Hindawi
Security and Communication Networks
Volume 2021, Article ID 8146553, 11 pages
https://doi.org/10.1155/2021/8146553

Research Article

Access Control beyond Authentication

Javier Junquera-Sánchez, Carlos Cilleruelo, Luis De-Marcos, and José-Javier Martinez-Herráiz

Computer Science Department, University of Alcalá, Alcalá, Spain

Correspondence should be addressed to Carlos Cilleruelo; carlos.cilleruelo@uah.es

Received 3 June 2021; Revised 30 July 2021; Accepted 7 September 2021; Published 1 October 2021

Academic Editor: Luigi Catuogno

Nowadays, the Zero Trust model has become one of the standard security models. This paradigm stipulates as mandatory the protection of each endpoint, looking for providing security to all the network. To meet this end, it is necessary to guarantee the integrity of the access control systems. One possibility for bringing security to the different endpoints is continuous authentication, as an access control system. Continuous authentication is the set of technologies capable of determining if a user's identity remains in time; whether he is the legitimate user (i.e., the only one who should know the secret credentials) or the identity has been impersonated by someone else after the authentication's process was completed. Continuous authentication does not require the active participation of the user. Aiming to identify the different technologies involved in continuous authentication's implementations, evaluation methods, and its use cases, this paper presents a systematic review that synthesizes the state of the art. This review is conducted to get a picture about which data sources could allow continuous authentication, in which systems it has been successfully implemented, and which are the most adequate ways to process the data. This review also identifies the defining dimensions of continuous authentication systems.

1. Introduction

The increase in the use of mobile devices with access to critical resources also increases the possible attack surface of digital assets. A mobile phone or laptop can now be a possible entry point to a private company's network or data. These devices can easily be stolen or accidentally left unlocked and unattended.

Taking this into account, the classic model based on well-defined perimeter security policies is no longer effective [1]. It is also necessary to highlight elements such as the cloud that redefines perimeters with new architectures and interconnections between systems. The security paradigm based on a Zero Trust model [2] now demands new designs of the methodology in security protection and information access for each system. Under the umbrella of endpoint detection and response technologies [3], continuous authentication (CA) aims to ensure that only authorized users interact with the system.

1.1. A Systematic Literature Review Necessity. An effective way to continuously identify a user is by the analysis of the interactions with a device. Even though every interaction with a device may produce a digital fingerprint [4] (behavioural biometric), it is not easy to determine how many different interactions exist and how many of them are required to uniquely identify a user. Determining which continuous authentication technologies exist and are effective facilitates new research that avoids replication and focuses on unexplored areas. Similarly, practitioners and system developers can focus on proven approaches for their implementations of CA solutions.

A systematic review is also convenient to get acquainted with the terminology, common parameters, and techniques used in this research field. These are useful to make future results more accessible to the scientific community and allow research papers to be more homogeneous and accessible. An unbiased systematic review also points to the most relevant research results in the field, and it is an initial point for

researchers in the area [5]. This paper also aims to provide a taxonomy of existing CA approaches. Finally, this SLR identifies the limitations of current systems and the boundaries of CA as a research field, offering guidance for future research. The remainder of this paper is structured as follows. The Background section documents the principles of continuous authentication as well as the concept of Systematic Literature Review (SLR). Methodology section explains the methodology followed to perform the review. One of the objectives of this paper is to perform the literature review with the fewer biases possible, so this section is fundamental. Search Strategies section states the definition of different search strategies that will be used to provide the studies to review. Findings section presents a purely technical analysis of the research studies (i.e., just documenting the elements which fit into the defined methodology). Discussion section contains how the findings, documented in the Findings section, shape the state of the art in CA and the gaps that can be approached in future works. Finally, the Conclusions section provides concluding remarks of the paper. The materials produced to support the research process, and for structuring the documentation of the review, are provided as supplementary material (available here).

2. Background

2.1. Systematic Literature Review. A Systematic Literature Review (SLR) is a method of study focused on synthesizing all possible information about a specific research field. An SLR will be conducted through identification, selection, and evaluation of the state of the art [6].

2.2. Continuous Authentication. Continuous authentication (CA) could be defined, within an access control system, as a new stage of authentication after the initial authentication has been completed, allowing for validation of a user or users during the session [7]. Checking if the users are who they claim to be during their session, it allows for further protection of information assets and also facilitates detecting stolen credentials or other authentication information.

To achieve CA, it is necessary to study the techniques that a machine can use to identify a user (i.e., which technologies allow to retrieve enough information to distinguish every single user). CA systems can be divided into two main families based on the capabilities they have for identifying the entity under evaluation:

(i) Session-based CA systems: the reliability of these systems are determined by the capacity to determine if the entity that is being evaluated has changed or is still the same during the session. For example, a system will be able to identify if the person who initiates a session is the same or if during this session changes. These systems should have a low False Rejection Rate (FRR).

(ii) CA systems based on behavioral fingerprint: these systems can process more information about the entity under evaluation. They can produce a digital fingerprint of users, in the same manner as a classical fingerprint is used to identify a person. The accuracy of these systems is based on their capacity for telling apart a user from the other users. These types of systems should present a False Acceptance Rate (FAR) close to zero.

On the other hand, based on the parameters collected to create these systems, it is possible to differentiate between.

(iii) Hard biometrics (intersession): the biometric data does not change throughout the period that the system is active. However, this group could also include biometric data that only changes slightly or remains the same during long periods of time.

(iv) Soft biometrics (intrasession): soft biometrics are biometric data that will only be valid for a few weeks or days during a session, for example, the colour of a t-shirt.

As shown in Figure 1, these two dimensions determine the potential applications of a continuous authentication system. However, it is necessary to understand having a passive nature (i.e., not interrupting or interfering with the user's tasks) is considered a viability requirement for any CA approach.

Even though the most obvious application of these systems is the ones authenticating human users, it is also necessary to consider that they can be applied to other different entities (e.g., to authenticate devices in an IoT-based smart grid [8]).

3. Methodology

This SLR was divided into three stages: method definition, document compilation, and analysis of the documents and synthesis of results. To accomplish our objective (i.e., developing a rigorous literature study), we followed up the methodology proposed by Arksey and O'Malley [9]. This methodology is divided into the following five stages:

(1) Identifying the research questions

(2) Identifying relevant studies

(3) Selecting studies based on well-defined criteria

(4) Extracting relevant data in a structured manner

(5) Analyze the data and extract results

Across this section, the first three stages as well as the research questions are described in detail. And, later on, the Search Strategies section provides further details of the specific details of the Method Definition. Results are also presented in a separate section.

3.1. Method Definition. The definition of the method to conduct the analysis includes the following steps:

(1) Research questions: determining the questions that are relevant for getting a picture of the state of the art of CA systems.

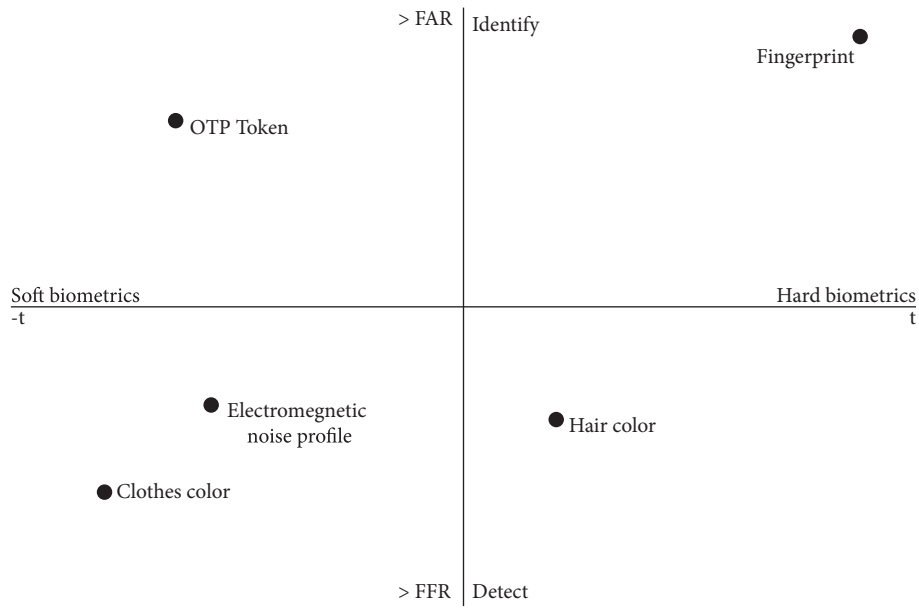

Figure 1: Permanence/distinctiveness map in continuous authentication.

(2) Identifying search strategies including the keywords and sources: the aim is that the search can be replicated.

(3) Identifying inclusion/exclusion criteria: An objective evaluation process must be defined to determine which results fit the SLR goals or, at least, which provide enough information to answer the research questions. Also, the analysis seeks to avoid biases derived from secondary research works. In this phase, a list of criteria is defined to decide the inclusion or exclusion of search results.

(4) Quality Evaluation Strategy: defining the quality criteria that the studies must meet to be included in the study.

(5) Data Extraction Strategy: determining how the data of the studies will be collected so that it can be used to address the research questions.

(6) Elaboration of supporting materials: building supporting evidence (tables, forms, etc.) that facilitates understanding the results and provide evidence to ensure the integrity of the process and its results.

3.2. Document Compilation. The compilation of documents comprised three steps:

(1) Search in data sources: the 20 most cited of each of the data sources are selected.

(2) Metadata extraction: title, authors, number of pages, etc.

(3) Selection based on inclusion/exclusion criteria: initial filtering based on the abstract to remove unrelated studies was followed by a quick inspection to determine if the remaining studies meet the inclusion/exclusion criteria.

3.3. Analysis of the Studies. Document compilation was followed by an analysis of the research studied following the next steps:

(1) Due to the volume of data that a complete analysis requires, the 80 papers (20 results of 6 different sources) were studied in three iterations using the following approach:

  (a) The first three papers from each source were used to create a first picture of the state of the art.

  (b) Up to 5 papers were then added to complete state of the art.

  (c) If the new papers (second step) changed substantially the results we get from the first step, the following studies of search results would also be analyzed, up to 10 per source. We set the limit to 10 because after applying the inclusion/exclusion criteria on the search results because the sample to be analyzed can be different for each source.

(2) Instead of evaluating the studies returned by each source in turn, one study from each source was selected each time. Thus, if there were 5 different data sources, every 5 research papers studied would include one paper from each source.

  To detect coding errors, each time a paper was analyzed, the reviewer name was included, and the evaluation status was updated in a common document used by all the reviewers.

(3) Determining the research questions that each research study addresses.

(4) Developing the data extraction strategy, taking into account that if at this moment it was found that any study did not meet the inclusion criteria or the quality, it would be removed and the decision was recorded.

(5) Analysis of results: when all data (i.e., the elements defined by this procedure) was extracted from original sources, it was analyzed and presented as answers to the research questions in the form of an R/RQ matrix to synthesize the state of the art.

3.4. Research Questions (RQ). In this work, we aim to synthesize the state of the art of CA by analyzing how relevant existing studies address the following research questions. Questions with an identifier are available in the Supplementary Material (see Table of Selected Papers, Results of the Search, and Research Questions):

(i) RQ1: which information allows to perform continuous authentication?

(ii) RQ2: how is data obtained?

(1) RQ2.a: what mechanisms are used to obtain data? Which procedures, devices, or combination of devices enables data collection for CA (e.g., capturing heart activity could be done through electrocardiography or using a microphone)?

(2) RQ2.b: what characterizes the data (e.g., the feature extracted to characterize the heart activity could be the distance between frequency peaks, a wavelet spectrum, etc.)?

(iii) RQ3: what mechanisms are used to process this data?

(1) RQ3.a: how is the data synthesized? How is the data encoded for subsequent processing? What parameters are extracted to generate a digital model?

(2) RQ3.b: how is the decision model built? How a decision model is generated and how it defines the identity of the user (e.g., machine learning and statistics)?

(iv) RQ4: how can CA be integrated into an access control system?

(1) RQ4.a: how does it react in case of an incident detection? Given that the ideal is that the system never disturbs the work of a legitimate user, how does the access control system act if the CA system fails to authenticate the user?
What is the most reliable way to achieve this, taking into account the capabilities that an attacker with access to the machine can have?

(2) RQ4.b: how different models can be combined to produce greater accuracy?
What combinations of systems can offer a more reliable result, and how they can be combined?

(v) RQ5: where can continuous authentication be applied?
In which fields or on which systems can continuous authentication be a contribution?

(vi) RQ6: is it possible to generate a unique fingerprint? Or is it only possible to verify if what is on the other side remains to be the same?

(1) RQ6.a: what hard biometric systems exist? What features, regardless of the accuracy of the systems, will be representative of the actor life?

(2) RQ6.b: what soft biometrics systems exist? What elements are usually part of the identity of the actor, and therefore, allow their recognition throughout (at least) one session?

An example of a piece of research that answers all the questions is the following:

We will authenticate people through the typing of text peculiarities (RQ1). Through the camera (RQ2.a), we will analyze the hand position each time keyboard shortcuts are used (RQ2.b). Furthermore, we will record the posture of the hand when someone types and the distance between your fingers (RQ3.a). This information will allow us to generate a model using OpenCV (RQ3.b). Having these data sources, it is possible to contrast the typing speed captured by the camera with the speed at which the keys enter the system (RQ4.b), and if the system fails, we will request authentication again (RQ4.a). Given that according to the results of the research, each user types in a unique way (RQ6 and RQ6.a), we could implement this in all offices so that users do not have to block their equipment when they go out for lunch (RQ5).

4. Search Strategies

This section details the most important steps of the method definition stage introduced in the previous section. It describes the search strategy, inclusion and exclusion criteria, quality evaluation strategy, and data extraction strategy.

4.1. Data Sources. The search was carried out using the engines provided by the following sources:

(i) Google Scholar (https://scholar.google.com/)

(ii) ACM Digital Library (https://dl.acm.org/)

(iii) IEEE Xplore (https://ieeexplore.ieee.org/Xplore/home.jsp)

(iv) SpringerLink (https://link.springer.com/)

(v) ScienceDirect (https://www.sciencedirect.com/)

(vi) ArXiv.org (https://arxiv.org/)

4.2. Study Categories. As long as they meet the inclusion criteria and quality criteria, this SLR considered the three following types of studies:

(i) Papers

(ii) Patents

(iii) Nonacademic white papers

4.3. Search Terms and Results Storage. To find research papers related to continuous authentication, the search term used was "continuous authentication." Furthermore,

advanced search options were configured to search in the abstract, when the search engine has this option or on the full text otherwise (e.g., ACM Digital Library has the option of searching within the abstract, but in Google Scholar we had to set up the search to find the terms "anywhere in the article"). The first 20 search results from each source, ordered by the number of citations can be found in the Supplementary Material.

4.4. Inclusion and Exclusion Criteria. All the results obtained in the data sources were saved, but only studies that met the following criteria were analyzed:

(i) Primary research: only primary research was included. Secondary sources such as reviews or studies of the state of the art were not included.

(ii) No posters: although they may be useful to complement this, posters usually do not provide enough information to build a solid analysis and may generate biases when interpreting results.

(iii) No duplicates: when two data sources return the same result, the second instance is removed.

(iv) English-only papers: as English is the language used for scientific communication [10].

(v) Research papers that, even using the search term "continuous authentication," do not fit our definition were excluded. Examples of this case include the following:

  (i) Papers addressing how to use an authentication factor repetitively
  (ii) Studies focusing on data validation instead of entities
  (iii) Studies based exclusively on classical authentication (tokens)

(vi) All the papers must be published in peer-reviewed sources

4.5. Quality Evaluation Strategy. The quality of each study for this SLR was assessed in terms of the following criteria:

(i) It includes experimentation.

(ii) It uses public datasets that enable replicating the results.

(iii) The performance is over 70% for at least one of the target metrics.

(iv) Simplicity: it is easy to validate the results, and it is a method that can be implemented in other systems. To measure the complexity of the solution, from 1 to 5 (being 1 very simple and 5 very complex), we use the following scale:

  (1) Reads logs from the system
  (2) It is necessary to run a specific software
  (3) It is necessary to use a common IO device (e.g., webcam and mouse)
  (4) It requires a specific IO device (e.g., brainwave sensor)
  (5) Requires that the user follows a specific task (e.g., do a task which is not part of his activity with the system)

(v) The study contains enough information to reproduce the experiment

(vi) Number of different evaluation methods

(vii) Number of research questions addressed

Those studies, which meet at least half of these quality criteria and address at least three research questions, were included in this SLR. Studies not meeting the criteria were excluded and recorded.

4.6. Data Extraction Strategy. The final step before analysis and synthesis is to define a systematic method to extract and code the data from the studies.

4.6.1. Research Questions. An R/RQ matrix relates each study with the research questions that it addresses.

4.6.2. Metadata. The following metadata was gathered for each study: title, authors (only the two first ones), publication date, venue (journal, conference, etc.), type (paper, conference, book, or patent), and number of pages.

4.6.3. CA Data. The following data was gathered for each study about CA:

(i) Entities involved: people, machines, and other

(ii) Data source studied (RQ1)

(iii) Device of the CA system (e.g., mobile and computer) (RQ2.a)

(iv) IO method to obtain the user's data (e.g., camera and keyboard) (RQ2.a)

(v) What makes the input data useful to perform continuous authentication? (i.e., which peculiarities does this data have that allows identifying a user?) (I) (RQ2.b)

(vi) How is the model built? (S) (RQ3.a)

(vii) Evaluation method (P) (RQ3.b)

(viii) Type of continuous authentication (RQ6): the quadrant that best identifies the approach from Figure 1 (permanence/distinctiveness ratio).

(ix) System applications (RQ5)

(x) Is there any kind of experimentation reported in the research?

(xi) If there is experimentation, what is the size of the population?

(xii) Is there a public dataset? (RQ2)

(xiii) What is the reported performance of the research results?

(xiv) Is the method reproducible?

(xv) From 1 to 5, how complex is the solution?

(1) Reads system logs
(2) Develops a program that evaluates user behaviour
(3) Requires a specific IO device/method, but it is common
(4) Requires a specific unusual IO device/method
(5) Requires that the users modify the way they work

(xvi) Comments

4.6.4. Support Documents. Supporting documents included tables to save the search results and the data extracted, tables to check each inclusion/exclusion criteria for each study, and the R/RQ matrix to determine the relationship between studies (R) and research questions (RQ). The data extraction strategy of elements related to continuous authentication was coded using Google Drive survey.

5. Findings

5.1. Process Findings. This section summarizes the main findings of the literature review. The complete table of selected papers, search results, and research questions are included as supplementary material (see Table of Selected Papers, Results of the Search, and Research Questions).

5.2. Selected Primary Research Works. 84 papers of the initial 122 met the inclusion criteria. 38 were removed for the following reasons:

(i) 26 did not meet inclusion/exclusion criteria

(ii) 5 documents were not accessible

(iii) 7 duplicated

Of all these papers, 30 studies were included in the first two iterations of the analysis. The complete list can be found under the "Selection of Articles" sheet of the Supplementary Material (see Table of Selected Papers, Results of the Search, and Research Questions). Three of them were also removed after checking the quality criteria as follows:

(1) Two papers met exclusion criteria:

(i) Not fitting with the focus of this study (R028, [11]).
(ii) It is considered a secondary research work for the purpose of this review. Its objectives are to develop an adversary modelling system (R086 [12]).

(2) One paper did not contain enough information to be able to assess and rate (R044 [13])

6. Results of the Research

After evaluating the remaining 30 documents and carrying out the data extraction process, we found the following results.

6.1. R/RQ Relationship. While the vast majority of studies document the entire characterization and modelling process of the actor for authenticating this character, very few fit it into an access control system or propose a system to be able to contrast the results of their method with other authenticator.

When determining the position of the solution in the permanence/distinctiveness, Figure 1, only a few studies gave a clear answer or the authors did not address the problem in a similar dimension, despite using the same indicators when focusing the study (R027, [14]).

The "RQs" Table 1 presents the matrix of the relationship between the research questions and the research studies that address them. The complete detailed table can be found in the Supplementary Material (see).

6.2. Technologies Evaluated. Almost all of the 30 research studies included in this review analyzed methods to authenticate people, except one (R085, [15]) that presents a method to authenticate machines through the analysis of the electromagnetic radiation they produce. The relationships between the technologies used are presented in Figure 2.

Along this work, we identified that 40% of the studies used mobile phones to authenticate users, contrasting with the 13% focusing on computers. Only one of the previously analyzed research studies explicitly applies continuous authentication to both, mobile phones and computers, and just one aims to perform continuous authentication on smart glasses (R066, [16]). The remaining studies do not explicitly indicate if authentication takes place on any specific device, but they describe different use cases, such as authenticating drivers who get in and out of the vehicle (carriers) or monitoring workstations (which could be associated mainly with desktop computers).

The main IO methods used to get data from the actor to be authenticated are

(i) Touch screen: most used to collect characteristic gestures of a user, but also as a method to input text through different typing methods

(ii) Mobile phone sensors: the accelerometer, gyroscope, or magnetometer of the phone are often used to complement other measures, in the context of the user activity; although sensor information can also be used on its own to characterize user patterns (R005, [17]).

(iii) Camera: mainly through facial recognition and evaluation of other session observable characteristics such as clothing, hair colour, and glasses

(iv) Keyboard and mouse: patterns of use of both devices, present in all computers (also through soft-keyboards in mobile phones), can also be used to identify or complement user modelling

We also found two CA research studies that analyze brain activity (R045, [18]; R063, [19]). Their implementation is rather complex requiring specific hardware and working conditions. In terms of hardware requirements, the only

Table 1: R/RQ relationship.

Code	R001	R005	R006	R007	R008	R023	R027	R028	R030	R031	R045	R046	R048	R049	R063	R065	R066	R068	R069	R083	R084	R085	R087	R104	R106	R107	R109	R110	R113
RQ1	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
RQ2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓	✓
RQ2.a	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✓
RQ2.b	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓
RQ3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓
RQ3.a	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓
RQ3.b	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓
RQ4	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
RQ4.a	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
RQ4.b	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗
RQ5	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓
RQ6	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✓
RQ6.a	✓	✓	✓	✗	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✓
RQ6.b	✓	✗	✗	✗	✓	✓	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓

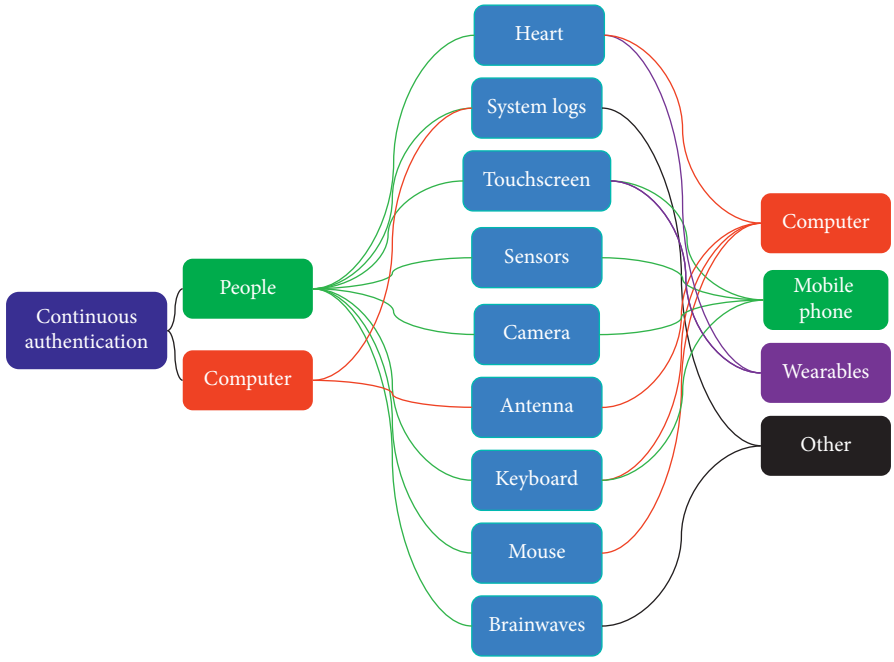

Figure 2: Continuous authentication components' relationship.

other exception was R023 [20], which required a special camera. The rest of the studies can be put in practice in common existing environments and devices, requiring only in a few cases to have access to system logs.

6.3. Data Processing Approaches. We found the following artificial intelligence algorithms in the studies analyzed as part of this SLR:

(i) Support Vector Machine (SVM): it is one of the most used classification techniques, and 10 of the 30 research papers analyzed use SVM. Depending on the type of samples of the dataset, different SVM can be used:

  (i) Canonical SVM when there are at least two sets of data, SVM can be applied to differentiate the values generated by the genuine actor from the other possible values generated by others. If we had data from 100 users, we could generate a model that would allow us to differentiate one of them from the remaining 99.

  (ii) One-class SVM when there is only one dataset: if there is only legitimate user data and a system wants to classify new data as similar or different.

(ii) *k*-nearest neighbours: this algorithm groups and classifies new instances by comparing them to their closest *k* data entries of the existing dataset.

(iii) Eigenfaces is a method for facial recognition based on the reduction of facial images to a series of characteristic vectors. This method generates a facial base model (see Figure 3), called *F*, and stores the identity of each user and the variation with respect to *F* for reconstructing the face model later.

Figure 3: Example of eigenfaces' models [29].

(iv) Interactive Artificial Bee Colony (IABC): in R046 [21] research, IABC is used as a method for optimizing eigenfaces. It simulates the behaviour of a bee colony searching for natural resources.

(v) Artificial Neural Network (ANN): this method combines and connects a set of simpler decision-making systems, simulating the behavior of neurons, to recognize patterns (R065, [22]; R049, [23]).

(vi) State-Space Models: one of the simplest ways to approach a classification problem is to model it as a state diagram (as in the case of R109, [24]). Examples of other state-space models include decision trees (DT), Random Forests Classifiers (RFC) (R084, [25]), or decision models based on Markov processes, such as Markov Chains or Hidden Markov Models (R049, [23]; R113, [26]).

(vii) Other probabilistic models: R084 [25] compares different methods including logistic regression and Bayesian classifiers (Naive Bayes). R048 [27] and R110 [28] use simple statistical models.

6.4. Experimentation. All the studies analyzed in this review included practical experimentation with users. The average sample is 58.75 subjects.

6.5. Rating Metrics. The following metrics were used to evaluate the quality of the results of the CA systems presented in the studies that are part of this SLR:

(i) False Acceptance Rate (FAR): it measures the percentage of identification instances in which illegitimate users are incorrectly accepted as authorized users.

(ii) False Rejection Rate (FRR): it measures the percentage of identification instances in which authorized users are incorrectly rejected as illegitimate users.

(iii) Equal Error Rate (EER): it is the minimum point at which FAR and FRR meet. It is a measure of the global effects of the system considering both incorrectly accepted and incorrectly rejected instances. If this rate exceeds 50%, the system performs worse than a random classifier.

The EER achived by R109 [24] is between 34% and 49%, but no other papers show an average EER value higher to 30%.

6.6. A Taxonomy for Continuous Authentication. Figure 4 shows that although most of the systems create reliable and permanent models of users, none manages to create a unique behavioral fingerprint of each user. The absence of systems based exclusively on CA may be because such a system does not contribute substantially to the security of assets. Continuous authentication systems could be a great addition, in terms of accuracy, to other approaches (such as the use of light biometrics in R046, [21]).

Results then suggest that our initial bidimensional model for characterizing users in terms of permanence/distinctiveness is appropriate. R027 [14] presents a four-dimensional model for CA methods:

(i) Universality: whether it can be used with all actors of the population targeted by the methods.

(ii) Distinctiveness: to what extend the method tells apart the individual from the population; it can tell whether the actor evaluated is *X* or is Y, or only can determine "you were *X*, and you are not *X* anymore."

(iii) Permanence: for how long the model produced is valid without requiring new training or rebuilding, that is, how long the actor's behavior (fingerprint) does not change.

(iv) Collectibility: the features allow CA data to be gathered and encoded. They must be quantitatively measurable.

Further, R084 [25] introduces the following additional dimensions:

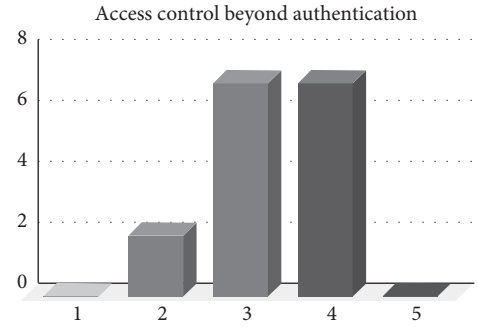

Figure 4: CA system type (1: session CA; 5: behavioral fingerprint CA).

(v) Efficiency: if the system involves mobile phones, which are devices with limited resources, with autonomy that depends on battery consumption.

(vi) Acceptability: determines the level of invasiveness in the user's environment of the CA method.

(vii) Mocking rate: unlike the error rates, the mockery rate measures the effectiveness of the CA system for preventing attacks that falsely recreate the identity of the legitimate user.

7. Discussion

EER is the most common metric to evaluate CA systems. In contrast with machine learning research, where classification is usually measured in terms of positive or negative results (false positives and false negatives), CA results are expressed in terms of acceptance and rejection rates (FAR and FRR). Only the terminology is different, emphasizing the nature of CA as a method for access control.

In quantitative terms, any CA approach with an EER around 30% is considered acceptable, while the best state of the art results report EERs below 10%. Although these EER values are reasonably good (i.e., allow the CA system to work as it should), it must be taken into account that their results are circumscribed to very specific experimental conditions.

HMOG [17] plays a central role in current CA literature, both as holistic research in mobile CA and as a source for further research through its public dataset.

7.1. CA Literature Gaps. This review delimitates the boundaries of CA research. The majority of studies are circumscribed to very specific conditions, sometimes in laboratories, and they do not address the possible consequences of changing the scope to a real-life scenario (i.e., how could it impact model availability). Further, a closer analysis of CA studies that are specific for mobile environments shows that several of them may be difficult to implement in current devices because of technical limitations, such as APIs collecting all user interactions. Approaches such as Touchalytics [30] can only be implemented in a closed run environment with a given application.

Further analysis is also required to determine the features that sustain the initial hypothesis of what CA

approaches can do. Finding new behavioural patterns would mean identifying new methods for CA.

There is still room for improvement and a long way to go until CA systems can generate a unique and durable fingerprint that facilitates noninvasive ways of authentication. Only three of the studies reviewed here [20, 26, 30] consider the possible intersession changes in user models.

Finally, the second iteration of this SLR did not make any substantial changes to the results of the first iteration although it provided more studies that extended and completed the initial analysis. The second iteration did not provide any new use cases scenarios or the involvement of new devices. However, it is necessary to mention that this iteration shows the increased dominance of mobile phones, as the most important target use case for CA research.

8. Conclusions

This paper presents a systematic literature review of CA. After an initial search that returned 120 studies, the 30 most cited papers that met the inclusion criteria took part in the next stage of the study. Results of our review reveal the existing technologies and methods for CA as well as their current limitations. We described the behavioural features used for CA and the techniques to extract and process them. We also describe the main measures used to evaluate the performance of CA systems. Finally, this study also suggests a taxonomy to categorize CA approaches.

This review also describes current trends for CA and the expected levels of performance required for CA systems. Additionally, we suggest the limitations of the existing state of the art for CA research, which may act as a guide for the direction of future research articles. Finally, this review also identifies several research gaps in the CA field, outlining other different lines for new contributions.

8.1. Future Work. Existing research on CA not only shows its impact on the protection of existing systems but also shows that there is still room for new studies, particularly in the line of long-term CA technologies. In what follows, we suggest a few of them.

The fingerprinting aspect (i.e., the possibility of generating a behavioral fingerprint, easy and discreetly to obtain, and from which the user cannot detach itself) also arises the need for studying its ethical impact. Addressing an evaluation from an ethical point of view could be useful to mitigate the impact of these approaches on the privacy of personal data.

Further, the possibility of applying identity analysis systems to other nonhuman actors (e.g., such as the authentication between machines shown in (R085, [15])) opens the door for its use in securing industrial or IoT-related environments.

Finally, due to the character of the review, several novel approaches or commercial products have not been taken into account. Developing a less formal scientifically grounded search method could lead to discovering additional areas or applications of CA.

Data Availability

The data in table used to support the findings of this study are included within the supplementary information file(s).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project was supported by the European Union's Horizon 2020 Research and Innovation Program under grant agreement no. 826284 (ProTego).

Supplementary Materials

The materials produced to support the research process, and for structuring the documentation of the review, are provided as supplementary material. The file "Appendix A. Search results (en).pdf" contains a list of all the papers indexed in the early stages of the research. For each one, the columns represent the following: (1) Origin: search engine source; (2) Code: internal code to identify the paper across different support files; (3) Title; (4) Authors; (5) Publishing date; (6) Where: publication name; (7) Type of publication: e.g., journal, conference; (8) Included: checkbox to indicate if the paper becomes included in our review; (9) Pages: length (i.e., the amount of pages) of the paper; (10) Annotations: internal notes. (*Supplementary Materials*)

References

[1] C. DeCusatis, P. Liengtiraphan, S. Anthony, and M. Pinelli, "Implementing zero Trust cloud networks with transport access control and first packet authentication," in *Proceedings of the 2016 IEEE International Conference on Smart Cloud (SmartCloud)*, pp. 5–10, New York, NY, USA, November 2016.

[2] Information Technology Laboratory Computer Security Division, "Zero trust architecture: comment on draft NIST SP 800-207 | CSRC," 2019, https://csrc.nist.gov/News/2019/zero-trust-architecture-draft-sp-800-207.

[3] A. Chuvakin, "Named: endpoint threat detection & response," 2013, https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/.

[4] E. Mistek, M. A. Fikiet, S. R. Khandasammy, and I. K. Lednev, "Toward locard's exchange principle: recent developments in forensic trace evidence analysis," *Analytical Chemistry*, vol. 91, no. 1, pp. 637–654, 2019.

[5] J. Aguado-Delgado, J.-M. Gutiérrez-Martínez, J. R. Hilera, L.de. Marcos, and S. Otón, "Accessibility in video games: a systematic review," *University Access in the Information Society*, 2018.

[6] R. Armstrong, B. J. Hall, J. Doyle, and E. Waters, "Scoping the scope' of a cochrane review," *Journal of Public Health*, vol. 33, no. 1, pp. 147–150, 2011.

[7] BioCatch, "From Login to Logout: Continuous Authentication with Behavioral Biometrics," 2019, https://www.biocatch.com/resources/white-paper/from-login-to-logout-continuous-authentication-with-behavioral-biometrics.

[8] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia, Computer Science*, vol. 34, pp. 532–537, 2014.

[9] H. Arksey and L. O'Malley, "Scoping studies: towards a methodological framework," *International Journal of Social Research Methodology*, vol. 8, no. 1, pp. 19–32, 2005.

[10] I. López-Navarro, A. I. Moreno, M. A. Quintanilla, and J. Rey-Rocha, "Why do I publish research articles in English instead of my own language? differences in Spanish researchers' motivations across scientific domains," *Scientometrics*, vol. 103, no. 3, pp. 939–976, 2015.

[11] G. Ryu, S. Park, D. Choi et al., "Active authentication experiments using actual application usage log," in *Proceedings of the ASIA CCS'18: ACM Asia Conference on Computer and Communications Security Incheon, Incheon, Republic of Korea*, June 2018.

[12] P. Peris-Lopez, L. González-Manzano, C. Camara, and J. M. de Fuentes, "Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things," *Future Generation Computer Systems*, vol. 81, pp. 67–77, 2018.

[13] A. E. d. Oliveira, G. H. M. B. Motta, and L. V. Batista, "A multibiometric access control architecture for continuous authentication," in *Proceedings of the 2010 IEEE International Conference on Intelligence and Security Informatics*, p. 171, Vancover, Canada, May 2010.

[14] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: an experimental study on smartphones," in *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security, SOUPS '14*, pp. 187–198, USENIX Association, Menlo Park, CA, USA, July 2014.

[15] J. Wang, M. Ni, F. Wu, S. Liu, J. Qin, and R. Zhu, "Electromagnetic radiation based continuous authentication in edge computing enabled internet of things," *Journal of Systems Architecture*, vol. 96, pp. 53–61, 2019.

[16] J. Chauhan, H. J. Asghar, A. Mahanti, and M. A. Kaafar, "Gesture-based continuous authentication for wearable devices: the smart glasses use case," in *Applied Cryptography and Network Security, Lecture Notes in Computer Science*, M. Manulis, A.-R. Sadeghi, and S. Schneider, Eds., pp. 648–665, Springer International Publishing, New York, NY, USA, 2016.

[17] Z. Sitová, J. Sedenka, Q. Yang et al., "HMOG: new behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2016.

[18] I. Nakanishi and T. Yoshikawa, "Brain waves as unconscious biometrics towards continuous authentication-the effects of introducing PCA into feature extraction," in *Proceedings of the 2015 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS*, pp. 422–425, Nusa Dua Bali, Indonesia, November 2015.

[19] M. Shozawa, R. Yokote, S. Hidano, C.-H. Wu, and Y. Matsuyama, "Brain signal based continuous authentication: functional NIRS approach," in *Advances in Computational Intelligence*, I. Rojas, G. Joya, and J. Cabestany, Eds., pp. 171–180, Springer, New York, NY, USA, 2013.

[20] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Looks like eve: exposing insider threats using eye movement biometrics," *ACM Transactions on Privacy and Security*, vol. 19, no. 1, pp. 1–31, 2016.

[21] P. Tsai, M. K. Khan, J. Pan, and B. Liao, "Interactive artificial bee colony supported passive continuous authentication system," *IEEE Systems Journal*, vol. 8, no. 2, pp. 395–405, 2014.

[22] S. R. d. L. Silva Filho and M. Roisenberg, "Continuous authentication by keystroke dynamics using committee machines," in *Intelligence and Security Informatics, Lecture Notes in Computer Science*, S. Mehrotra, D. D. Zeng, H. Chen, B. Thuraisingham, and F.-Y. Wang, Eds., pp. 686-687, Springer, New York, NY, USA, 2011.

[23] E. C. Popovici, L. A. Stancu, O. G. Guta, S. C. Arseni, and O. Fratu, "Combined use of pattern recognition algorithms for keystroke-based continuous authentication system," in *Proceedings of the 2014 10th International Conference on Communications (COMM)*, pp. 1–4, Toronto, Canada, May 2014.

[24] U. Mahbub, J. Komulainen, D. Ferreira, and R. Chellappa, "Continuous Authentication of Smartphones Based on Application Usage," 2018, https://arxiv.org/abs/1808.03319.

[25] M. Smith-Creasey and M. Rajarajan, "A novel word-independent gesture-typing continuous authentication scheme for mobile devices," *Computers and Security*, vol. 83, pp. 140–150, 2019.

[26] A. Roy, T. Halevi, and N. Memon, "An HMM-based behavior modeling approach for continuous mobile authentication," in *Proceedings of the 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3789–3793, Florence, Italy, May 2014.

[27] Ananya and S. Singh, "Keystroke dynamics for continuous authentication," in *Proceedings of the 2018 8th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, pp. 205–208, Noida, India, January 2018.

[28] A. Acar and H. Aksu, A. Selcuk uluagac and K. akkaya, WACA: wearable-assisted continuous authentication," 2018, https://arxiv.org/abs/1802.10417.

[29] W. Commons, "Tinderbox eigenfaces models," 2019, https://en.wikipedia.org/w/index.php?title=File:Tinderbox_eigenfaces_models.jpg&oldid=887229639.

[30] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "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, pp. 136–148, 2013.