized user is the one holding the phone by the way they swipe on social media [13]. It can also be done with regards to the device's actions, such as determining that an authorized device is being communicated with by leveraging latency timings [14]. This second case is outside of the scope of this study.

Continuous Authentication over behavioural biometrics schemes aim to defend against session hijacking attacks [27]. The use of IoT devices can largely benefit such schemes by adding sensors that allow a user's behaviour to be more precisely monitored when accessing sensitive systems, making a session hijack less destructive as the adversary can be detected and their authorization revoked after a shorter amount of time.

Continuous Authentication on behavioural biometrics being a layer built on top of behaviour-based authentication, for the purpose of this study, only the base authentication scheme of proposals Continuous Authentication proposals will be considered. Metrics related to continuous authentication cannot be compared to authentication scheme metrics, as the goals and assumptions are different.

3.5 Performance Metrics

Many proposed authentication schemes make use of machine learning to differentiate authorized users from attackers. In order to measure the performance of such schemes, various performance metrics have been used in order to numerically represent how powerful the proposed schemes are. In general, a machine learning model's performance is usually measured based on a confusion matrix, as shown in table 1. This matrix shows the counts of True Positives, True Negatives, False Positives and False Negatives, respectively abbreviated as TP, TN, FP, FN. In authentication, Positive and Negative are often substituted by Acceptance and Rejection, making them True Acceptance, True Rejection, False Acceptance and False Rejection [20].

From these measures, in the case of authentication schemes, authors will commonly use the following metrics [19]:

- Accuracy: the probability of a correct declaration. This alone is often insufficient to draw conclusions, as it will vary depending on the ratio of authorized/unauthorized users in the test data set.
$$\frac{(TA + TR)}{TA + TR + FA + FR}$$
- True Acceptance Rate: the probability of an authorized user being detected as authorized.
$$\frac{TA}{TA + FR}$$
- True Rejection Rate: the probability of an unauthorized user being detected as unauthorized.
$$\frac{TR}{TR + FA}$$
- False Acceptance Rate (FAR): the probability of an unauthorized user being detected as authorized. This metric is of often considered the most important, as it's the rate at which an attacker will be authorized by mistake. This is a security issue and needs to be minimized.
$$\frac{FA}{TR + FA}$$
- False Rejection Rate (FRR): the probability of an authorized user being detected as unauthorized. This metric is useful to assess usability, as it's the likelihood of a user not being authorized though they should be. This is a usability problem and needs to be minimized.
$$\frac{FR}{TA + FR}$$
- Precision: the proportion of acceptances that were correct [53].
$$\frac{TA}{TA + FA}$$

- Recall: the proportion of authorized users that were identified as such [53].

$$\frac{TA}{TA + FR}$$

- F-measure: a measure that represents both the precision and the recall, harmonized. This is to be maximized [30].

$$\frac{2PR}{P + R}$$

- Receiver Operator Characteristic Curve (ROC curve): Curve representing the FAR and FRR by varying the confidence threshold required to authorize. This lets us visually see the strong points of the model and determine its usability in various applications.
- Equal Error Rate (ERR): The point at which the the FAR and FRR are equal in the ROC curve. This metric allows a unification of the two error metrics, but doesn't take into account the real-world requirements (some sensitive applications may require a lower FAR, while others applications (such as continuous authentication) may require a lower FRR).
- Area Under the ROC Curve (AUROC) and Gini Coefficient (GC) are other ROC curve related measurements, but they are rarely measured in proposals.

4 THREAT MODELS

4.1 Threats

4.1.1 Unauthorized users obtaining access to a device. If an malicious, unauthorized user gets access to a device, this can cause many issues. It may compromise privacy by granting them access to the device's content, as well as the possibility to use the device to cause damage to property or life. It is clear that unauthorized access is to be avoided.

4.1.2 Entities obtaining access to private training data. Because of the addition of machine learning, a new threat is added: a malicious party may compromise the privacy of a user by learning about the machine learning model or original training data. This means that in addition to having to protect the devices from unauthorized use, it will be necessary to defend the data held, and the data sent to and from the devices within a given scheme. This may require homomorphic encryption, or schemes of the same goal, if this data is to be sent to a semi-trusted cloud server [41].

4.2 Attacks

Attacks on classical authentication schemes are usually better addressed by behavioural authentication, but some new threats can come up.

4.2.1 Shoulder Surfing. A shoulder surfing attack occurs when an attacker looks at what a user is entering to obtain the key to their device. This is a dangerous attack in knowledge-based schemes, as the knowledge of a PIN or password compromises the entire system. This issue is mostly avoided in behaviour-based authentication schemes, as someone's behaviour is much more difficult to mimic than a six digit number.

4.2.2 Session Hijacking Attack. A session hijacking attack occurs when an unauthorized user takes advantage of an session opened by an authorized user. This attack is still possible in the case of behaviour-base authentication, but the advent of continuous authentication is able to mitigate this issue.

4.2.3 Smudge Attack. This attack involves using the "smudge" left on a touchscreen after a user has authenticated themselves, leaving hints as to what the PIN/password may be. This attack's potential is greatly reduced in behaviour-based authentication.

4.2.4 Membership Inference Attacks. Membership inference attacks use sets of techniques to determine whether a certain data point had a certain feature in a machine learning model's training data [40]. This may be done, for instance, by testing the sensitivity of the model to a change of the targeted input, which may leak information about how confident a model is, showing that a similar input may have been part of the original dataset.

This attack is possible in the case of behaviour-based authentication, as it almost always involves machine learning classification.

4.2.5 Mimic Attack. An attacker may attempt to mimic a user's behaviour and way of acting. This is an attack that mainly affects behaviour-based authentication, and is highly debated in the literature. It is a difficult task to measure the risk of this type of attack occurring, but minimizing the False Positive Rate may help in that context.

5 SURVEY OF RECENT PROPOSALS

In 2019, Watanabe et al. ade use of two acceleration inputs, showing the large accuracy benefit of adding a second sensor for authentication. With minimal pre-processing and using a common machine learning algorithm (Random Forest), they were able to achieve a high 95.3% accuracy.

The same authors later modified and improved their model by incorporating anomaly detection to further improve accuracy. They also gave more precise information about their results, allowing for easier comparison thanks to the use of the FAR and FRR metrics [2].

In 2021, Papavasileiou et al. proposed to use smart socks and a smart shoes prototype to build a model to authenticate users. They made use of ground contact force sensors and accelerometers to classify people based on their gait. The scheme was found to have a great accuracy, and they tested it against a Gait Mimicking attack by asking a subject to mimic another subject's gait. The result of this test was that the FAR was greater than when a person wasn't trying to mimic someone else's manner of walking, but the attack's accuracy was still low (15%). They also found that accuracy depends on time of the day, as fatigue may affect the way someone walks, and walking speed [4].

In 2017, Wang et al. developped a behaviour-based identification scheme using gait, with the input coming from the WiFi Signals (Channel state information, or CSI) of a laptop from a standard router. They used the variation of this signal as an input to an SVM classifier, obtaining a 92% accuracy within 6 meters. This shows great potential for IoT integration; multiple CSI could be obtained due to the number of WiFi enabled devices, allowing for more accurate authentication [11] [12].

Study	Input	Preprocessing	Features	Algorithm	Test Size	Performance
Wang et al. 2017 [12]	Gait: Wifi Channel State Information using a laptop and home router (not taking advantage of IoT)	Principal Component Analysis, Noise removal	Gait Cycle time	Support Vector Machine (SVM)	50	ACC: 92% Limit of 6 meters
Watanabe et al. 2019 [1]	Gait: Acceleration data from a phone and smartwatch	Noise removal	Median, Variance, Minimum Value, Sum of Squared Differences (SSD), Normalized Correlation Coefficient, Maximum Interval, Minimum interval, Cycle	Random Forest	15	ACC: 95.3%
Watanabe et al. 2020 [2]	Gait: Acceleration data from a phone and smartwatch	Noise removal	Mean, Difference of Means, SD, Difference in SD, Maximum Value, Difference in Max, Minimum Value, Difference in Min, Local Max Interval, Local Min Interval, SSD	GMM, Isolation Forest	11	FAR: 13.6%, FRR:3.6% using GMM FAR: 8.3%, FRR: 9.5% using Isolation Forest
Papavasileiou et al. 2021 [4]	Gait: Acceleration and Ground Contact Force data from Smart Socks or Smart shoes	Moving Average Filter, Gait Cycle Detection, Auto-Encoding	Early or Late sensor fusion	SVM, Softmax	10	EER: 0.01%
Krašovec et al. 2020 [15]	Personal Computer (Accelerometer, gyroscope attached to mouse and keyboard, ressource utilization monitor) Force sensors under the keyboard/mouse Passive infrared sensors Hall sensors	Fast Fourier Transforms (FFT)	Means, SD, Mean Crossing Rate, 10hz Bins, Min, Max, Jumps, Start-End Deltas	Random Forest	3, 7, 11, 15	ACC: 99.3% (Continuous Auth.)
Sahu et al. 2021 [17]	Smartphones and Healthcare Sensors: Heart rate, Accelerometer, Proximity, GPS, Temperature, Rotation, Magnetic field	Average of previous points for missing values	Mean, SD, Maxi, Min, Root Mean Square, Skewness, Range, Mean Deviation	Recurrent Neural Network	10	Accuracy: 97% FAR: 3.5% FRR: 2.4%
Lee et al 2021 [9]	Touchscreen	Mean-standard deviation, Scaling	Total distance, Displacement, Average touch speed, Average touch area, Average angle, Relative finger positions	Isolation Forest, Gaussian Mixture	20	Accuracy: 91.5%
Duraibi 2020 [6]	Microphone (Voice)	Threshold based de-noising	Mel Frequency Cepstral Coefficient (MFCC)	Hidden Markov model (HMM)	-	-
Ashabani et al. 2018 [52]	Smartphone (network usage)	Noise removal, Removing rare categories	Date, Time, Package name, Foreground Cellular Time, Foreground WiFi Time	Random Forest	10	F-Measure: 96.5%

Table 2: A table showing the inputs, pre-processing steps, features, classification algorithms, test size and performance of proposals made for Behaviour-Based authentication.

In 2020, Krašovec et al. explored how multiple sensors can be used for continuous authentication. They prepared a room containing gyroscopes, accelerometers, force sensors, passive infrared sensors and hall sensors to be used as a testbed. Subjects were then asked to interact with the room and given tasks. The data coming from the sensors while they perform those tasks was recorded and features were extracted from it. The authors then fed those features to a Random Forest classifier, which they found to be the best performing among the ones they attempted, and were able to accurately (99.3%) verify the identity of pre-authentified users [15].

In 2021, Sahu et al. developed an authentication scheme for health care that is based on the inputs of a smartphone and health care sensors (heart rate and temperature). They fed features of these inputs to a Recurrent Neural Network with a Long-term Short memory algorithm, an influential algorithm proposed in 1997 by Hochreiter et al. [42] [17]. When this scheme was tested with

10 participants, they achieve a high 97% accuracy, which was a large improvement to previous models which only made use of smartphones' behavioural data.

In 2021, Lee et al. published a proposal to make use of a simple gesture on small touchscreens, an L shape with 3 fingers, to authenticate users. By making use of the behavioural data (speed of the gesture, distance, etc.) and biometric data (distances between finger), they achieved a 91.5% accuracy in authentication with 20 subjects. They assessed the efficacy of attacks, showing the model to be resistant to attacks; they were successful 6.39% of the time on average. They also assessed the effect of time on the accuracy of the algorithm, as time can affect the behavioural biometric. They found no significant drop in accuracy over a period of a month [9].

In 2020, Duraibi described methods for voice-based authentication and proposed a model for using a phone's microphone for behavioural authentication. The author proposed to feed the processed input data into a Hidden Markov model, which is known for its performance in speech-recognition. The proposal, however, was not implemented and tested [6].

In 2018,Ashabani and Mahmoud proposed a model to authenticate users based on their behaviour on an IoT app. After testing multiple algorithms, Random Forests, Decision Tree, KNeighborsClassifier, GaussianProcessClassifier, LogisticRegression, GaussianNB, MLPClassifier, QuadraticDiscriminantAnalysis, Support Vector Machine, NearestCentroid, RidgeClassifier, and BernoulliNB, they determined that random forests yielded the best accuracy. Their scheme achieved an F-measure of 96.5% with a dataset of 10 individuals [52].

6 TAKEAWAYS AND FUTURE WORKS

6.1 Resilience to Time

Time can affect the accuracy of a behaviour-based authentication schemes by changing the way the user acts and moves. For instance, a teen's gait can go through considerable change during puberty [49]. A person's voice also changes as they get older. Someone may start doing their swiping gestures faster as they get used to an application.

This may mean the authentication method will need to be retrained on the user's behaviour again after a period of time, which may be longer or shorter depending on the model and input features. The resilience to time of a model needs to be assessed over a long enough period of time to notice changes. Lee et al. did such an assessment over a month, which would probably not be enough to notice changes on hand size, but enough to notice a change in the way a user does the gesture [9]. The retraining of the model on data from successful authentication can be an avenue to solve the problem.

6.2 Resilience to a Physical and Emotional State Changes

People's behaviour can change based on their physical and emotional state. This means that a classifier may not recognize the legitimate user if they aren't in the same state as when the model was trained. For example, a knee injury may make the individual walk in a different way. Boyd et al., in 2005, cited factors which can affect gait recognition such as [45]:

- Terrain
- Injury
- Footwear
- Muscle development
- Fatigue
- Physical training
- Cultural artifacts (mince, swagger, etc.)
- Personal idiosyncrasies

Similarly, methods based on vocal signature can be affected by time, sickness, mood, etc.

Certain proposals, such as the one made by Papavasileiou et al, take this into account and train the model on multiple walking speeds and times of the day [4]. Having a model that first detects the stats of the individual, taking that into account when classifying, may resolve this issue for some cases.

However, quantifying the impact on authentication of factors related to physical and emotional state would benefit the field by helping understand the practicality and limitations of different models. Models that are more resilient to changes in these factors may also be developed from this better understanding of their impact.

6.3 Privacy-Preservation

The use of behavioural authentication can be a risk for privacy, whether it is done locally or delegated to a cloud provider. Protecting the training and user data becomes essential, but the computational power required for doing so may be too high for IoT devices.

Research in energy efficient data protection schemes for behavioural data would be required before its implementation becomes feasible, as to avoid risking individuals' privacy.

6.4 Resistance to Mimicking

While some studies attempt to measure their model's performance against mimic attacks, this is mostly done by individuals who never tried to mimic someone else's behaviour before. The attack may be more powerful than we might expect when done by an experienced attacker.

This risk was assessed in the past by Mjaaland et al., but they could not show improvement of the attackers over sessions [51]. This however doesn't rule out the possibility of imitation being possible, especially if the model's training data is accessed, as the attacker could attempt to directly mimic the sensors' outputs in their own training. Papavasileiou et al. have attempted the mimicking attack without training and showed that it had a better success rate than luck [12].

Further investigation is necessary to assess the full risk related to this attack.

6.5 Comparison of The Effects of Different Pre-Processing Methods on Performance

The majority of current schemes base their classification on a single type of data; combining different data sources may yield much greater accuracy. The rise of IoT is an opportunity to complement CSI with acceleration data from a smartwatch, adding this to the key stroke patterns of on a laptop.

This could be done through an additional layer of machine learning, which can take the outputs of well researched models and combine them to make a more informed decision. More complex schemes could be developed, and models taking for input many data sources could be the leap forward in behavioural authentication.

6.6 Combination of Different Classes of Behavioural Data

The majority of current schemes base their classification on a single type of data; combining different data sources may yield much greater accuracy, as seen in [15]. The rise of IoT is an opportunity to complement CSI with acceleration data from a smartwatch, adding this to the key stroke patterns of on a laptop.

This could be done through an additional layer of machine learning, which can take the outputs of well researched models and combine them to make a more informed decision. More complex schemes could be developed, and models taking for input many data sources could be the leap forward in behavioural authentication.

6.7 Guidelines for Performance Metrics

Currently, performance metrics are all over the place in behaviour-based authentication proposals. Since authorization has a different role than identification, the usual accuracy metric is not enough to give the full picture of the performance of an authentication scheme. Clear and well documented guidelines would benefit the community by allowing easier comparison between models and better assessment of the strengths and weaknesses they may have.

6.8 Computational Performance

6.8.1 Computational Performance Metrics. The current literature doesn't often address the computational cost of machine learning models. In the case of IoT, a higher computational cost may be a deal breaker for certain proposals. However, due to heterogeneity in hardware and networks, it is difficult to compare computational performance metrics.

The presence of cloud computing may allow for an opportunity to do so. Performance could me measured in cloud servers with standardized computational powers, allowing for latency and speed to be measured in a comparable manner.

6.8.2 Computational Performance Optimization. The majority of proposals use standard, general-use machine learning classifiers, such as SVM, Isolation Forest, and Random Forest. This can lead to a higher computational requirement than needed; making these solutions difficult to use in IoT.

The use of specialized classifiers can also be a solution to lower the computational requirement of machine learning models. This was done for instance in Duraibi's study [6], where a Hidden Markov model was used for voice recognition, since it tends to perform better at this specific task.

6.8.3 Distribution of the Work. Recently, proposals have been made for distributing the workload of machine learning models to many IoT devices (federated learning and split-learning). This may be a path to solve the performance issue without having to lower the computational requirements of a model, but requires more research to be applicable, as the current network usage requirements are high [50].

7 CONCLUSION

This survey looked at various behaviour-based authentication for the IoT ecosystem. We can see from the current literature that this field is gaining traction, with schemes being proposed at a fast pace. Progress in accuracy and applicability of behaviour-based authentication is steady, and novel solutions to its various challenges are being proposed.

While gait is the most studied behaviour for authentication, other types of behaviours, such as touch gestures and voice, show promising results. Some are more suited to continuous authentication, like gait, while others are capable of authenticating in less time, like touch gestures.

Some challenges remain unsolved for behaviour-based authentication to make its way into mainstream systems and ecosystems.

One major challenge of behaviour-based authentication is the fact the accuracy of the model can decrease over time and depending on the user's physical and emotional state. Quantifying the impact of these factors would be a first step to finding solutions.

Attacks by mimicking still aren't sufficiently understood to say that they would be difficult to pull off. Experienced attackers may be able to achieve them with a high success rate, especially in the presence of training data. Further research is required to assess the risk this poses.

Privacy is also an ongoing issue with behaviour-based authentication. More efficient schemes to protect the behavioural training data in transit and in storage are needed.

Computational and network requirements remain high for most schemes, making them difficult to put in practice without more work. Further optimization, better classifier choices and federated/split learning could help solve these issues.

Metrics related to system performance and computational performance are used without homogeneity in the literature, making it difficult to compare different proposals' strengths and limitations. Guidelines addressing those metrics would help avoid this issue.

Proposals tend to use varied pre-processing methods, even when the goal is the same. These methods should be assessed for their usefulness in different behavioural inputs.

Most proposals focus on a specific type of behaviour, but their combination have been shown to produce better results if done properly. More research on ways to combine behavioural data would benefit the field.

To conclude, the impressive progress of behaviour-based authentication in IoT sets high hopes for widespread adoption in the near future. Recent works have shown the vast array of potential input devices that may allow to authenticate user seamlessly, without the requirement for additional effort from the part of the users. Thanks to the omnipresence of sensors and computers in our daily lives, we may be closer than we think to a reality where needing to remember passwords is a thing of the past.

REFERENCES

[1] Watanabe, Kazuki, et al. "Gait-Based Authentication for Smart Locks Using Accelerometers in Two Devices." Advances in Networked-Based Information Systems, 2019, pp. 281–291., doi:10.1007/978-3-030-29029-0_26.

[2] Watanabe, Kazuki, et al. “Gait-Based Authentication Using Anomaly Detection with Acceleration of Two Devices in Smart Lock.” Lecture Notes in Networks and Systems, 2020, pp. 352–362., doi:10.1007/978-3-030-33506-9_31.

[3] Aman, Faiz, and C Anitha. “Motion Sensing and Image Capturing Based Smart Door System on Android Platform.” 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, doi:10.1109/icecds.2017.8389871.

[4] Papavasileiou, Ioannis, et al. “Gaitcode: Gait-Based Continuous Authentication Using Multimodal Learning and Wearable Sensors.” Smart Health, vol. 19, 2021, p. 100162., doi:10.1016/j.smhl.2020.100162.

[5] Liu, Tao, et al. “A Wearable Ground Reaction Force Sensor System and Its Application to the Measurement of Extrinsic Gait Variability.” Sensors, vol. 10, no. 11, 2010, pp. 10240–10255., doi:10.3390/s101110240.

[6] Duraibi, Salahaldeen, et al. “Voice Biometric Identity Authentication Model for IOT Devices.” International Journal of Security, Privacy and Trust Management, vol. 9, no. 2, 2020, pp. 1–10., doi:10.5121/ijsptm.2020.9201.

[7] Merlin, S. Sengole, and A. Chandrasekar. “Towards Mobile Cloud Authentication and Gait Based Security Using Time Warping Technique.” Cluster Computing, vol. 22, no. S5, 2017, pp. 10595–10604., doi:10.1007/s10586-017-1136-5.

[8] Chen, Dongxiang, et al. “A Behavioral Authentication Method for Mobile Based on Browsing Behaviors.” IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 6, 2020, pp. 1528–1541., doi:10.1109/jas.2019.1911648.

[9] Lee, Jiwoo, et al. “Advanced Authentication Method by Geometric Data Analysis Based on User Behavior and Biometrics for IOT Device with Touchscreen.” Electronics, vol. 10, no. 21, 2021, p. 2583., doi:10.3390/electronics10212583.

[10] Kumar, Vivek, and Sangram Ray. “Continuous Behavioral Authentication System for IOT Enabled Applications.” Proceedings of International Conference on Network Security and Blockchain Technology, 2022, pp. 51–63., doi:10.1007/978-981-19-3182-6_5.

[11] Shahzad, Muhammad, and Munindar P. Singh. “Continuous Authentication and Authorization for the Internet of Things.” IEEE Internet Computing, vol. 21, no. 2, 2017, pp. 86–90., doi:10.1109/mic.2017.33.

[12] Wang, Wei, et al. “Gait Recognition Using WIFI Signals.” Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2016, doi:10.1145/2971648.2971670.

[13] Naji, Zakaria, and Driss Bouzidi. “Deep Learning Approach for Dynamic Swipe Gestures Based Continuous Authentication.” Lecture Notes on Data Engineering and Communications Technologies, 2023, pp. 48–57., doi:10.1007/978-3-031-27762-7_5.

[14] Al-Sadi, Mohammed, et al. “Lento: Unpredictable Latency-Based Continuous Authentication for Network Intensive IOT Environments.” Future Generation Computer Systems, vol. 139, 2023, pp. 151–166., doi:10.1016/j.future.2022.09.023.

[15] Krašovec, Andraž, et al. “Not Quite Yourself Today.” Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 4, no. 4, 2020, pp. 1–29., doi:10.1145/3432206.

[16] Ghosh, Nirnay, et al. “Softauthz: A Context-Aware, Behavior-Based Authorization Framework for Home IOT.” IEEE Internet of Things Journal, vol. 6, no. 6, 2019, pp. 10773–10785., doi:10.1109/jiot.2019.2941767.

[17] Sahu, Amiya Kumar, et al. “Deep Learning-Based Continuous Authentication for an IOT-Enabled Healthcare Service.” Computers and Electrical Engineering, vol. 99, 2022, p. 107817., doi:10.1016/j.compeleceng.2022.107817.

[18] Jayawardana, Oshan, et al. “Non-Contrastive Learning-Based Behavioural Biometrics for Smart IoT Devices.” ArXiv Preprint, vol. 2210, no. 12964, 2022, doi:10.48550/arXiv.2210.12964.

[19] Sugrim, Shridatt, et al. “Robust Performance Metrics for Authentication Systems.” Proceedings 2019 Network and Distributed System Security Symposium, 2019, doi:10.14722/ndss.2019.23351.

[20] Farik, Mohammed, Lal, Nilesh, Prasad, Shalendra. A Review Of Authentication Methods. International Journal of Scientific and Technology Research. 5. 246-249, 2016.

[21] Jain, Anil K., et al. “50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities.” Pattern Recognition Letters, vol. 79, 2016, pp. 80–105., doi:10.1016/j.patrec.2015.12.013.

[22] Cutting, James E., and Lynn T. Kozlowski. “Recognizing Friends by Their Walk: Gait Perception without Familiarity Cues.” Bulletin of the Psychonomic Society, vol. 9, no. 5, 1977, pp. 353–356., doi:10.3758/bf03337021.

[23] Crompton, Malcolm. “Biometrics and Privacy the End of the World as We Know It or the White Knight of Privacy?” Australian Journal of Forensic Sciences, vol. 36, no. 2, 2004, pp. 49–58., doi:10.1080/00450610409410597.

[24] Jain, Rubal, and Chander Kant. “Attacks on Biometric Systems: An Overview.” International Journal of Advances in Scientific Research, vol. 1, no. 7, 2015, p. 283., doi:10.7439/ijasr.v1i7.1975.

[25] Alaswad, A.O. Vulnerabilities of Biometric Authentication “Threats and Countermeasures”. 2006.

[26] Khan, Hassan, et al. “Evaluating Attack and Defense Strategies for Smartphone Pin Shoulder Surfing.” Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, doi:10.1145/3173574.3173738.

[27] Al-Naji, Fatimah Hussain, and Rachid Zagrouba. “A Survey on Continuous Authentication Methods in Internet of Things Environment.” Computer Communications, vol. 163, 2020, pp. 109–133., doi:10.1016/j.comcom.2020.09.006.

[28] Deutschmann, Ingo, et al. “Continuous Authentication Using Behavioral Biometrics.” IT Professional, vol. 15, no. 4, 2013, pp. 12–15., doi:10.1109/mitp.2013.50.

[29] Frank, Mario, et al. “Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication.” IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, 2013, pp. 136–148., doi:10.1109/tifs.2012.2225048.

[30] Hripcsak, G. “Agreement, the F-Measure, and Reliability in Information Retrieval.” Journal of the American Medical Informatics Association, vol. 12, no. 3, 2005, pp. 296–298., doi:10.1197/jamia.m1733.

[31] Nespoli, Pantaleone, et al. “A Dynamic Continuous Authentication Framework in IOT-Enabled Environments.” 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, 2018, doi:10.1109/iotsms.2018.8554389.

[32] Peng, Ge, et al. “Continuous Authentication with Touch Behavioral Biometrics and Voice on Wearable Glasses.” IEEE Transactions on Human-Machine Systems, vol. 47, no. 3, 2017, pp. 404–416., doi:10.1109/thms.2016.2623562.

[33] Jordan, M. I., and T. M. Mitchell. “Machine Learning: Trends, Perspectives, and Prospects.” Science, vol. 349, no. 6245, 2015, pp. 255–260., doi:10.1126/science.aaa8415.

[34] Farrokhnia, Mohammadreza, et al. “A SWOT Analysis of CHATGPT: Implications for Educational Practice and Research.” Innovations in Education and Teaching International, 2023, pp. 1–15., doi:10.1080/14703297.2023.2195846.

[35] McFarland, Tim. “Reconciling Trust and Control in the Military Use of Artificial Intelligence.” International Journal of Law and Information Technology, 2023, doi:10.1093/ijlit/eaad008.

[36] Coelho, Jorge, and Luís Nogueira. “Enabling Processing Power Scalability with Internet of Things (IOT) Clusters.” Electronics, vol. 11, no. 1, 2021, p. 81., doi:10.3390/electronics11010081.

[37] Kotsiantis, Sotiris. Kanellopoulos, Dimitris. Pintelas, P.. “Data Preprocessing for Supervised Learning.” International Journal of Computer Science. 1. 111-117. 2006.

[38] Vincent, Pascal, et al. “Extracting and Composing Robust Features with Denoising Autoencoders.” Proceedings of the 25th International Conference on Machine Learning - ICML ’08, 2008, doi:10.1145/1390156.1390294.

[39] G, Ranganathan. “A Study to Find Facts behind Preprocessing on Deep Learning Algorithms.” Journal of Innovative Image Processing, vol. 3, no. 1, 2021, pp. 66–74., doi:10.36548/jiip.2021.1.006.

[40] Farhad Farokhi, Mohamed Ali Kaafar. "Modelling and Quantifying Membership Information Leakage in Machine Learning." arXiv:2001.10648, 2021, doi:10.48550/arXiv.2001.10648.

[41] Yang, Wencheng, et al. “A Review of Homomorphic Encryption for Privacy-Preserving Biometrics.” Sensors, vol. 23, no. 7, 2023, p. 3566., doi:10.3390/s23073566.

[42] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," in Neural Computation, vol. 9, no. 8, pp. 1735-1780, 15 Nov. 1997, doi: 10.1162/neco.1997.9.8.1735.

[43] Grossberg, Stephen. “Recurrent Neural Networks.” Scholarpedia, 2013, www.scholarpedia.org/article/Recurrent_neural_networks.

[44] Bishop, Chris M. “Neural Networks and Their Applications.” Review of Scientific Instruments, vol. 65, no. 6, 1994, pp. 1803–1832., doi:10.1063/1.1144830.

[45] Boyd, Jeffrey E., and James J. Little. “Biometric Gait Recognition.” Advanced Studies in Biometrics, 2005, pp. 19–42., doi:10.1007/11493648_2.

[46] L. Rabiner and B. Juang, "An introduction to hidden Markov models," in IEEE ASSP Magazine, vol. 3, no. 1, pp. 4-16, Jan 1986, doi: 10.1109/MASSP.1986.1165342.

[47] L. Krupp, C. Wiede and A. Grabmaier, "Approximate Fast Fourier Transform-based Preprocessing for Edge AI," 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA), Stuttgart, Germany, 2022, pp. 1-8, doi: 10.1109/ETFA52439.2022.9921684.

[48] Noble, William S. “What Is a Support Vector Machine?” Nature News, Nature Publishing Group, 2006, www.nature.com/articles/nbt1206-1565.

[49] Sudlow, Anthony, et al. “Which Factors Influence Running Gait in Children and Adolescents? A Narrative Review.” International Journal of Environmental Research and Public Health, vol. 20, no. 5, 2023, p. 4621., doi:10.3390/ijerph20054621.

[50] Y. Gao et al., "Evaluation and Optimization of Distributed Machine Learning Techniques for Internet of Things," in IEEE Transactions on Computers, vol. 71, no. 10, pp. 2538-2552, 1 Oct. 2022, doi: 10.1109/TC.2021.3135752.

[51] Mjaaland, Bendik B., et al. “Walk the Walk: Attacking Gait Biometrics by Imitation.” Lecture Notes in Computer Science, 2011, pp. 361–380., doi:10.1007/978-3-642-18178-8_31.

[52] Y. Ashibani and Q. H. Mahmoud, "A Behavior Profiling Model for User Authentication in IoT Networks based on App Usage Patterns," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 2018, pp. 2841-2846, doi: 10.1109/IECON.2018.8592761.

[53] David, Olson L, and Delen Dursun. “Advanced Data Mining Techniques, Springer, 1st Edition.” Advanced Data Mining Techniques, Scholars Portal, pp. 138.