Examining the Current Status and Emerging Trends in Continuous Authentication Technologies through Citation Network Analysis

Article *in* ACM Computing Surveys · April 2022

DOI: 10.1145/3533705

CITATIONS
13

READS
788

3 authors, including:

Jongkil Jay Jeong
University of Melbourne
29 PUBLICATIONS **161** CITATIONS

SEE PROFILE

Yevhen Zolotavkin
Tampere University
27 PUBLICATIONS **101** CITATIONS

SEE PROFILE

Examining the Current Status and Emerging Trends in Continuous Authentication Technologies through Citation Network Analysis

JONGKIL JAY JEONG, YEVHEN ZOLOTAVKIN, and ROBIN DOSS, Cyber Security Cooperative Research Centre & Deakin University - Centre for Cyber Security Research & Innovation (CSRI)

Continuous Authentication (CA) technologies enable users to be authenticated beyond just the point of entry. In this article, we conduct a comprehensive review of over 2300 articles to (a) identify the main components of CA research to date, and (b) explore the current gaps and future research directions. Through a Citation Network Analysis (CNA), we identified that there are currently three primary focus research areas on CA - Keystroke Dynamics; Mouse Movements; and Mobile Device Touch, as well as identify an emerging trend in more recent studies on multi-modal CA authentication which utilises the numerous sensors that are embedded in modern mobile devices. This study also highlights the current gaps in the literature such as the need for a consensus over how to evaluate the application and utility of CA, and the need to examine the feasibility of CA technologies that currently exist based on more use case studies.

CCS Concepts: • **Security and privacy** → **Authentication**; • **Human-centered computing** → **Social network analysis**.

Additional Key Words and Phrases: continuous authentication, literature review, biometric authentication, citation network analysis

ACM Reference Format:
Jongkil Jay Jeong, Yevhen Zolotavkin, and Robin Doss. 2022. Examining the Current Status and Emerging Trends in Continuous Authentication Technologies through Citation Network Analysis. *ACM Comput. Surv.* 56, 4, Article 111 (April 2022), 31 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The ability to identify users over digital channels such as mobile interfaces, internet browsers, and internet-enabled central authentication points has become a critical, yet complex challenge for many institutions. In particular, verifying a user's identity claim remotely via a digital service is fraught with opportunities for an attacker to successfully impersonate a user.

This is further complicated when the majority of authentication mechanisms focus solely on identity verification at the point of entry which implies that as long as the original login session is actively used, there is no mechanism to verify that the initial authenticated user is still the user in control of the device maintaining the session. For example, users may share their passwords with family members, friends, colleagues, or an already authenticated user may walk away without

Authors' address: Jongkil Jay Jeong, jay.jeong@deakin.edu.au; Yevhen Zolotavkin, yevhen.zolotavkin@deakin.edu.au; Robin Doss, robin.doss@deakin.edu.au, Cyber Security Cooperative Research Centre & Deakin University - Centre for Cyber Security Research & Innovation (CSRI), Geelong, Victoria.

0360-0300/2022/4-ART111 $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

locking his/her computing platform (e.g., laptop) at which point a malicious actor may be able to successfully impersonate a user [2].

To ensure that a user is authenticated even after the initial authentication phase, recent studies have started to examine potential authentication methods which actively monitor a user or a device during the entire session up to its termination. This process is know as Continuous Authentication (CA), and it is defined as the methods and techniques to enable authentication systems to effectively and reliably authenticate, verify and identify individuals throughout the entirety of a session by collecting detailed information about their physical attributes and/or behavioural patterns [39].

The importance of CA is confirmed by a number of emerging industrial initiatives. For example, Continuous Access Evaluation Protocol (CAEP) is a prt of the Shared Signals and Events Framework. The goal of the framework is to enable sharing of security events, state changes, and other signals between related and/or dependent systems. It allows managing access to resources and enforcing access control restrictions across distributed services operating in a dynamic environment. CAEP is intended to be used between cooperating Transmitters and Receivers such that Transmitters may send continuous updates, while Receivers can attenuate access to shared human or robotic users, devices, sessions and applications [26].

However, despite a large body of research and knowledge emerging within the CA space, it has largely remained silo-ed based on the disciplinary background and interest of the researcher. Furthermore, real-life applications of such technology have been limited and have also met challenges surrounding privacy, security and usability concerns. For instance, current CA techniques that depend on specialised hardware and/or require users to carry additional devices (e.g., a smartphone), raising additional concerns about its perceived intrusive nature. In addition, the scope and breadth of the body of knowledge on CA transpires across multiple disciplinary areas, all specialising in a particular topic which has made it difficult to grasp the full picture. Therefore, the main purpose of this paper is to:

- ***RQ1*** *What are the currently established research agendas on Continuous Authentication?*;
- ***RQ2*** *What are the emerging research trends and current knowledge gaps pertaining to Continuous Authentication?*

To address our primary research questions, we first examined the background literature on CA through a meta-analysis of 24 prior survey papers. This helped establish a solid foundation of the main concepts, models and theoretical frameworks of CA. Due to the large body of literature identified through this preliminary meta-analysis, we decided to develop a *Citation Network Graph (CNG)* based on the 2300 articles referenced amongst these papers. Subsequent analysis of the CNG enabled us to address RQ1 which was identifying the current resarch on CA (Keystroke Dynamics, Mouse Movements and Mobile Device Touch Interfaces) and also address RQ2 by identifying the emerging trends (Fusion of techniques and the focus on mobile devices) and future challenges (evaluation methods; security and privacy considerations; innovation in hardware and standardisation) within CA as well.

Based on the analysis of the results, we identified an emerging trend where CA research is gravitating towards multi-modal methods of biometric authentication technologies aided by smartphones. This is not only due to the accessibility, affordability and the variety (and power) of sensors that are embedded into these devices. However, the outcome of our study also indicates that the efficacy of such methods are yet to be fully tested due to the discrepancies in how success and failure rates pertaining to these methods are benchmarked.

The remainder of the paper is structured as follows. In Section 2, we provide the background literature and current research status of CA based on the analysis of 24 literature survey papers identified. This is followed by Section 3 where we present a detailed overview of the research

methodology, and how CNA was conducted across 1789 studies which identified current and emerging themes within CA. Results from the data analysis are then presented in Section 4, followed by a comprehensive discussion on how the CNA results address our two primary RQ's in Section 5. We then conclude our study in Section 6 by covering the main implications of our study for both Research and Practice, and address the limitations of this study and directions for future research.

2 RELATED WORKS

A comprehensive body of knowledge already exists on CA covering various concepts, models and theoretical frameworks. However, this rapid growth in CA literature has also resulted in fragmentation of the research. This fragmentation is based on the disciplinary area and paradigm of the researcher themselves, resulting in a need to systematically categorise and synthesise the extensive knowledge that is already out there. This sentiment is also shared amongst other scholars, based on the ever increasing number of literature review studies on the subject.

One approach to the reviewing task would be to select publications with the topics satisfying the definition of CA presented in the introduction. Unfortunately, further requirements to the 'detailed information' aspect (as per the definition) of CA remain vague. To overcome the issues of insufficient granularity of the definition we use a different approach: we select the publications stating they are CA-related. In the absence of detailed definitions and industrial standards dealing with CA such self-proclaimed relation with the domain is the consensus among the researchers **[39, 100]**.

Furthermore, more recent studies which have emerged have started to classify CA based on its method (Biometrics vs. Non-biometric) and device mode (Sensors vs. Mobile Device vs. IoT) [15, 39, 51] further encompassing the need to systematise the extensive body of knowledge that currently exists.

Author	Period covered	No. of References	Applied Method	Device	Technique
Al Abdulwahid et al. [5]	2003-2014	48	Meta-Analysis	Generic	Multi-Modal Biometrics
Abuhamad et al. [1]	2005-2020	187	Meta-Analysis	Sensors	Behavioural Biometrics
Al-Naji & Zagrouba [6]	2015-2019	162	Meta-Analysis	IoT	Blockchain
Alotaibi & Alruban [9]	2003-2017	39	Systematic Review	Mobile	Biometrics
Ayeswarya & Norman [15]	2010-2018	135	Critical Review	Generic	Biometrics
Dahia et al. [34]	2003-2019	86	Meta-Analysis	Generic	Physiological Biometrics
Eberz et al. [37]	2003-2019	86	Meta-Analysis	Generic	Behavioural Biometrics
Ellavarson et al. [39]	2008-2018	122	Systematic Review	Mobile	Behavioural Biometrics
Gonzalez-Manzano et al. [51]	2010-2018	199	Meta-Analysis	IoT	Biometrics
Hernandez-Alvarez et al. [54]	2006-2020	125	Systematic review	Sensors	Biometrics
Karnan et al. [62]	N/A	72	Meta-Analysis	Generic	Biometrics
Liang et al. [69]	N/A	167	Meta-Analysis	IoT	Behavioural Biometrics
Mahfouz et al. [70]	2002-2017	60	Meta-Analysis	Mobile	Behavioural Biometrics
Mosenia et al. [77]	2004-2015	180	Meta-Analysis	Sensors	Physiological Biometrics
Oak [84]	2002-2016	25	Meta-Analysis	Generic	Behavioural Biometrics
Ouch et al. [85]	2000-2013	37	Meta-Analysis	Generic	Multi-modal Biometrics
Patel et al. [86]	2004-2016	76	Meta-Analysis	Mobile	Biometrics
Pisani& Lorena [89]	1998-2012	49	Systematic Review	Generic	Behavioural Bieomtrics
Sadikan et al. [91]	2002-2018	63	Meta-Analysis	Generic	Behavioural Biometrics
Samangouei et al. [92]	N/A	66	Meta-Analysis	Mobile	Physiological Biometrics
Spolaor et al. [99]	2007-2015	32	Meta-Analysis	Mobile	Biometrics
Stylios et al. [100]	2006-2020	174	Systematic Review	Mobile	Behavioural Biometrics
Yampolskiy & Govindaraju [110]	N/A	N/A	Meta-Analysis	Generic	Behavioural Biometrics
Zhong & Deng [114]	N/A	115	Meta-Analysis	Generic	Behavioural Biometrics
This Study (2021)	***2002-2021***	***2322***	***Social Network Analysis***	***Generic***	***Generic***

Table 1. Literature Review Studies on Continuous Authentication

Therefore, to ensure that this *breadth* on CA is captured in this study, we went through a systematic process to identify the main literature survey papers that exist on CA. We first conducted

an extensive database search(i.e. JSTOR, SCOPUS, EBSCO, Google Scholar) based on the following search criteria:

Search String ("continuous authentication" OR "active authentication" OR "Behaviometrics") AND("Literature Review" OR "survey paper")

From the preliminary search result of approx. 670 papers, a total of 24 literature review papers were selected after filtering studies that were deemed to be (a) non-survey; (b) non-subject related; (c) non-peer reviewed; or (d) duplicate studies. These papers were then categorised (table 1) based on the time period covered; number of references included; research methodology applied; and the classification of CA based on the type of device and techniques used for CA.

The type of method applied for the literature review was included as the general aims, synthesis and analysis of studies may differ substantial based on the literature review methodology applied. A ***Systematic Review*** integrates and/or compares findings from the existing body of literature by identifying themes and constructs that exist within the studies. A ***Meta-Analysis*** is a technique which uses quantitative and statistical methods to summarize and highlight the effects of the current body of literature. Finally, a ***Critical Review*** expresses the author's point of view based on experience, expert knowledge and also an extensive coverage of the literature.Generally, it goes beyond mere description to include degree of analysis and conceptual innovation and typically results in a hypothesis or model [52].

In addition, the classification of CA based on the device used and the technique applied was considered to be an integral part of the synthesis process as varying levels of accuracy were expected based on the device and technique combination utilised [7, 15]. An extensive review and comparison between the different device and techniques used for CA is presented below in Section 2.1 and 2.2.

Based on these 24 papers, a comprehensive overview and background of the current body of knowledge on CA research categorised based on device and technique is presented as follows..

2.1 Continuous Authentication Devices

Recent advancements in technologies have resulted in a diverse range of devices such as mobile phones, wearable sensors, RFID tags, IoT devices and the like to become mainstream. The literature survey papers examined largely follow these device types, often falling under three primary categories - Internet of Things (IoT), Mobile and Sensors. Below, we examine the literature on these three device categories in further detail.

2.1.1 Internet of Things (IoT). [6, 51, 69]

IoT is a paradigm representing any object that can be readable, recognisable, locatable, addressable and controllable via the Internet [51]. Given the proximity and immersive nature of IoT devices and their users, the application of such devices in CA has become attractive and justifiable. This is because these devices are capable to authenticate users on an ongoing and real-time basis for many practical purposes: (a) to verify identity; (b) to support access control functions; (c) to provide cybersecurity protection and so on. Furthermore, the increasing capacity, capability and adoption of certain devices has resulted in the quality and diversity of data captured to be improved considerably [6, 51, 69].

Firstly, studies examined how to overcome the limitations caused by resource capacity (storage; computational power; battery etc.) of IoT devices. Second, studies have also examined the security issues stemming from the use of IoT devices for CA [6, 51]. Finally, another area of focus was how the connected nature of IoT devices could provide pervasive services which presents the ability for a user to share one authentication session across multiple IoT devices [69]. However, the

research has also been critical of the largely hypothetical nature of studies examining IoT, with limited to no linkage to any concrete real life scenarios. Gonzalez-Manzano et al. [51] identified in their survey study that out of the 199 studies evaluated, 54 presented a general, hypothetical approach with no connection to a real application or use case. For instance, Preuveneers & Joosen [90] recommends dynamic context fingerprinting as an improved means for CA. This was done without realizing that the collection of location data for such approach may not be feasible when there are certain connection constraints such as in instances where a suitable network connection is not available. Issues like this encourage the evaluation of each proposal in a particular scenario. All the examined survey papers recommend that suitable feasibility studies are conducted. This relates to the applications and limitations of IoT devices for CA purposes: they must be carried out on a specific scenario basis [6, 51, 69].

2.1.2 Mobile Devices. [9, 39, 70, 86, 92, 99, 100]
A large proportion of the population now own and use a mobile device and the number of sensors, services and devices embedded within these devices continue to increase as per fig. 1. Therefore, these mobile devices have been considered to be suitable for capturing and processing data for CA purposes.

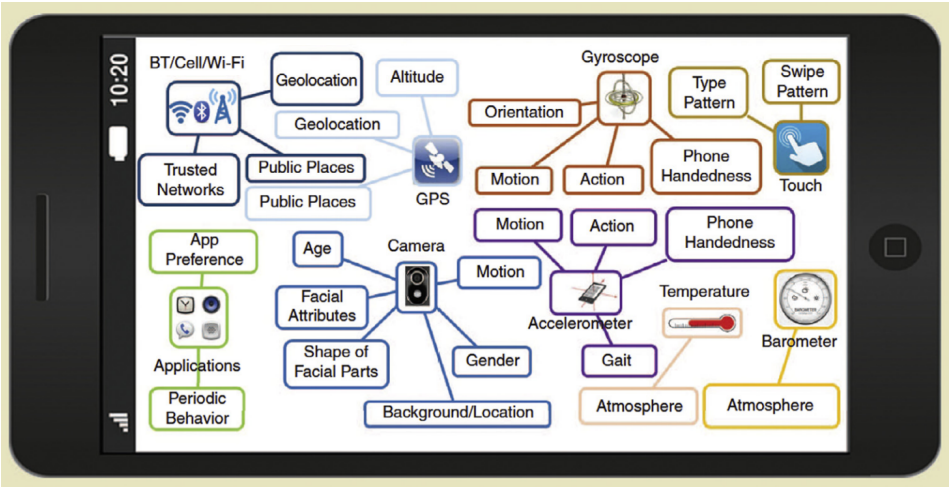

Fig. 1. Sensors, Services and Devices in Mobile Devices for CA [9]

It must be noted that studies within this space are split between two fundamentally different applications of CA.

The first group of survey papers covered the literature on how CA can be used as an additional layer of security when protecting sensitive and important data on the mobile device itself [9, 86, 92, 100]. Stylios et al. [101] highlighted the fact that a high percentage of users (24%) stored highly sensitive information such as their PIN, passwords and credit card numbers within their mobile devices via text messages, images and contact lists resulting in significant exposure to various risks as they mostly depended on security controls at the device level (i.e. point of entry). Similar points are raised by Abuhamad et al. [1] where they outline how traditional means of authentication on mobile phones often fail after the point of entry and rely heavily on knowledge based authentication methods (e.g. passcodes etc.), and presents an overview of the current state-of-the-art approaches for CA using sensors embedded into mobile phones. Therefore, the studies examined by these survey

papers primarily focus on how CA can be utilised as a means of secondary-authentication without the need for users to periodically re-authenticate themselves when protecting their sensitive and confidential data and information [9].

The second group of examined studies focused on how mobile phones can be used to CA users to an external system or network [70, 99]. Both the surveys carried out by Mahfouz et al. and Spolaor et al. [70, 99] focused on synthesising studies that examined biometric authentication methods via smartphones. Across both groups of studies, there was a consensus on the challenges of carrying out CA through mobile devices. The first is that biometric features - both physiological and behavioural can change over time for any individual and that mobile devices do not have the necessary mechanisms to capture and monitor these changes over time [99]. The second is that there is no consensus over the *combination* of biometric features that needs to be collected to ensure the highest level of security and accuracy. Third, the review studies identified that there is no consensus on standards and protocols to sufficiently benchmark, test and evaluate mobile devices and the various CA methods that can be applied. The final challenge identified is that there is a lack of understanding on the optimal balance between usability and privacy when it comes to CA through mobile devices.

Irrespective of application type, there are some common research challenges that must be overcome for mobile devices to be effectively and efficiently utilised for CA purposes. Ellavarason et al. [39] provides a clear synthesis of these challenges through their survey study which is based on (1) Consideration of the frequency, rate and range of data collection and the variance it causes in CA; (2) Consideration of the users psychological factors especially when it comes to collection of physiological biometric traits; (3) Addressing privacy issues and concerns through the development of newer privacy enhancing technologies; (4) Establishment of a standard protocol to benchmark data acquisition via mobile devices. The authors suggest that, for example, developing metrics to measure data quality using swipe and keystroke dynamics can be a valuable contribution; and (5) Explore adoption and acceptance factors across multiple user groups.

2.1.3 Sensors. [1, 54]

Abuhamad et al. [1] and Hernandez et al. [54] examined the literature on how various sensors embedded across different devices can be utilised for CA purposes. There is a consensus within this research realm that as the number and sophistication of sensory modules such as motion sensors (e.g., gravity, accelerometer, gyroscope, and magnetometer), environmental sensors (e.g., light, temperature, barometer, and proximity), and position sensors (e.g., GPS and compass) within a device improves, it enables far more accurate and secure authentication as the quality and quantity of information provided is enhanced.

Furthermore, these sensors can also be used to capture both physiological and behavioural biometric data as well as improving feature robustness and system effectiveness [1]. Using sensory data, a background process continuously and implicitly captures not only a single user's behaviour to perform an active and transparent authentication, but has the capacity to work as identifiers which can authenticate a large set of authorised users as well [51, 69].

Studies examined by Hernandez et al. [54] suggest that there are two primary methods for obtaining CA features. **Raw features** are directly obtained from a particular device, e.g., sensor, mobile device, and so on. This information is directly used in the authentication process and typically include body related, motion sensors, environmental sensors, position sensors, and mobile device platform information. **Derived features** are produced after some kind of processing of raw features. Typical examples include gait, position in the seat, biometric trait, touch dynamics, location, text properties and contextual features.

A review of the literature however suggests that certain limitations remain within sensors as they operate at the lowest level of systems architecture, and therefore heavily rely upon the collection and processing of raw data. The synthesis of studies conducted by Hernandez et al. [54] identified that particular types of sensors such as accelerometers and gyroscopes were prone to data injection attacks that can result in manipulation of data. In addition to these adversarial attacks, [1] also highlighted the challenges pertaining to *background noise* and the *computation and memory overhead* associated with utilising sensor based CA.

2.2 Continuous Authentication Techniques

CA is dependent not only on the device used, but also the technique it utilises. CA techniques can be largely categorised into those which utilise biometric techniques and those that do not [15]. Within biometric methods, these are further sub-categorised into behavioural or physiological as per fig. 2. The literature also suggests the emergence of another category as well: multi-modal which refers to when two or more biometric techniques are used in conjunction.

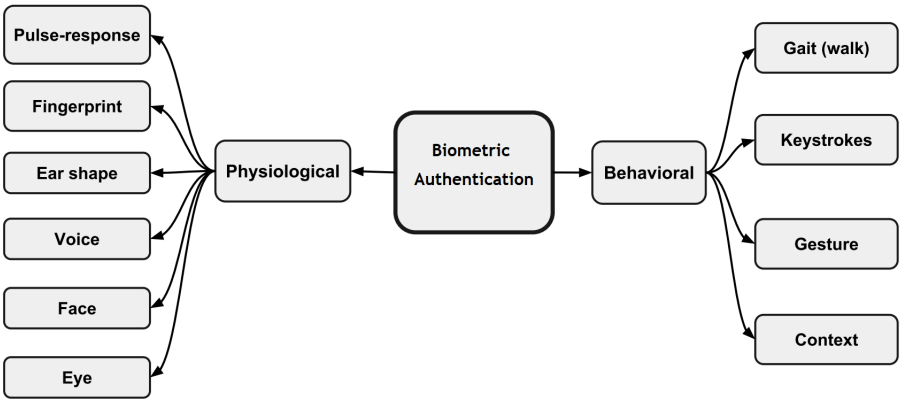

Fig. 2. Physiological vs. Behavioural Authentication [99]

2.2.1 *Biometric.*

Biometric based authentication identifies a person and verifies their authenticity automatically based upon the measurement of a persons characteristics (fig. 2) [21]. As per Oak [84], for a parameter to be called a biometric identifier, it must satisfy the following properties:

(1) Universality: Every person must posses that particular characteristic. (e.g. DNA vs. Birthmarks etc.)
(2) Uniqueness: The characteristics must be different from person to person. (e.g. fingerprint vs. blood type etc.)
(3) Permanence: The characteristic must not disappear nor change drastically over time. (e.g. retina scan vs. hormonal levels etc.)
(4) Collectability: The characteristic must be obtainable in a fast and accurate manner through a feasible method. (e.g. voice vs. 'self-confidence' levels etc.)
(5) Circumvention: The parameter must be difficult to replicate or forge.

There are two types of biometric features that can be processed. Physiological biometrics are biological and/or chemical traits that are innate or naturally grown (e.g. facial structure; palm and

fingerprint and iris etc.) while behavioral biometrics are mannerisms or traits that are learned or acquired (e.g. voice; handwriting style, mouse and keyboard interaction etc.) [62].

Biometric based authentication protocols can be logically divided into two distinct phases. The first is the **enrollment phase** where the data pertaining to the user is acquired, processed and stored in a database repository for future reference. The second is the actual **authentication phase**, where the users biometric features are acquired and matched once again with the data captured and stored during the enrollment phase [62]. In the context of CA, the literature primarily focuses on the second phase (authentication), and how to address the significant difficulties and challenges pertaining to *actively* and *seamlessly* capturing different forms of biometric data to continuously authenticate the user.

Next, we examine the current literature on behavioural, physiological and multi-modal biometrics for CA purposes in further detail.

2.2.2 *Behavioural.* [1, 37, 39, 69, 70, 84, 89, 91, 101, 110, 114]

Behavioral biometrics are built based on an individual's behavioral characteristic such as how they type, walk or behave in a certain context [70, 84]. Although a variety of different methods for behavioural biometrics exist as per fig. 2, Oak [84] systematically classified them into five primary categories as per table 2 below.

Type	Description
Authorship based	It is based on the analysis of a work produced by the user. The system identifies styles and characteristics particular to a user as he writes/ draws and verification is done based on the matches of these characteristics.
HCI Based	Based on constructing a user identity based on traits and mannerisms exhibited by the user while interacting with devices and systems via mouse movements or touchscreen strokes.
Indirect HCI	Compiles data based on low-level data (e.g. system call traces, audit logs, execution traces, call stack analysis etc.) left behind by a user based on normal HCI actions.
Motor-Skills Based	Identifies a user based on a combination of their muscle, bone and nervous system movements and actions.
Purely Behavioural	Quantifies a users ability to strategise, innovate, critically and creatively think when performing certain actions and tasks.

Table 2. Behavioural Biometric Subtypes [84]

In addition to these classifications, a number of methods for sensing behavioural biometrics for CA have been explored. Liang et al. [69] conducted a comprehensive comparison based on vulnerability; discreteness, obtrusiveness and privacy features for each category of behavioural biometric. For instance, keystroke dynamics which is captured through signals produced via typing is considered to be secure and private but lack discreteness and obtrusiveness [107]. Another example is body gestures collected through mouse and/or head movement signals which they considered to be private, but fell short on the security, discreteness and obtrusiveness categories.

Gonzalez et al. [51] in their systematic review noted that the application of such biometric techniques are often utilised via software products, as opposed to hardware solutions. Furthermore, they also identified that behavioural biometrics dominated the marketplace when it came to CA. Interestingly, they suggest that there is a keen focus on biosignals and touch features in both market and academia, resulting in an alignment and rare symbiosis between the two areas. However, they highlight how this connection is yet to be leveraged, presumably due to the lack of standards, best practices and common ground pertaining to the behavioural biometric CA technologies being explored.

Stylios et al. [101] also carried out a systematic literature review on CA using behavioural biometrics, and highlighted some of its advantages and shortcomings. Firstly, they state that there

is strong evidence to support the fact that the behavior of each user can be profiled on the basis of their application usage patterns with high levels of accuracy. They state that users may be differentiated based on not only the type and frequency of applications they use, but also how they interact (e.g. store data; make calls; swipe across the UI etc.) with the device as well. On the other hand, they also highlight that there are a lack of practical application of CA schemes, primarily due to the highly intrusive nature of the data that must be collected (e.g. voice and text; geolocation; website cookies etc.) and the risk of false positives/ false negatives.

2.2.3 Physiological. [34, 76, 92]

Physiological biometrics utilises parts of the human body such as the iris and fingerprint for scanning, recognition of facial patterns, examining hand geometry, vein checking and facial thermogram [15].

In Dahia et al. [34], their study provides an overview of different physiological methods for CA. In regard to fingerprints and facial recognition, they state that as the cost of these sensors become cheaper, it has enabled these sensors to be embedded across a wide range of daily devices such as smartphones, laptops and mice. In regard to fingerprints, they state the point that the technique has largely been neglected over the past decade (unless it is combined with other forms of biometric authentication measures), due to the fact that there still remains an undesirable amount of user cooperation required. For instance, one of the studies quoted suggest that CA systems require an average of 8.68 fingerprint sample requests per hour (one request every 7 minutes) to be effective [16]. Regarding facial recognition, they highlight the fact that faces constantly change over time due to aging; facial hair modification and/or makeup or facial accessories and is also prone to error rates associated with lighting and facial expression variations and poses that may alter the data captured through these devices. Therefore, Dahia et al. [34] argues that these physiological biometric methods may only be feasible in certain circumstances and/or environments.

In Mosenia et al. [76], their study focused on reviewing the literature on the main factors that impact the error rates associated with physiological / biomedical traits. Their study reveals that Electrocardigram (ECG) and electronencephalogram (EEG) monitors have shown promising results for regular authentication systems, but have significant limitations when it comes to CA due to two primary reasons. First, they argue that the literature suggests that the requirements of the sensors that capture EEG/ECG signals significantly limit their applicability, and second suggest that results from studies have determined that the processing of EEG/ECG signals for authentication is resource-hungry. As such, they describe several research directions that future studies should facilitate in regard to designing and developing CA systems based on physiological biometric traits as follows.:

(1) The need for low power sensors to ensure that energy consumption is optimised;
(2) The consideration of minimising the invasive capture methods associated with certain technologies;
(3) Ensuring that the pervasive use of biomedical traits do not lead to privacy and security threats;
(4) Mitigating the issues surrounding calibration and noise cancellation;
(5) The need for these devices to process a larger capacity of data through new hardware architectures or more efficient software platforms;
(6) The need to explore how the data collected can be stored and processed through cloud computing.

2.2.4 Multimodal. [5, 85]

Multimodal biometrics uses information from two or more biometrics whereas uni-modal biometric uses information from one biometric. Multimodal biometrics is more advantageous than uni-modal. The advantages of the multimodal biometric system include accuracy, liveness detection, security, universality and cost-effectiveness. Multimodal biometrics is a fusion of uni-modal biometrics designed to overcome the problem of uni-modality such as noisy data, spoofing, non-universality and inter-class similarities [15]. Mahfouz et al. [70] suggests that fusing different behavioral biometric traits can improve the authentication accuracy and address some limitations and problems.

A synthesis of the literature presents different scenarios where biometric techniques for CA purposes can be fused together. This may be done at a Sensory Level which combines raw data captured from different sensors for the same biometric trait. Feature Levels combine different feature vectors extracted from a number of biometric modularities into one new feature vector. Next are Score Levels which matches scores of each authentication modality, and then applies the combination for authentication purposes. Finally it can also be done at a Decision level which comprises of decisions multiple classifiers to make the final decision [70]. Irrespective of the techniques that are fused together, Al Abdulwahid et al. [5] suggested that to ensure successful implementation of CA, the following characteristics must be addressed:

(1) Ensure a high level of transparency is maintained;
(2) Leverage existing devices without requiring additional devices;
(3) Incorporate a variety of different biometric techniques;
(4) Ensure that CA measures for each identity is managed;
(5) Function with minimal processing overhead;
(6) Provide a system architecture which is compatible and sound;
(7) Implement and evaluate through real and live data;
(8) Ensure that a trial with sufficient number of users is conducted;
(9) Cover issues pertaining to trust, privacy and management;

Crawford et al. [32] demonstrated that behavioral biometrics reduced the need for re-authentication by 67% in comparison to knowledge-based methods, i.e., adding a remarkable improvement in usability. In terms of exploiting access privilege, the authors showed that an intruder could perform more than 1,000 tasks on successfully gaining access to a mobile device using a knowledge based authentication scheme; however, the intruder can hardly achieve one task if the mobile device uses a multimodal behavioral biometrics-based method [69].

2.2.5 Non-Biometric. [6]

From the 24 literature survey papers identified as per table 1, a single paper focused on synthesising the literature on utilising Blockchain for CA purposes [6]. Through a comprehensive literature review, they identified several studies that have explored how Blockchain is a feasible solution when it comes to CA due to its decentralised, autonomous and trustless characteristics. In addition, studies examined argue that performance wise, Blockchain is able to provide significant improvements in accuracy over preexisting solutions, with certain studies such as Agrawal et al. /cite8462513 suggesting that they were able to reach 99.30% accuracy despite being in its initial preliminary stages. Furthermore, research on this subject argue that the distributed nature of Blockchain makes the system more robust and immune to single point of failure [6].

However, certain limitations are also highlighted where Blockchain technology for CA purposes in Al-Naji et al. [6] as well. The most critical is the continuous power drain that Blockchain technologies will create on IoT devices due to the need for signals and data to be continuously sent and received from devices. As such, one of the recommendations made is that further research is required on technology that can operate on low power consumption such as Bluetooth Low

Energy (BLE) or Zigbee that is a technology to be battery friendly and little energy to operate on Wi-fi without compromising performance. In addition, they recommend that methods for a single consensus algorithm (PoW) be explored outside of the Blockchain technology which will enable that the transaction be validated through external devices (such as IoT) without compromising privacy, cost or reserach overhead.

3 RESEARCH METHODOLOGY

For the purpose of this study, we developed a network of citations based on the literature survey papers (table 1) to cover the substantial body of research on CA that exists. This was deemed necessary as it was difficult to get a broad overview of the *main* topics pertaining to CA or the current trends emerging from this field or research due to the silo-ed and fragmented nature of CA. Below, we explain the methodology used to develop our citation network, and subsequent analysis procedures of this network.

3.1 Research Method

For the purpose of this paper, we use a network of citations of past articles covering CA as the unit of analysis for our literature review.

A citation can be defined as a connection between existing and new knowledge and is used as an indicator for how the research has progressed over time [111]. A citation network is a special form of a social network with journals, articles, and authors acting as nodes and citations representing the connections (edges) between these nodes [88]. Past research on CNA mostly addressed the importance of specific scientific journals, but CNA is also a valid research method for journal-focused investigations, enabling an in-depth analysis of the concepts and developments in a defined area of research in an objective and unbiased way [88].

The usage of CNA for literature reviews is already an established research approach, and there are a plethora of literature past and present that have yielded useful results from this approach [93**?**]. As the primary aim of this study is to examine how research on CA is currently established and growing as a disciplinary area, we apply SNA methodologies which enables us to identify and group the connection between the nodes and the scientific boundaries established within CA [71]. Building upon these former studies, we performed an in-depth literature review on CA *modes* consisting of over 2300 articles [59], which is by far the largest accumulation and dissemination of knowledge on CA to date.

3.2 Research Design and Data Collection

To establish a concrete boundary of the review, this study adhered to a systematic literature review process as follows.:

(1) Identify key literature survey papers on CA.
(2) Derive list of all references from table 1.
(3) Identify most cited papers in CA from reference list.
(4) Create Citation Graph based on papers identified in item 3.
(5) Conduct Citation Network Analysis on graph.

item 1 was carried out as detailed in Section 2 of this paper, which resulted in the 24 papers selected for the purpose of this study as per table 1. For item 2, we collated the entire list of references derived from these 24 studies, and then cross-compared them to remove any duplicates. As such, a substantial number of studies from the outside of these 24 papers has been included in our analysis. A total of 2322 studies were identified from this process. To address item 3, we determined the most influential papers from these studies by filtering only sources which were cited by 3 or

more of the survey papers listed in table 1. This process identified 29 papers as per section 6.2. We then obtained a list of all studies that have cited the list of core papers from section 6.2 that resulted in a total of 1789 papers[1]. For item 4, VOSviewer - a software tool for creating maps to visualise and explore network data was utilised to build a network based on citation relations obtained as per item 3 [106]. This data was then exported to Gephi, a software platform that enables visualisation, exploration of graphs and networks that was used to build the citation graph as per fig. 3 [19]. This graph was created through applying community detection algorithms to understand the nature of relationship between the citations in Gephi. A detailed analysis of the techniques and analysis methods to address item 5 are presented in the next subsection.

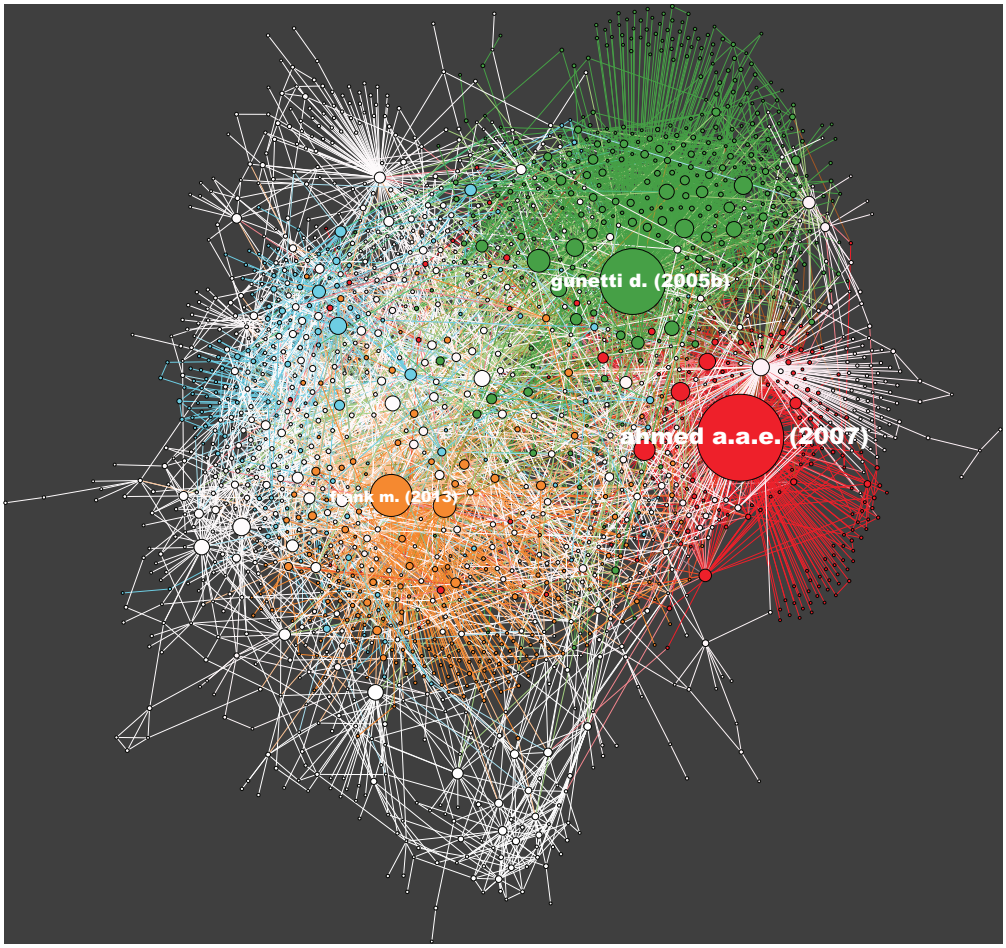

Fig. 3. Citation Graph with all Edges

3.3 Data Analysis

Visual representation of the nodes and edges of the citation graph plays an important role for interpreting the major trends and topics in the CA literature. Below, we describe the techniques and tools utilised to ensure that the visual graphs produced via Gephi can assist with the CNA [30].

[1]For the complete list of the papers see [59]

3.3.1 Node Diameter.
Node diameter refers to the size of each node based on the incoming citation numbers. For the purpose of our study, we determine the node diameter based on the inward links amongst the citation nodes, also known as in-degree. This is because they are the most common means to graph the influence of each paper, and provides a simple way to visualise this information [27].

From our data analysis, the **Average in-degree** for our graph is 2.45. This implies that the average number of inward citations per node is approx. 2.5 per study. For comparison purposes, the largest node which is represented by Ahmed & Traore [4] has an in-degree value of 46.

3.3.2 Spatialisation and Colour Clusters.
Both spatialisation and colour clustering techniques rely upon the concept of '*modularity*'. Modularity in networks and graphs can be used to measure the strength of division of a network into modules (also called groups, clusters or communities). Networks with high modularity have dense connections between the nodes within modules (groups) but sparse connections between nodes in different modules. Due to this quality, modularity is often used in optimization methods for detecting community structure in networks. The difference however is that modularity can be expressed either by the location and distance between nodes (spatialisation) which is used to build a Cartesian map of the nodes, whilst specific colour clusters enables the grouping of similar research papers. Further details pertaining to both Spatialisation and Colour Clustering via Gephi is provided in Appendix 6.2.

Spatialization The aim of the spatialization process is to transform the citation network into a map.For this process, we utilised `ForceAtlas2` - a force-directed layout that is close to other algorithms used for network spatialization through Gephi. `ForceAtlas2` simulates a physical system in order to spatialize a network. Nodes repulse each other like charged particles, while edges attract their nodes, like springs. As a result, structural proximities of the graph are turned into visual proximities which is helpful in the analysis of social networks. One of the advantages of visualization using `ForceAtlas2` is that it provides "live" spatialization: when the algorithm is initiated the layout changes in time and user decides on when to stop it. Although Gephi allow to adjust parameters of `ForceAtlas2`, we used standard mode (e.g. $(1, -1)$) for the purpose of our study. To improve the spatialization performances on big graphs (such as ours) `ForceAtlas2` is equipped with *approximate repulsion* force-calculation algorithm [18]. This parameter was enabled for the analysis.

Color-clustering Gephi supports simple heuristic method that was first described in [22]. It is based on modularity optimization allowing to extract the community structure of large networks. Gephi implementation of color-clustering based on modularity is a slight modification of the original method in Blondel et al. [22]. The settings allow a user to change 'resolution' parameter that was described in Lambiotte et al. [66]. This parameter allows to control the number of resulting communities: values that are lower than 1 produce smaller communities, values that are larger than 1 produce larger communities. For our analysis we used default value of 1.

3.3.3 Nodes and Edges.
The edges for the citation graph where defined by VOSviewer in a trivial manner: they are based on the citation data collected from the Scopus. In contrast, the size of the nodes is specified by us based on the in-degree for each node. This size also affects the spatialization of the graph since non-overlapping option was enabled by us. Gephi allows to define node diameter as a non-linear function of in-degree. For example, in our case the node diameter is defined using cubic splines.

3.4 Core Analysis (k-value)

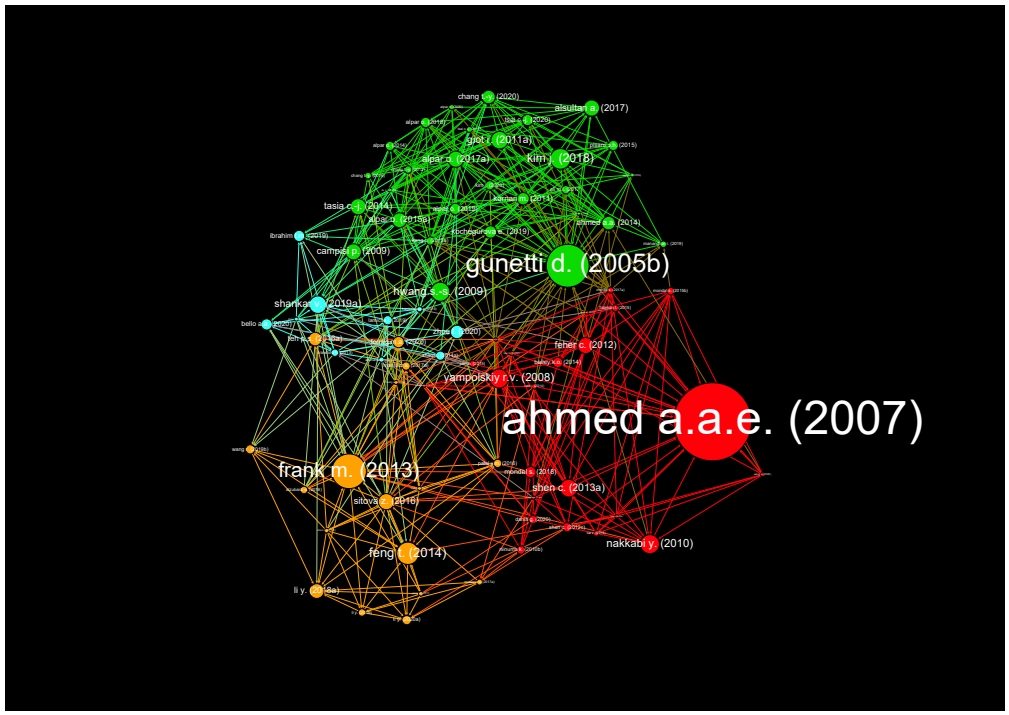

Fig. 4. Citation Graph based on Core Nodes with k-value > 8

Coreness is a measure that can help identify tightly interlinked groups within a network. A k-core is a maximal group of entities, all of which are connected to at least k other entities in the group. There is a recursive procedure to obtain k-core graph: all the nodes of degree smaller than k should be recursively removed, until the degree of all remaining vertices is equal or larger than k.

k-core decomposition has found a number of applications. For instance, it has been extensively used for social network analysis, visualization of complex graphs, to analyze the static structure of large-scale software systems, etc.. Further information on the topic, covering the main concepts, important algorithmic techniques as well as some application domains, may be found in Montresor et al. and Tixier et al. [75, 104].

Due to substantial number of nodes and edges in the citation graph (fig. 3) of this study the boundaries of the communities that are identifiable on fig. 3 are unclear. This is because there exist misalignment between the results of spatialization and color-clustering. To ensure that only the primary communities are clearly identified and to improve the interconnectdness of the nodes, k-core 8 with in-degree values of above 10 were applied to filter the citation graph that resulted in four primary colour clusters (Green; Red; Orange and Light Blue) containing a total of 38 nodes as per fig. 4.

4 RESULTS

Based on the colour-clustering of the 38 nodes, we conducted a detail analysis of the content [58]. This content analysis enabled us to not only determine the central research areas based on the four colour clusters as per fig. 4, but also enabled us to synthesize key details from each bide in

regard to the following attributes: Weighed-in-Degree (WiD), device type; technique, accuracy and summary. As such, we combined details pertaining to device and technique for CA (described in Section 2) with the influence that the publication analyzing this technique has in academic domain (e.g. importance as per CNA). This allows us to foresee on which areas of CA will be prioritized by academics in the nearest future and why.

Accuracy rates for corresponding CA techniques described in the papers were included because they were identified as a key subject matter across the majority of core nodes examined. Gonzalez et al. and Oak [51, 84] suggests that there is a consensus on measurements between authors when it comes to evaluation metrics, with the defacto standard being the Equal Error Rate (EER) which reflects the error rate at a threshold setting where the False Accept Rate (FAR), False Reject Rate (FRR) are equal. Therefore, we extract the EER, FAR and FRR rates from our core nodes (if applicable) to ensure comparison of the performance of the various CA systems that are covered.

Below, we present the results from our CNA analysis categorised based on the main colour clusters.

4.1 Main CA Concepts

Based on our analysis, we identified three large clusters (Green; Red; Orange), which represent the main CA research areas. Below, we examine the nodes pertaining to each cluster in detail, to determine the established research agendas within CA.

4.1.1 Green Cluster: Keystroke Dynamics. [2]

Of the 38 citation nodes 18 were part of the green cluster area as per fig. 4. Based on our content analysis as per table 3, we were able to determine that papers within this cluster are primarily focused on ***Keystroke Dynamics based Continuous Authentication (KDCA)*** - a form of behaviour biometric authentication based on comparing five feature extraction pattern analysis of how users press and release keys when interacting with devices. Authors point out the simplicity and accuracy of CA through keystroke dynamics, resulting in shorter training times and the ability to operate when there are limited resources available [29]. A closer examination of the green cluster nodes identified several important points pertaining to KDCA which are highlighted and synthesised as follows.

Firstly, studies which examined KDCA could be categorised based on whether it focused on *free-text* or *fixed-text* based methods. The majority of early research into keystroke dynamics was primarily focused on how users would enter fixed texts (e.g. usernames and passwords etc.) in both the enrollment and authentication phases. For instance, studies such as Campisi et al. [25] based their study on analysing keystroke analysis based on fixed alphabetic strings on a mobile phone keypad. Proponents of fixed-text KDCA argue that the relative simplicity and high levels of accuracy are its greatest strengths along with its ability to authenticate users based on shorter-text lengths.

On the other hand, the majority of nodes identified in table 3 based their study on the *free-text* analysis of keystroke dynamics [4, 13, 29, 53, 63, 65, 105]. Free-text KDCA focuses on profiling and authenticating a user based on the keystroke patterns that resonate with little to no restrictions over what or how they type [65]. Proponents of free-text based KDCA argue that the profiling phase of users becomes much easier when authenticating users based on the freedom for users to formulate their own keystroke input structure. Furthermore, they also argue that accuracy levels pertaining to authentication is improved as well, with Gunetti et al. [53] suggesting their KDCA of free text resulted in a False Alarm Rate (FAR) of less than 5%, and an Impostor Pass Rate (IPR) of less than 0.005%. Studies do however highlight that although users have the freedom to enter

[2]For the full summary of the papers in the clusters see [60]

Author	Year	WiD	Device	Technique	Accuracy	Summary
Gunetti & Picardi [53]	2005	36	Generic	Keystroke	FAR 5%	Present a method to compare typing samples of free text that can be used to verify personal identity. The authors demonstrate that even few lines of text collected in different working sessions may be sufficient to reach a high level of accuracy.
Hwang et al. [94]	2009	24	Mobile	Keystroke	EER 4%	Explore the effectiveness of user authentication using keystroke dynamics-based authentication on mobile devices.
Kim et al. [64]	2018	22	Generic	Keystroke	EER 0.44%	Explore new keystroke dynamics-based authentication (KDA) based on adaptive feature extraction as well as machine learning techniques.
Tasia et al. [102]	2014	20	Mobile	Generic	EER 14.1-62.8%	Developing computation efficient statistical classifier for low-power mobile devices to authenticate users.
Giot et al. [50]	2011	19	Generic	Keystroke	EER 15.28%	Propose a new method based on the Support Vector Machine (SVM) learning.
Campisi et al. [25]	2009	19	Mobile	Keystroke	EER 13%	Propose authentication using keystroke dynamics acquired during the process of typing fixed alphabetic strings on a mobile phone keypad.
Alsultan et al. [13]	2017	16	Generic	Keystroke	FAR 0.011%, FRR 0.28%	Use non-conventional keystroke (free text) features for user authentication based on word-per minute; up-down and negative up-down characteristics.
Karnan et al. [62]	2011	15	Generic	Keystroke	-	Review various features and feature extraction methods in keystroke. Special attention is paid to classification methods.
Chang et al. [29]	2020	14	Generic	Keystroke	EER 13.2%	Propose new soft biometrics and a new classifier for free text authentication in English.
Alpar [11]	2017	14	Generic	Keystroke	EER 4.1%	Proposes a new keystroke authentication concept: to extract frequency features and to conduct classification in frequency domain.
Alpar [10]	2015	13	Generic	Touch	EER 2.5%	Improves security of pattern password authentication using touching duration as biometric traits.
Ahmed & Traore [3]	2014	12	Generic	Keystroke	EER 2.13-2.46%	Present a new approach for the free text analysis of keystrokes. It combines monograph and digraph analysis, and uses a neural network to predict missing digraphs based on the relation between the monitored keystrokes.
Chang et al. [28]	2012	11	Mobile	Keystroke	EER 6.9-12.2%	Propose a new graphical-based password KDA system for touch screen handheld mobile devices. The paper explores a pressure feature, which is convenient for touch screen handheld mobile devices.
Tsai & Huang [105]	2020	11	Generic	Keystroke	EER 10.4%	Employ keystroke dynamics to detect predetermined, fraudulent instant messages.
Alpar [12]	2019	11	Generic	Multi-modal	EER 1.4-3.21%	Develop a novel frequency-based authentication system - TAPSTROKE, as a prospective protocol for small touchscreens and an alternative authentication methodology for existing devices utilising touch and keystroke analysis.
Kochegurova et al. [65]	2019	11	Generic	Keystroke	FAR 0%, FRR 2.4%	Perform user authentication based on hidden monitoring of keystroke dynamics during typing of a free text (Russian and English).
Ali et al. [8]	2017	10	Generic	Keystroke	-	Survey the most recent research on keystroke dynamic authentication. This includes methods and algorithms used by researchers, the accuracy rate, and the limitations.
Kim & Kang [63]	2020	10	Mobile	Keystroke	EER 0.1%	Propose a novel freely typed text-based KDA method for mobile devices by collected data from three different smartphone sensors while typing in two languages (English and Korean).

Table 3. Green Cluster: Keystroke Dynamics based CA

whatever they wish for authentication purposes, a minimum amount of text is still needed in order to make the analysis of the keystroke to be meaningful.

Secondly, there was also a difference in the device used to capture the keystroke analysis - whether through a physical hardware device (i.e. keyboard), or a virtual touch screen (i.e. virtual keyboard). Studies such as the one by Kim et al. [64] based their new KDCA on extracting features from an interchangeable set of user-dependent keystroke features by considering the typing speeds of two consecutive keys (digraphs) on a physical keyboard. On the other hand, a separate study by Kim & Kang [63] proposes KDCA methods for mobile devices based on the feature extraction of users typing in two separate languages (English and Korean) via a virtual keyboard on a mobile phone. Both studies present very high accuracy evaluation scores, with the KDCA based on physical hardware measured at EER 0.44%, and results for the virtual keyboard measured at EER 0.1%. These

studies do acknowledge the need for a cross comparison between the different input devices used for KDCA, along with tests that consider a wide variety of different languages as well [64].

One final noteworthy point on KDCA is the varying rates of accuracy - ranging from 0.1% [63] to up to 62.8% [102]. Furthermore, several studies also provide their EER rates based on range values [4, 102]. which may raise questions around why such variance exists. The primary reason why this variance exists is due to the fact that the accuracy rate of KDCA depends on a number of details. This includes: (a) the number of participants and impostors; (b) whether the text is arbitrary or pre-defined; (c) the length of the text; (d) the input device (or the type of the keyboard); (e) features extracted from the input data; (f) pre-processing and filtering techniques; (g) classification method and number of classes; (h) how training and testing samples are defined.

4.1.2 Red Cluster: Mouse Movements.

Indicated by the red cluster area in fig. 4, 7 out of the 38 core citation nodes (table 4) were identified as studies focusing on ***Mouse Movement based Continuous Authentication (MMCA)***. Similar to KDCA, MMCA also works by extracting behavioural biometric but instead of keystrokes, it extracts its features based on patterns such as how users move their mouse; drag-and drop items; or point and click etc. using their peripheral device [4].

Author	Year	WiD	Device	Technique	Accuracy	Summary
Ahmed & Traore [4]	2007	46	Generic	Mouse	FAR 2.46%, FRR 2.46%	Introduce a new form of behavioral biometrics based on mouse dynamics based on data processed and detected using artificial neural networks. The authors describe architecture and implementation for the detector: it covers all the relevant phases of the biometric data. Conducted by the authors experiments demonstrate improved accuracy of the proposed detection technique.
Nakkabi et al. [78]	2010	21	Generic	Mouse	FAR 0%, FRR 0.36%	Propose a mouse dynamics biometric recognition system which improves performance by developing separate models for separate feature groups involved.
Feher et al. [41]	2012	20	Generic	Mouse	EER 10%	Introduce a novel method that continuously verifies users according to characteristics of their interaction with the mouse.
Shen et al. [96]	2013	19	Generic	Mouse	FAR 0.87-8.74%, FRR 0.69-7.69%	Present a simple and efficient user authentication approach based on a fixed mouse-operation task.
Yampolskiy & Venu [110]	2008	17	Generic	Mouse	-	A survey which defines the behavioural biometrics as a domain where features of interest include skills, style, preference, knowledge, motor-skills or strategy used by people while accomplishing different everyday tasks.
Bailey et al. [17]	2014	12	Generic	Multi-Modal	FAR 2.10%, FRR 2.24%	Present a behavioural biometric system that fuses user data from key-board, mouse, and Graphical User Interface (GUI) interactions.
Mondal & Bours [74]	2018	10	Mobile	Swipe	FAR 0%, FRR 0%	Introduce the concept of adversary Continuous Identification (CI) which follows Continuous Authentication (CA) by examining swipe gesture data from mobile devices.

Table 4. Red Cluster: Mouse Movement Based CA

A more detailed examination of the nodes on MMCA revealed several improvements to the feature extraction technique since first introduced by Ahmed & Traore [4]. In Nakkabi et al. [78], they introduce additional feature extraction factors such as Movement Speed compared to travelled Distance (MSD), Movement Direction Histogram (MDH), average Movement speed per Movement Direction (MDA), Average movement speed per Type of Action (ATA), Action Type Histogram (ATH), Travelled Distance Histogram (TDH), Movement elapsed Time Histogram (MTH).

Shen et al. [96] takes this one step further by differentiating features from mouse movement by traditional holistic features (mouse-click; movement offset and elapsed time etc.) with procedural features such as speed curve against time, acceleration curve against time etc. Data collected via these features are then classified utilising multiple techniques resulting in not only a reduction of error rates (FAR 0.87%, FRR 0.69%), but also a drastic improvement of the time associated with data collection (e.g. 11.8 seconds for up to 800 operations extracted).

More recent nodes from this cluster group such as Mondal & Bours [74] have started to apply the feature extraction details from MMCA to *swipe gestures* associated with interactions with a mobile device for authentication purposes. For example, among other features extracted by the authors are: Action duration, Begin X, Begin Y, End X, End Y, Distance end-To-end, Movement variability, Orientation and Direction. In their study, they applied three different verification processes and all different combinations of the settings with two separate sets of data to analyse the efficacy of swipe gesture based data for CA purposes.

4.1.3 Orange Cluster: Mobile Device Touch Interface.

6 out of the 38 core nodes were identified to reside in the orange cluster as per fig. 4. An in-depth investigation into these studies which is summarised in (table 5 identified that the majority of these nodes focused on ***Continuous Authentication through Mobile Device's Touch Interface (MDTI)***. These studies primarily focused on investigating novel methods to continuously authenticate users based on how they interact with the touchscreen of a smart phone.

Author	Year	WiD	Device	Technique	Accuracy	Summary
Frank et al. [46]	2013	35	Mobile	Touch	EER 0-4%	Investigate ways to continuously authenticate users based on 30 behavioural touch features (e.g. timing; pressure; area etc. a user may take through the touchscreen of a smart phone. This information was extracted by the authors from the raw touchscreen logs: it demonstrates that different users populate distinct sub-spaces of this feature space. The logs reflect information about basic navigation maneuvers performed by the smartphone users. The authors proposed a classification framework that learns these maneuvers during an enrolment phase.
Feng et al. [43]	2014	20	Generic	Touch	TPR 91%, TNR 93%	Develop Touch based Identity Protection Service (TIPS) that implicitly and unobtrusively authenticates users in the background by continuously analyzing touch screen gestures in the context of a running application
Sitova et al. [98]	2016	15	Mobile	Multi-modal	EER 7.16-10.05%	Introduce a multi-modal behavioural authentication system utilising hand movement, orientation and grasp (HMOG) for mobile phone users.
Teh et al. [103]	2016	14	Mobile	Touch	-	Conducts a survey on touch dynamics authentication in mobile devices to provide some insights and comparative analysis of the current state of the art in the topic area, including data acquisition protocols, feature data representations, decision making techniques, as well as experimental settings and evaluations.
Li et al. [68]	2018	13	Mobile	Generic	EER 3.0%	Propose a novel sensor-based continuous authentication system (SensorSA) by leveraging the accelerometer, gyroscope, and magnetometer built in smartphones to monitor a user's behavioural biometric patterns.
Ferrag et al. [45]	2020	10	Mobile	Generic	-	Presents a comprehensive investigation of authentication schemes for smart mobile devices based on a survey. Their study indicates that CA measures must be incorporated for mobile devices to ensure full protection against these threats. In their study, threat models are synthesised into five categories, and the countermeasures to these threats are classified into four distinct methods.

Table 5. Orange Cluster: Mobile Device Touch Interface Nodes on CA

In Frank et al. [46], they initially propose a set of 30 behavioural touch features that can be extracted from raw touchscreen logs and demonstrate that different users populate distinct subspaces of this feature space. The authors collected touch data from users interacting with a smart phone using basic navigation actions. For this, the authors focus on single-touch gestures. They also distinguish vertical strokes from horizontal strokes due to the ease of comparison of the strokes within each trigger action than across different trigger actions. In addition to these initial features, Feng et al. [43] also introduces two new sets of behavioural and contextual features to improve performance under uncontrolled environments. The first are additional biometric features - swipe/zoom speed, click gap, contact size etc.), along with a second set of behaviour features - touch location, swipe/zoom length, swipe/zoom curvature.

Although many of the studies in this cluster space highlight the benefits of MDTI due to its ubiquitous nature, a number of studies highlight the difficulties balancing the accuracy rates

vs. ensuring that the practicality of MDTI is not compromised. The study by Feng et al. [43] acknowledged the fact that a larger authentication length is required to guarantee higher levels of accuracy, but also result in longer delays. For example, when the authentication length is 8, the true positive and true negative already exceeds 90%. This explains why the authentication length is set to 8 in on-device testing. In Teh et al. [103], they identify several limitations of MDTI for CA purposes due to the complexity of training the classifier to differentiate between the owner of the device; a authorised 'guest' vs. an impersonator. Due to these difficulties, researchers within this space observe that MDTI should not be aimed at replacing explicit authentication mechanisms, but rather as a multi-factor authentication method which complements other approaches until future studies are able to address the limitations identified as per above [43, 103].

4.2 Emerging Trends in CA

In addition to the three key research areas as per identified in Section 4.1, the CNA also identified emerging research areas within CA based on their position and citation path analysis. These papers are indicated by the light blue cluster in fig. 4, and is positioned in a way that it demonstrates convergence between the three dominant research topics represented by the green, red and orange clusters respectively. Based on table 6, we can see a clear differentiation from the three node clusters when it comes to the primary device and technique examined for CA purposes.

Author	Year	WiD	Device	Technique	Accuracy	Summary
Shankar & Singh [95]	2019	15	Mobile	Multi-modal	EER 0.03-0.05%	Present a method to continuously authenticate users on mobile devices through data collected via multiple sensors (e.g. gyroscope and accelerometers etc.) which are then used to determine Gait and idle sitting positions of a user.
Zhao et al. [113]	2014	12	Mobile	Touch	EER 4.1-9.6%	Propose the application of a statistical touch dynamics image trained from graphical touch gesture features of users.
Zhou et al. [115]	2017	12	IoT	Brainwaves	FRR 4.71%	Propose a novel CA system using biometric data extracted from brainwave signals from devices located on IoT based networks.
Lamiche et al. [67]	2019	10	Mobile	Multi-modal	EER 1%	Examine the usage of gait patterns and keystroke dynamics to develop a new multimodal CA system.
Ibrahim & Sellahewa [56]	2019	10	Mobile	Multi-modal	EER 8.39%	Conduct a holistic analysis of CA through identifying behavioural biometric features through Pattern Unlock features on a mobile phone. The paper stresses the importance of how to evaluate features on a independent and collective basis as the performance and accuracy of CA may vary based on these details.
Crouse et al. [20]	2020	10	Mobile	Multi-modal	-	A comprehensive survey exploring state-of-the-art machine-learning algorithm solutions which can help improve security of mobile phone devices.

Table 6. Light Blue Cluster: Multi-Modal CA based on Mobile Devices

The first noticeable trend is that there is now a clear consensus of examining CA techniques involving a fusion of multiple biometric authentication techniques. In a number of studies [56, 67, 95, 115] they all introduce novel CA systems based on a fusion of multiple biometric features extracted from devices. For example, the authors of Shankar & Singh [95] utilize gyroscope and accelerometers within mobile phone device. In Lamiche et al. [67], the authors use gait patterns and keystroke dynamics to build a new multimodal CA system.

The second is the focus on *mobile devices* as the primary device to extract, store, process and send this multi-modal biometric data. This observation is supported by multiple publications in the 'Light Blue Cluster' [20, 56, 67, 95, 113]. One possible explanation for this phenomenon is that mobile devices: (a) are owned by the majority of the population in developed countries; (b) can be easily carried by the users; (c) contain multiple sensors that can be utilized for the purpose of CA; (d) become increasingly powerful in computational sense which simplifies the tasks of autonomous 'on-the-fly' signal processing, feature extraction, and classification.

4.3 Summary

In the majority of the studies represented by the core nodes examined fig. 4, a systematic process is undertaken during evaluation of various CA devices and techniques. We summarize it as follows. First, it needs to be decided on what data (signal) is collected and how. Second, it is required to decide what features are to be composed (and how) from that collected data/signal. We observed that in many cases features can be explained (e.g. have some sort of behavioral/physiological/biometrical meaning). Third, it is common to reduce the set of initial features. This is usually done through the techniques for dimensionality reduction such as, for example, Principal Component Analysis (PCA), relative entropy, frequency filters, etc. This step helps to reduce noise and/or redundant information which normally improves classification. Fourth, classifiers must be trained using supervised/unsupervised techniques. This may be accomplished through one- or multi-class classification frameworks. For example, one-class classification is suitable for authentication tasks since it answers 'yes/no' question. Multi-class approach may be used for identification: if authentication fails (e.g. the subject is labeled as 'impostor') it may be possible to identify the subject (if corresponding information is present in the database). Fifth, it is necessary to test the classifier. This allows to determine error rates, such as EER or Area Under the Curve (AUC) for Receiver Operating Characteristics (ROC). The obtained information, for instance, allows to determine the trade-off between usability and residual risks in the designed CA system.

5 DISCUSSION

Building upon our predefined research questions, our research goal was to analyse the substantial body of literature on Continuous Authentication to date in order to synthesise the key concepts and detect knowledge gaps that future research can address moving forward. Below, we discuss the implication and knowledge gaps as per the findings and results in further detail.

5.1 Current Research Status

Through a Citation Network Analysis on the core papers identified within CA section 6.2, we identified that there are three important research areas within this disciplinary area - Keystroke Dynamics (KDCA); Mouse Movement Analysis (MMCA) and Touch based CA through Mobile devices (MDTI) respectively. To the best of our knowledge, we are the first who use CNA to analyse CA. This allows us to obtain fruitful results that can not be easily achieved by merely analysing paper titles and keywords.

Interestingly, all three of the key CA research clusters are Human Computer Interaction (HCI) based behavioural biometric authentication techniques (table 2), focusing on methods to construct the users identity based on traits and mannerisms exhibited by an individual whilst interacting with a device or system. We believe that this is the case because HCI techniques can assist in collecting individual (and unique) information from the users in a seamless and non-intrusive manner: users interact with their devices on a day-to-day basis and authentication can be a bi-product of such interaction.

There is also an emphasis on developing classification algorithms based on Machine Learning methods to help improve the accuracy, security and scalability of CA technologies. For example, we observe substantial shift from statistical classifiers to more advanced classifiers such as SVM with non-linear kernels and ANN which happens over time. This is because the dimensions of the characteristics and signals collected during modern CA sessions tend to increase. As such, redundancy of information that is necessary for classification accumulates dis-proportionally within different parts of the signal. In addition, there is a stronger demand for 'on the fly' classification where the result may be skewed towards more recent samples.

5.2 Emerging Trends and Future Challenges

Based on our CNA, we were able to identify an emerging trend in CA research which was highlighted as the light-blue cluster in fig. 4. On closer observation, these studies all have the following aspects in common. Below, we discuss in detail the emerging research trends in CA along with the research challenges and gaps that need to be addressed as we move forward with the research on this subject matter.

Firstly, most take a multi-modal approach which refers to a fusion of various biometric authentication techniques. This makes sense as the light-blue cluster is conveniently located on the cross-roads between the three major research areas that were identified. This is due to recent advancements in technology which has led to devices containing multiple sensors that are able to extract different biometric features. This can happen simultaneously or in turns. Simultaneous collection of the information from several modalities can improve the accuracy of authentication. On the other hand, different characteristics that are collected in turns can reduce the invasive nature of CA and make the process more convenient for the user.

The benefit of this is that users do not need to perform any specific action (such as typing or mouse clicking) at a specific time. Instead, the users can act naturally and with minimal constraints. Secondly, these emerging studies focus heavily on the usage of mobile devices as the primary device to capture, store, process and send data. This aligns with the modern trend where mobile devices become: a) better equipped with various sensors; b) more powerful and hence capable to process (and classify) more data on the fly. Finally, novel techniques fusing the latest research on biomedical techniques (i.e. brainwaves) have also started to emerge based on our analysis. Due to quite restrictive nature of the experimental environments it, however, remains to be seen whether these technologies will become popular in the nearest future. However, there are several research challenges that must be addressed for future research on CA to achieve more accurate, secure and user friendly results.

Firstly, although there is a consensus of evaluation metrics when it comes to CA through Equal Error Rates (EER), there are still challenges remaining around what the *acceptable* benchmark is. This is because utility of CA can not be defined in disconnection from traditional authentication: CA is usually used in tandem with standard authentication methods. The prevailing number of studies is, however, focused on FAR, FRR, EER and not on how to combine CA with standard authentication in an optimal way. For example, high FRRs can be tolerated (e.g. have substantially good utility) if traditional authentication requires entering PIN (only) when CA fails to identify a user. This contrasts with the situation when users undergo 2-stage MFA: even negligible FRR can add substantial burden for a user.

In addition, EER rates are dynamic in the sense that it decreases as the amount of data collected increases, but there is still no consensus as to what the optimal EER rate vs. data collection timeframe should be considering that studies imply that it takes months of data for EER rates to reach optimal rates. For example, based on the results of our study, we identified significant variations in the evaluation scores ranging for EER rates of 0.1% to over 15%. This may be due to the variation in the number of study participants; the combination of device and technique used; and the details of the experiment itself (e.g. text length).

Secondly, future studies should not only focus on solutions based on authentication accuracy, but also ensure it takes into consideration the security and privacy issues that are associated in the minds of CA users. For example, it is important to ensure that templates and signals collected during CA sessions are protected from the adversary. Replay attack that are commonly addressed in biometrics have not been considered in CA to date. A possible solution might require utilization of Trusted Programming Modules (TPMs) and/or Trusted Execution Environments (TEEs) that are

now parts of many mobile phone models. Only Lamiche et al. [67] from the core group of studies examined considered how their CA technology would influence privacy and security matters. We consider this an issue, and especially for the situations where the data captured during CA can not be processed within the device boundaries (e.g. needs to be sent to the central server).

Thirdly, future studies must not depend too heavily on merely pre-existing software solutions that focus the majority of their attention on behavioural biometric techniques. The results from this paper suggest that there is a significant dependence on software solutions utilising biometric techniques, with little focus placed on innovative hardware device solutions and non-biometric techniques. Instead, purposely designed hardware may be better suited for CA than a generic device (such as mobile phone) with pre-installed software. This is because in addition to more secure architecture hardware tools for CA may have better energy efficiency, may last longer without recharge, emits less radiation, smaller form factor, better usability, cheaper to reproduce. Hardware may be easier replaceable if lost. It can have less privacy concerns since it can be easily disabled/switched off. As a result, this causes less concerns associated with 'spying' for users: users can 'cut off' from CA after the working session which contrasts with how personal mobile phones are used.

Fourthly, a significant research challenge is the lack of a systematic framework and methodology which enables cross-comparative studies to determine its efficacy to be carried out. Having these frameworks and standards in place is important as it will provide future studies the necessary structure to determine what features must be extracted; which techniques and algorithms are most suitable for filtering the data and classification; and how performance should be evaluated when it comes to CA systems. For example, a standard with requirements for CA conformance may be developed, similar to how ISO/IEC 30136 describes evaluation of the accuracy, secrecy, and privacy of biometric template protection schemes. Interestingly enough, these suggestions are largely in tune with prior studies such as Gonzalez-Manzano et al. [51], who not only presented the steps needed for unifying design processes surrounding CA, but also the ongoing challenges and issues pertaining to each step as per fig. 5.

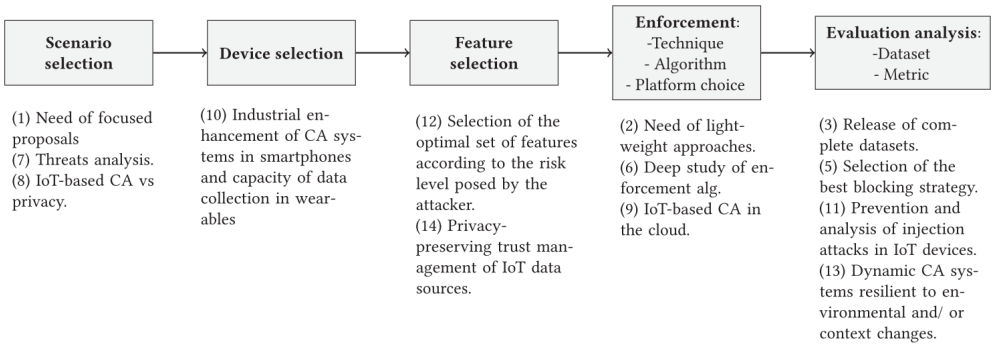

Fig. 5. Design process of an IoT-based CA approach (Adopted from [51])

Finally, real use-cases are non-existent as there is no study which has examined the feasibility of device/technique combination for CA purposes based on different settings. For instance, studies fail to discriminate between where CA must occur - remotely or on premises. It is also unclear on whether the process of CA should be supervised or unsupervised, what is the cost of the system, how should the equipment be calibrated, what are the threats and how to mitigate them. In certain

situations, a verified user may want someone to take their place intentionally. Therefore, the enrollment phase of CA is equally as critical although the examination of studies highlights the fact that this is largely neglected.

5.3 Implications for Theory and Practice

From a theoretical perspective, our study makes significant theoretical contributions on understanding the current body of knowledge and emerging trends in CA. Furthermore, to the best of our knowledge, this is the first study to apply CNA within the context of CA. Our study demonstrates how CNA can help systematically identify, examine and synthesise the large extant of literature that spreads across a wide range of disciplinary areas without bias.

We also took recommendations on board from Edwards [38], who recommended that literature reviews conducted via Social Network Analysis (SNA) methods such as CNA take a mixed-methods approach by utilising visualisation and measurement applications. As such, we not only took a systematic approach manually to careful curate and select the main literature survey papers associated with CA, but also utilised popular tools such as VOSViewer and Gephi to aid with the visualisation of the large body of literature collected.

From a practical perspective, this study not only provides a broad overview of the dominant CA techniques, devices and frameworks that an organisation may wish to adopt, but also provides decision makers a reference point when comparing what the most *appropriate device and technique combination* pertaining to CA is feasible for their particular situation based on the expected accuracy rates and training time necessary.

6 CONCLUSION

The primary aim of our study was to synthesis the large breadth of CA literature that exists across multiple interdisciplinary backgrounds. Through a systematic process of identifying the most important core papers within CA through a Citation Network Analysis, we were able to address both of our main research questions that were stipulated in the beginning of this study. To the best of our knowledge, this is the only paper which provides a comprehensive overview and synthesis of the entire breadth of literature on CA.

6.1 Addressing the RQ

Regarding **RQ1**, we were able to determine three main research areas within the CA landscape based on the nodal distance and colour clusters that emerged from our analysis. The first research area was on Keystroke Dynamics Continuous Authentication Technologies, the second on Mouse Movements for Continuous Authentication whilst the final area was on Touch based Continuous Authentication. These results indicate that the dominant subject matters on CA were predominately based on HCI-based behavioural biometric techniques.

As for **RQ2**, we identified that emerging research topics on CA were based on a fusion of biometric technologies, which was made possible through the widespread adoption of mobile devices. This shift towards a specific direction may be due to the widespread usage of mobile devices and technological advancements when it comes to the multiple sensors and arrays it contains. Several gaps pertaining to a lack of standards which resulted in difficulties comparing different device+technique combinations for CA, along with no real life use cases associated with CA were also identified, in which encourage future studies to address.

6.2 Limitations and Future Studies

Our study has its boundary and scope. In the introduction, we highlighted that due to the vagueness of the definitions for CA, the initial papers were selected based on the declarations (about the

topic, keywords, etc.) made by their authors. This kind of initial selection can be criticized. Despite methods allowing select papers on a more justifiable basis are yet to be specified, one approach to extend the boundaries is to use a larger subset of keywords and literature survey papers.

Yet another limitation of our paper is due to a strong emphasis on well-established (e.g. often cited) research directions in the field of CA. This explains why newer (and less cited) publications are eliminated from fig. 4. We believe that setting limits on the period of time elapsed since the publication date is one way to analyze new trends in CA in greater detail (and without bias towards well-established papers).

As stated in section 2.2.5, non-biometric CA techniques are known from the literature. However, papers representing these techniques are absent from the clusters on fig. 4. This is due to several factors. First, among 2322 papers identified as per item 2 in section 3.2, the number of non-biometric CA papers is low. This may be explained by a relatively strong depart of CA papers towards biometric techniques. Second, cross-citations between papers studying biometric and non-biometric techniques are infrequent. In future studies, this limitation will be addressed by a separate analysis of CA implemented through biometric and non-biometric approaches.

We recommend that future research on CA related topics can examine the gaps identified through this study - in particular the resource management, efficacy rate and security and privacy issues which seems to be prevalent across all forms of CA techniques and devices.

ACKNOWLEDGMENT

This work was partially supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Program.

REFERENCES

[1] Mohammed Abuhamad, Ahmed Abusnaina, DaeHun Nyang, and David Mohaisen. 2020. Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey. *IEEE Internet of Things Journal* 8, 1 (2020), 65–84.

[2] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac, and Kemal Akkaya. 2018. Waca: Wearable-assisted continuous authentication. In *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 264–269.

[3] Ahmed A. Ahmed and Issa Traore. 2014. Biometric Recognition Based on Free-Text Keystroke Dynamics. *IEEE Transactions on Cybernetics* 44, 4 (2014), 458–472. https://doi.org/10.1109/TCYB.2013.2257745

[4] Ahmed Awad E Ahmed and Issa Traore. 2007. A new biometric technology based on mouse dynamics. *IEEE Transactions on dependable and secure computing* 4, 3 (2007), 165–179.

[5] Abdulwahid Al Abdulwahid, Nathan Clarke, Ingo Stengel, Steven Furnell, and Christoph Reich. 2015. A survey of continuous and transparent multibiometric authentication systems. In *European Conf. on Cyber Warfare and Security*. 1–10.

[6] Fatimah Hussain Al-Naji and Rachid Zagrouba. 2020. A survey on continuous authentication methods in Internet of Things environment. *Computer Communications* (2020).

[7] Eesa Al Solami, Colin Boyd, Andrew Clark, and Asadul K Islam. 2010. Continuous biometric authentication: Can it be more practical?. In *2010 IEEE 12th International Conference on High Performance Computing and Communications (HPCC)*. IEEE, 647–652.

[8] Md Liakat Ali, John V Monaco, Charles C Tappert, and Meikang Qiu. 2017. Keystroke biometric systems for user authentication. *Journal of Signal Processing Systems* 86, 2-3 (2017), 175–190.

[9] Saud Alotaibi and Abdulrahman Alruban. 2017. A systematic literature review of behavioural profiling for smartphone security: Challenges and open problems. (2017).

[10] Orcan Alpar. 2015. Intelligent biometric pattern password authentication systems for touchscreens. *Expert Systems with Applications* 42, 17 (2015), 6286–6294. https://doi.org/10.1016/j.eswa.2015.04.052

[11] Orcan Alpar. 2017. Frequency spectrograms for biometric keystroke authentication using neural network based classifier. *Knowledge-Based Systems* 116 (2017), 163–171. https://doi.org/10.1016/j.knosys.2016.11.006

[12] Orcan ALPAR. 2019. TAPSTROKE: A novel intelligent authentication system using tap frequencies. *Expert Systems with Applications* 136 (2019), 426–438. https://doi.org/10.1016/j.eswa.2019.06.057

[13] Arwa Alsultan, Kevin Warwick, and Hong Wei. 2017. Non-conventional keystroke dynamics for user authentication. *Pattern Recognition Letters* 89 (2017), 53–59. https://doi.org/10.1016/j.patrec.2017.02.010

[14] Adam J Aviv, Katherine L Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. 2010. Smudge attacks on smartphone touch screens. *Woot* 10 (2010), 1–7.

[15] S Ayeswarya and Jasmine Norman. 2019. A survey on different continuous authentication systems. *International Journal of Biometrics* 11, 1 (2019), 67–99.

[16] Antonia Azzini, Stefania Marrara, Roberto Sassi, and Fabio Scotti. 2008. A fuzzy approach to multimodal biometric continuous authentication. *Fuzzy Optimization and Decision Making* 7, 3 (2008), 243.

[17] Kyle O. Bailey, James S. Okolica, and Gilbert L. Peterson. 2014. User identification and authentication using multi-modal behavioral biometrics. *Computers Security* 43 (2014), 77–89. https://doi.org/10.1016/j.cose.2014.03.005

[18] Josh Barnes and Piet Hut. 1986. A hierarchical O (N log N) force-calculation algorithm. *nature* 324, 6096 (1986), 446–449.

[19] Mathieu Bastian, Sebastien Heymann, and Mathieu Jacomy. 2009. Gephi: An Open Source Software for Exploring and Manipulating Networks. http://www.aaai.org/ocs/index.php/ICWSM/09/paper/view/154

[20] Auwal Ahmed Bello, Haruna Chiroma, Abdulsalam Ya'u Gital, Lubna A Gabralla, M Abdulhamid Shafi'i, and Liyana Shuib. 2020. Machine learning algorithms for improving security on touch screen devices: a survey, challenges and new perspectives. *Neural Computing and Applications* (2020), 1–28.

[21] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. 2002. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC)* 5, 4 (2002), 367–397.

[22] Vincent D Blondel, Jean-Loup Guillaume, Renaud Lambiotte, and Etienne Lefebvre. 2008. Fast unfolding of communities in large networks. *Journal of statistical mechanics: theory and experiment* 2008, 10 (2008), P10008.

[23] Patrick Bours and Soumik Mondal. 2015. Performance evaluation of continuous authentication systems. *IET Biometrics* 4, 4 (2015), 220–226.

[24] Carmen Camara, Pedro Peris-Lopez, Lorena Gonzalez-Manzano, and Juan Tapiador. 2018. Real-time electrocardiogram streams for continuous authentication. *Applied Soft Computing* 68 (2018), 784–794.

[25] P. Campisi. 2009. User authentication using keystroke dynamics for cellular phones. *IET Signal Processing* 3 (July 2009), 333–341(8). Issue 4. https://digital-library.theiet.org/content/journals/10.1049/iet-spr.2008.0171

[26] T. Cappalli and A. Tulshibagwale. 2021. *OpenID Continuous Access Evaluation Profile 1.0.* Technical Report. https://bitbucket.org/openid/risc/src/master/openid-caep-specification-1_0.txt.

[27] P.J. Carrington, J. Scott, and S. Wasserman. 2005. *Models and Methods in Social Network Analysis.* Cambridge University Press.

[28] Ting-Yi Chang, Cheng-Jung Tsai, and Jyun-Hao Lin. 2012. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *Journal of Systems and Software* 85, 5 (2012), 1157–1165. https://doi.org/10.1016/j.jss.2011.12.044

[29] Ting-Yi Chang, Cheng-Jung Tsai, Jen-Yuan Yeh, Chun-Cheng Peng, and Pei-Hsuan Chen. 2020. New soft biometrics for limited resource in keystroke dynamics authentication. *Multimedia Tools and Applications* 79, 31 (Aug. 2020), 23295–23324. https://doi.org/10.1007/s11042-020-09042-x

[30] Ken Cherven. 2015. *Mastering Gephi network visualization.* Packt Publishing Ltd.

[31] Nathan L Clarke and Steven M Furnell. 2007. Authenticating mobile phone users using keystroke analysis. *International journal of information security* 6, 1 (2007), 1–14.

[32] Heather Crawford, Karen Renaud, and Tim Storer. 2013. A framework for continuous, transparent mobile device authentication. *Computers & Security* 39 (2013), 127–136.

[33] David Crouse, Hu Han, Deepak Chandra, Brandon Barbello, and Anil K Jain. 2015. Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data. In *2015 International Conference on Biometrics (ICB).* IEEE, 135–142.

[34] Gabriel Dahia, Leone Jesus, and Mauricio Pamplona Segundo. 2020. Continuous authentication using biometrics: An advanced review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 10, 4 (2020), e1365.

[35] Ron Davidson and David Harel. 1996. Drawing graphs nicely using simulated annealing. *ACM Transactions on Graphics (TOG)* 15, 4 (1996), 301–331.

[36] Mohammad Omar Derawi, Claudia Nickel, Patrick Bours, and Christoph Busch. 2010. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.* IEEE, 306–311.

[37] Simon Eberz, Kasper B Rasmussen, Vincent Lenders, and Ivan Martinovic. 2017. Evaluating behavioral biometrics for continuous authentication: Challenges and metrics. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security.* 386–399.

[38] Gemma Edwards. 2010. Mixed-method approaches to social network analysis. (2010).

[39] Elakkiya Ellavarason, Richard Guest, Farzin Deravi, Raul Sanchez-Riello, and Barbara Corsetti. 2020. Touch-dynamics based Behavioural Biometrics on Mobile Devices–A Review from a Usability and Performance Perspective. *ACM Computing Surveys (CSUR)* 53, 6 (2020), 1–36.

[40] Mohammed E Fathy, Vishal M Patel, and Rama Chellappa. 2015. Face-based active authentication on mobile devices. In *2015 IEEE international conference on acoustics, speech and signal processing (ICASSP)*. IEEE, 1687–1691.

[41] Clint Feher, Yuval Elovici, Robert Moskovitch, Lior Rokach, and Alon Schclar. 2012. User identity verification via mouse dynamics. *Information Sciences* 201 (2012), 19–36. https://doi.org/10.1016/j.ins.2012.02.066

[42] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunar, Yifei Jiang, and Nhung Nguyen. 2012. Continuous mobile authentication using touchscreen gestures. In *2012 IEEE conference on technologies for homeland security (HST)*. IEEE, 451–456.

[43] Tao Feng, Jun Yang, Zhixian Yan, Emmanuel Munguia Tapia, and Weidong Shi. 2014. TIPS: Context-Aware Implicit User Identification Using Touch Screen in Uncontrolled Environments. In *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications (HotMobile '14)*. Association for Computing Machinery, New York, NY, USA, Article 9, 6 pages. https://doi.org/10.1145/2565585.2565592

[44] Tao Feng, Xi Zhao, Bogdan Carbunar, and Weidong Shi. 2013. Continuous mobile authentication using virtual key typing biometrics. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 1547–1552.

[45] Mohamed Amine Ferrag, Leandros Maglaras, Abdelouahid Derhab, and Helge Janicke. 2020. Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. *Telecommunication Systems* 73, 2 (Feb. 2020), 317–348. https://doi.org/10.1007/s11235-019-00612-5

[46] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2012. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security* 8, 1 (2012), 136–148.

[47] Arne Frick, Andreas Ludwig, and Heiko Mehldau. 1994. A fast adaptive layout algorithm for undirected graphs (extended abstract and system demonstration). In *International Symposium on Graph Drawing*. Springer, 388–403.

[48] Lex Fridman, Steven Weber, Rachel Greenstadt, and Moshe Kam. 2016. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal* 11, 2 (2016), 513–521.

[49] Thomas MJ Fruchterman and Edward M Reingold. 1991. Graph drawing by force-directed placement. *Software: Practice and experience* 21, 11 (1991), 1129–1164.

[50] Romain Giot, Mohamad El-Abed, Baptiste Hemery, and Christophe Rosenberger. 2011. Unconstrained keystroke dynamics authentication with shared secret. *Computers Security* 30, 6 (2011), 427–445. https://doi.org/10.1016/j.cose.2011.03.004

[51] Lorena Gonzalez-Manzano, Jose M De Fuentes, and Arturo Ribagorda. 2019. Leveraging user-related internet of things for continuous authentication: A survey. *ACM Computing Surveys (CSUR)* 52, 3 (2019), 1–38.

[52] Maria J Grant and Andrew Booth. 2009. A typology of reviews: an analysis of 14 review types and associated methodologies. *Health information & libraries journal* 26, 2 (2009), 91–108.

[53] Daniele Gunetti and Claudia Picardi. 2005. Keystroke analysis of free text. *ACM Transactions on Information and System Security (TISSEC)* 8, 3 (2005), 312–347.

[54] Luis Hernández-Álvarez, José María de Fuentes, Lorena González-Manzano, and Luis Hernández Encinas. 2021. Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review. *Sensors* 21, 1 (2021), 92.

[55] Yifan Hu. 2005. Efficient, high-quality force-directed graph drawing. *Mathematica journal* 10, 1 (2005), 37–71.

[56] Nasiru Ibrahim and Harin Sellahewa. 2019. Android Pattern Unlock Authentication-effectiveness of local and global dynamic features. In *2019 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, 1–5.

[57] Mathieu Jacomy, Tommaso Venturini, Sebastien Heymann, and Mathieu Bastian. 2014. ForceAtlas2, a continuous graph layout algorithm for handy network visualization designed for the Gephi software. *PloS one* 9, 6 (2014), e98679.

[58] Jongkil Jeong. 2021. CA Core Nodes Summary (FINAL).docx. https://doi.org/10.6084/m9.figshare.14608065.v1

[59] Jongkil Jeong. 2021. CA Lit Review Papers based on SNA. https://doi.org/10.6084/m9.figshare.14608077.v1

[60] Jay Jeong, Yevhen Zolotavkin, and Robin Doss. [n. d.]. *Examining the Current Status of Continuous Authentication Technologies through Citation Network Analysis*. Technical Report. https://doi.org/10.6084/m9.figshare.14593947.

[61] Tomihisa Kamada, Satoru Kawai, et al. 1989. An algorithm for drawing general undirected graphs. *Information processing letters* 31, 1 (1989), 7–15.

[62] Marcus Karnan, Muthuramalingam Akila, and Nishara Krishnaraj. 2011. Biometric personal authentication using keystroke dynamics: A review. *Applied soft computing* 11, 2 (2011), 1565–1573.

[63] Junhong Kim and Pilsung Kang. 2020. Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features. *Pattern Recognition* 108 (2020), 107556. https://doi.org/10.1016/j.patcog.2020.107556

[64] Junhong Kim, Haedong Kim, and Pilsung Kang. 2018. Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection. *Applied Soft Computing* 62 (2018), 1077–1087. https://doi.org/10.1016/j.asoc.2017.09.045

[65] Elena Kochegurova, Elena Luneva, and Ekaterina Gorokhova. 2018. On continuous user authentication via hidden free-text based monitoring. In *International Conference on Intelligent Information Technologies for Industry*. Springer, 66–75.
[66] Renaud Lambiotte, J-C Delvenne, and Mauricio Barahona. 2008. Laplacian dynamics and multiscale modular structure in networks. *arXiv preprint arXiv:0812.1770* (2008).
[67] Imane Lamiche, Guo Bin, Yao Jing, Zhiwen Yu, and Abdenour Hadid. 2019. A continuous smartphone authentication method based on gait patterns and keystroke dynamics. *Journal of Ambient Intelligence and Humanized Computing* 10, 11 (2019), 4417–4430.
[68] Yantao Li, Hailong Hu, Gang Zhou, and Shaojiang Deng. 2018. Sensor-Based Continuous Authentication Using Cost-Effective Kernel Ridge Regression. *IEEE Access* 6 (2018), 32554–32565. https://doi.org/10.1109/ACCESS.2018.2841347
[69] Yunji Liang, Sagar Samtani, Bin Guo, and Zhiwen Yu. 2020. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. *IEEE Internet of Things Journal* 7, 9 (2020), 9128–9143.
[70] Ahmed Mahfouz, Tarek M Mahmoud, and Ahmed Sharaf Eldin. 2017. A survey on behavioral biometric authentication on smartphones. *Journal of information security and applications* 37 (2017), 28–37.
[71] Linda S Marion, Eugene Garfield, Lowell L Hargens, Leah A Lievrouw, Howard D White, and Concepción S Wilson. 2003. Social network analysis and citation network analysis: Complementary approaches to the study of scientific communication. Sponsored by SIG MET. *Proceedings of the American Society for Information Science and Technology* 40, 1 (2003), 486–487.
[72] Shawn Martin, W Michael Brown, Richard Klavans, and Kevin W Boyack. 2011. OpenOrd: an open-source toolbox for large graph layout. In *Visualization and Data Analysis 2011*, Vol. 7868. International Society for Optics and Photonics, 786806.
[73] Yasuo Matsuyama, Michitaro Shozawa, and Ryota Yokote. 2015. Brain signal s low-frequency fits the continuous authentication. *Neurocomputing* 164 (2015), 137–143.
[74] Soumik Mondal and Patrick Bours. 2018. A continuous combination of security forensics for mobile devices. *Journal of Information Security and Applications* 40 (2018), 63–77. https://doi.org/10.1016/j.jisa.2018.03.001
[75] Alberto Montresor, Francesco De Pellegrini, and Daniele Miorandi. 2012. Distributed k-core decomposition. *IEEE Transactions on parallel and distributed systems* 24, 2 (2012), 288–300.
[76] Arsalan Mosenia, Susmita Sur-Kolay, Anand Raghunathan, and Niraj K Jha. 2016. CABA: Continuous authentication based on BioAura. *IEEE Trans. Comput.* 66, 5 (2016), 759–772.
[77] Arsalan Mosenia, Susmita Sur-Kolay, Anand Raghunathan, and Niraj K Jha. 2017. Wearable medical sensor-based system design: A survey. *IEEE Transactions on Multi-Scale Computing Systems* 3, 2 (2017), 124–138.
[78] Youssef Nakkabi, Issa Traore, and Ahmed Awad E. Ahmed. 2010. Improving Mouse Dynamics Biometric Performance Using Variance Reduction via Extractors With Separate Features. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 40, 6 (2010), 1345–1353. https://doi.org/10.1109/TSMCA.2010.2052602
[79] Mark EJ Newman. 2004. Analysis of weighted networks. *Physical review E* 70, 5 (2004), 056131.
[80] Mark EJ Newman. 2006. Modularity and community structure in networks. *Proceedings of the national academy of sciences* 103, 23 (2006), 8577–8582.
[81] Koichiro Niinuma, Unsang Park, and Anil K Jain. 2010. Soft biometric traits for continuous user authentication. *IEEE Transactions on information forensics and security* 5, 4 (2010), 771–780.
[82] Andreas Noack. 2007. Energy models for graph clustering. *J. Graph Algorithms Appl.* 11, 2 (2007), 453–480.
[83] Andreas Noack. 2009. Modularity clustering is force-directed layout. *Physical Review E* 79, 2 (2009), 026102.
[84] Rajvardhan Oak. 2018. A literature survey on authentication using Behavioural biometric techniques. *Intelligent Computing and Information and Communication* (2018), 173–181.
[85] Roger Ouch, Begonya Garcia-Zapirain, and Roman Yampolskiy. 2017. Multimodal biometrie systems: A systematic review. In *2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*. IEEE, 439–444.
[86] Vishal M Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello. 2016. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine* 33, 4 (2016), 49–61.
[87] Ge Peng, Gang Zhou, David T Nguyen, Xin Qi, Qing Yang, and Shuangquan Wang. 2016. Continuous authentication with touch behavioral biometrics and voice on wearable glasses. *IEEE transactions on human-machine systems* 47, 3 (2016), 404–416.
[88] Rik Pieters, Hans Baumgartner, Jeroen Vermunt, and Tammo Bijmolt. 1999. Importance and similarity in the evolving citation network of the International Journal of Research in Marketing. *International Journal of Research in Marketing* 16, 2 (1999), 113–127.
[89] Paulo Henrique Pisani and Ana Carolina Lorena. 2013. A systematic review on keystroke dynamics. *Journal of the Brazilian Computer Society* 19, 4 (2013), 573–587.
[90] Davy Preuveneers and Wouter Joosen. 2015. Smartauth: Dynamic context fingerprinting for continuous user authentication. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*. 2185–2191.
[91] Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, and Mohd Farhan Md Fudzee. 2019. A survey paper on keystroke dynamics authentication for current applications. In *AIP Conference Proceedings*, Vol. 2173. AIP Publishing LLC, 020010.

[92] Pouya Samangouei, Vishal M Patel, and Rama Chellappa. 2017. Facial attributes for active authentication on mobile devices. *Image and Vision Computing* 58 (2017), 181–192.
[93] Nikolaus Schmidt, Mario Müller, and Christoph Rosenkranz. 2015. Identifying the giants: a social network analysis of the literature on information technology outsourcing relationships. (2015).
[94] Seong seob Hwang, Sungzoon Cho, and Sunghoon Park. 2009. Keystroke dynamics-based authentication for mobile devices. *Computers Security* 28, 1 (2009), 85–93. https://doi.org/10.1016/j.cose.2008.10.002
[95] Vishnu Shankar and Karan Singh. 2019. An intelligent scheme for continuous authentication of smartphone using deep auto encoder and softmax regression model easy for user brain. *IEEE Access* 7 (2019), 48645–48654.
[96] Chao Shen, Zhongmin Cai, Xiaohong Guan, Youtian Du, and Roy A. Maxion. 2013. User Authentication Through Mouse Dynamics. *IEEE Transactions on Information Forensics and Security* 8, 1 (2013), 16–30. https://doi.org/10.1109/TIFS.2012.2223677
[97] Terence Sim, Sheng Zhang, Rajkumar Janakiraman, and Sandeep Kumar. 2007. Continuous verification using multimodal biometrics. *IEEE transactions on pattern analysis and machine intelligence* 29, 4 (2007), 687–700.
[98] Zdeňka Sitová, Jaroslav Šeděnka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, and Kiran S Balagani. 2015. HMOG: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security* 11, 5 (2015), 877–892.
[99] Riccardo Spolaor, QianQian Li, Merylin Monaro, Mauro Conti, Luciano Gamberini, and Giuseppe Sartori. 2016. Biometric Authentication Methods on Smartphones: A Survey. *PsychNology Journal* 14, 2 (2016).
[100] Ioannis Stylios, Spyros Kokolakis, Olga Thanou, and Sotirios Chatzis. 2021. Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Information Fusion* 66 (2021), 76–99.
[101] Ioannis C Stylios, Olga Thanou, Iosif Androulidakis, and Elena Zaitseva. 2016. A review of continuous authentication using behavioral biometrics. In *Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference*. 72–79.
[102] Cheng-Jung Tasia, Ting-Yi Chang, Pei-Cheng Cheng, and Jyun-Hao Lin. 2014. Two novel biometric features in keystroke dynamics authentication systems for touch screen devices. *Security and Communication Networks* 7, 4 (2014), 750–758. https://doi.org/10.1002/sec.776 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.776
[103] Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. 2016. A survey on touch dynamics authentication in mobile devices. *Computers Security* 59 (2016), 210–235. https://doi.org/10.1016/j.cose.2016.03.003
[104] Antoine J-P Tixier, Maria Evgenia G Rossi, Fragkiskos D Malliaros, Jesse Read, and Michalis Vazirgiannis. 2019. Perturb and combine to identify influential spreaders in real-world networks. In *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. 73–80.
[105] Cheng-Jung Tsai and Po-Hao Huang. 2020. Keyword-based approach for recognizing fraudulent messages by keystroke dynamics. *Pattern Recognition* 98 (2020), 107067. https://doi.org/10.1016/j.patcog.2019.107067
[106] Nees Jan Van Eck and Ludo Waltman. 2013. VOSviewer manual. *Leiden: Univeristeit Leiden* 1, 1 (2013), 1–53.
[107] Esra Vural, Jiaju Huang, Daqing Hou, and Stephanie Schuckers. [n. d.]. Shared research dataset to support development of keystroke authentication. In *IEEE International joint conference on biometrics*. IEEE, 1–8.
[108] Chris Walshaw. 2000. A multilevel algorithm for force-directed graph drawing. In *International Symposium on Graph Drawing*. Springer, 171–182.
[109] Hui Xu, Yangfan Zhou, and Michael R Lyu. 2014. Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 187–198.
[110] Roman V Yampolskiy and Venu Govindaraju. 2008. Behavioural biometrics: a survey and classification. *International Journal of Biometrics* 1, 1 (2008), 81–113.
[111] Dang Yaru. 1997. Structural modeling of network systems in citation analysis. *Journal of the American Society for Information Science* 48, 10 (1997), 946–952.
[112] Xi Zhao, Tao Feng, and Weidong Shi. 2013. Continuous mobile authentication using a novel graphic touch gesture feature. In *2013 IEEE sixth international conference on biometrics: theory, applications and systems (BTAS)*. IEEE, 1–6.
[113] Xi Zhao, Tao Feng, Weidong Shi, and Ioannis A Kakadiaris. 2014. Mobile user authentication using statistical touch dynamics images. *IEEE Transactions on Information Forensics and Security* 9, 11 (2014), 1780–1789.
[114] Yu Zhong and Yunbin Deng. 2015. A survey on keystroke dynamics biometrics: approaches, advances, and evaluations. In *Recent Advances in User Authentication Using Keystroke Dynamics Biometrics*. Number 1. Science Gate Publishing, 1–22.
[115] Lu Zhou, Chunhua Su, Wayne Chiu, and Kuo-Hui Yeh. 2017. You think, therefore you are: transparent authentication system with brainwave-oriented bio-features for IoT networks. *IEEE Transactions on Emerging Topics in Computing* 8, 2 (2017), 303–312.

APPENDIX A: SPATIALIZATION AND COLOUR CLUSTERTING THROUGH GEPHI

Spatialization ForceAtlas2 is a force-directed layout that is close to other algorithms used for network spatialization. This also explains why ForceAtlas2 is the default layout algorithm in Gephi [57].

One of the advantages of visualization using ForceAtlas2 is that it provides "live" spatialization: when the algorithm is initiated the layout changes in time and user decides on when to stop it. On the other hand, continuous nature of ForceAtlas2 does not allow to implement simulated annealing, auto-stop feature, phased strategies, graph coarsening [35, 55, 72, 108]. In addition, with the aim to improve user experience developers avoided strategies where forces do not apply homogeneously such as in [47, 61].

ForceAtlas2 simulates a physical system in order to spatialize a network. Nodes repulse each other like charged particles, while edges attract their nodes, like springs. As a result, structural proximities of the graph are turned into visual proximities which is helpful in the analysis of social networks. Nonetheless, position of a node at certain point in time can not be interpreted on its own and has to be compared with the other nodes. This is because the result varies depending on the initial state, and it is possible that the process is stuck in a local minimum. In spite of its heuristic nature, it has been shown that such spatialization has substantial explanatory ability: actors have more relations inside denser groups than outside them [79, 80, 83].

Energy model of ForceAtlas2 plays important role in explaining the outcomes of spatialization. It relies on 2 expressions that define *attraction* and *repulsion* forces. In physical systems, these forces depend on the distance d between the interacting entities: closer entities attract less and repulse more than more distant entities and vice versa. Generic formulas for attraction and repulsion forces are $F_a = k_a d^a$ and $F_r = -k_r d^{-r}$, respectively. The interdependence between distance and forces can be linear, exponential or logarithmic. There is a convention to express the model using a pair $(a, -r)$. For example, a popular LinLog algorithm is characterized by $(0, -1)$, and Fruchterman-Rheingold algorithm is $(2, -1)$ [49, 82]. Main model characteristic for ForceAtlas2 is $(1, -1)$.

In ForceAtlas2, due to $k_a = 1$ attraction force between any two nodes n_i and n_j, $i \neq j$, is $F_a(n_i, n_j) = d(n_i, n_j)$. The repulsion force is $F_r(n_i, n_j) = k_r \frac{\big(\deg(n_i)+1\big)\big(\deg(n_j)+1\big)}{d(n_i,n_j)}$, where $\deg(n_i)$ and $\deg(n_j)$ are in-degrees for nodes n_i and n_j, respectively.

The settings in Gephi allow to adjust parameters of ForceAtlas2. For our analysis we used standard mode (e.g. $(1, -1)$). It is, however, possible to use an alternative (*logarithmic*) attraction force, $F_a(n_i, n_j) = \log\big(1 + d(n_i, n_j)\big)$, which switchesForceAtlas2 into a LinLog mode. If the latter mode is selected, it may also be required to adjust *scaling parameter* k_r. We used default value $k_r = 2$. The main purpose of parameter *gravity* is to compensate repulsion for nodes that are far away from the center. There are two options for gravity in Gephi: a) 'standard gravity' $F_g(n) = k_g\big(\deg(n) + 1\big)$, and b) 'stronger gravity' $F_g^{'}(n) = k_g\big(\deg(n) + 1\big)d(n)$. This force is directed to the center of the spatialization space, and distance $d(n)$ is measured from node n to that center. We used $k_g = 1$. Parameter *edge weight* can be adjusted to increase attraction force based on the weight of the edges. This parameter is unimportant for our analysis since the weight of all the edges in our citation graph is 1. Parameter *Dissuade Hubs* can be enabled and is meant to grant nodes with a high in-degree a more central position than nodes with a high out-degree. For this, attraction force is defined as $F_a(n_i, n_j) = \frac{d(n_i,n_j)}{\deg(n_i)+1}$. Dissuade Hubs was disabled for our layout. If *Prevent Overlapping* is selected the repulsion is modified in a way that the nodes do not overlap. This is implemented by taking into account the size of the nodes in computing the distance for both attraction and repulsion forces. This parameter was enabled in our analysis. To improve spatialization performances on big graphs

(such as ours) `ForceAtlas2` is equipped with *approximate repulsion* force-calculation algorithm [18]. This parameter was enabled for the analysis.

Color-clustering Gephi supports simple heuristic method that was first described in [22]. It is based on modularity optimization allowing to extract the community structure of large networks. The objective function for optimization is defined as: $Q = \frac{1}{2m}\sum_{i,j}\left[A_{i,j} - \frac{k_i k_j}{2m}\right]\delta(c_i, c_j)$, where $A_{i,j}$ represents the weight of the edge between i and j, $k_i = \sum_j A_{i,j}$ is the sum of the weights of the edges attached to vertex i, c_i is the community to which vertex i is assigned, function $\delta(u, v)$ takes value 1 if $u = v$ and 0 otherwise, $m = \frac{1}{2}\sum_{i,j} A_{i,j}$. The task is then to find c_i for all nodes i such that Q is maximized.

The method consists of two phases that are repeated iteratively. When initiated, in the first phase the method assigns different community to each node of the network, e.g. $c_i \neq c_j$ iff $i \neq j$. Then, for each node i the method evaluates the gain of modularity that would take place by removing i from its community and by placing it in the community of j. The node i is then placed in the community for which this gain is maximum. This process is applied repeatedly and sequentially for all nodes until no further improvement can be achieved and the first phase is then complete. It should be noted that due to heuristic nature of the method the order at which the nodes are considered may affect resulting modularity and computational performance.

During the second phase the method builds a new network whose nodes are now the communities found during the first phase. The weights A_{c_i,c_j} of the the links between the new nodes are the sum of the weights of the links between (old) nodes i, j in the corresponding (old) communities c_i, c_j: $A_{c_i,c_j} = \sum_{l\in c_i}\sum_{m\in c_j} A_{l,m}$. Links between (old) nodes of the same community lead to self-loops for this community (e.g. self-loops for the new nodes). Once this second phase is completed the method shifts to the next iteration and applies the first phase again. By construction, the number of meta-communities either decreases or remains unchanged with each subsequent iteration of the method. The iterations are repeated until there are no more changes in the structure and Q is maximized.

Gephi implementation of color-clustering based on modularity is a slight modification of the original method in [22]. The settings allow a user to change 'resolution' parameter that was described in [66]. This parameter allows to control the number of resulting communities: values that are lower than 1 produce smaller communities, values that are larger than 1 produce larger communities. For our analysis we used default value of 1.

APPENDIX B: MOST CITED STUDIES IN CA BASED ON TABLE 1

Author	Publication year	Cited by, nr.	Applied Method	Device	Technique
Ahmed et al. [4]	2007	408	Research paper	Generic	Behavioural Biometrics
Aviv et al. [14]	2010	835	Research paper	Generic	Behavioural Biometrics
Azzini et al. [16]	2008	75	Research paper	Generic	Multi-modal Biometrics
Bergadano et al. [21]	2002	649	Research paper	Generic	Behavioural Biometrics
Bours et al. [23]	2015	37	Research paper	Generic	Multi-modal Biometrics
Buschek et al. [34]	2015	122	Research paper	Generic	Behavioural Biometrics
Camara et al. [24]	2018	31	Research paper	Sensor	Multi-modal Biometrics
Clarke et al. [31]	2007	376	Research paper	Mobile	Behavioural Biometrics
Crawford et al. [32]	2013	112	Research paper	Mobile	Generic
Crouse et al. [33]	2015	94	Research paper	Mobile	Generic
Derawi et al. [36]	2010	454	Research paper	Mobile	Behavioural Biometrics
Fathy et al. [40]	2015	111	Research paper	Mobile	Multi-modal Biometrics
Feng et al. [42]	2012	340	Research paper	Mobile	Behavioural Biometrics
Feng et al. [44]	2013	89	Research paper	Mobile	Behavioural Biometrics
Frank et al. [46]	2013	747	Research paper	Mobile	Behavioural Biometrics
Fridman et al. [48]	2016	193	Research paper	Mobile	Multi-modal Biometrics
Gonzalez-Manzano et al. [51]	2019	12	Systematic Review	Various	Generic
Gunetti et al. [53]	2005	558	Research paper	Generic	Behavioural Biometrics
Matsuyama et al. [73]	2015	16	Research paper	Sensor	Generic
Mosenia et al. [76]	2016	45	Research paper	Generic	Multi-modal Biometrics
Niinuma et al. [81]	2010	243	Research paper	Generic	Multi-modal Biometrics
Patel et al. [86]	2016	241	Meta-Analysis	Mobile	Generic
Peng et al. [87]	2016	57	Research paper	Mobile	Multi-modal Biometrics
Sim et al. [97]	2007	293	Research paper	Generic	Multi-modal Biometrics
Sitová et al. [98]	2015	258	Research paper	Mobile	Behavioural Biometrics
Stylios et al. [101]	2016	18	Critical Review	Mobile	Behavioural Biometrics
Xu et al. [109]	2014	198	Research paper	Mobile	Behavioural Biometrics
Yampolskiy et al. [110]	2008	395	Systematic Review	Various	Behavioural Biometrics
Zhao et al. [112]	2013	83	Research paper	Mobile	Behavioural Biometrics