IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Systematic Literature Review on Latest Keystroke Dynamics Based Models

SOUMEN ROY[1], JITESH PRADHAN[2], ABHINAV KUMAR[2], DIBYA RANJAN DAS ADHIKARY[2], UTPAL ROY[3], DEVADATTA SINHA[1], RAJAT KUMAR PAL[1], (Member, IEEE)

[1]Department of Computer Science and Engineering, University of Calcutta, Acharya Prafulla Chandra Roy Siksha Prangan, JD-2, Sector - III, Saltlake City, Kolkata - 700106, India (e-mail: soumen.roy_2007@yahoo.co.in, devadatta.sinha@gmail.com, pal.rajatk@gmail.com)
[2]Department of Computer Science and Engineering, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha-751030, India (e-mail: jiteshpradhan@soa.ac.in, abhinavanand05@gmail.com, dibyadasadhikary@soa.ac.in)
[3]Department of Computer System Sciences, VisvaBharati, Santiniketan 731235, India (e-mail: roy.utpal@gmail.com)

Corresponding author: Dibya Ranjan Das Adhikary (e-mail: dibyadasadhikary@soa.ac.in).

ABSTRACT The purpose of this study is to conduct a comprehensive evaluation and analysis of the most recent studies on the implications of keystroke dynamics (KD) patterns in user authentication, identification, and the determination of useful information. Another aim is to provide an extensive and up-to-date survey of the recent literature and potential research directions to understand the present state-of-the-art methodologies in this particular domain that are expected to be beneficial for the KD research community. From January 1st, 2017 to March 13th, 2022, the popular six electronic databases have been searched using a search criterion ("keystroke dynamics" OR "typing pattern") AND ("authentication" OR "verification" OR "identification"). With this criterion, a total of nine thousand three hundred forty-eight results, including duplicates, were produced. However, one thousand five hundred forty-seven articles have been chosen after removing duplicates and preliminary screening. Due to insufficient information, only one hundred twenty-seven high-quality quantitative research articles have been included in the article selection process. We compared and summarised several factors with multiple tables to comprehend the various methodologies, experimental settings, and findings. In this study, we have identified six unique KD-based designs and presented the status of findings toward an effective solution in authentication, identification, and prediction. We have also discovered considerable heterogeneity across studies in each KD-based design for desktops and smartphones separately. Finally, this paper found a few open research challenges and provided some indications for a deeper understanding of the issues and further study.

INDEX TERMS Behavioural Biometrics, Computer Security, Keystroke Dynamics, Trait Prediction, Typing Patterns, User Authentication, User Identification

I. INTRODUCTION

Computing and mobile devices have been identified as the primary sources of private and highly confidential information [1] because of their availability, affordability, and excessive use. There is a need for a strict as well as usable user authentication technique before accessing this information due to confidentiality, existing privacy laws, intellectual property, etc. [2]. As per Lowe's hierarchy of Authentication [3], "*Authentication is the process of one agent should become sure of the identity of the other*". Formally, "*An Authentication protocol is designed to assure an agent A as to the identity of the other agent B with whom A is running the protocol*". Here, the user authentication agent confirms the user's identity with the previously stored template/model/reference/knowledge and allows the user to access and process. The traditional PIN/password/sketch method is common because it is cost-effective, simple, and quick enough for frequent logins. However, these methods are vulnerable to several attacks, such as brute-force and smudging [4]. In addition, it has been found that an employee spends a lot of time on password-related activities [5]. Furthermore, a large number of users show their interest in favour of additional security [6]. Along

with, session hijacking is still possible in the traditional way [7]. To deal with these issues, biometric systems along with keystroke dynamics (KD) have received greater attention. Beyond KD-based authentication, KD-based identification and prediction models have been an active area of research due to their cost-effective, easily available features and ease of integration.

A. USER AUTHENTICATION TECHNIQUE AND ITS TYPE

Usually, user authentication involves confirming with a certain degree of sureness that the electronic form of the user's identity represented in the collaborative system corresponds to the real-life individuality of the user. It verifies the owner's legitimate claim and controls unauthorised access. This authentication process is based upon the combination of the following four parameters [8] – (1) Knowledge (*something we know* such as PIN, password, sketch, etc.) [9], (2) Token (*something we own or have* such as smart card, debit, credit card, etc.) [10], (3) Physical traits (*something we are born with* such as the face, fingerprint, hand geometry, etc.) [11], and (4) Behavioural traits (*something we have gained or the way we do* such as the way a user walks, talks, types, holds the phone, receives phone calls, moves the mouse, etc.) [11].

Based upon these above mentioned parameters, the following user authentication techniques have been established:

- *Knowledge-based authentication:* It uses a username and a password, PIN, or graph pattern as knowledge. If this knowledge entered by a user matches that previously stored, then the user is judged to be genuine and given access. This one-factor authentication technique is common due to its simplicity and usability [4]. However, this technique is vulnerable to several attacks mentioned in Subsection I-B.
- *Token-based authentication:* This scheme uses some physical items called tokens/possessions. A PIN is given to aid in the authentication. A user's token and a PIN make it a two-factor authentication technique. It is also vulnerable to attacks mentioned in Subsection I-B.
- *Biometric characteristics-based authentication:* Biometrics is the technology that analyses human characteristics for automated personal authentication. In this scheme, behavioural or physiological characters are used [12]. The most challenging issues in developing efficient and privacy-preserving biometric authentication systems are the immunity to spoofing attacks, the irremovability of biometric data, and the assurance that sensitive data remains private.
- *Combined/Multi-factor/Multimodal authentication:* In this scheme, more than one authentication scheme is combined to make a more powerful (with an increasing level of resistance) access control system [13]. It may be more than one biometric human characteristic [14] (i.e., face and voice, gesture and voice, face and gesture, etc.) authentication scheme.

An authentication system based on only one attribute to reduce and prevent intrusions is not enough strong [15]. Many of these biometric traits in human recognition are still not definite [16]. Furthermore, current methods, including physical biometrics in smartphone security, have several shortcomings [17]. Among all the methods, *knowledge-based* is the cheapest, most convenient, and popular [18]. However, each of these techniques has its own merits and demerits. Along with, it has been established that none of these techniques is self-sufficient for security purposes [19]. As a result, *multi-factor authentication* has gained greater attention. A comparison of the authentication models has been shown in Table 1.

The selection of this technology depends on the application context, device suitability, and usability. For example, *knowledge-based* is a common and widely used authentication technique on both desktops/laptops and smartphones, where the ATM uses two factors - *token-based* and *knowledge-based* in order to meet the government privacy laws. Due to the hardware unavailability and unconstrained configuration of the devices, *knowledge-based* authentication is common and popular in all kinds of access control. Where PIN, password, and sketch are legitimate claims that prevent unauthorised access to the systems. But users are uninspired when choosing a healthy PIN, password, and sketch due to their trouble in remembering, high cognition, and multiple accounts. Still, users have been compromising with this technology. Text-based authentication is vulnerable to *shoulder surfing attacks*, *dictionary attacks*, *brute-force attacks*, and *smudge attacks*. It needs additional mechanisms to improve security without hampering its own merits. However, it is not suitable in a continuous domain where user identity will be continuously verified throughout the whole session.

B. AUTHENTICATION ATTACKS

An authentication attack means granting authentication to the resource without the correct credential. This part is needed in understanding the attacks for better security designs. The common attacks in *knowledge-based* authentication are listed below.

- *Brute-force attacks [21]:* It is a computerised trial process that involves guessing some sample passwords or usernames for a single account. If an attacker gets a user's personal information and compares it with a single username or password, the attacker may acquire access to that account.
- *Dictionary attack:* Generally, people choose their passwords from a relatively small dictionary. It may contain the users' parents' names, some ideal person's name, known phone numbers, or kids' names. The attacker may get access to the users' accounts if they know their personal information.
- *Shoulder-surfing attack [22]:* It is a type of attack in which the attacker guesses the password through direct observation or the use of spy or CCTV cameras [23]. Since public places, including railway stations, classrooms, and cybercafes, are almost covered by these

TABLE 1. Authentication technologies and their usage parameters. Some of these parameters have been explained in a study [20]. The possibilities show the benefits and drawbacks of known techniques for future progress

Technology	Parameters	Clue	Type	Possibilities
Knowledge-based	*something we know*	PIN, password, sketch	S	*
Token-based	*something we own or have*	Smart card, debit, credit card, etc. and PIN	S	**
Physical biometric	*something we are born with*	Face, fingerprint, hand geometry etc.	S/C	***
Behavioural biometric	*something we have gained or the way we do*	The way we walk, talk, type, etc.	S/C	***
Multi-modal	Combined	Combination of more than one schemes	S/C	**/***

S->Static, C->Continuous, *->One factor authentication, **->Two factor authentication, ***->Multi factor authentication

cameras, hiding finger movements while pressing passwords is uncomfortable.

- *Phishing attacks:* It is a *web-based* attack where an attacker criminally gets users' sensitive information for their use. In this case, the attacker opens websites with similar names and the same appearance as the home page and then obtains sensitive information fraudulently.
- *Key-loggers attack:* It is a software program where all the keystroke records, including password text, are stored in a file, and an attacker finds the password by spoofing the file and getting access to the account.
- *Smudge attacks [24]:* Extraction of a sketch from fingerprint smudges. This is a common attack on touchscreen devices.
- *Session hijacking:* When a valid session is taken over by an unauthorised user, it is called *session hijacking*.

C. BEYOND AUTHENTICATION DESIGN

Identification is just similar to *Recognition*, where patterns are previously known for more than one user and the claim pattern wants to be that someone. Several research [25]–[27], suggested supervised learning models to identify previously recorded users. In the case of *Verification*, is just similar to *Validation*, where patterns of a user are previously known by an authority and the claim pattern is validated by that authority. *Authentication* is analogous to *Liveness detection*, which is the process of allowing access to the users by validating the claim patterns with stored patterns for a certain time. Beyond authentication, typing tendency can be used to recognise a user's identity from a group if the model has previously known patterns for that user.

On the other hand, age [28], gender [29], handedness [30], hand(s) used [31], neural stress [32], and education level [30] are all relevant information that may be determined for a number of fascinating applications. Since people generate millions of typing patterns each session, this might be a realistic technique to extract this useful and important information. As a result, predictive models that go beyond authentication utilising KD attributes are more practicable and should be investigated.

D. MOTIVATION OF THE STUDY

KD, a four-decade-old biometric technology, continues to face challenges in data collection, template construction, classification, and template adaption in both desktop and smartphone contexts. At the beginning of KD literature, authentication models using KD features were the main focus area. However, in the recent past, several service-oriented models (i.e., identification and prediction) using KD features have been proposed beyond authentication. Therefore, it needs to understand how KD-based models can be operated for a variety of useful and interesting applications. Authentication, identification, and prediction are the main three models that can be found in the KD literature. On the other hand, KD itself can be classified into two main categories depending on the input freedom - (1) static mode (where input is restricted) and (2) dynamic mode (where input is not restricted). An authentication model in static mode could be used as an entry-point access control, whereas an authentication model in dynamic mode could be useful for active authentication. Similarly, identification and prediction models can be subdivided into static and dynamic modes. In this way, a total of six categories of KD-based designs have been identified in the present study. State-of-the-art models of each design have not been reviewed earlier, which motivates us to present a comprehensive review in the particular domain for each unique design.

The KD-based designs are facing several challenges due to various troubles in the data acquisition method [33], unconstrained mental state [34], illness [35], cognitive deficiency [36], fine motor abilities [37], and personal qualities [38] with other unavoidable external factors that limit their goal. Therefore, it is important to predict this information based on similar patterns for the implementation of interesting applications. In addition, many studies [39]–[42], used these extra features like age and gender as extra features to improve the performance of the user authentication model. Therefore, it is also essential to predict this useful information as soft biometric traits.

However, a user creates thousands of keystrokes in a single session that provides rich features. Recently, KD on smartphones has gained popularity due to the sensor technology attached to each smartphone and its availability with all the amenities at a low cost. It increases the collectability power of the KD-based models in the smartphone environment, enabling them to achieve acceptable accuracy and reliability. Therefore, KD is still a growing extension of the appropriate security solution as well as identification and prediction. It is important to understand how the increasing use of sensor

technology creates both opportunities and challenges for developing the next generation of KD-based systems.

E. PREVIOUS SURVEY

A study [43] in 2010 reviewed some subsets of KD and provided some recommendations and guidelines for further study in this domain. In 2012, a study [44] discussed the data acquisition methods used, approaches adopted, search heuristics, factors affected, performances achieved, and usages of this technology. In the next year, another study [45] surveyed some papers on the following topics: features used, benchmark datasets developed, and methods adopted. In the same year, a study [46] surveyed up-to-date literature on data acquisition protocols, feature extraction, methods recommended, methodologies used, especially for user authentication, and results obtained, and provided suggestions, opportunities, and recommendations. Another study [47], provided some insights into the current state-of-the-art methodologies including data acquisition, feature representation, classification, etc. for the smartphone environment. In the same year, another study [48] reviewed some existing classification methods, features, and input texts and provided a limitation of the solutions. In recent years, a study [49] surveyed KD-based emotion recognition models. Their effort was to answer the important six research questions for further development of an emotion recognition system using KD attributes. The suggested review is not a conventional literature review. We have followed the Systematic Reviews and Meta-Analyses 2020 model for systematic review and responded to a set of research questions. It includes extensive statistics, the most recent findings (aggregate score, effect size, study heterogeneity), research gaps, opportunities, and hints for future research directions.

F. OBJECTIVES

This paper provides adequate information about the work done before and effective suggestions and recommendations to develop an efficient model of KD-based user authentication, identification and prediction systems applicable for both desktop and touch screen environments. Many papers in the form of journals, conference articles, and master's theses have been published on the topics related to KD in recent years. We have tried to cover most of the high-quality research in this paper and provide the latest trends in the topic area.

The primary goals and contributions of this paper are to present an up-to-date, comprehensive survey that includes the most recent works and investigates the most recent findings, effects from aggregate findings, and significant levels of the effects. The other objectives and contributions are listed below.

- **OB1:** Identify the six unique service-oriented KD-based designs suitable for a variety of applications using both conventional keyboards and smartphones.
- **OB2:** Provide the most recent research trends in desktop, laptop, and smartphone environments.
- **OB3:** Provide a brief view of shared datasets for entry-point and active authentication/identification and prediction using a conventional keyboard and touch screen.
- **OB4:** Provide the methodologies, including data acquisition setups, predefined arrangements, device selections, and input selections.
- **OB5:** Provide detailed feature extraction and presentation strategies for both structured and unstructured patterns.
- **OB6:** Provide a suitable pattern classification strategies for a unique KD-based design.
- **OB7:** Provide a brief knowledge of pattern adaptation techniques to address concept drift.
- **OB8:** Provide the detailed evaluation metrics applicable to data acquisition, authentication, adaptation, identification, and prediction process.
- **OB9:** Provide the up-to-date achievements in different KD security designs from 2017 to 2022.
- **OB10:** Provide several tables and charts to understand the present performance of different KD-based models and study bias.
- **OB11:** Provide a large set of challenges, research gaps, study directions, and opportunities for future work.

We also found the answers to the following hypothesises in designing the unique KD-based models.

- **H1:** Each verification of static KD-based model for entry-point access control in desktops or laptops is measuring an identical finding?
- **H2:** Each verification of static KD-based model for entry-point access control in smartphones is measuring an identical finding?
- **H3:** Each verification of dynamic KD-based model for active/continuous authentication in desktop or laptop is measuring an identical finding?
- **H4:** Each verification of dynamic KD-based model for active/continuous authentication in smartphones is measuring an identical finding?
- **H5:** Each identification of a static KD-based model for identifying a user once using a conventional keyboard on a desktop or laptop is measuring an identical finding?
- **H6:** Each identification of a static KD-based model for identifying a user one time using typing tendency on the touchscreen of a smartphone is measuring an identical finding?
- **H7:** Each identification of a dynamic KD-based model for identifying users continuously using a conventional keyboard on a desktop or laptop is measuring an identical finding?
- **H8:** Each identification of a dynamic KD-based model for identifying users continuously using typing patterns on the touchscreen of a smartphone is measuring an identical finding?
- **H9:** Each prediction of a static KD-based model for the determination of useful information one time using the conventional keyboard of a desktop/laptop is measuring

an identical finding?

- **H10:** Each prediction of a static KD-based model for the determination of useful information one-time using typing patterns on the touchscreen of a smartphone is measuring an identical finding?
- **H11:** Each prediction of the dynamic KD-based model for the determination of useful information continuously using the conventional keyboard of a desktop or laptop is measuring an identical finding?
- **H12:** Each prediction of the dynamic KD-based model for the determination of useful information using typing patterns on the touchscreen is measuring an identical finding?

G. NOVELTY OF THE STUDY

This is the first study that identified various distinct KD-based models suitable for unique and interesting applications. The proposed study also offered an up-to-date (from 2017 to 2022) and complete systematic literature review that takes into account the greatest number of investigations on KD-based models (Verification in Static Mode, Verification in Dynamic Mode, Identification in Static Mode, Identification in Dynamic Mode, Prediction in Static Mode, and Prediction in Dynamic Mode) that have not previously been reported.

Furthermore, the extension of this study covered the latest data acquisition procedures for developing benchmark datasets with the most recent (highly configured) devices for next-generation KD-based systems. This work also explored the latest state-of-the-art feature extraction, classification, and adaptation methodologies for improving KD-based models. This is the first study that explored the most recent findings for each type of KD-based model and provided meta-analysis results to summarise and assess past findings. In addition, a substantial number of outstanding challenges and prospects for future study have been highlighted. Furthermore, this study answered twelve hypotheses using meta-analysis and provided an aggregate score, effect size, and significant level of effect for each model.

H. STRUCTURE

The rest of the paper is constructed with the basic ideas of KD and its applications in Section II, systematic review methodology has been described in Section III, and shared KD datasets and protocols used in literature have been presented in Section IV, numerous feature arrangements in Section V, several anomaly detections, and adaptation algorithms suitable for authentication in Section VI, latest studies and obtained results in Section VII, and finally, the challenges and opportunities in Section VIII. Since the size of this paper is large, we provide the knowledge flow of the article in Fig. 1. This will help the reader to follow this review article.

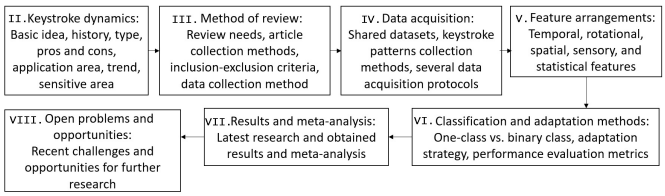

FIGURE 1. Flow of this study for better readability. Section II provides a clear idea of KD-based models for beginners. Section III states the methodology for this study. Section IV gives several protocols for the development of new datasets. Section V introduces several feature vectors of KD-based systems. Section VI gives the details of classifiers and adaptation techniques used in the literature for KD pattern classification. Section VII provides the summary statistics and shows the heterogeneity across studies. Finally, Section VIII states the recent challenges, KD study directions, and opportunities for further research

II. KEYSTROKE DYNAMICS

It is well established that KD is a potential and versatile behavioural biometric that can be easily and cost-effectively captured by many devices, not limited to smartphones, computer keyboards, and touchpads [50]. This is the study where people can be well-known for their typing style, much like handwriting. It is a software-based method [51] that can be easily integrated with an existing knowledge-based security system to make the authentication process stricter, better, and more secure without interrupting the system's own merits [52]. It also enables security during the entire session, continuously [53].

A. HISTORY

KD as a biometric characteristic is not a new concept. It was first formally investigated by Bryan and Harter in their study [54] in 1897, as part of a study on skills gained by telegraph operators. In 1975, Spillane suggested in an IBM technical bulletin that typing rhythms on a conventional desktop keyboard could be used to identify the user. [55]. The bulletin described KD as a concept. Forsen et al. in their study [56] in 1977, conducted preliminary tests of whether KD could distinguish typists. Gaines et al. [57] in 1980 produced an extensive report of their investigation with seven typists into KD. The first patent was approved in the KD domain in the year 1986 by J.D. Garcia et al. [58]. As per them, the keyboard can be used as a security apparatus. They have used the timing delay between two successive strokes on a keyboard as a KD feature vector. Leggett and Williams introduced the first dynamic families of KD [59] in 1988. They proposed that a KD be used as a safeguard for the password and dynamic identity verifiers.

B. KEYSTROKE DYNAMICS SYSTEM DESIGNS (CONTRIBUTION TO OB1)

KD is a technology to identify users based on their regular typing rhythms [60]. It enhances the security level and can be used to identify an individual [61]. KD can be either static (fixed text) or dynamic (free text) [62]. In static KD, the user needs to type the predefined text for each entry. Where dynamic families allow the users to type any text they wish, some reference templates match the claimed samples.

Fig. 2 shows the unique system design for KD-based models (authentication, identification, and prediction). Each of these models differs in numerous respects, including input,

output, model construction, classification, and decision. For example, the input in implementing an authentication model is the samples of a subject; the input in implementing an identification model is samples of multiple subjects with subject identifiers; whereas the input in implementing a prediction model is samples of several subjects from various groups labelled with meaningful information. Similarly, the output of the authentication model is "Valid" or "Invalid", whereas the output of the identification model is the identifier information of the claimed user. The output of the prediction model varies depending on the information on which it is developed. Depending on the input and output of these models, the model construction, classification, and decision-making procedure are selected. Each model may be separated further into static and dynamic modes. These models are selected depending on the application's suitability. The data acquisition parts of these models are similar, but the building model and classification results are unique. We have divided the KD-based models into the following ways in which KD could be managed. The first sub-category is static and dynamic, where each sub-category could be used in three types of applications (verification, identification, and prediction).

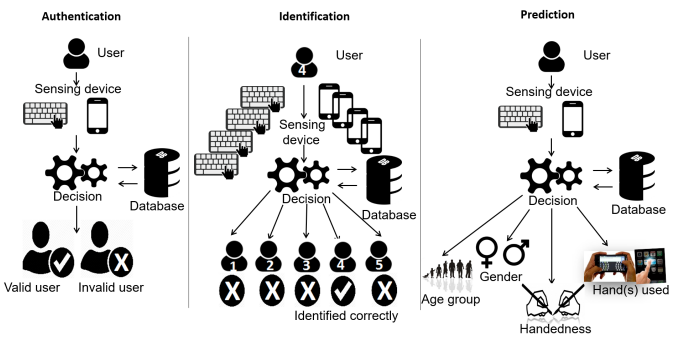

FIGURE 2. Unique system design: authentication/verification confirms the genuineness of claim sample, identification/recognition recognises the claim sample, and prediction/extraction predicts the personal traits

- *Verification in Static Mode (ViSM):* In this mode, the user's current sample (claim sample) is verified with the previously stored template [47]. The system decides whether the claim sample is genuine or an imposter at the beginning of any security session for a predefined arrangement such as a typing pattern for fixed-text. Any authentication point, such as a student or employee attendance system, phone unlocking, intrusion detection at an entry-point, or application login, falls into this category. The main intention of this model is to safeguard the passwords from brute-force, dictionary, and shoulder-surfing attacks.
- *Verification in Dynamic Mode (ViDM):* In this mode, user identity is verified during the entire session, considering there is no predefined arrangement. Here, users are free to type any text [47]. The system with this design captures only the patterns generated continuously instead of the text and authenticates the user repeatedly at regular intervals until the end of a session. For example, implicit and active authentication for mobile, desktop/laptop, or installed applications such as mobile banking, e-wallet, and e-learning where the genuineness of the user throughout a session is very important. The main intention of this model is to prevent the devices from being hijacked during sessions.
- *Identification in Static Mode (IiSM):* In this mode, the user's current sample or claim sample is used to check the user's identity from multiple users' templates. This mode shows a model with the samples collected from multiple users in the training phase. In contrast, in testing, a user is identified by the claim sample at the beginning of any session for a predefined arrangement (fixed-text). Air travel entry-point security where the user books a ticket for a given input and validates while travelling.
- *Identification in Dynamic Mode (IiDM):* In this mode, the user's identity is tested during the session without considering the predefined arrangement (free-text). Example - online examination, criminal investigation.
- *Prediction in Static Mode (PiSM):* This is the knowledge-discovery model for predefined arrangements. Knowledge may be one of the user's traits or mental status. Example - gender, age, handedness, hand(s) used, typing skill, educational level, and emotional state.
- *Prediction in Dynamic Mode (PiDM):* This is also a knowledge-discovery model, but a prediction model based on the patterns created without considering predefined arrangements. Example - Parkinson's disease [37] or neural stress [32] prediction without restricting predefined inputs.

Fig. 3 presents the latest contributions to the specific mode of KD-based design. A large number of studies (15.91% of the latest KD-based designs) have been conducted on ViSM for desktops and laptops. It is 29.70% of the total KD literature for the desktop/laptop environment. It has been observed that less effort has been given to the patterns generated through special peripherals (other devices like wearable on-body IoT devices for measurement of brain signals, heart rate variability, and body part movements while typing). Figure shows that no prediction models (PiSM and PiDM) has been conducted using the patterns generated through other peripherals while typing on a conventional keyboard and touchscreen. ViSM design in desktop/laptop and IiDM in smartphone environments has been analysed more. The main reason for these statistics is that a large number of standard datasets are available for ViSM on desktops and easily available sensors' data for IiDM on smartphones. These statistics also indicate that less effort has been given to the predictive model for a variety of interesting applications.

As of now, no design is definite because of various data acquisition troubles due to lack of standardization [28], intra-class variation due to illness, tiredness, position variability

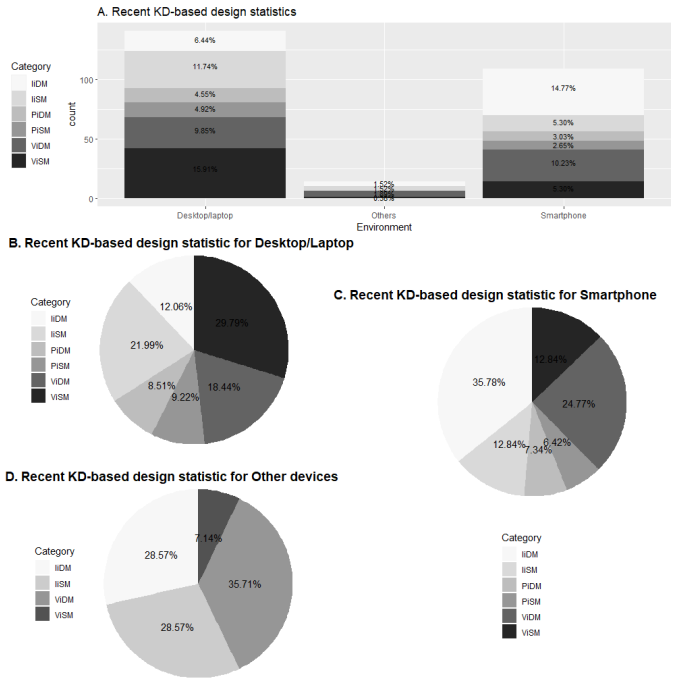

FIGURE 3. Latest contributions to the specific mode of KD-based systems. Fig. A presents the KD-based model distribution of the total selected articles. Fig. B presents the latest contribution statistics for desktops. Fig. C presents the latest contribution statistics for smartphones. Fig. D presents the latest contribution statistics for other devices

[63], unavoidable external factors [64], the uncertain performance of detector [65], low user discriminable power, usability control, time taking training phase, etc. As a result, KD-based models without proper treatment have poor performance that does not allow them to use this technique in practice.

C. STRENGTH OF KEYSTROKE DYNAMICS BASED SYSTEMS

The following are plenty of plus points about being used for KD as an entry-point and active authentication, one-time and continuous recognition of a user, and determination of a user's traits, stress level, etc. for predefined and unrestricted inputs:

- *Affordability:* Essential hardware resources like keyboards, attached sensors like gyroscopes, and a few lines of a computer program like event-driven are the only requirements for the purpose. It made it cheaper and more easily available and could be used in the multimodal biometric solution.
- *Scalability:* KD-based system has the ability to handle many inputs. In addition, users have the option to change the acceptance threshold depending on their typing behaviour and the consistency level of their typing. It provides flexibility, satisfaction, and strictness to the system.
- *Compatibility:* It could be used to address security demands like password hardening, fixed-text, free-text, adaptive, implicit, passive, continuous user identity verification, identification, and prediction.
- *Maintainability:* Changing input pass-phrase (s) changes the pattern accordingly. It minimises the chances of long-lasting damage.
- *Collectivity:* Any activity on a keyboard or touchscreen generates numerous patterns that are measured by the equipped sensors to measure the orientation, force, touch coordinates, flight time, fingertips size, multi-touch features, and pressure, all of which resist ageing.
- *Continuity:* It can monitor the user's activity continuously, which means it re-authenticates the user's identity as many times as possible without requiring any effort, until the end of any session.
- *Transparency:* With no interruption, this method recognises the user's gesture implicitly.

D. CHALLENGES OF KD-BASED SYSTEMS

The following are the points that made this technically challenging and against KD:

- *Acceptability:* It is well-studied in literature, but it is the least biometric modalities [16] to be used in practice due to poor performance, intra-class variation, poor data quality, and limited discriminable patterns.
- *Dependency:* Higher clock resolution is more suitable for generating a continuous pattern [66]. Therefore, the system's performance may vary with changing machines. Typing style may also change in hardware variabilities like cross-device matching, keyboard layout, shape, and size.
- *External factors:* Illness, mental state, emotional status [67], tiredness, and keyboard experience level do not allow for the measurement of a consistent pattern due to cognitive and fine motor deficiencies. Similarly, the unavoidable noisy patterns generated in different positions like sitting, standing, walking, and travelling on a bus is a major challenges for system designers. Each user should have the typing pattern, but the quality, sample size, and consistency level are not stable because of a variety of problems such as word choice, lack of standardization, etc.
- *Energy consumption:* Operating sensors for a longer time consumes enormous energy. It reduces the battery life and may not be suitable for battery-power constraints devices in continuous configuration.

E. AREA OF APPLICATION

Many potential and demanded application areas have been identified where KD is involved, such as

- *Device/application/data security:* KD has started to design an effective biometric authentication system. It enables features that prevent unauthorised access to the device/application/data. It can be used to fortify existing PIN/password-based authentication systems. Likewise, it also enables security throughout the session by monitoring and analysing continuous activities [68].

- *Human-computer-interaction:* KD enables the features to detect the age group below 18, which could be an effective way to design a model to protect the kids from Internet threats by implementing a restricted firewall that will be more suitable for that particular user [69]. We could implement age- and gender-specific product recommendation services in e-commerce problems by recognising age groups and gender. It also enables designing a system where age and user-specific content or advertising may reach the proper consumers effectively [38].
- *Forensics/Surveillance:* KD predictive model could be effective for describing cybercriminals. Here, criminals can use multiple phones or accounts to commit any crime, but the way of typing can not be changed. KD can also recognise the criminal's age [70], [71], gender [70], [72], handedness [28], [70], hand (s) used [11], [70], typing skill [73], and education level [74], which may help to identify the criminals using a conventional keyboard. It has also been reported that these clues can also be identified using a smartphone as well [75], [76]. The suspect's age, gender, handedness, and hand(s) used can all be used to identify them.
- *Emotion recognition:* Emotion depends on the cognitive load, which can be determined by the KD. KD could be used to detect psychological stress [32], depression and mania [77], Liar [78], could be useful in intelligent game controlling [79], measuring emotional stress level of programmers for difficulty level and length of programs [80], continuous monitoring of cognitive status [81], recognising learner's emotion and engagement in online learning [82], etc.
- *Mental health status monitoring:* Fine motor skills have a relationship with KD. By recognising this skill, KD could be used in the following areas - Parkinson's disease detection [83], [84], mental health monitoring using chat session [85], Alzheimer's disease prediction [86], mild cognitive impairment [36], clinical disability in multiple sclerosis [87], [88], quantification of traumatic brain injury [89], identifying spastic diplegia under cerebral palsy [90], stress monitoring [82].

F. COMMERCIAL APPLICATIONS

With academic research, many security firms have been working on KD. The following are the products, companies, and working principles of KD.

- *BioPassword [91]:* It was formed in 2002 by AdminOne Security in Washington, USA. It takes multiple samples (by default, 15) of usernames and passwords to train the model. BioPassword 4.5 is implemented for Windows NT/2000 servers. It is a software alternative to a hardware biometric solution.
- *AuthenWare [92]:* It was developed in 2006 by AuthenWare Corp., Florida, USA. It is a leading cybersecurity software provider focused on fighting against identity theft for larger enterprises. It takes either the username and password or any text to train the model. Likewise, it is based on "Nural" fuzzy logic. The company has developed several products based on KD. It uses two-factor authentication, which is accurate and transparent to the users.
- *Phylock gmbH:* It is a German-based product, awarded by a TV certificate for software quality, functional safety, and data security. It takes no password for security.
- *Pehavio Sec:* This company claimed, their product ensures that user accounts are always in the right hands. They developed apps for mobile and browsers for desktop environments. They fused the features of KD, mouse movement, pressure, and acceleration. Likewise, they claimed that it was useful for banking transactions.
- *Biochec:* It is two-factor authentication. This is a New York, USA-based product. It requires a user ID and password along with KD features.
- *TypeSense [93]:* It was developed by Deepnet Security, a London, UK-based company. It is a multifactor authentication method that combines voice, face, and KD. It was developed for an employee's flexible environment and uses auto-corrective training and adaptive learning.
- *DSGatewayTM:* It was developed by Delfigo Security in Boston, USA. It is one of the pioneers in the field of keystroke biometrics. It uses multiple factors, including device identity.
- *Behavio Sec [94]:* It is developed by a Sweden-based company. It provides a continuous authentication solution. It is being used for online fraud detection. Likewise, it has received many awards since 2012.
- *ID Control [95]:* Netherlands based company offers KeystrokeID. Here, no specific interaction is required to train the model. It covertly collects the patterns that are used in the e-government, e-business, and e-finance fields.
- *iMagicSoftware:* A California-based company provides a trustable password that is compatible with all browsers and across all platforms. Trustable Passwords Enterprise Suite is being used by many enterprises, such as health care, finance, oil, and gas. It helps websites to provide authentication, fraud prevention, and identity protection.
- *Probays:* It was developed by a French-based company. It uses Bayesian computing for KD in web applications.
- *Scant Analytics:* It was developed by a Washington-based company. For stronger authentication, they combined typing rhythm with IP address and browser information such as cookies.
- *TypingDNA [96]:* It was developed by a New York, USA-based company. It was started in 2014 and released its first product in 2016. Here, user-friendly authentication replaces SMS. It provides secured identity verification without having to whip out the phone. It uses simple captcha codes.

G. INCREASING RESEARCH TREND (CONTRIBUTION TO OB2)

The latest trend in authenticating and identifying users is through the potential of biometrics [97]. Recently, KD on smartphones has gained popularity because of the sensor technology attached to the smartphone. After releasing Android 2.3 in 2010, the gyroscope, accelerometer, and rotation became important features [98]. These give the extra opportunity to present the orientation of the phone and the forces in different directions while typing, zooming, and browsing and provide a logical pattern to verify the users and the determination of several useful pieces of information for interesting applications (auto profiling, age-gender specific product recommendation, neural disease diagnosis, etc.).

As with the increasing trend of using sensors, technology creates opportunities and challenges for developing the next version of KD-based systems. It has become a buzzword in recent years in academic and commercial circles because of the viability of using the multiple sensors attached to each smartphone, transparency to the user, and a non-invasive and covert method of data collection. The number of publications in recent years and the increasing trend in KD research has been presented in Fig. 4.

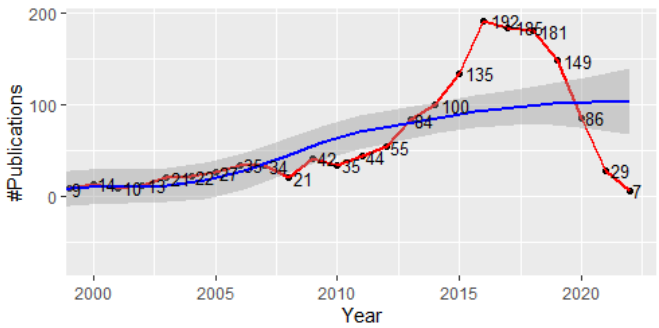

FIGURE 4. KD-based research trend: Number of publications during the recent years. Line in red (bold) represents the number of publications in the respective years. The line in blue (thin) represents the increasing trend of KD research

The most recent publications, taking into account the environments, input types, and sizes chosen, features considered, and classification methods used, are shown in Fig. 5. Figure shows that 50.49% of articles are published in the form of journal. KD for desktop/laptop has been studied at 52.23%. As an input type, 52.99% of studies used free-text inputs. In the case of predefined text, 36.01% of studies have been conducted for short text. A large number of studies (60.98%) used temporal features for their studies. As a classifier, 25.39% of studies used Neural Networks in their implementation. These statistics represent the current state of KD-based models as well as significant research needs. In 5.87% of research, KD features with wearable IoT devices (i.e., Implantable Medical Devices) for Electroencephalography (EEG) and Electrocardiogram (ECG) data were investigated. Similarly, a smaller proportion of research (25%) investigated combination characteristics.

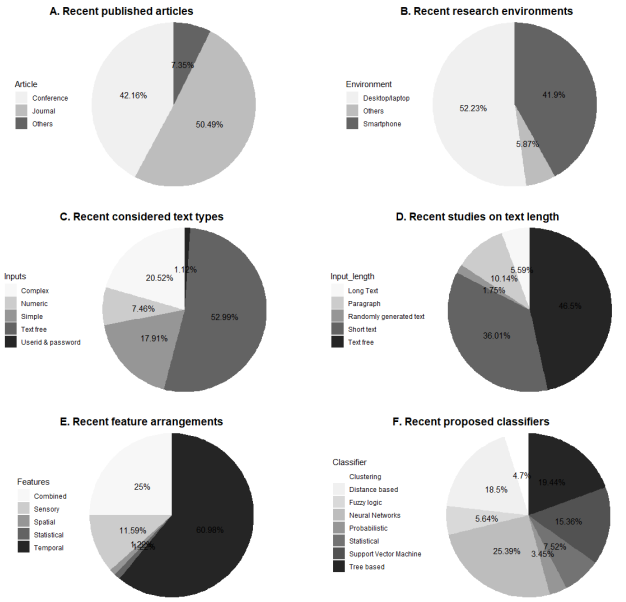

FIGURE 5. The latest publication (between 2017 and 2022) statistics on the various domains of KD. Fig. A - Percentage of publications in the form of journals, conferences, and others (book chapters, workshops, patents, theses, etc.), Fig. B - Percentage of studies with data collected from desktop/laptop keyboards, smartphones, and others (IoT enabled devices), Fig. C - Percentage of studies considering different input types, Fig. D - Percentage of studies considering different input lengths, Fig. D - Percentage of studies considering different feature arrangements, and Fig. E - Percentage of studies approaching different classifiers

The following are the research areas where researchers are interested - (a) Improving accuracy through techniques such as feature fusion [99], [100], score fusion [101], [102], feature selection [103], [104], anomaly detection [105], [106], and others. (b) Domain adaptation for cross-device validation [107], [108], (c) Real-world dataset collected using IoT-enabled device with typing patterns [109], some times data are being collected in different positions [110] through a variety of applications like arithmetic games [111], e-wallet [112], video clips for emotional changing [113], (d) Usability control specifically in active authentication where data are being captured continuously [114], to balance the device and application levels security, (e) Computation and energy consumption specifically in the area of a smartphone where battery power is limited [110], (f) Design some useful intelligent applications including auto-profiling user [40], disease prediction [32], age-restricted security control, gender-specific advertisement, password recovery mechanism [115]. For beginners, these provide a clear understanding of how to identify the main area of KD-based research.

III. METHODOLOGY

We have followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses 2020 (PRISMA 2020) guidelines [116] for systematic review and meta-analysis.

A. PLANNING AND REVIEW NEEDS

The primary purpose of this systematic review is to outline the use of KD attributes in various system designs in order to provide a comprehensive review of KD-based models. A systematic review is necessary to address particular problems in order to achieve focused KD-based models, individual discoveries leading to common outcomes, and new arrangements for future approaches. Heterogeneity and bias across studies need to be understood with this review to aggregate the findings and missing studies. The PRISMA 2020 protocol's step-by-step methodology [116] has been followed for this systematic review.

B. ELIGIBILITY CRITERIA

Because the evolution of each KD-based model measure is unique, it is impossible to summarise the findings using the same assessment technique. The KD-based model is classified into three parts: verification, identification, and prediction. Each of these categories is broken further into static and dynamic modes. Desktops and smartphones, on the other hand, are categorised in each section as data acquisition devices. As a consequence, present study has been classified into 12 categories (3 (verification, identification, and prediction) $\times$ 2 (static and dynamic modes) $\times$ 2 (desktop and smartphone)).

C. INFORMATION SOURCE

We have collected the articles from six reputed databases with a single search key, as depicted in Table 2 from January 1st, 2017 to March 13th, 2022. The most recent search was conducted on April 22nd, 2022. However, the first item was added to Mendeley on March 25th, 2017, and we continued to add auto-suggested articles on KD.

D. INCLUSION-EXCLUSION CRITERIA

We have chosen journals, edited books, and conference articles published in English between 2017 and 2022 (1st April). Then we used Mendeley for article duplication. We deleted duplicate articles and chose only quantitative research for the meta-analysis. However, we considered recent high-quality studies for descriptive statistics in feature, classifier, and device selections. To extract information, we have divided the articles into 12 groups (depending on environments and KD-based models) by primary screening. The steps in the inclusion of an article have been presented in Fig. 6 as per the recent guidelines.

E. DATA COLLECTION PROCESS

We have set up a Google sheet to collect data from each article. We then extracted all the following information from the selected articles - authors' name, the title of the article, year of publication, subjects, results (in specified metrics), available standard deviation or confidence interval, category (ViSM, ViDM, IiSM, IiDM, PiSM, or PiDM), environment (desktop, smartphone, or other), feature set (temporal, spatial, sensory, contextual, or combined), classification techniques (one or multi), used datasets (public or own), data acquisition protocol (application interface, duration, controlled or uncontrolled environment, etc.), special arrangement in developing datasets (for developing own), publication information, and traits (for predictive models only). To achieve the findings and variations in the outcomes, many formulae and techniques were employed. In several situations, we conferred with co-authors about exact measures. The first article was reviewed on February 18th, 2020. Searching, downloading, and data gathering were all extended until April 1st, 2022.

F. STUDY RISK OF BIAS ASSESSMENT

To summarise the findings, we utilised the forest plot and the inverse variation technique. We have utilised a funnel plot to identify bias and missing research.

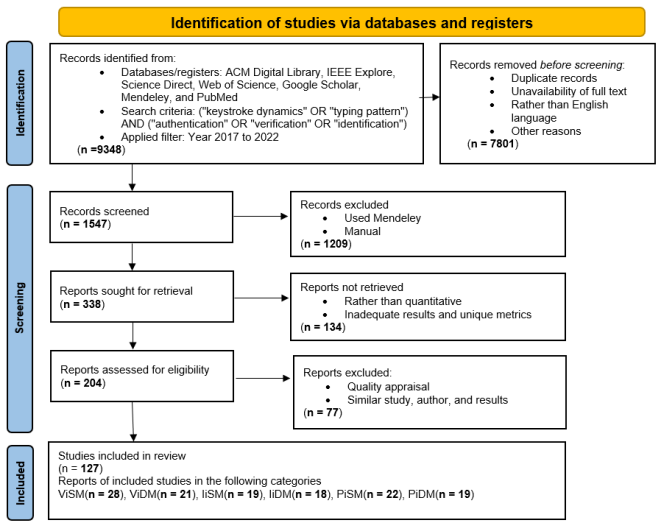

FIGURE 6. Flowchart of the study selection, search criteria, screening, inclusion strategy, and study categorization. This flowchart enables us to select the suitable articles in each category

IV. DATA ACQUISITION PROTOCOLS AND SHARED DATASETS

A. SHARED KEYSTROKE DYNAMICS DATASETS (CONTRIBUTION TO OB3)

In KD research, more time is spent on the data acquisition section than on addressing challenging issues, because data acquisition is the most fundamental and essential part of any behavioural biometric system like KD. As a result, various datasets have been produced with different experimental setups. Researchers developed datasets, considering only their temporal requirements and method of application. Separate datasets are suitable in different application domains. For the latest studies, many datasets have been created, but the authors have not shared their datasets because of privacy issues. Only a few (below 4%) datasets have been shared.

TABLE 2. Source of studies, search criteria, and number of articles found. While the syntax is different, the search key is the same for each database. Date criteria were added by filtering where date search could not be made part of the search key

Database	Search key	#Studies
ACM Digital Library	[[Title: keystroke dynamics] OR [Title: keystroke biometrics] OR [Title: typing behaviors] OR [Title: typing patterns] OR [Title: touch dynamics] OR [Title: touch analysis]] AND [[Title: authentication] OR [Title: verification] OR [Title: classification] OR [Title: identification] OR [Title: recognition]] AND [[Abstract: keystroke dynamics] OR [Abstract: keystroke biometrics] OR [Abstract: typing behaviors] OR [Abstract: typing patterns] OR [Abstract: touch dynamics] OR [Abstract: touch analysis]] AND [[Abstract: authentication] OR [Abstract: verification] OR [Abstract: classification] OR [Abstract: identification] OR [Abstract: recognition]] AND [Publication Date: (01/01/2017 TO 12/31/2022)]	826
IEEE Xplore	("Keystroke dynamics" OR "Keystroke biometrics" OR "Typing behaviors" OR "Typing patterns" OR "Touch dynamics" OR "Touch analysis") AND ("Authentication" OR "Verification" OR "Classification" OR "Identification" OR "Recognition")	186
Science Direct	("Keystroke dynamics" OR "Keystroke biometrics" OR "Typing behaviors" OR "Typing patterns" OR "Touch dynamics" OR "Touch analysis") AND ("Authentication" OR "Verification")	2593
Google Scholar	("Keystroke dynamics" OR "Keystroke biometrics" OR "Typing behaviors" OR "Typing patterns" OR "Touch dynamics" OR "Touch analysis") AND ("Authentication" OR "Verification" OR "Classification" OR "Identification" OR "Recognition")	5400
PubMed	("Keystroke dynamics"[Title/Abstract] OR "Keystroke biometrics"[Title/Abstract] OR "Typing behaviors"[Title/Abstract] OR "Typing patterns"[Title/Abstract] OR "Touch dynamics"[Title/Abstract] OR "Touch analysis"[Title/Abstract]) AND ("Authentication"[Title/Abstract] OR "Verification"[Title/Abstract] OR "Classification"[Title/Abstract] OR "Identification"[Title/Abstract] OR "Recognition"[Title/Abstract] "Recognition")	5
Mendeley	Auto suggested articles were added	338
Total		9348

1) Shared keystroke dynamics datasets collected through conventional keyboards

Many datasets were produced using a variety of keyboards, but few of them have been shared. Most of the datasets were collected for predefined texts that are well suited for static authentication and applicable at entry-point security. A few datasets were developed for predefined paragraphs or randomly generated texts that are well suited for continuous authentication, and applicable for active authentication. In some cases, personal information about users, such as their age, gender, handedness, hand(s) used, and typing skills, is available and could be used in predictive models and soft biometric techniques. There are a few datasets were developed from patients diagnosed with early-stage Parkinson's disease (PD) disease for the determination of PD using KD attributes. Since the typing pattern changes throughout the day or in between two days, samples of the user need to be collected in multiple sessions with several repetitions. Some of the few datasets that were developed in one session will not be suitable for developing user authentication or identification systems. The following is the list of shared datasets collected using the conventional keyboard of desktop or laptop devices.

- *LOY2004:* This dataset was collected by Loy et al. in 2004 in their study [117] for introducing the pressure feature in KD. They used a pressure-sensitive special keyboard to develop the patterns. It could be useful to show the impact of pressure on KD-based systems. However, this dataset was produced only in one session for the purpose of developing a user identification system in a static model based on pressure data.
- *DSN2009:* This dataset was collected by Killourhy and Maxion in 2009 in their study [65]. The popularity of the dataset in terms of the large number of samples collected from each subject in multiple sessions. This dataset is common in the KD community for designing ViSM model for desktop environment.
- *GREYC2009:* This dataset was collected by Giot et al. in 2009 in their study [118]. The popularity of the dataset in terms of a large number of subjects and the reasonable number of samples and repetition were considered. This is one of the most commonly used datasets for ViSM on the desktop environment.
- *CMU2012:* This dataset was collected by Killourhy in 2012 for a PhD thesis [73]. It contains samples of three unique types of text and is popular for many samples. This is useful for text type analysis in the desktop environment for static user authentication (ViSM).
- *GREYC-NISLAB:* This soft biometric KD dataset was created by Idrus et al. [119] in 2013 in their study of soft biometric trait identity prediction. The speciality of this dataset is that it contains soft biometric traits like age, gender, and handedness. It could be used in ViSM, IiSM, and PiSM designs for desktop environments.
- *YZUN soft biometric keystroke:* This dataset was collected by Uzun et al. [71] in 2016 to identify the age group, children, and adults. The speciality of the dataset is that it contains many samples from child users. This dataset is useful in identifying the age group (below 18) to protect kids from online threats in a desktop environment.
- *KBOC 2016:* This dataset was collected by a study [120] for different passwords from 300 participants in 4 sessions with 28 repetitions. They only recorded the timing features and used a desktop keyboard with a 40 ms clock resolution machine. It is suitable for designing one-time user authentication (ViSM).

- *BeiHang:* The study [121] collected a dataset of usernames and passwords from 117 participants in both online and offline modes. They collected the standard timing features of dwell time and flight time. It is suitable for designing one-time user authentication on a desktop (ViSM).
- *Buffalo's:* This dataset [122] collected KD and mouse dynamics features for long text through a QWERTY keyboard from 157 participants in 3 sessions and 1 repetition. They collected the typing and mouse activities for 50 minutes. It is well suited to designing continuous user authentication (ViDM).
- *Si6 k-profile:* This dataset [123] collected split sentences from literature through a web-based application from 63 participants in 66 sessions. It is suitable to design a distance-based continuous user authentication system (ViDM).
- *Clarkson:* The dataset [124] collected the timing features from 39 participants in 2 sessions through a QWERTY keyboard in offline mode. This dataset is well suited for designing fixed and free text user authentication (ViSM and ViDM) on a desktop computer.
- *BIOCHAVES:* A study [125] collected the timing features for a paragraph through the Brazilian layout keyboard in offline mode from 47 participants. They collected the dataset for several simple, daily used, short texts as well as free text. It is also suitable for fixed and free text system designs (ViSM and ViDM).
- *Calot:* Another study [126] collected timing features for any text using a desktop keyboard from 409 participants, suitable for active authentication (ViDM).
- *neuroQWERTY Parkinson's:* The dataset (neuroQWERTY MIT-CSXPD) was developed by a study [127]. This dataset is useful for developing and testing the PD detection model. This is a well-balanced dataset for PD, which was collected using the conventional keyboard of the Lenovo G50-70 i3-4005U. Here, only the timing features were collected from the 42 early-stage PD patients, and 43 healthy control subjects. It is well suited for PiDM design.
- *Tappy Parkinson's:* Another dataset [128] collected timing features from 200 users through the desktop keyboard for designing the predictive model for detecting PD (PiDM).
- *Lie detection:* A study [129] collected timing features from 60 participants to design a liar detection model using the KD method.

2) Shared keystroke dynamics datasets collected through smartphones

Shared KD datasets collected using phones are limited. However, the attached sensors of smartphones increase the features' collectability power. The following is the list of datasets collected using smartphones for smartphone security, stress determination, etc.

- *RHU Keystroke:* This dataset is collected by Abed et al. in 2014 in the study [130]. The speciality of the dataset is that it is collected through a Windows phone app to introduce KD in the mobile environment. It is useful for static user authentication (ViSM) in a mobile environment where no advanced sensors are not equipped.
- *MOBIKEY:* This KD of a mobile dataset was created by Antal et al. in 2016 in the study [131]. The speciality of the dataset is that it contains more advanced features like pressure, accelerometer, and velocity along with timing features. Different types of inputs were considered. This dataset is useful for entry-point user authentication (ViSM) where advanced sensors are attached.
- *HMOG:* This dataset is collected by a study [132] for continuous authentication of smartphone users. This dataset contains the pattern which describes how a user grasps, holds, and taps on the smartphone. It is well suited for ViDM design in a smartphone environment.
- *Touchalytics:* This dataset was collected by a study [133] using four smartphones and 41 users. It contains the pattern of how a user swipes and strokes while reading text and capturing images on a touchscreen. It is well suited for continuous user authentication (ViDM).
- *Antal:* This dataset is collected by a study [134] while scrolling by 71 users using eight smartphones, well suited for active authentication.
- *Teh:* This dataset was collected by a study [135] for three different scenarios: as usual, controlled, and different location environments through different sizes of smartphones, tablets, and laptops from 150 participants. It is well suited for designing the PIN security (ViSM) of mobile devices.
- *Coakley:* A study [136] collected this dataset from 52 users using smartphones for a fixed-size, 10-digit number. Several features were recorded, including timing, gyroscope, and touchscreen-based features. It is well suited to designing ViSM models using advanced sensory features.
- *Yuksel:* The dataset [112] was collected for randomly generated texts using smartphones. The sensors' data, including gyroscope and accelerometer readings at 60 ms intervals, were collected for 76 participants by running a mobile wallet application.
- *Kim:* Another study [137] collected timing, rotational, and touch screen features for 20 predefined texts from 50 participants. It is suitable for validating ViSM models for unique inputs.
- *Stress:* A study [32] created this dataset for emotional stress (ES) detection. They collected data from 46 participants. An extended version of their dataset was collected from 95 users and is available online. Here, data were collected through smartphone devices. There are 112 features, including gyroscope, accelerometer, magnetometer, proximity, light, and orientation data. These data samples were collected during a stressful task (the task should be completed on time) from 95

users. Similarly, non-stress full data was collected from the same user without being time-bound. It is well suited for PiDM model for the determination of ES.

We summarised the details of the data acquisition protocols in the following tables. Since data acquisition protocols are different in fixed (static) and free (dynamic) text modes. We used separate tables for each. Table 3 presents a brief view of the shared datasets collected for predefined texts. These datasets do not meet the criteria for active or continuous authentication. However, a few datasets are available for both smartphone and desktop active authentications, listed in Table 4. The list of the shared dataset is large, however, each dataset is developed through unique data acquisition protocols. In the case of fixed input datasets, mainly three types of texts were considered - Simple (S), Complex (C), and Numeric (N) in different lengths. Whereas key duration (KD) and latency time (L) were commonly used features collected using QWERTY of AZERTY keyboard layouts. It is essential to understand how the performance of KD-based models varies as inputs or input types vary.

B. DATA ACQUISITION METHODS AND TOOLS (CONTRIBUTION TO OB4)

Data acquisition is the most essential part of KD-based study. In this process, a powerful and efficient keystroke capture tool is required that can capture the multidimensional feature vectors needed to build up a strong dataset. A study [141] collected only the time interval features by using an IBM-compatible PC-based data acquisition system implemented by FORTRAN and assembly language programming in 1996. A study [142] developed Java-based data acquisition tools, and they developed a web-based applet to collect the keystroke patterns from various (uncontrolled) locations. Another study [143] developed a TouchLogger based on JavaScript to get the accelerometer and gyroscope data while typing on a touch screen. Different tools have been developed to meet the demands of the security domain.

A study [144] developed an application for the Android mobile platform to collect data on the way individuals draw lock patterns on a touch screen. Another study [145] developed another Android app to get the timing parameters along with fingertips, size, and key pressure. Various apps were created in various computer languages for various objectives, but the majority of the time, Java Applets were used to collect data on the desktop and JavaScript was utilised in a web-based environment. Nowadays, JavaScript APIs (Application Programming Interfaces) of different sensors are available to get the data of gyroscope, accelerometer, and accelerometer including gravity, for the advancement of the KD-based system.

Data acquisition methods with special arrangements are described in Table 5 and Table 6. It will help the researcher to develop benchmark datasets in unique configurations.

C. SCENARIO SELECTION (STATIC OR DYNAMIC MODE)

The KD model can be classified into two main types - (a) *static/fixed*, where one predefined input is used to train and test the model, and (b) *dynamic/continuous*, where the input is free. The trend of these models has been presented in Fig. 7. As per the statistical measurement in the figure, continuous and fixed-text scenarios have been studied almost equally in the recent past. Due to the unstructured patterns in continuous mode, the performance of these patterns is not much more impressive than in fixed-text mode. However, the continuous mode has the extra advantage of restricting session hijacking. A summary of studies undertaken in the last six years has been described in Table 7. In static models, numeric, simple, and sometimes complex types of text like passwords were considered. On the other hand, some studies have yielded good results by reorganising any activity without relying on inputs. Therefore, the data acquisition protocol is different depending on the mode.

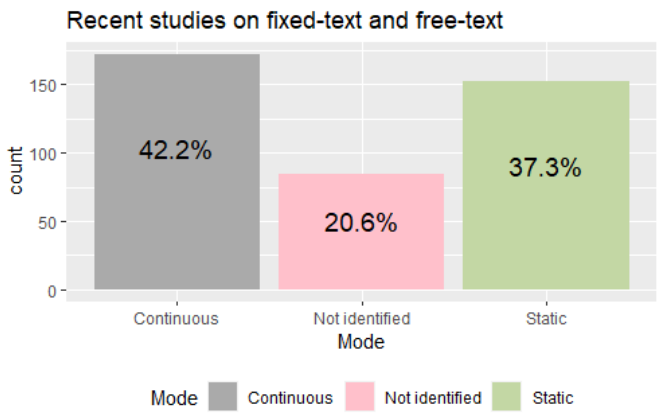

FIGURE 7. The percentage distribution of the most recent research included fixed texts for static authentication and free text (continuous) for active authentication. It demonstrates that continually produced patterns outnumber fixed text inputs

D. INPUTS SELECTION

Numeric inputs with different lengths (4, 6, 8, and 10 digits) for predefined inputs have been identified in the literature. However, most of the studies considered simple daily-used words because users constantly type these inputs, which are very useful for recording natural typing patterns. This text can be classified as short, medium, or sometimes paragraphs or sentences. A few studies tested the validity of KD-based systems on password-related typing using complicated inputs such as passwords. Captcha selection has also been observed in several studies. These captcha-typed texts are short, but they are as complex as a password. The percentage distribution of the latest studies that considered different input lengths has been presented in Fig. 8. Short inputs have been reported to be extensively analysed.

The continuous model is quite useful to prevent attacks like session hijacking. In this case, there are not only typing

TABLE 3. Detail of data acquisition protocols for some of the few publicly available KD datasets for ViSM and IiSM. Bold-faced text indicates that the dataset was collected through smartphones

Dataset name	Input	Input type	Features	#Sub.	#Rep.	#Ses.	Device
LOY 2004 [117]	"try4-mbs"	C	P, L	100	10	1	Special keyboard
DSN 2009 [65]	".tie5Roanl"	C	KD, L	51	50	8	QWERTY
GREYC 2009 [118]	"greyc laboratory"	S	KD, L	100/133	12	4	AZERTY
GREYC-NISLAB (P1, P2, P3, P4, P5) [119]	"leonardo dicaprio", "the rolling stones", "Michael schumacher", "red hot chilli peppers", "United States of America"	S	KD, L	110	10	2	AZERTY and QWERTY
CMU2012 (P1, P2, P3) [73]	"412 193 7761", "hester", ".tie5Roanl"	N, S, C	KD, L	40, 38, 65	50, 50, 50	4, 4, 8	AZERTY Keyboard
RHU Keystroke [138]	"rhu.university"	S	KD, L	51	5	3	Nokia Lumia 920
MOBIKEY (P1,P2,P3) [131]	".tie5Roanl", "kicsikutyatarka", "Kk-tsf2!2014"	C, S	L, P, V, A, D, etc.	54	>30	2	Nexus 7 tablet, Mobil LG Optimus L7 II P710
UZUN (P1,P2) [71]	"Mercan Otu", ".tie5Roanl"	S, C	KD, L	100	5	1	QWERTY keyboard
KBOC 2016 [120]	Different passwords	C	KD, L	300	4	28	Collected through online competition
BeiHang [121]	User name and password	S	KD, L	117	-	-	Collected in both online and offline modes
Teh [135]	"5560", "1379666624680850"	N	KD, L, P, Area	150	-	-	Featured phones, smartphones, digital tablets and laptops
Coakley [136]	"914 193 7761"	N	KD, L, P, Area, A, V	52	10	30	Five identical Android LG-D820 Nexus 5

#Sub.->Subject, #Rep.->Repetition,#Ses.->Session, C->Complex, S->Simple, N->Numeric
P->Pressure, KD->Key duration, L->Latency, V->Velocity, A->Acceleration, D->Distance

TABLE 4. Detail of data acquisition protocols for some of the few publicly available datasets for ViDM and IiDM. Bold-faced text indicates that the dataset was collected through a smartphone

Source	Activity	Features	#Subject
HMOG [132]	Grasp, holds, taps (60 features)	Orientation, acceleration, magnetometer data at 100Hz	100
Touchalytics [133]	Swiping direction, velocity, stroke direction (30 features)	Variable frequencies (median of 17ms)	41
Antal [134]	Horizontal and vertical scrolling	Time, touch co-ordinates, pressure, fingertips size	71
Yuksel [112]	Typing randomly generated texts	Gyroscope and accelerometer at 60ms interval, soft biometric traits, statistical features	76
Kim [137]	20 predefined texts	Timing, gyroscope, accelerometer, rotation, touchpoint, statistical features	50
Calot [126]	Text free character typing	Timing features	409
Dhakal [139]	Text free character typing	Timing and statistical features	168000
Buffalo's [122]	Character typing for long text	Mouse co-ordinates, timing of key press, release, left click	157
LASER 2012 [140]	Character typing for a paragraph	KD, Latency time	20
Si6 k-profile [123]	Character typing for split sentences from literature	Digraph time	63
Clarkson [124]	One hour of character typing	KD, Latency, Digraph, Trigraph	39
BIOCHAVES [125]	Character typing for a paragraph	DD	47

patterns, but also a variety of activities that can be measured for better quality active authentication models. Some of the few studies considered shaking, tapping, scrolling, and dragging on a mobile screen.

The trend of selecting inputs has been presented in Fig. 9. The majority of recent research favoured text-free inputs. The user's cognitive burden will be low in the case of simple text, which may result in persistent patterns. It lowers the rate of false rejection. Text-free, on the other hand, is a simple and easy-to-use interactive solution.

E. DEVICE SELECTION

The selection of data acquisition devices is also important with input selections. Several recent studies have noted whether KD models are not only made on products produced from conventional keyboards but have also used various smartphone devices and IoT devices. Researchers select the devices that must have the ability to acquire the multidimensional features at a certain frequency [47]. Several studies used a variety of data acquisition devices to validate KD-based models. Different types of input devices (smartphones and tablets with different screen sizes) have been used for cross-device validation. At the same time, the selection of

TABLE 5. Special arrangements in desktop/laptop environment to develop datasets to meet the specific objective. It demonstrates how patterns for fixed-text and continually typing free text were created using a number of apps with varying sample rates. It provides a multitude of directions for future dataset development

Study	Year	Env.	Type	Special arrangement	Objective
[146]	2017	D	F	HTML and Javascript	To collect KD data through web-page
[147]	2017	D	F	Implemented in python micro framework flask	Web-based application to collect KD data
[148]	2017	O	C	Data sampling rate at 100Hz	For down sampling to 50Hz, 30Hz, 10Hz, 3Hz as per demand
[149]	2018	D	C	VB .NET for windows form application	To collect KD data for frequent English terms
[139]	2018	D	F	HTML, CSS, and JavaScript	To collect typing style while transcribe 15 English sentences
[150]	2018	O	F	Triboelectric Nanogenerator	For developing intelligent keyboard
[151]	2019	D	C	HTML, JavaScript and MySQL	To collect KD data from students through online courses
[152]	2019	D	F	JavaScript	To collect KD data for web-based password driven systems
[153]	2019	D	F	Django web app	To collect KD data
[154]	2019	D	F	Kotlin language, JavaFX	To collect KD data with sound
[155]	2019	D	F	HTML and JavaScript	To collect KD data via crowdsourcing
[156]	2019	D	C	Application developed by VB C#	To collect KD data continuously
[157]	2019	D	C	"Pynput" keyboard event listener library	To collect KD data
[158]	2019	D	C	Copy task and email, copy task and academic writing	To understand the cognitive loads for different task
[159]	2020	D	C	Java	To collect 20 mins. of typing
[60]	2020	D	C	EEG while typing	To collect EEG signal at 1000Hz while typing
[160]	2020	D	F	ASP.Net and VB.Net	To collect KD data for web-based security
[161]	2020	D	F	Five different tasks were given	To collect KD data in virtual education
[162]	2021	D	F	Converted timing features to barcode	To classify barcodes
[163]	2021	D	F	Collected EEG data with keystrokes	To implement multimodal biometric system
[1]	2022	O	F	Collected keystroke trajectory feature	To implement multimodal biometric system
[164]	2022	O	C	Designed Loggerman application	To collect heart rate variability while typing

Env.->Environment, D->Desktop/Laptop, O->Other devices like wearable, IoT devices, EEG->Electroencephalography, F->Fixed-text, C->Continuous

TABLE 6. Special arrangements in smartphone environment to develop datasets to meet the specific objective. It demonstrates a variety of apps for collecting real-world data under various data acquisition protocols

Study	Year	Env.	Type	Special arrangement	Objective
[165]	2018	S	C	Data collection from four different scenarios	For position validation
[166]	2018	S	C	100Hz sampling	To collect patterns while walking
[167]	2018	S	C	App to collect sensory readings at 50Hz	Rate was empirically found suitable
[168]	2018	S	C	2 mins.	To collect touchscreen gesture
[169]	2018	S	F	Data collected in every 0.004Sec.	To improve the performance of KD systems
[170]	2018	S	C	Used different sampling rates: 48kHz, 96kHz and 192kHz	Higher sampling rate can achieve more accurate
[171]	2018	S	C	Used sampling rate 50Hz	To collect continuous patterns of activity
[172]	2018	S	C	Used sampling rate 100Hz	To collect continuous patterns of activity
[173]	2018	S	C	Device Analyzer app	To collect multimodal data
[174]	2018	S	C	Collected in five unique contexts and five positions	To understand the performance in different contexts and positions
[175]	2019	S	C	20ms interval data collection	To collect gesture-typing interactions in a word-independent format
[176]	2019	S	C	BrainRun educational game	Develop dataset for implicit authentication
[83]	2019	S	C	iPrognosis application	To detect Parkinson's patient data
[35]	2019	S	C	TypeOfMood (Android app)	Depressive disorder
[112]	2019	S	F	Wallet application	To collect real environmental KD data
[177]	2019	S	F	JAVA language	To develop password hardening models
[178]	2020	S	F	Developed mobile app	To check the effect of position
[137]	2020	S	C	Used languages English and Korean	For language dependent patterns
[32]	2020	S	C	Orientation is limited in portrait mode	To collect the pattern in one scenario
[179]	2020	S	C	Develop BiAffect (Mobile app)	To investigate the effects of mood, age, and diurnal patterns

Env.->Environment, S->Smartphone, F->Fixed-text, C->Continuous

such devices is important since the devices vary in different ways, such as size, type, clock resolution, etc.

A few latest studies used TOSHIBA Dynabook RZ82/T [189], MacBook Pro [206], ASUS K56C [207] for laptop security. A study [208] used Emotiv EPOC to measure cognitive load in addition to KD features while typing on a device with limited sensors like a conventional keyboard. Some IoT devices, like FLORA 9-DOF LSM9DS0 and Pulse Sensor Amped [209], Samsung Gear Live Smartwatch [210] also be used in the same process to monitor the high dimension features.

The percentage distribution of the latest considered environments has been presented in Fig. 10. The figure indicates that KD on smartphones is gaining popularity. However, the

TABLE 7. Different texts and the studies for static and continuous models in different environments in the latest research. It motivates new KD researchers to pick inputs according on user appropriateness or situational demands

Input	Interaction type	Example	Studies	Purposes	Env.
Numeric	4 digits PIN	"1111", "1234"	[180]	S	A, D, T
	6 digits PIN	"766 420"	[169], [181]–[184]	S	D, T
	8 digits PIN	"92092401"	[185]	S	D, T
	10 digits PIN	"9468553594"	[168], [186]	S	D, T
Simple	Daily used words	"Kolkata"	[29], [187]	S	D, T
	Common words	"the", "is", "to", "it"	[149], [175], [188]	S, C	D, T
	Chat	"Hello"	[103], [111]	C	D, T
	Family name	-	[189]	S	D, T
	C code	-	[170]	C	D, T
	Paragraph	Paragraph from a literature	[156], [190]	C	D, T
	Sentences	"A quick brown fox jumps . . . "	[74], [191], [192]	S, C	D, T
Complex	Password	".tie5Roanl", "tie5Roalnb"	[25], [182], [193]–[198]	S	D, T
	Randomly generated	CAPTCHA	[112], [199]	S	D, T
Word independent	Typing	Any text	[175]	S, C	D, T
Activity	ShakeIn	Picking up phone calls	[200]	S	T
	Sketch	Graphical password	[23]	S	T
	Swipe	Web-surfing	[176], [201], [202]	S, C	T
	Zoom (in/out)	Picture browsing	[171], [203]	C	T
	Holding	Orientation	[204]	S, C	T
	Tapping	Playing game	[176], [176], [205]	C	T

Env.->Environment, S->Static model, C->Continuous model,A->ATM machine, D->Desktop/Laptop , T->Touchscreen phone

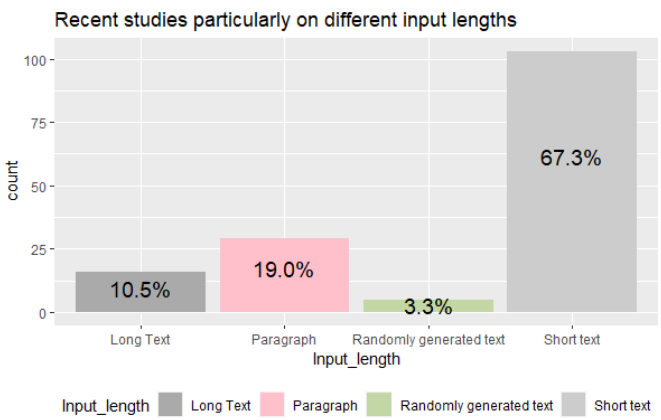

FIGURE 8. The percentage distribution of the lengths of the most recently considered inputs. It demonstrates that shorter sentences were given more weight. However, random sentences, paragraphs, and long texts were also examined

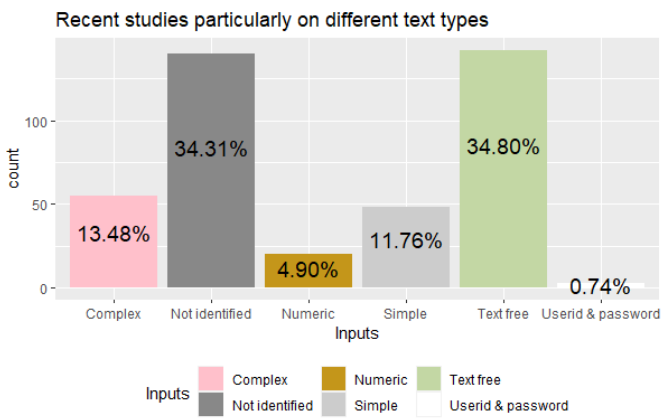

FIGURE 9. The percentage distribution of the most recent research for various inputs. It demonstrates that free-texts were evaluated in addition to simple, numeric, complicated, or user ID and password. However, free text is being researched more extensively

desktop environment is also popular in several studies.

F. SUBJECT SIZE AND SUBJECT SELECTION

Generally accepted that the experiment includes a large number of subjects to signify the scalability of the study. But in KD research, most of the studies included a small number of subjects (less than 50). In some few cases, the subject size is large. A few studies [155], [179], [211] included 250 subjects where a study [212] considered 300 subjects. A study [213] included 283 subjects, while some of the few studies [102], [214]–[217] considered more than 300 subjects. A recent study [218] used GPower for estimating sample size.

In KD research, most of the studies included patterns collected from college or university students, teachers, support staff, etc. which do not represent the global population. Careful consideration in selecting the participants is needed since the typing pattern varies depending on age group, gender, experience level at a keyboard, education level, etc.

G. MAINTAINED SESSION AND INPUT REPETITION

In biometric science, specifically behavioural biometrics, samples in different sessions are captured for mainly two reasons - (a) to verify the model performance, and (b) to update the stored template. Therefore, a large number of

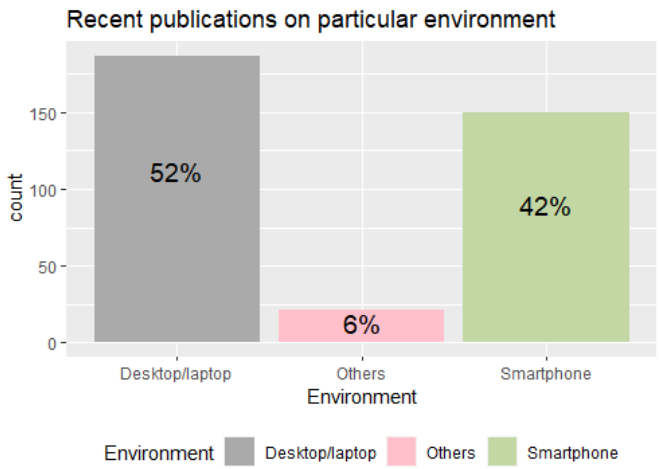

FIGURE 10. The percent distribution of the most recent research in distinct contexts. It demonstrates that smartphones and other IoT devices are equally appealing to the desktop/laptop environment (EEG, wearable smartwatches, etc.)

samples from different sessions need to be recorded. Almost all studies used a session below 20.

To generate the biometric template, a large number of input repetitions are needed to build a more robust model. In the literature, we found that fewer than 50 inputs have been considered in almost all cases.

H. DURATION AND INTERVAL

A study [77] collected the data for 8 weeks for continuous authentication. Similarly, some of the studies [219]–[221] collected the data only for 2 weeks. Another study collected data for 3 weeks. Some studies [156], [222] collected for 6 months, whereas a study [223] considered only one month. Differently, a study [175] collected the patterns until 100 words were typed.

Some studies collected the pattern for a short period. A study [209] used 12 sec. Another study [224] used 20 sec. Similarly, a study [190] used 4 mins. A bit higher time (15 mins.) has been used by some studies [225], [226]. Another recent study [107] used two different time durations (30 mins. and 55 mins.). A study [112] used 60 ms interval for the 1-minute duration of typing.

I. TYPING POSITIONS

In the case of a desktop environment, the position is not frequently varied. But positions may change (sitting on a chair to sitting on a bed) while considering the laptop environment. On the other hand, smartphone positions based on the user's sitting, standing, walking, laying, downstairs, upstairs, etc. positions are frequently changed. The limited study collected the pattern in different positions. A study [167] collected the patterns in four different positions. Another study [110] collected the pattern in four positions, keeping three positions the same as the previous. There are few studies [175], [178], [227] used the patterns collected in two to three positions.

V. FEATURE EXTRACTION AND NORMALIZATION (CONTRIBUTION TO OB5)

Researchers carry the feature extraction process for selections from the universal features that are distinctive and readily available to all the user's typing patterns. In KD, motor behaviour, motion behaviour, and pressure behaviour feature subsets can be captured. But motor behaviour features are common on many keyboards and can be applied to a touch screen device. Although, motion behaviour can only be used in a touch environment, where pressure can be measured with a pressure-sensitive keyboard.

Researchers often use two features - key hold and latency times in desktop/laptop environments. Key hold time refers to the time between pressing and releasing a single key, and latency time refer to the time between pressing and releasing two successive keys. Researchers used a series of key hold times and latency times in most of the previous approaches. Nowadays, the timing features are not limited specifically to the touch screen, since a variety of advanced features are easily available in recent smartphones.

This section illustrates how a variety of factors may be utilised as a feature set, how features can be retrieved in various ways, and what advanced features can be added in the next conceivable feature arrangements.

A. FEATURE TREND

Fig. 11 presents the percentage distribution of the feature arrangements in the latest studies from the year 2017 to 2022. Temporal characteristics have been extensively researched in both the desktop and smartphone domains. The other features, on the other hand, are exclusively found in smartphones. Here, the combined feature implies that the objective is to increase performance by combining sensory, spatial, and temporal features.

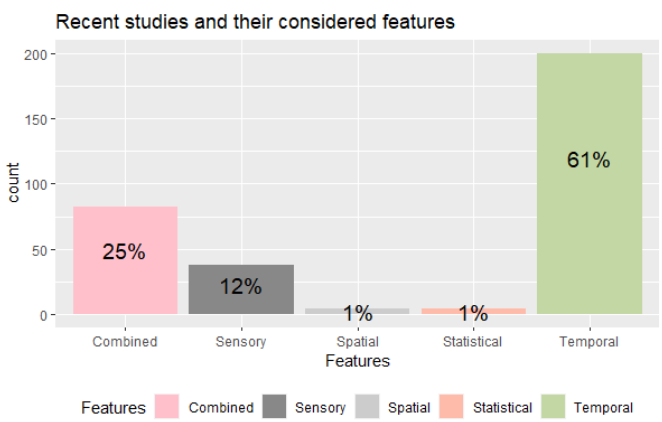

FIGURE 11. The percent distribution of feature configurations employed in the most recent investigations. It demonstrates that the temporal characteristics are more polar. Recent KD researchers, on the other hand, are interested in combination of features (temporal, spatial, and sensory)

B. TEMPORAL FEATURES

Temporal features are generally treated as timing features. It combined dwell/hold time, flight time, latency time, bi-graph/digraph time, trigraph time, n-graph time, and total and average time. These features can be found by calculating a series of press and release timestamps in a millisecond.

- Key Duration/hold/dwell/ time (KD/KH-Time): The time interval between pressing a key and releasing it.
- Down Down Latency Time (DD-Time): The time elapsed between two consecutive presses.
- Up Up Latency Time (UU-Time): The time elapsed between two successive releases.
- Up Down Latency Time (UD-Time)/flight time: the amount of time between one key release and the next keypress.
- Di-graph Latency Time (Digraph-Time)/bigraph time: The time interval between one keypress and the following key release mentioned in the study [228]
- Trigraph Latency Time (Trigraph-Time): The time elapsed between pressing one key and releasing the third key.

These easily available features are common (61% during the last six years) in both desktop and smartphone environments. However, most of the time, these features are combined with the sensor and touchscreen-based features on a smartphone.

C. MOTION/SPATIAL FEATURES

In smartphones, entry point and active authentication use mainly two types of features -

(1) Touch-screen-based features - it includes touch events (press and release time, pressure, swiping, zooming). It requires specific action. This feature can be classified into two main subcategories -

- Coordinating features - it includes touchpoint coordinates, the distance between two constitutive touchpoints, velocity, etc.
- Spatial features - it includes touch area and pressure.

(2) Sensor-based features - it includes continuously captured sensory data (gyroscope, acceleration, rotation, magnetometer, GPS) at a certain rate. Motion sensors measure acceleration and rotational forces along three axes. It does not depend on a specific action on the screen. Recently, researchers are more interested in the following features.

- Gyroscope - a gyroscope detects the current orientation of the phone and any possible spin or rotational changes. It is employed to measure any rotation of the device.
- Acceleration - it is the measurement of any movement (linear) of the phone, including the fall of the owner when holding the phone or the free fall of the phone.
- Gyroscope including gravity - it is the measurement of direction and magnitude of gravity.
- Orientation - computed from the angular velocity detected by the gyroscope, which is expressed as three axes.
- GPS location - it represents latitude and longitude, suitable for context-aware authentication.

(3) Combined features - We could combine these two features to enhance the performance of the authentication model. Combined features include touch-screen-based features for a specific action and covertly collected sensory data simultaneously.

D. ENVIRONMENTAL AND POSITIONAL FEATURES

Environmental features include battery signal, application context, cell power, etc. Where positional features include GPS, Wi-Fi, etc. could be useful for context-aware authentication [229].

E. STATISTICAL FEATURES

The use of statistical features extracted from raw features is not new. Multiple recent studies [194], [230]–[235] used these features to tackle continuous data stream. The following formulas listed in Table 8 are used to get the statistical measurements of the pattern in a fixed window length. A histogram is also used to get the density of different data values within a range.

TABLE 8. Statistical features from raw data for continuous generated patterns in a window length

Name	Formula	It measures
Minimum	$Min = \min(x_i), \forall i = 1, 2, 3, ..n$	the lowest element in the data
Maximum	$Max = \max(x_i), \forall i = 1, 2, 3, ..n$	highest element in the data
Average	$Avg = \frac{1}{n}\sum_1^n(x_i), \forall i = 1, 2, 3, ..n$	detect the central tendency
Standard deviation	$Std = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2}$	variation in the data
Median	$Med = x_{(i)}[0.5(n+1)]$	50% of data
Q_1	$Q_1 = x_{(i)}[0.25(n+1)]$	25% of data
Q_3	$Q_3 = x_{(i)}[0.75(n+1)]$	75% of data
Kurtosis	$Kur = \sqrt{\sum_{i=1}^{n}\frac{x_i - Avg^3}{(n-1)Std^3}}$	peakedness in the data stream
Skewness	$Skew = \sqrt{\sum_{i=1}^{n}\frac{x_i - Avg^4}{(n-1)Std^4}}$	asymmetry in the data stream

F. OTHER FEATURES

There are other possible measures, like the choice of shift and control keys, the frequency of error, error-correcting methods, keystroke sound, placement of finger, etc.

A study [236] used a special type of keyboard (triboelectric keystroke device) to convert typing motion to electrical signals for data analysis. Another study [150] used a non-mechanical-punching keyboard based on a triboelectric Nanogenerator to convert typing patterns to electrical signals.

G. FEATURE REPRESENTATION AND SELECTION METHODS

A large number of studies have been identified that used different feature representations and selection. Table 9 presents

the feature representation strategies considered in the literature for different environments to collect sensory and touch-based features. Timing aspects are frequent while using traditional keyboards, but sensory and spatial features are utilised in sensor-enabled devices. Because of the differences in datasets, feature configurations, classifiers, and metrics, we cannot compare these findings. Another Table 10 provides the feature selection methods adopted in the latest literature. With these tables, researchers can gain a better understanding of this process and work toward better feature arrangements.

H. NORMALIZATION

This process is required for faster computation. There are several normalisation processes, including min-max, standardization [253], fuzzy normalization, etc. A study [254] used fuzzy-based normalisation to reduce the false acceptance and rejection rate. Another study [255] used min-max normalization due to the fact that most of the feature's values are not normally distributed.

VI. CLASSIFICATION AND ADAPTATION METHODS

Classification is the most critical job of any KD-based system [48]. To analyse the KD characteristics, several classification methods have been adopted. Some are acceptable in their error rate, but in some cases, it harms usability. In most of the latest studies, researchers are interested in enhancing the performance of the KD models, ignoring the fact that the design may lead to unusable results. But with everyday technology and frequently switching applications, users need a more secure and usable system [256]. Therefore, careful consideration in selecting a classifier is an important issue. In a recent study [5], Shannon Entropy, Chunking Theory, and Keystroke Level Model were all used. The latest trends of adopted classification methods undertaken in different system designs have been presented in Fig. 12.

Because just one user's sample is accessible during training and collection of all imposters' patterns is not possible at that time, one-class classifications or unsupervised ML approaches are more practical in constructing ViSM and ViDM designs. Supervised approaches are employed in IiSM, IiDM, PiSM, and PiDM. However, for real-world evaluation, the evaluation technique for identification and prediction models differs. The system should be familiar with samples of a person while doing identification. On the other hand, in prediction, tested samples of a subject will never be a part of the training set for its practical scenarios.

A. CLASSIFICATIONS (CONTRIBUTION TO OB6)

1) One-class classifications

In developing user authentication systems (ViSM and ViDM), an ML model with the user's and imposters' samples has not yet been applied in the real-world scenario because there are millions of potential imposters. Thus, it is not possible to obtain all the prospective imposter patterns at the time of building the model. The solution is to build a model with the user's samples and use it to detect imposters using

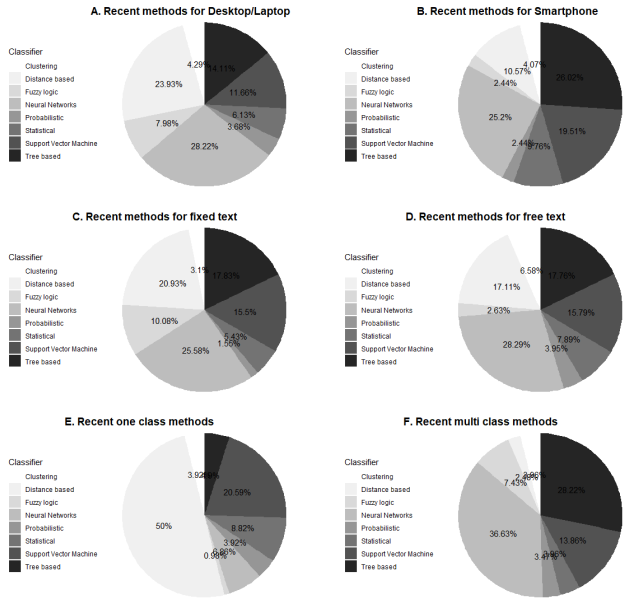

FIGURE 12. Percentage of the proposed approaches in different domains and platforms. Fig. A - Percentage distribution of the recent approaches in the desktop/laptop environment, Fig. B - Percentage distribution of the recent approaches in the smartphone environment, Fig. C - Percentage distribution of the recent approaches to fixed texts, Fig. D - Percentage distribution of the recent approaches to free texts, Fig. E Percentage distribution of the recent approaches for one class classifications, and Fig. F Percentage distribution of the recent approaches to multi-class classifications

the same sort of similarity measures or anomaly detection score. This type of problem is known as an anomaly or novelty detection [65]. This type of intrusion detection gets affected by many factors [257]. Several anomaly detectors have been identified in the KD literature that is suitable for implementing user authentication systems (ViSM and ViDM).

It is usual to discover anomalies using classical statistics such as mean, median, and standard deviations. Various pattern recognition approaches have been popular over the years and have been applied to KD. The choice of an anomaly detector is essential in analysing KD features since the performance of one detector varies significantly across datasets gathered in different data acquisition configurations. The following are the anomaly detection techniques suitable for ViSM and ViDM models.

- *Neural network-based classifiers:* Autoencoder is an advanced deep learning-based anomaly detector that has been adopted in several studies. A study [258] used this method for analysing KD characteristics and reduced 58% of EER. In this class of feature-learning approaches, the inputs are renovated into an abstract representation to be used in pattern recognition and classification. Another study [259] proposed this one-class classification method to develop smartphone continuous authentication based on the gyroscope and accelerometer pattern while holding the phone and achieved 2.2% of EER. Another study [106] found this model as one of

TABLE 9. Features representation considered in the literature

Study	Year	Env.	Method	Results (%)	Text freedom?	Features	Feature representation strategy
[200]	2017	S	SVM	EER 1.2	Yes	G, A, R, TP, SF	Shaking radius, corrected and tangential velocity
[237]	2017	S	SM	EER 2.4	Yes	G, A, R	Time-, frequency- and wavelet-domain features
[209]	2018	O	NN	Acc.98.5	Yes	G, A, R	Time-, frequency- and wavelet-domain features
[168]	2018	S	SM	EER 0.0	Yes	T, P, TP	Scroll and drag magnitude value
[238]	2018	D	SM	Acc. 99.0	Yes	T	Dynamic time series
[236]	2018	O	SVM	Acc. 98.7	No	T, P	Analog electrical signals
[239]	2018	D	SM	Acc. 98.24	Yes	T	Keystroke Time Series, Discrete Fourier Transform and Discrete Wavelet Transform
[174]	2018	S	SM	EER 2.21	Yes	T, G, A, R, SF	Time-, frequency- and wavelet- domain features
[111]	2018	D	TB	Acc. 91.0	Yes	T	Wiener filtering algorithm, Fast Fourier transform
[240]	2019	D	SM	Acc. 99.67	Yes	T	Keystroke time series
[220]	2019	S	SVM	Acc. 95.0	Yes	T, G, A, TP	96 features
[241]	2019	D	SVM	EER 3.71	Yes	T	Combines the mouse feature and the keystroke feature
[242]	2019	D	SM	Acc. 92	No	T	Three different feature sets
[243]	2019	S	SVM	Acc. 97.1	Yes	T, G, A, R, TP	WiFi, GPS location and app usage
[244]	2019	S	TB	Acc. 94.26	Yes	T, P, SF	71 features
[137]	2020	S	Stat.	EER 1.0	Yes	T, G, A, R, TP, SF	Heterogeneous features
[26]	2020	D	Stat.	Acc. 90.5	No	T	15, 20, 30 features

O->Other devices, D->Desktop/laptop, S->Smartphone, NN->Neural network, SM->Similarity measure, SVM->Support Vector Machine, Acc.->Accuracy, Stat.->Statistical measure, TB->Tree based,T->Timing, G->Gyroscope, A->Accelerometer, R->Rotation, TP->Touchpoint, SF->Statistical features, P->Pressure, R->Rotation

TABLE 10. Feature selection methods in the literature and observed results

Study	Year	Feature selection	Environment	Input free-dom?	Results (%)
[109]	2017	CBFS	Others	Yes	Acc. 99.6
[7]	2018	GA	Smartphone	Yes	Acc. 97.9
[196]	2018	mRMR	Smartphone	No	EER 0.97
[245]	2018	GA	Desktop	No	EER 1.0
[246]	2018	Deep features	Smartphone	Yes	Acc. 97.8
[112]	2019	CBFS	Smartphone	No	Acc. 100.0
[78]	2019	PCA	Smartphone	Yes	Acc. 90.0
[247]	2019	GA	Desktop	No	EER 5.3
[110]	2019	Binary PSO	Smartphone	No	EER 0.13
[216]	2019	ACO	Desktop	No	EER 0.15
[248]	2019	GA	Smartphone	No	Acc. 100.0
[249]	2019	GA	Smartphone	No	EER 0.0
[250]	2019	Hybrid binary PSO	Desktop, Smartphone	No	Acc. 87.0
[204]	2019	PCA	Smartphone	Yes	Acc. 99.6
[251]	2019	GA	Desktop	No	EER 5.0
[252]	2019	Grid search	Desktop	No	EER 5.22
[178]	2020	PSO	Smartphone	No	EER 2.2
[32]	2020	GR	Smartphone	Yes	Acc. 87.56

CBFS->Correlation Based Feature Selection, GA-> Genetic Algorithm, PCA->Principle Component Analysis, PSO->Partica Swam Optimization, GR->Gain Ratio, mRMR->Minimum redundancy maximum relevance, ACO->Ant Colony Optimization

the top anomaly detectors via the Keystroke Biometrics Ongoing Competition (KBOC), which achieved 9.82% of EER on the public KD dataset collected in the semi-controlled environment through the desktop keyboard to develop a one-time user verification model. A study [260] utilized this algorithm to transform source domain samples to target domain samples in cross-domain keystroke biometrics. Another recent study [261] used Autoencoder to extract features for the promising performance of the KD system based on data collected from an intelligent keyboard. The main three issues with this model are - (a) it takes too long to train the model, (b) a large dataset is required, and (c) deploying this model on less computationally capable devices such as a smartphone is difficult.

- *Support vector-based classifiers:* Support Vector Machine (SVM) in study cite [262] has recently gained great interest in various domains of pattern recognition for a variety of reasons, including higher classification rate, less time to train the model, which is shorter than neural networks, variation in the model, and easily available open-source tools. LIBSVM [263]. It aims to maximise the distance from the decision boundary to the nearest data points (support vectors). A study [106] found it as one of the great models achieved by 7.40% of EER in user identity verification through a desktop keyboard. Another study [118] obtained 10.68% of EER using a one-class support vector machine (OCSVM) on public datasets. A study [264] applied this algorithm for smartphone user authentication based on sensor data. They observed less than 1% of EER based on 10 actions. Another study [265] applied this algorithm for smartphone continuous authentication. They observed 4.66% EER for 5 sec. of activity on a smartphone. A recent study [266] used this method to implement implicit and continuous authentication for smart home users and observed an accuracy of at least 95.29%. A recent study [219] used OCSVM for continuous authentication of smartphone users. Another study [267] used

OCSVM for analysing accelerometer data for active authentication. This method has been used in many studies [268]–[270] for transparent authentication of smartphone users.

- *Static based classifiers:* Haider et al. described Outlier-count [271] in the name of "statistical technique." In the training phase, the detector calculates two common statistical measures: the mean and standard deviation of each feature vector. A study [65] used to set this threshold by 1.96 for detecting outliers. The study [272] re-implemented it for comparison of performance with other detectors on various datasets, and found it to be one of the top detectors in their study.
- *Distance based (angle) classifiers:* A study [273] adopted Cosine similarity for analysing touch-based smartphone features in 2016. In the same year, a study [274] used four detectors (Euclidean, Cosine, Manhattan, and Correlation distance) for active authentication using a smartphone. They achieved the best EER of 18.44% for Cosine. Another study [275] adopted the same detector, including Euclidean and Manhattan, for implementing continuous authentication using a conventional keyboard in 2018. They found a lower average error rate (FAR 16.25%, FRR 40.35%) while using Manhattan. However, another study [276] proposed Cosine similarity in the same year and achieved EER 7.8% which is impressive and comparatively better than Manhattan, but they used touch-based features for smartphone continuous authentication. A recent study [277] proposed using cosine similarity as a scale-free detector to mitigate the negative impact while the speed of different users varied significantly. However, Cosine is the least successful algorithm [278] in KD. But a recent study [213] used this algorithm and achieved an impressive error rate ranging from 0% to 13%.
- *Distance based (in the time domain) classifiers:* Dynamics Time Warping (DTW) measures the optimum alignment of two-time series data in different lengths. This algorithm was applied to the performance history of a study [279]. They used this method to implement the implicit authentication model while picking up the phone. A study [192] used this method to show the impact of window length on KD model accuracy.
- *Distance based classifiers:* There are many similarities based anomaly detectors that have been adopted in the KD domain. Among them, Euclidean distance, Manhattan distance [28], [98], [280], Scaled-Manhattan distance [65], [106], [132], [257], [281], Mahalanobis distance, Lorentzian distance [28], [272], [282], Bhattacharyya distance [283], [284], Gower distance [272], [282], Minkowski distance [11] are common.
- *Clustering:* Kang et al. described the k-means detector in their study [285]. They used a k-means clustering algorithm to identify clusters in the training samples, and then they calculated the closeness of the test vector to any of the clusters.
- *Fuzzy logic based classifiers:* A study [286] applied Fuzzy c-mean clustering for more flexibility regarding fuzzy membership functions. Here, an individual's samples have been treated as one class, and all remaining users' samples have been treated as another class.

2) Binary classifications

While developing or building user identification (IiSM and IiDM) and prediction (PiSM and PiDM) models, samples of multiple users are needed. Several binary classification approaches have been identified in the KD literature. Among them, support vector-based, tree-based, and neural network-based approaches are common and achieve impressive performance.

- *Support vector-based classifiers:* It creates the optimum gap between two different categories of samples. It has been adopted in many domains because of its strong mathematical foundation. This binary classifier has been used in several studies [7], [201], [204], [220], [241], [287]–[291] in the KD domain, and this is the widely used classifier in IiSM, IiDM, PiSM, and PiDM system designs.
- *Tree based classifiers:* After SVM, the most widely used classifiers are Random Forest (RF) [168], [177], [178], [184], [186], [288], [291]. However, Decision Tree (DT) [182], [204], [292], J48 [114], [293], XGBoost [25], [27], [195], [294], [295], AdaBoost [111] have been also identified in KD domain. Most of these tree-based classifiers are time-inefficient, but their performance in accuracy is impressive. In the case of XGBoost, it is ten times faster than gradient boosting. In addition, it can be executed on a low-configured device like a smartphone. Therefore, while implementing KD in smartphones, XGBoost will be effective. On the other hand, due to high variability in keystroke patterns, a study [296] used an ensemble model of RF to reduce offer-fitting.
- *Neural network based classifiers:* Several neural network based architectures have been adopted in many studies. recurrent neural network (RNN) [297], deep neural networks (DNN) [249], neural networks (NN) [193], [292], [298], artificial neural networks (ANN) [7], [184], [289], convolutional neural networks (CNN) [68], [299], multi-layer perceptron (MLP) [217].
- *Probabilistic based classifiers:* Several studies [149], [175], [177], [300] have identified Naive Bayes (NB) as a classifier for KD systems and discovered it to be effective in KD models.
- *Fuzzy logic based classifiers:* Each time, the touch-point may not be the same. While considering these touch coordinate-based features, a study [301] used a fuzzy classifier. Another study [302] used this to separate users based on pressure. This classifier employs several rules based on the training samples. A study [303] shows that the composite fuzzy classifier outperforms SVM and RF. Similarly, a study [304] compared fuzzy classifier with other previously proposed four ap-

proaches and found that the classifier is more impressive than others. Another study [305] mentioned that a neural network with fuzzy logic increases the system's learning ability of keystroke patterns.

- *K-nearest neighbour:* There are few studies [149], [168], [202], [249] applied this method for implementing KD systems. A recent study [178] used this as a classifier for three-step mobile authentication using KD. A study provided statistical evidence that confirms SVM and RF are better than this model in accuracy. However, this method is better than NB [177] because it is quite fast and will be effective for re-authentication. Another study [306] used it to determine fatigue using KD patterns.

B. ADAPTATION TECHNIQUES (CONTRIBUTION TO OB7)

Biometric samples vary over time (concept drift) for mainly two reasons - switching conditions and ageing [307]. This degrades the recognition performance over time. Adaptation in the user's biometric template adapts to deal with this uncertainty problem (intra-class variation) [267], [308], [309]. It depends on several parameters [310] - (a) *Stored template* - it is composed of several samples that describe the biometric reference, (b) *Adaptation mechanism* - the strategy for dealing with upkeep, (c) *Decision threshold* - it allows the system to be updated, and (d) *Adaptation periodicity* - it occurs after each successful authentication or after a pre-determined period. However, in KD, most of the studies concentrated on template updation mechanisms. After each successful authentication, this mechanism restores the templates. The following mechanisms have been identified in the literature.

- *Sliding/moving window:* This mechanism receives a set of query samples and replaces the older ones, keeping the same template size on a First In First Out (FIFO) basis.
- *Growing window:* After each successful classification, the new set of samples will be added to the existing instead of being replaced in the sliding window.
- *Double serial adaptation:* It is based on user and time-dependent adapted threshold criterion with the combined performances of sliding-window and growing-window mechanisms to minimize the user's sample for defining the KD template and has been used by a study [247]. The authors used two thresholds - the first threshold is a user-specific threshold used for identity verification, and the second threshold is a time-dependent threshold used for adaptive permission. The sliding window will be applied if the size of the user's reference is reached to the maximum (here, arbitrarily set at 10), otherwise, a growing window will be applied.
- *Double parallel adaptation:* This algorithm uses two models in memory. One is adopted by Growing-window and the other is adopted by Sliding-window [311].
- *Adaptive learning:* It changes the model by building a new one with the collected samples using transfer learning [312]. This study confirms the new KD model exhibits higher performance than the previously trained model. Another study [313] proposed a novel adaptive strategy in KD for the current environmental factors.
- *Least frequently used:* This is similar to the sliding window, but replacement is done differently. Here, the least frequently used samples will be replaced by a set of new query samples.
- *Usage control:* It checks the matching score from the oldest to the newest and then allows for adaptation [309]. It keeps the most recent samples and removes all the remaining.
- *Extended replacement:* It uses usage control and removes samples with a low score and adds a new set of samples.
- *Doddington zoo:* This classification has been applied to classifying the user into multiple categories, and each category has been adapted by a specific adaptation strategy [314].
- *Immune positive selection:* This adaptation mechanism is inspired by the natural immune system. A key algorithm used in this adaptation strategy is *Self-detector*, where all the samples will be copped as detectors at the training phase. A study [309] used this strategy and improved the performance of the KD model.

C. PERFORMANCE EVALUATION METRICS (CONTRIBUTION TO OB8)

The performance of biometric systems is commonly measured by several metrics. But all these metrics are not significant in any system design. According to a study [307], the detailed metrics are only useful for user authentication. However, different metrics are useful to measure different types of KD models. A study [315] suggests separate metrics for verification and identification systems. The following are the different systems and their corresponding metrics.

1) Performance evaluation metrics for data acquisition

Failure to Enrol Rate (FET): It measure the likelihood that arises when samples are not properly captured due to inconsistency in typing behaviour and the user is incapable of enrolling [316], [317].

Failure To Acquire Rate (FTAR): It measures the comfort of the user while typing. It is close to zero for simple and short text [318].

Typing Error Rate (TER): It measures the typing errors.

$$TER = \frac{\#backspace}{\#inputlength} \times 100\% \tag{1}$$

2) Performance evaluation metrics for authentication model

Equal Error Rate (EER): It is used to evaluate the performance of the model. This is a very popular metric in one-class classification or user identity verification. This is the measure where the False Acceptance Rate (FAR) or Type II error rate and the False Rejection Rate (FRR) or Type I error rate are

the same for an acceptance threshold defined by Equation 2.

False Acceptance Rate (FAR): FAR is defined as the percentage ratio between falsely accepted illegal users and the total number of imposters accessing the system, defined by Equation 3. It determines how often an intruder can bypass the methods successfully. The lower rate of FAR indicates a higher security level.

False Rejection Rate (FRR): FRR refers to the percentage ratio between falsely denied genuine users and the total number of genuine users accessing the system, defined by Equation 4. It signifies how often a real user will not be verified successfully. A higher rate of FRR indicates the non-usability level.

Half Total Error Rate (HTER): For overall performance measure, another metric - HTER, also known as balanced accuracy, is also used in literature defined by Equation 5 [319].

$$EER = FAR\% = FRR\% \tag{2}$$

$$FAR = \frac{Numberof falselyacceptedillegitimateusers}{Totalnumberofimposters} \times 100\% \tag{3}$$

$$FRR = \frac{Numberof falselydeniedlegitimateusers}{Totalnumberofgenuineusers} \times 100\% \tag{4}$$

$$HTER = \frac{FAR + FRR}{2}\% \tag{5}$$

In the user authentication model, if we increase the threshold value, the FRR will be decreased, and consequently, the FAR will be increased. If we decrease the threshold value, the security will be increased, then FAR will be decreased, but FRR will be increased. Therefore, careful consideration of the threshold value is an important issue. To test the user authentication system, a few parameters (EER, FAR, FRR, etc.) have been identified to evaluate the performance of the user authentication system. As the European standard for access control specifies that FAR must be less than 1% and FRR must be no more than 0.001% [320].

In KD literature, the common metric is EER. Several recent studies [137], [160], [178], [194], [321]–[323] used this metric to measure the performance of their proposed model. A study [324] used both EER and accuracy to measure the performance of a distance-based detector. A few studies [153], [325], [326] used FAR and FRR for the model performance. These metrics are common in the user authentication model, which is widely accepted in industry and academia [327]. Accuracy is also a metric used in several studies [26], [195], [231], [291], [297], [328]. A study [241] used three metrics - FAR, FRR, and EER to measure the performance of the support vector-based model. In the study [215] for a tree-based model, the F_1 score was used.

A study [319] used HTER with FAR and FRR for the performance of the proposed model, *ITSME*. Another study [329], used the same metric to show the impact of application context on KD.

3) Performance evaluation metrics for adaptive authentication

Imposter Update Selection Rate (IUSR): The rate at which imposter samples are involved in template adaptation.

$$IUSR = \frac{\#impostersamplesverifiedasgenuine}{\#testedimpostersamples} \times 100\% \tag{6}$$

Genuine Update Miss Rate (GUMR): The rate at which genuine samples are not involved in template adaptation.

$$GUMR = \frac{\#genuinesamplesnotverifiedasgenuine}{\#testedimpostersamples} \times 100\% \tag{7}$$

These two metrics (IUSR and GUMR) are specific to adaptive biometric systems [307], [310].

4) Performance evaluation metrics for identification model

The following are the four parameters that are used to get such metrics: Number of Positive Class Truly Classified (TP), Number of Negative Class Truly Classified (TN), Number of Positive Classes Falsely Classified (FP) and Number of Negative Class Falsely Classified (FN).

Accuracy shows the ratio between correctly identified and total instances.

$$Accuracy = \frac{(TP + TN)}{(TP + FN + FP + TN)} \times 100\% \tag{8}$$

False Match Rate (FMR), False Non-Match Rate (FNMR) along with EER have been used to measure the zero-effect imposter attacks [251]. These metrics have been introduced by a study [330]. There have been a few studies that used the same metrics [331], [332].

$$FMR = \frac{FP}{(FP + TN)} \times 100\% \tag{9}$$

$$FNMR = \frac{FN}{(FN + TP)} \times 100\% \tag{10}$$

5) Performance evaluation metrics for predictive model

Since the class distribution of the used dataset may be uneven, the accuracy alone is not enough to measure the performance of the predictive model. The following five relevant metrics are common - Accuracy, Sensitivity, Specificity, AUC (Area Under Curve), and ROC (Receiver Operating Curve).

The sensitivity indicates how well the positive classes are correctly identified, while specificity indicates how well the negative classes are correctly identified. Both specificity and sensitivity were used in the recent study [187] for performance analysis of the model (extracting PD by analysing KD features). These two are important and common metrics in medical science where data points for a specific disease are rare. AUC is an area under ROC that is used to summarise

model performance as a single value [232]. It shows the overall performance of the model.

ROC is a line chart that represents how the true positive rate changes with changing the false positive rate. But considering multiple metrics in a performance comparison of the approaches is not possible. At that time, AUC or ROC is used.

The following Equations 8 to 14 were used to calculate the metrics as per the study [333].

$$Sensitivity = \frac{TP}{(TP+FN)} \times 100\% \quad (11)$$

$$Specificity = \frac{TN}{(FP+TN)} \times 100\% \quad (12)$$

$$F_1 score = \frac{2TP}{(2TP+FP+FN)} \times 100\% \quad (13)$$

$$AUC = (1 + \frac{TP}{(TP+FN)} - \frac{FP}{(FP+TN)}) \times 100\% \quad (14)$$

6) Other metrics

Time for building and testing the model, battery consumption, especially for power-constrained devices like a smartphone, and resource usage like memory, are the metrics that can be used to measure the system performance of KD. The System Usability Scale (SUS) is an effective tool for measuring system usability [334].

VII. RESULTS AND DISCUSSIONS (CONTRIBUTIONS TO OB9 AND OB10)

A. RESULTS OF RECENT APPROACHES FOR VISM

A comparison of the recent approaches for ViSM has been presented in Table 11, undertaken by the researchers towards developing authentication models for desktops and laptops. Each study used only the timing features. However, the combination of these features is different in most of the models. A unique method for classification, including similarity measures to neural networks has been observed. The popular datasets that have been most cited are - CMU, GREYC, and WEBGREYC.

(Answer to H1) The summary statistics is depicted in Fig. 13. τ^2 shows the possibility of random variation, I^2 tells the magnitude of the variation, whereas, p tells the significant difference. We can see the p value of the Chi-square test is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since, heterogeneity is 100% (between 75% and 100%) thus confirming considerable heterogeneity, which means each study is significantly different from the other. It has been also observed that 6.34% of EER could be achieved with a range of 4.54% to 8.87%. The vertical line represents the aggregate results and the box plot for each study represents the individual results. The distance from the vertical line to each plot indicates the difference between aggregated and individual results (effect size). The width of each box plot indicates the weight of the results. The weight of the studies has also been presented for further development of the KD-based ViSM security design for desktops or laptops.

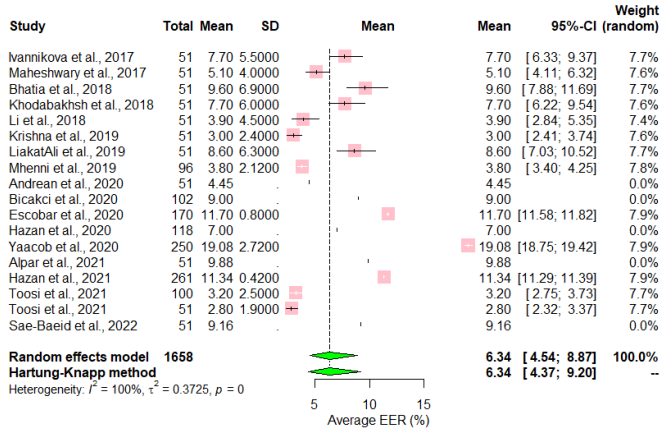

FIGURE 13. Forest plot: Summary of findings for ViSM in desktop/laptop environment. Here, Total is the number of subject, Mean is the average EER, and SD is the variation

(Answer to H2) In the case of ViSM on a smartphone, it has been observed the popularity of OCSVM and similarity-based methods as classifiers, as presented in Table 12. Some studies used temporal features with sensory input, whereas some studies added spatial features. Each study used its datasets because all these features are not available in the shared datasets for predefined inputs. Fig. 14 depicts a summary statistics of the most recent studies. We can see the p value of the Chi-square test is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since heterogeneity is 100% thus confirms considerable heterogeneity, which means each study is significantly different from the other. The average EER is 6.15% within the range of 2.49% to 15.19% (at 95% significance level).

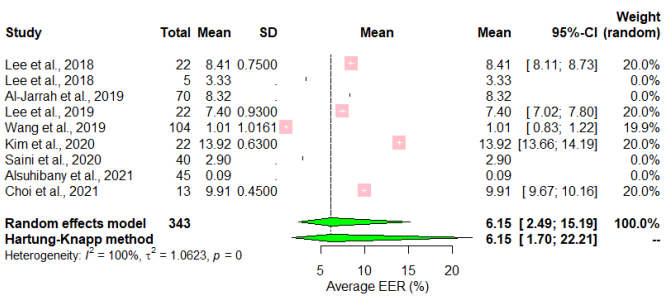

FIGURE 14. Forest plot: Summary of findings for ViSM in smartphone environment

B. RESULTS OF RECENT APPROACHES FOR VIDM

(Answer to H3) Classification methods undertaken by the researchers in recent studies for developing the KD models for continuous/adaptive/implicit user authentication on desktops and laptops have been presented in Table 13. It has been found that unique timing feature sets have been analysed with unique classifiers. Fig. 15 shows the summary

TABLE 11. Comparison of the proposed approaches to ViSM in the desktop/laptop environment

Ref.	Study	Year	EER (%)	Features	Method	Dataset
[105]	Ivannikova et al.	2017	7.7	KH, DD, UD	Dependence Clustering with Manhattan	CMU
[335]	Maheshwary et al.	2017	5.1	KH, DD, UD	Neural Network	CMU
[336]	Bhatia et al.	2018	9.6	KH, DD, UD	Generalised Fuzzy Model	CMU
[337]	Khodabakhsh et al.	2018	7.7	KH, DD, UD	Scaled Manhattan	CMU
[338]	Li et al.	2018	3.9	KH, DD, UD	Random Forest	CMU
[339]	Krishna et al.	2019	3.0	KH, DD, UD	Modified Differential Evolution	CMU
[340]	LiakatAli et al.	2019	8.6	KH, DD, UD	POHMM/SVM	CMU
[63]	Mhenni et al.	2019	3.8	KH, DD, UU, DU, UD	Doddington zoo classification	CMU, WEBGREYC
[323]	Andrean et al.	2020	4.45	KH, DD, UD	Multilayer Perceptron	CMU
[341]	Bicakci et al.	2020	9.0	UD, UU	Ensemble	Own
[161]	Escobar et al.	2020	11.7	KH, DD	Bhattachariyya distance with Gaussian Mixture Models	Own
[228]	Hazan et al.	2020	7.0	DD, UU, DU, UD	Statistical heuristics algorithm	WEBGREYC
[211]	Yaacob et al.	2020	19.08	KH, DD, UD, UU	Soft biometric	Own
[162]	Alpar et al.	2021	9.88	Time to Barcode	OCSVM	Own
[342]	Hazan et al.	2021	11.34	KH, DD, UU, DU, UD	X-means clustering	CMU, GREYC, WEBGREYC
[269]	Toosi et al.	2021	3.2	DD, UU, DU, UD	Dynamic Time Wrapping	GREYC
[269]	Toosi et al.	2021	2.8	KH, DD, UD	Dynamic Time Wrapping	CMU
[343]	Sae-Baeid et al.	2022	9.16	KH, DD, UU, DU, UD	Manhattan	CMU, WEBGREYC

POHMM->Partially observable hidden Markov model

TABLE 12. Comparison of the proposed approaches for ViSM in smartphone environment

Ref.	Study	Year	EER (%)	Features	Method	Dataset
[98]	Lee et al.	2018	8.415	Sensory	OCSVM	Own
[169]	Lee et al.	2018	3.33	DU, UD, DD, UU, Sensory	OCSVM	Own
[344]	Al-Jarrah et al.	2019	8.32	KH, UD, DD, Pressure, Area	Median-Absolute-Deviation and the Average- Absolute-Deviation	Own
[181]	Lee et al.	2019	7.4	Temporal, Spatial, Motion	Manhattan	Own
[110]	Wang et al.	2019	1.007	Temporal, Sensory, Pressure	SVM	Own
[321]	Kim et al.	2020	13.92	Temporal, Sensory, Spatial	Manhattan	Own
[178]	Saini et al.	2020	2.9	DD, DU, UD, UU, Rotation	Random Forest	Own
[345]	Alsuhibany et al.	2021	0.086	Timing, Sensory	Euclidean distance	Own
[346]	Choi et al.	2021	9.915	KH, DU, UU, DD, UD, Pressure, Spatial, Motion	OCSVM	Own

statistics using a forest plot. We can see the p value of Chi-square test is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since, heterogeneity is 100% thus confirming considerable heterogeneity, which means each study is significantly different from the other. We found 5.67% of the average EER.

(Answer to H4) In case of continuous authentication in smartphones, OCSVM and similarity/distance-based classifiers are common, as per the Table 14. In recent years, the number of sensory features has been gradually increasing for smartphone security. Here, sensor-based features like gyroscope and accelerometer are combined with touch-based features like coordinate and touch area, with context-based features like Wi-Fi and cell tower. Fig. 16 presents the summary of the latest model performances and their heterogeneity of them. We observed a very low EER of 1.55% which is significantly better than static mode. Furthermore, we can see the p value of Chi-square test is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since, heterogeneity is 100% thus confirming considerable heterogeneity, which means each study is significantly different from the other.

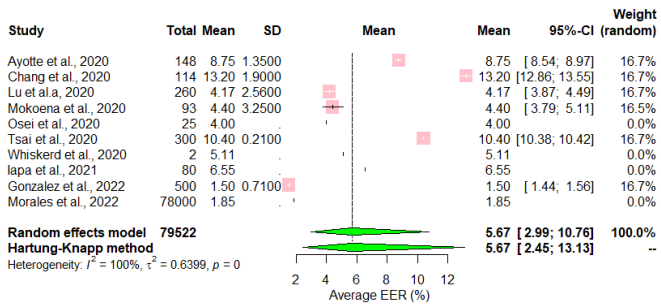

FIGURE 15. Forest plot: Summary of findings for ViDM in desktop/laptop environment

TABLE 13. Comparison of the proposed approaches to ViDM in the desktop/laptop environment

Ref.	Study	Year	EER (%)	Features	Method	Dataset
[347]	Ayotte et al.	2020	8.75	DU	Instance-basedTail Area Density	Clarkson II
[159]	Chang et al.	2020	13.2	KH, UD, DD, UU	k-means with Euclidean	Own
[348]	Lu et al.a	2020	4.17	DU	CNN and RNN	Clarkson II, Buffalo
[213]	Mokoena et al.	2020	4.4	KH, UD, DD, DU, UU	Cosine similarity	Villani
[152]	Osei et al.	2020	4.0	KH, UD	Euclidean+Manhattan	Own
[212]	Tsai et al.	2020	10.4	DU, UD, DD, UU	Voting-based statistical classifie	Own
[234]	Whiskerd et al.	2020	5.11	DD	Canberra distance	Own
[349]	Iapa et al.	2021	6.55	Digraph	Manhattan	Own
[350]	Gonzalez et al.	2022	1.5	Temporal	Spoofing	3 shared datasets
[351]	Morales et al.	2022	1.85	Temporal	Distance metric learning	Aalto

CNN->Convolutional neural networks, RNN->Recurrent Neural Network

TABLE 14. Comparison of the proposed approaches to ViDM in smartphone environment

Ref.	Study	Year	EER (%)	Features	Method	Dataset
[352]	Abuhamad et al.	2020	0.09	Sensory	LSTM	Own
[353]	Kalita et al.	2020	5.07	KH, DD, UD, Pressure	GMM	Own
[354]	Keykhaie et al.	2020	2.4	Sensory	DNN	Own
[354]	Keykhale et al.	2020	0.7	Sensory	DNN	Own
[137]	Kim et al.a	2020	0.55	Temoral, Spatial, Statistical	Kolmogorov-Smirnov statistics and Cramér–von Mises criterion	Own
[345]	Alsuhibany et al.	2021	0.0	Timing, Sensory	Euclidean distance	Own
[355]	Incel et al.	2021	3.5	Sensory, Statistical	SVM	Own
[17]	Stragapede et al.	2022	6.5	Sensory	RNN	HuMIdb
[1]	Tse et al.	2022	2.25	Trajectory	RNN	Own

LSTM->Long Short-Term Memory, GMM->Gaussian Mixture Model, DNN->Deep Neural Network

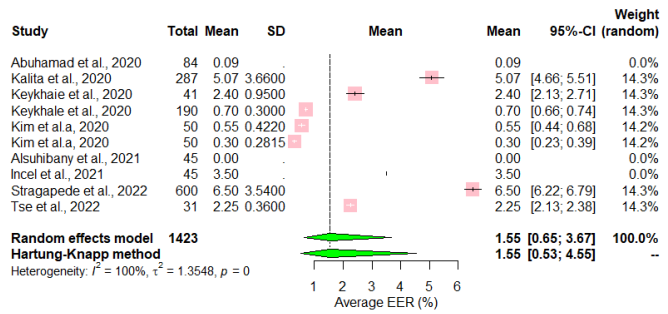

FIGURE 16. Forest plot: Summary of findings for ViDM in smartphone environment

C. RESULTS RECENT APPROACHES FOR IISM

(Answer to H5) Table 15 lists out the recent approaches and results for the user identification model of a desktop or laptop using fixed inputs. The common classifiers are two-class classification methods. Here, XGBoost, SVM, and neural network-based models were used on the unique combination of feature arrangements. It has been found that more than 90% of accuracy can be achieved with this design. The results and heterogeneity across studies are summarised in Fig. 17. We observed that 90.38% of accuracy could be achieved. Because of the feature layout, classification technique, subject selection, and inputs, each study differs greatly. We can see the p value of Chi-square test is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since, heterogeneity is 100% thus confirming considerable heterogeneity, which means each study is significantly different from the other.

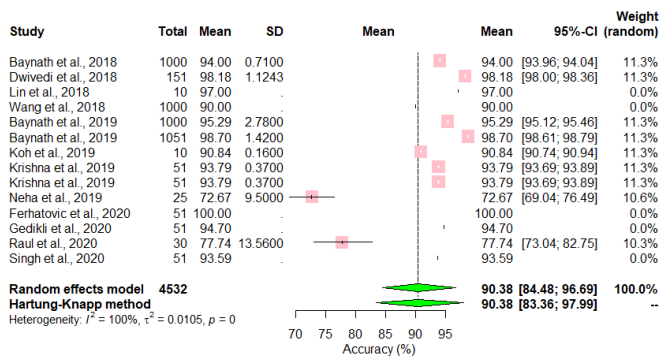

FIGURE 17. Forest plot: Summary of findings for IiSM in desktop/laptop environment

(Answer to H6) Identifying the users through their typing styles on a smartphone for fixed inputs has been conducted in limited studies. The comparison of the proposed approaches is presented in Table 16. However, impressive results have been found. The summary statistics of the latest studies have been depicted in Fig. 18. It has been found that 94.90% of accuracy could be achieved with this KD system design. We can see the p value of Chi-square test is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across

TABLE 15. Comparison of the proposed approaches to IiSM in the desktop/laptop environment

Ref.	Study	Year	Accuracy (%)	Features	Method	Dataset
[356]	Baynath et al.	2018	94.0	Temporal	NEAT	Own
[295]	Dwivedi et al.	2018	98.18	KH, DD, UU, DU, UD	XGBoost	CMU, GREYC
[357]	Lin et al.	2018	97.0	Temporal	CNN	Own
[358]	Wang et al.	2018	90.0	Temporal	SVM	Own
[359]	Baynath et al.	2019	95.29	Temporal	ACO-ANN	Own
[102]	Baynath et al.	2019	98.7	KH, DD, UD	NEAT	CMU
[185]	Koh et al.	2019	90.84	KH, UD, DU, DD	Artificial Bee Colony	Own
[27]	Krishna et al.	2019	93.79	KH, DD, UD	XGBoost	CMU
[27]	Krishna et al.	2019	93.79	KH, DD, UD	XGBoost	CMU
[360]	Neha et al.	2019	72.67	Temporal	MJ48	Own
[361]	Ferhatovic et al.	2020	100.0	KH, DD, UD	Long Short-Term Memory	CMU
[194]	Gedikli et al.	2020	94.7	KH, DD, UD	NN	CMU
[26]	Raul et al.	2020	77.74	Temporal, NC	SVM	Own
[25]	Singh et al.	2020	93.59	KH, DD, UD	XGBoost	CMU

XGBoost->eXtreme Gradient Boosting, NN->Neural Networks, NC->non-conventional, NEAT->NeuroEvolution of the augmenting topology

studies. Since, heterogeneity is 99% thus confirming considerable heterogeneity, which means each study is significantly different from the other.

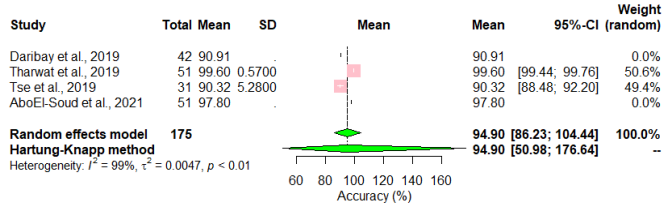

FIGURE 18. Forest plot: Summary of findings for IiSM in smartphone environment

D. RESULTS OF RECENT APPROACHES FOR IIDM

(Answer to H7) A comparison of the approaches to IiDM in the desktop and laptop environments has been presented in Table 17. The accuracy observed in the latest studies is quite impressive. Fig. 19 shows the overall statistics of this design, which calculates 95.24% of the possible accuracy in this configuration. We found 98% of heterogeneity, which indicates significant results across studies. Because unique datasets were used by the previous studies. We can see the p value of Chi-square test is $<$0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since, heterogeneity is 98% thus confirming considerable heterogeneity, which means each study is significantly different from the other.

(Answer to H8) In the recent past, a large number of studies have been conducted and proposed several methods for identifying users through the help of a smartphone and the attached sensors, as presented in Table 18. Here, all the studies are different in several ways, including feature arrangement, classification method, and dataset. Fig. 20 presents the summary statistics of the latest studies. We observed considerable heterogeneity across studies. We also found that 88.83% of accuracy could be achieved in this mode of design, which is more challenging than this design on a desktop

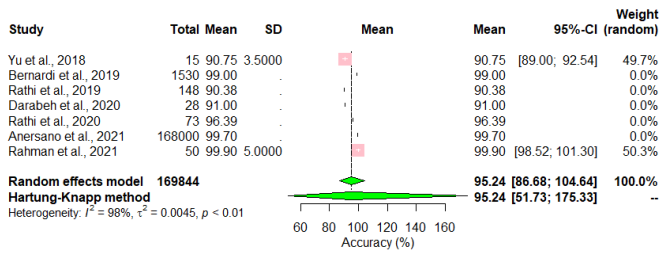

FIGURE 19. Forest plot: Summary of findings for IiDM in desktop/laptop environment

or laptop. We can see the p value of the Chi-square test is $<$0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since, heterogeneity is 100% thus confirms considerable heterogeneity, which means each study is significantly different from the other.

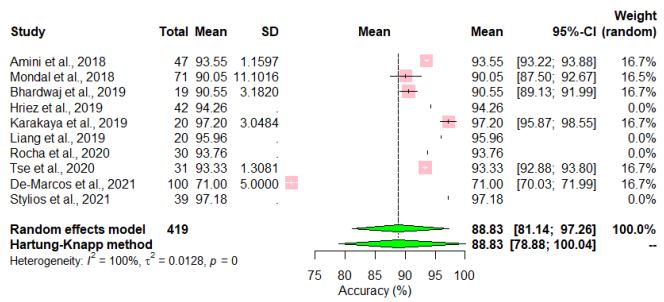

FIGURE 20. Forest plot: Summary of findings for IiDM in smartphone environment

E. RESULTS OF RECENT APPROACHES FOR PISM

(Answer to H9) Several predictive models have been proposed based on KD attributes. The approaches, evaluation settings, and the achieved results have been presented in Table 19. Multiple traits (age group, gender, handedness, typing skill, hand(s) used, culture, and education level) have been observed to be extracted with high accuracy from typing

TABLE 16. Comparison of the proposed approaches to liSM in the smartphone environment

Ref.	Study	Year	Accuracy (%)	Features	Method	Dataset
[195]	Daribay et al.	2019	90.91	Sensory	XGBoost	Antal
[248]	Tharwat et al.	2019	99.6	Temporal	Bagging	RHU
[300]	Tse et al.	2019	90.32	Spatial, temporal, swipe	LDA	Own
[4]	AboEl-Soud et al.	2021	97.8	Temporal	Random Forest	RHU

LDA->Linear Discriminant Analysis

TABLE 17. Comparison of the proposed approaches to liDM in the desktop/laptop environment

Ref.	Study	Year	Accuracy (%)	Features	Method	Dataset
[111]	Yu et al.	2018	90.75	Audio	AdaBoost algorithm	Own
[217]	Bernardi et al.	2019	99.0	Statistical	MLP	Own
[287]	Rathi et al.	2019	90.38	DU	Fuzzy Kernel Support Vector Machine	Buffalo
[362]	Darabeh et al.	2020	91.0	KH, DU, Digraph, Trigraph	Random Forest	Own
[363]	Rathi et al.	2020	96.39	DU	Neutrosophic Inference Model	Buffalo
[53]	Anersano et al.	2021	99.7	Statistical	Ensemble	Three shared datasets
[163]	Rahman et al.	2021	99.9	EEG, UU, DD, UD	Random Forest	Own

TABLE 18. Comparison of the proposed approaches to liDM in the smartphone environment

Ref.	Study	Year	Accuracy (%)	Features	Method	Dataset
[224]	Amini et al.	2018	93.55	Sensory	LSTM	Own
[7]	Mondal et al.	2018	90.05	Sensory, Statistical	Fusion	Touchalytics
[364]	Bhardwaj et al.	2019	90.55	UD, DU, DD	Fusion	Own
[244]	Hriez et al.	2019	94.26	Sensory	Random Forest	Antal
[204]	Karakaya et al.	2019	97.2	Sensory, Statistical	Decision forest	HMOG
[291]	Liang et al.	2019	95.96	Sensory, Statistical	MLP	Touchalytics
[365]	Rocha et al.	2020	93.76	Time, intensity, are	Distance	Own
[297]	Tse et al.	2020	93.335	Spatial, temporal, swipe	RNN	Own
[366]	De-Marcos et al.	2021	71.0	Sensory, Statistical	Ensemble	HMOG
[367]	Stylios et al.	2021	97.18	Spatial, Temporal, Pressure	MLP	Own

patterns on conventional keyboards. According to Fig. 21, the predictive model's overall performance is 91.09 percent. We found significant heterogeneity as a result of unique features, as well as, as usual, feature setting and approach. We can see the p value of Chi-square test is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since, heterogeneity is 100% thus confirming considerable heterogeneity, which means each study is significantly different from the other.

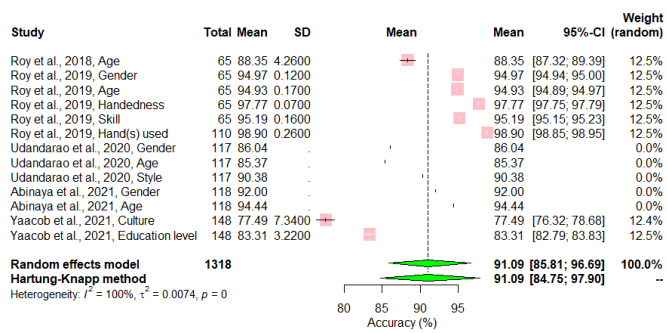

FIGURE 21. Forest plot: Summary of findings for PiSM in desktop/laptop environment

(Answer to H10) Similarly, PiSM in a smartphone environment has been studied for extracting age group, gender, and typing skills. The details of the methods and the feature arrangement have been presented in Table 20. It has been observed that only the timing features were analysed in the previous studies. Fig. 22 shows the overall performance statistic. It indicates 84.53% of accuracy could be achieved in this way of prediction, which is less than desktop. We can see the p value of the Chi-square test is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since heterogeneity is 100% thus confirms considerable heterogeneity, which means each study is significantly different from the other.

F. RESULTS OF RECENT APPROACHES FOR PIDM

(Answer to H11) Similarly, the PiDM mode of the KD-based model has been implemented in several studies for conventional keyboards, as depicted in Table 21. Here, we observed that not only the user's traits but also the stress of the user could be predicted. Fig. 23 shows the summary statistics of the latest studies. We observed considerable heterogeneity across the studies, where the average accuracy rate is 81.95%. We can see the p value of Chi-square test

TABLE 19. Predictive approaches for PiSM in a desktop or laptop environment

Ref.	Study	Year	Accuracy (%)	Features	Method	Dataset	Traits
[69]	Roy et al.	2018	88.35	KH, DD, UD	FRNN	CMU (P1)	Age
[28]	Roy et al.	2019	94.97	KH, DD, UD	FRNN	CMU (P1)	Gender
[28]	Roy et al.	2019	94.93	KH, DD, UD	FRNN	CMU (P1)	Age
[28]	Roy et al.	2019	97.77	KH, DD, UD	FRNN	CMU (P1)	Handedness
[28]	Roy et al.	2019	95.19	KH, DD, UD	FRNN	CMU (P1)	Skill
[28]	Roy et al.	2019	98.9	KH, DD, UD	FRNN	CMU (P1)	Hand(s) used
[31]	Udandarao et al.	2020	86.04	DU, UU, DD, UD	CNN	Own	Gender
[31]	Udandarao et al.	2020	85.37	DU, UU, DD, UD	CNN	Own	Age
[31]	Udandarao et al.	2020	90.38	DU, UU, DD, UD	CNN	Own	Style
[368]	Abinaya et al.	2021	92.0	UD, DD, DU, UU	PSO-NN	Own	Gender
[368]	Abinaya et al.	2021	94.44	UD, DD, DU, UU	PSO-NN	Own	Age
[369]	Yaacob et al.	2021	77.49	Temporal	SVM	Own	Culture
[369]	Yaacob et al.	2021	83.31	Temporal	SVM	Own	Education level

FRNN-> Fuzzy Rough Nearest Neighbour, PSO->Particle swarm optimization

TABLE 20. Predictive approaches for PiSM in the Smartphone environment

Ref.	Study	Year	Accuracy (%)	Features	Method	Dataset	Traits
[28]	Roy et al.	2019	83.87	Temporal	FRNN	RHU	Gender
[28]	Roy et al.	2019	87.91	Temporal	FRNN	RHU	Age
[29]	Roy et al.	2020	98.74	KH, DD, UU, UD, DU	Fusion	Own	Age
[29]	Roy et al.	2020	88.08	KH, DD, UU, UD, DU	Fusion	Own	Gender
[31]	Udandarao et al.	2020	88.37	DU, UU, DD, UD	CNN	Own	Gender
[31]	Udandarao et al.	2020	78.04	DU, UU, DD, UD	CNN	Own	Age
[31]	Udandarao et al.	2020	87.8	DU, UU, DD, UD	CNN	Own	Style
[38]	Roy et al.	2022	91.49	KH, DD, UU, UD, DU	Ensemble	Own	Age
[38]	Roy et al.	2022	62.07	KH, DD, UU, UD, DU	Ensemble	Own	Gender

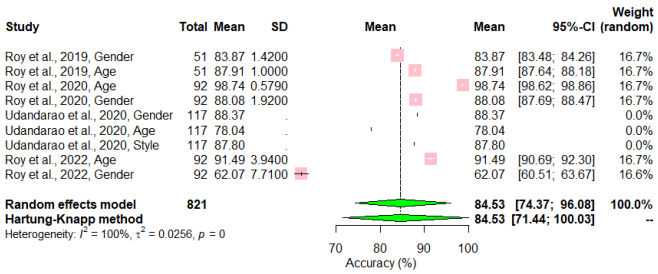

FIGURE 22. Forest plot: Summary of findings for PiSM in smartphone environment

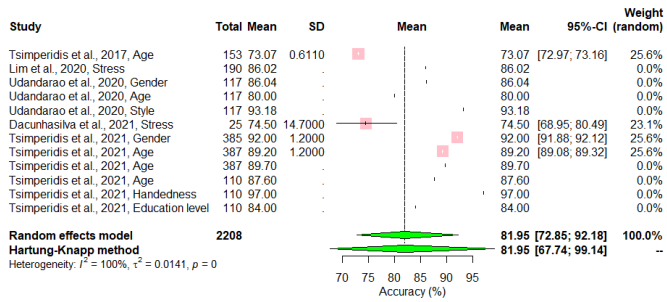

FIGURE 23. Forest plot: Summary of findings for PiDM in desktop/laptop environment

is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since, heterogeneity is 100% thus confirming considerable heterogeneity, which means each study is significantly different from the other.

(Answer to H12) The number of studies we found in the last six years for PiDM in the smartphone environment is less. Table 22 presents the study details that indicate stress with some of the few user traits that could be predicted. The summary statistics has been presented in Fig. 24, where we observed 87.95% of average accuracy in this mode of KD-based design. We can see the p value of Chi-square test is <0.01, rejecting the null hypothesis and thus suggesting heterogeneity across studies. Since, heterogeneity is 95% thus confirming considerable heterogeneity, which means each study is significantly different from the other.

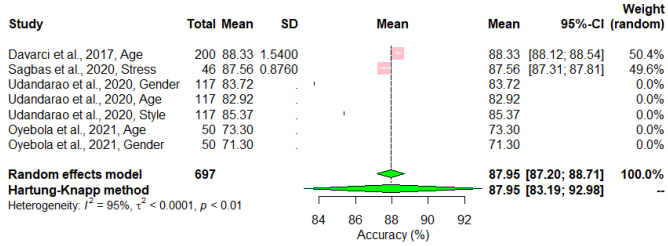

FIGURE 24. Forest plot: Summary of findings for PiDM in smartphone environment

TABLE 21. Predictive approaches for PiDM in a desktop or laptop environment

Ref.	Study	Year	Accuracy (%)	Features	Method	Dataset	Traits
[370]	Tsimperidis et al.	2017	73.067	DD, UD, DU, UU	ANN	Own	Age
[82]	Lim et al.	2020	86.02	DD	FFBP	Own	Stress
[31]	Udandarao et al.	2020	86.04	DU, UU, DD, UD	CNN	Own	Gender
[31]	Udandarao et al.	2020	80.0	DU, UU, DD, UD	CNN	Own	Age
[31]	Udandarao et al.	2020	93.18	DU, UU, DD, UD	CNN	Own	Style
[371]	Dacunhasilva et al.	2021	74.5	KH, DD, UD, DU, Pressure	KNN	Own	Stress
[372]	Tsimperidis et al.	2021	92.0	KH, DD, Digraph	RBFN	Own	Gender
[372]	Tsimperidis et al.	2021	89.2	KH, DD, Digraph	RBFN	Own	Age
[373]	Tsimperidis et al.	2021	89.7	KH, DD, Digraph	RBFN	Own	Age
[30]	Tsimperidis et al.	2021	87.6	KH, DD, Digraph	RBFN	Own	Age
[30]	Tsimperidis et al.	2021	97.0	KH, DD, Digraph	RBFN	Own	Handedness
[30]	Tsimperidis et al.	2021	84.0	KH, DD, Digraph	RBFN	Own	Education level

FFBP->Feed-forward back-propagation neural networks, RBFN->Radial Basis Function Network

TABLE 22. Predictive approaches for PiDM in the smartphone environment

Ref.	Study	Year	Accuracy (%)	Features	Method	Dataset	Traits
[374]	Davarci et al.	2017	88.33	Statistical	KNN	Own	Age
[32]	Sagbas et al.	2020	87.56	Sensory, Statistical	KNN	Own	Stress
[31]	Udandarao et al.	2020	83.72	DU, UU, DD, UD	CNN	Own	Gender
[31]	Udandarao et al.	2020	82.92	DU, UU, DD, UD	CNN	Own	Age
[31]	Udandarao et al.	2020	85.37	DU, UU, DD, UD	CNN	Own	Style
[375]	Oyebola et al.	2021	73.3	Temporal, Spatial, Pressure	Random Forest	Own	Age
[375]	Oyebola et al.	2021	71.3	Temporal, Spatial, Pressure	Random Forest	Own	Gender

K-NN->K-Nearest Neighbour

G. ASYMMETRY OF RESULTS AND MISSING STUDIES

We depicted the study bias with the help of a funnel plot in Fig. 25. All the individual studies are represented by filled dots, whereas the missing studies are represented by a circle. However, the accuracy of more than 100% is absurd in the case of identification and prediction.

VIII. OPEN PROBLEMS AND OPPORTUNITIES (CONTRIBUTION TO OB11)

Smartphones are transforming personal computers from fixed desktop and laptop systems to small portable devices. Nowadays, these devices are the key sources of sensitive and private data that inevitably pose serious security risks, which makes it imperative to secure them from intruders. Therefore, a strong, usable, and low-cost version of the authentication mechanism before accessing sensitive data and applications is the need of the hour. Existing security mechanisms like graph patterns, PINs, passwords, and fingerprints can simply serve as one-time verification of users at the beginning of any session. It leads to session hijacking [376]. Nowadays, active or continuous authentication has gained popularity to deal with this issue. Since the different applications demand different security needs, controlling the device and application-level security decreases the usability of that model, in addition to the issue of energy overhead, particularly for battery-constrained devices.

In online meetings, e-learning, attendance, and surveillance systems, identifying a person from a group is also vital. The current study examined the aggregate performance of the IiSM and IiDM for desktops and smartphones, and the results are excellent. However, just a few research using these models have been found in the literature. More research is needed before these strategies may be used in practice.

A predictive model was introduced in the KD literature to use the predictive scores and levels for soft biometric techniques. The main intention was to accelerate the performance of user authentication models by recognising personal traits as extra features. It has also been identified that adding more soft biometric features increases authentication performance. Therefore, identifying the user's traits has become important. On the other hand, a variety of useful information like cognitive deficiency and fine motor skills is important for interesting applications (cognitive load in effective e-learning and online competitive examinations; neural stress for short and long durations for determination of neural disease diagnosis and treatment, fine motor ability determination for early detection of Parkinson's disease, etc.). The determination of user traits using typing tendency has potential applications such as age-restricted access control, protecting children from online threats by recognising the age below 18 and incorporating firewalls appropriate for those users, age-gender specific recommendation systems, and so on.

Holding, typing, swiping, zooming, and picking up the

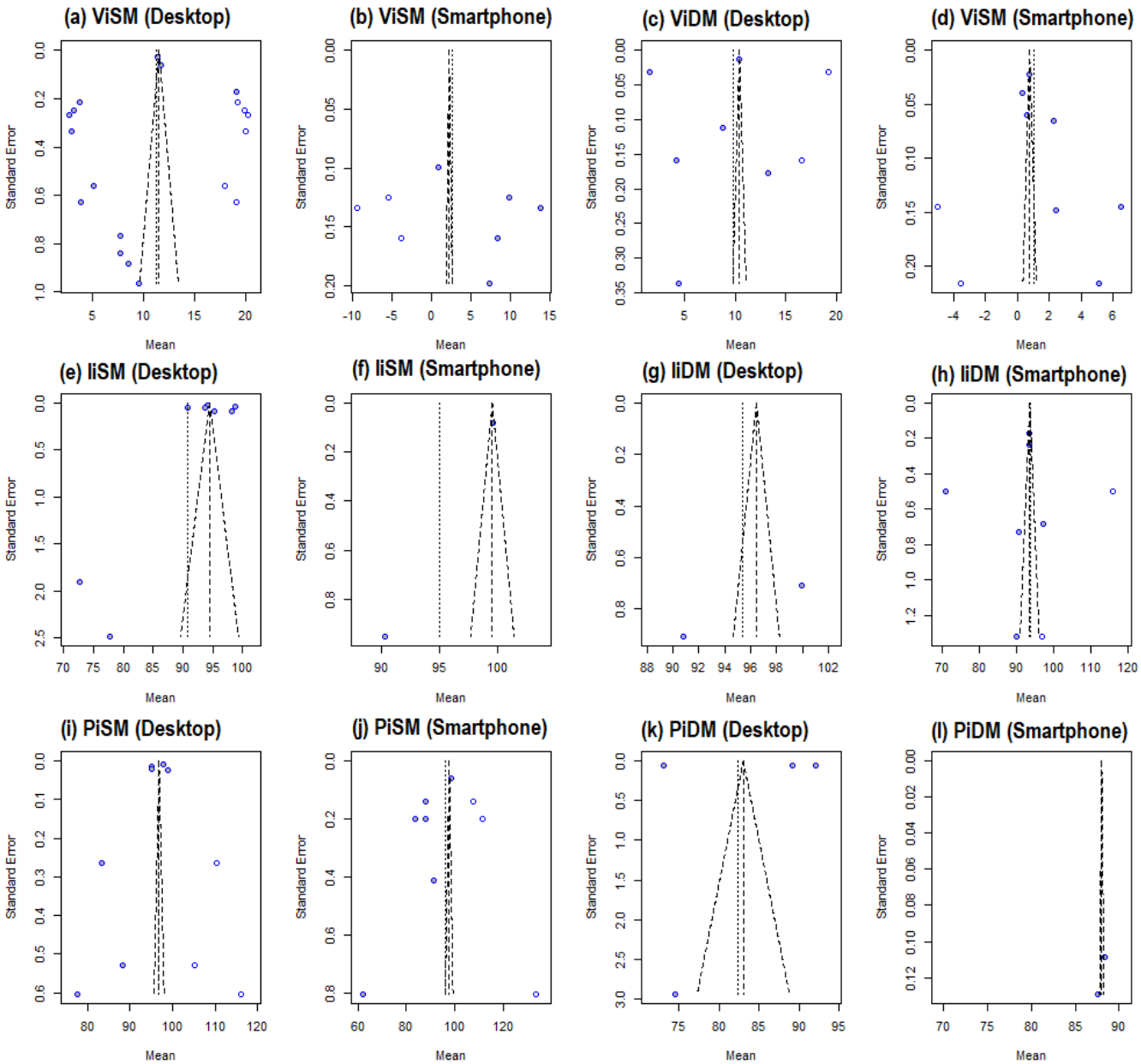

FIGURE 25. Funnel plots to assess asymmetry of results (filled points), and estimated and adjusted outcomes of missing studies by Trim and Fill method (circle points)

phone are the common activities that provide sensory and timing information that we need to measure and analyse along with KD attributes. As per the previous experiments, these activities are unique to each user and could be used for user authentication, identification, and prediction. Results and performing the ML modes show that the characteristics (a series of sensors' data) generated while typing could be effective to verify a user in an accurate and timely manner.

Covert methods of data capture and cost-effective implementation are the key advantages of KD compared with other biometrics like face or fingerprint recognition. Several issues, including a high rate of intra-class variation and cross-device validation, are associated with this mechanism. However, nowadays, the attached sensors of each smartphone give an extra opportunity to capture the orientation of the phone and the forces acting in different directions. In addition, several on-body IoT devices are now available at a low cost and could be used to generate patterns while typing. The series of data produced by sensors describes how a user touches the screen. Combining this raw sensor data with that developed during typing increases the level of usability and reliability. The research gaps, possibilities, and hints discovered suited for future KD-based research are listed below.

A. LIMITATION IN SHARING DATASETS

There are more than twenty-six datasets (3.5%) accessible in this area, each of which is distinctive in its manner (considering inputs of different lengths, types, and unique data acquisition devices in sizes, layouts, in different positions such as standing, sitting, from different groups such as a student of the university, using different data acquisition protocols such as controlled or uncontrolled environments, etc.). Each dataset was developed to solve a specific issue. As a result, to address a specific objective in this domain researchers developed temporal datasets and a maximum of them were not shared publicly.

The majority of the previous study gathered typing patterns from a specific group, such as college and university students. It decreases the scalability. Therefore, KD patterns should be gathered from a variety of groups (age, gender, handedness, hands used, education level, experience level on the keyboard, etc.) under uncontrolled situations (with eBanking, eHealth, social network interface, etc.) in a variety of positions (in standing, sitting, etc.) using a variety of devices (unique in size, weight, etc.) during a number of sessions with repeats. KD datasets need to develop in a variety of data acquisition settings, including typing tendency measurement with brain signals (EEG), heart rate signals (ECG), and patterns from implantable IoT devices, among others. To address issues such as medical diagnosis and mood analysis, this EEG and ECG variability is important. Since smartphones are now equipped with several sensors, it is necessary to incorporate all sensory features while typing. Soft biometric datasets are limited in KD literature. Therefore, personal information about users should be collected. It is essential to obtain feedback from each user about their experience in the data collecting technique in order to understand the usability score.

B. UNCERTAIN PERFORMANCE OF DETECTOR

The selection of an anomaly detector is an important issue in analysing KD characteristics since the performance of one detector jumps significantly in changing datasets collected in different data acquisition setups [65]. A study [377] used one-class SVM on touch-interaction behavioural datasets for continuous authentication in a smartphone. They observed 4.68% of FAR and 1.17% of FRR in the picture comparing activities. Another study [98] used the same detector on the PIN typing behavioural dataset but observed 7.89% of EER, comparatively higher than the previous study. Another study [378] used the same detector on the typing patterns of Arabic and English inputs on a desktop keyboard. They observed 16.9% of FAR and 42.3% of FRR for Arabic text, but it changed to 24.5% of FAR and 61.3% of FRR for English text. A study [379], used the same SVM for static user identity verification. They obtained 5.30% to 20.38% of FRR while keeping 0% of FAR for several short input texts.

Some of the few state-of-the-art detectors were compared soundly using numerous detectors on the same dataset, but the top-performing detectors are unique in each study. A study [65] compared 14 detectors and observed Manhattan (Scaled) is a top performer, similarly, a study [380] compared 20 detectors and observed Outlier-count is the most suited performer. Another study [106] tested the performance of numerous detectors using the Keystroke Biometrics Ongoing Competition (KBOC) and observed that the Manhattan distance is best matched with the lowest EER. These detector comparisons were done with certain preset, predefined configurations in the dataset gathered by conventional keyboards.

This comparison with other schemes like template formation, data augmentation, and soft biometrics is unsound. Since the evaluation performance of the detectors changes in other settings, it is important to compare the detectors with other arrangements. To our knowledge, no sound comparison has been done with other schemes, specifically on datasets collected via smartphone for continuous identity verification.

The primary hurdles in re-implementing and evaluating all previously proposed detectors in a common scenario using a common language (let's say Python) are code replicability and re-usability. However, fewer studies provided their codes for future usage.

C. PRIVACY PRESERVING ISSUE

According to a study [268], biometric authentication raises privacy concerns. To address this issue, a research [268] used a biohashing method to behavioural data obtained via smartphone. Another study [148] developed a lightweight key generation approach that gives appropriate security assurances against impersonation attacks using an on-body IoT device. However, it takes 4.6 seconds ($\approx$ 9 walking steps) to produce a 128-bit key, which adds an additional load. Recent works [381], [382], offered two cryptographic approaches to overcome this privacy risk (fuzzy hashing and fully homomorphic encryption). Another study [383], suggested a reliable and private approach for keystroke-based smartphone authentication.

D. ONE-CLASS CLASSIFICATION AND FEATURE SELECTION

In the case of focused applications such as user authentication, it is not always possible to collect all imposter patterns for negative class [384]. At the very beginning, only the owner's samples are accessible for the user to create their template. Therefore, anomaly detectors or one-class classification algorithms are more realistic and viable options than traditional binary-class classifiers. In the present study, we have explored a large set of one-class classifiers adopted in previous studies for ViSM and ViDM designs. Several anomaly detectors have not been tested yet and maybe the next detector - Additive symmetry, Divergence, Fidelity, Gower, Harmonic mean, Hassebrook, Jaccard, Jeffreys, Jensen-shannon, Motyka, Neyman, Ruzicka, Squared chi, Tanimoto, Wavehedges, etc. Because of the absence of negative class, there are difficulties in utilising traditional feature selection approaches in inducing improved performance

[385]. Therefore, the wrapper feature selection method is the most common in one-class classification.

E. ENERGY OVERHEAD

Another adverse issue in smartphone authentication is the power consumption for operating hardware resources over a long period of multi-sensor feature level fusion [386]. A study [387] mentioned that measuring gyroscope and accelerometer at 16Hz consumes energy at an overhead of 7.9%. According to another study [388], re-authentication uses 2.4% more battery. Therefore, measuring sensory data for a longer time leads to massive energy cost [110]. Most of the studies did not focus on how the resources were used, including power management. Mobile applications need to be endowed with the facilities to pause and resume the sensors' operation to save battery power, enabling longer usability.

It is better to capture the pattern for a longer period, at the cost of higher battery consumption. Then it is reasonable to ask what would be the optimum period and how to capture the pattern in both entry-point and continuous user identity verification. This will help to develop a more power-saving system. Careful consideration is needed in this regard because smartphones are energy-constrained. In this situation, data augmentation is suggested by [389]. As per the study, instead of taking sensory data for a longer time, synthetic data based on sensory data for a short burst of time is power and time-efficient.

F. LONGER DATA ACQUISITION TIME

A huge number of samples are required to develop a user's KD template in the authentication. It is a time-consuming method. To deal with this issue, synthetic samples are used. This way of generating artificial patterns is common in image recognition. It is also popular in KD pattern recognition. It increases the samples and enhances the robustness of the model. It also reduces the time needed to capture at enrolment. A recent study [265], was the first to use data augmentation in the KD domain. They found that augmented data is effective in using one-class SVM. However, the use of synthetic data in the identification and prediction models have not been explored much in the domain area.

G. TIME-SPAN OF A SESSION IN CONTINUOUS MODE

Xu et al. [148] used a 5-minute length of a session for continuous authentication using an on-body IoT device and generated signals. Another study [60] used the same duration for the implementation of KD-based continuous authentication using EEG signals for desktop. Whereas Yuksel et al. [390] used 1-minute duration to collect typing patterns via wallet apps for the same purpose. In case of predictive model, a study [226] used a 15-minute duration for identifying gender. In the case of the detection of Parkinson's disease, 15-minute of patterns were collected [225]. The effect of the time span in a session, window size for ML-ready patterns, and sampling rate on KD-based model performances has not been explored fruitfully in the literature. However, which has a huge impact on usability, needs to be investigated.

H. CAREFUL CONSIDERATION IN AUTHENTICATION DESIGN

The authentication mechanism will be more satisfied in a smartphone if the mechanism aims to have the following characteristics mentioned in the study [391] - (a) reduce user effort, (b) rely less on knowledge, (c) resist observation, and (c) provide more fine-grained protection. Another study [232] mentioned that the goals in system design are (a) implicitly, (b) continuity, (c) usability, and (d) low computational cost. A study [392] mentioned that smartphone authentication should achieve the following - (a) continuity, (b) unobservable, and (c) lightweight. Therefore, careful consideration during building the model is desired. This encourages the development of a viable KD-based authentication design.

I. SCORE FUSION METHOD

The performance of the anomaly detector as a classifier in authentication design jumps significantly due to minor changes in experimental conditions and dataset. As a result, the best detector across studies is varied. The decision level score fusion in one option boosts confidence in performance. In addition, researchers prefer score-level fusion approaches (combining the scores of multiple detectors) for use in reducing EER. There are several score fusion methods available, such as the sum rule, weighted sum rule, product rule, and min/max rule. But which method is suitable in KD, specifically in continuous mode, is still unclear. The scores of multiple detectors are needed to be fused using available score fusion methods. A study [132] reduced the EER from 19.67% to 10.05% in authentication design using score-level fusion.

J. COMPLEX REAL-WORLD SCENARIOS

The simulation of user authentication using KD characteristics in the past study considered the data from only two types of users - the device owner (genuine/legitimate user) and attackers (imposters/illegitimate users). But a real-world scenario would be much more complex. The device owner might provide access to family members or colleagues [391]. As per our knowledge, no study has been conducted on the datasets from the owner and the other users allowed by them. An identification model could be used to identify a particular family member. Similarly, an authentication model may operate after identifying a particular member. Therefore, a separate template needs to be recorded for each member.

K. CROSS-DEVICE VALIDATION

A study [107] collected the KD dataset from 70 users using three different devices (desktop: Dell Kb212-b, tablet: HTC Nexus 9, and phone: Samsung S6/HTC One), and they tested the cross-device validation in three different scenarios: desktop vs phone, desktop vs tablet, and tablet vs phone. They found impressive results with an accuracy of 99.31%,

99.33%, and 99.12% respectively, using the RF method. This evidence suggests that KD could be effective even in multi-device environments. Since the number of sensors and the clock resolution of three different devices may vary, they only collected the common temporal features (timing features) and extracted the statistical features for the model. Less effort has been given to addressing the problem of cross-device validation. In this context, no suitable dataset has been available to date. It would be better to develop the samples from each subject using multiple devices (i.e., several smartphones, each with its own screen size, weight, clock resolution, and operating system, were created by simulating highly secure apps such as e-banking, e-commerce, e/mHealth, and so on).

L. IMPROPER UTILIZATION OF FEATURES

Activities on touch screens produce a series of timing features that have been successfully used in identifying traits [28], [333]. In the previous studies, only timing feature vectors have been analysed which provides insufficient feature arrangements in predicting traits because of multiple factors, such as a higher rate of intra-class variation [198]. Typing patterns change frequently throughout the day or between two days [393]. It is determined by the user's mental state (excited, angry, sad, or normal) and position (sitting, walking, standing, running, jogging, or laying) [337], [394], [395]. Due to this fact, a study [333] used a score-fusion method where scores of multiple classifiers were considered. However, advanced sensing features like gyroscopes, accelerometers, and rotation information are readily available, prominent, and hidden features created simultaneously with the timing features. When a touch operation is performed, the smartphone's hardware automatically generates a set of data and reports them to the operating system as raw events. In particular, a one-touch operation generates a series of raw data.

M. DATA AUGMENTATION SCHEME

A recent study [389], proposed data augmentation that creates additional sensor data. This scheme reduces the data collection time and enhances the robustness and generalisation ability of the model. As per the study, it is effective to build an OCSVM. Another study [110] proposed Generative Adversarial Networks (GANs) to enhance the robustness of the continuous KD-based authentication model. However, the use of augmentation schemes to generate more realistic patterns and the effects on the classification performance in different settings have not been reported.

N. USABILITY IN ACTIVE AUTHENTICATION

Active authentication is the process of measuring and analysing biometric traits to verify the users' identities continuously and automatically [396]. It validates the genuineness of a user implicitly and continuously throughout the entire session and avoids session hijacking. In addition, minimal or no intervention is required to establish this process, which makes this technique burden-free. Furthermore, this technique could be used as an on-device or off-device security solution. The important characteristics of active authentication are continuity, usability, and transparency.

Usability is the fundamental challenge in active authentication. However, it is not definite to date. A suitable technique is required to enhance the usability of active authentication without compromising security. Therefore, controlling the trade-off between usability and security is a major concern. In addition, maintaining security at both the device and application level creates challenges. On the other hand, switching applications (with different security needs) frequently creates another challenge. Furthermore, operating multiple sensors for a longer period of time reduces battery life in battery-constrained devices.

O. FEATURE FUSION APPROACHES

The study [175] collected the sensor's data generated while typing (any text) on a smartphone from 20 users. They have taken the help of "derived features" from the raw data and score fusion of multiple machine learning approaches to get the optimum results. Another study [176] collected gyroscope, accelerometer, and rotation sensor information along with coordinates and the swipe direction by running a mathematical mobile game called the Brain Run app. They have focused on incorporating additional features generated while playing a mobile game for Implicit Continuous Authentication. Another study [390], collected the sensor's data through a wallet app. They mainly focused on incorporating statistical features like minimum, maximum, mean, and standard deviation along with soft biometric features like age and gender. These are the studies that suggest the feature fusion level approach in system design. However, numerous recent research have been claimed to have solely addressed temporal aspects rather than a mix of temporal, spatial, sensory, and statistical information. Section IV of the current study can assist researchers in collecting multi-modal features in both desktop and smartphone domains.

P. CONVENTIONAL MODEL EVALUATION TEST OPTION

In Biometric science, researchers collect samples from a user regularly to calculate intra-class variability. Similarly, the patterns in several sessions of each subject are collected to develop adaptation methods to address ageing. Therefore, researchers collect data in various postures and settings to measure the external influences. If we utilise the k-fold (5-fold or 10-fold) cross-validation evaluation method, samples from a subject may be distributed in the training and testing sets, resulting in unrealistic findings [38]. When a user checks his or her gender/age group/handedness/disease/stress, the data from that user should not be included in the training set. It requires careful consideration in the machine learning (ML) model evaluation. Studies [333] applied (Leave-One-User-Out Cross Validation) LOUOCV to address this problem. However, the non-uniformity of KD raises the additional difficulty of class imbalance in LOUOCV.

IX. CONCLUSIONS

Most of the recent state-of-the-art models in the KD domain have been reviewed in this study. This is the widest literature review on KD-based user authentication, identification, and prediction models that will encourage newcomers to work better in the topic areas. The details of the different system designs and the approaches planned in the last six years have been furnished. It also presents recent research directions on using feature arrangements, classification methods, and adaptation techniques that will encourage the future composition of KD-based models.

A comprehensive data acquisition setup and protocols for improving benchmark datasets have been provided. In both desktop/laptop and smartphone environments, data collection apparatus, inputs, devices, and modes of selection may be motivated to determine the best path for producing datasets.

In this review, 6.34% of aggregated EER for predefined inputs using conventional keyboards has been observed, which is suitable for entry-point user authentication, and could be used to safeguard the PIN/password, reducing the chances of brute-force, dictionary, and shoulder surfing attacks. For continuous user validity throughout a session in a desktop environment, the EER is slightly lower (5.67%) than fixed inputs, which could be useful for active/adaptive/passive/implicit/continuous user authentication that reduces the probability of session hijacking and reduces unproductive password related time.

In the case of one-time user identification from a group of users, an aggregate accuracy of 90.38% has been observed, which could be useful to identify a particular user from a group of users. However, identification through continuously generated patterns using a conventional keyboard is more accurate (95.24%) than the previous (predefined arrangement). In the case of a predictive model using the patterns developed by a conventional keyboard, 91.09% of aggregate accuracy in a static model has been observed, whereas it was significantly less (81.95%) in the dynamic mode, which could be used to predict users' traits, disease, etc.

With high dimensional features using recent sensors, 6.15% of aggregated EER using the predefined inputs has been observed for entry-point user authentication on a smartphone. However, it is 1.55% in the continuous domain. In the case of user identification for fixed input in a smartphone, 94.9% of aggregate accuracy has been observed, which is less than (88.83%) in dynamic mode. The predictive model achieved an aggregated accuracy of 84.53% and 87.95% for static and dynamic modes respectively.

This study also answered the twelve hypotheses and found considerable heterogeneity across studies for each KD-based design. It indicates that all the included studies for each design are significantly different from the others. The following factors may differ from one study to another - classification technique, feature arrangement, dataset, evaluation condition, subject selection, and so on. Therefore, proper assessment and configuration are necessary for any KD-based system to achieve acceptable performance. Furthermore, improvements to the future version of the KD-based system must be assessed under the same assessment conditions and dataset. Otherwise, it is impossible to compare and confirm the future model.

Finally, several issues, various opportunities, and hints have been identified and discussed addressing the recent complications. So that KD-based systems can meet their promises in both desktop and smartphone environments.

DECLARATIONS

Conflict of interest The authors state that they do not have any conflicts of interest

REFERENCES

[1] K.-W. Tse and K. Hung, "Framework for user behavioural biometric identification using a multimodal scheme with keystroke trajectory feature and recurrent neural network on a mobile platform," *IET Biometrics*, vol. 11, 2022.

[2] S. M. Matyas and J. Stapleton, "A Biometric Standard for Information Management and Security," *Computers & Security*, vol. 19, no. 5, pp. 428–441, 2000. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016740480005029X

[3] G. Lowe, "A Hierarchy of Authentication Specifications," in *Proceedings 10th Computer Security Foundations Workshop*, 1997, pp. 31–43.

[4] M. W. Abo El-Soud, T. Gaber, F. AlFayez, and M. M. Eltoukhy, "Implicit authentication method for smartphone users based on rank aggregation and random forest," *Alexandria Engineering Journal*, vol. 60, no. 1, pp. 273–283, feb 2021.

[5] B. Bhana and S. Flowerday, "Passphrase and keystroke dynamics authentication: Usable security," *Computers and Security*, vol. 96, 2020.

[6] S. Furnell, N. Clarke, and S. Karatzouni, "Beyond the PIN: Enhancing user authentication for mobile devices," *Computer Fraud & Security*, vol. 2008, no. 8, pp. 12–17, aug 2008.

[7] S. Mondal and P. Bours, "A continuous combination of security & forensics for mobile devices," *Journal of Information Security and Applications*, 2018.

[8] R. Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Technology & People*, vol. 7, no. 4, pp. 6–37, 1994.

[9] A. C. Iapa and V. I. Cretu, "Modified Distance Metric That Generates Better Performance for the Authentication Algorithm Based on Free-Text Keystroke Dynamics," *SACI 2021 - IEEE 15th International Symposium on Applied Computational Intelligence and Informatics, Proceedings*, pp. 455–460, may 2021.

[10] D. Palma and P. L. Montessoro, "Biometric-Based Human Recognition Systems: An Overview," *Recent Advances in Biometrics [Working Title]*, jan 2022. [Online]. Available: https://www.intechopen.com/online-first/80031

[11] S. Roy, U. Roy, and D. Sinha, "User Authentication: Keystroke Dynamics with Soft Biometric Features," in *Internet of Things (IOT) Technologies, Applications, Challenges and Solutions*, 1st ed., C. P. T. &. F. Group, Ed. Boca Raton, FL 33487-2742: CRC Press, 2017, ch. 6, pp. 105–124.

[12] I. Buciu and A. Gacsadi, "Biometrics systems and technologies: A survey," *International Journal of Computers, Communications and Control*, vol. 11, no. 3, 2016.

[13] A. Komarova and A. Korobeynikov, "Combined authentication schemes with increasing level of resistance and methods for improving the security of electronic signature schemes: Kombinirovannye Skhemy Autentifikaciis Povyshennym Urovnem Stojkostii Metody Povysheniya Bezopasnosti Skhem Elektro," *ACM International Conference Proceeding Series*, 2019.

[14] A. G. Martín, I. Martín de Diego, A. Fernández-Isabel, M. Beltrán, and R. R. Fernández, "Combining user behavioural information at the feature level to enhance continuous authentication systems," *Knowledge-Based Systems*, vol. 244, p. 108544, may 2022. [Online]. Available: https://doi.org/10.1016/j.knosys.2022.108544

[15] D. Rudrapal and S. Das, "Analysis and evaluation of keystroke duration of user's typing as a distinctive measure of recognition," *Lecture Notes in Electrical Engineering*, 2013. [Online]. Avail-

able: http://www.mendeley.com/research/analysis-evaluation-keystroke-duration-users-typing-distinctive-measure-recognition

[16] M. N. Yaacob, S. Z. S. Idrus, W. N. A. W. Ali, W. A. Mustafa, M. A. Jamlos, and M. H. A. Wahab, "Decision Making Process in Keystroke Dynamics," in *Journal of Physics: Conference Series*, vol. 1529, no. 2, 2020.

[17] G. Stragapede, R. Vera-Rodriguez, R. Tolosana, A. Morales, A. Acien, G. El, L. Lan, and G. Le Lan, "Mobile Behavioral Biometrics for Passive Authentication," *Pattern Recognition Letters*, mar 2022. [Online]. Available: http://arxiv.org/abs/2203.07300

[18] V. Zimmermann and N. Gerber, "The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes," *International Journal of Human Computer Studies*, 2020.

[19] H. M. Sim, H. Asmuni, R. Hassan, and R. M. Othman, "Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images," *Expert Systems with Applications*, 2014.

[20] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Computer Networks*, 2020.

[21] I. Kim, "Keypad against brute force attacks on smartphones," *IET Information Security*, vol. 6, no. 2, pp. 71–76, 2012.

[22] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," *SOUPS 2011 - Proceedings of the 7th Symposium on Usable Privacy and Security*, pp. 1–12, 2011.

[23] X. Yu, Z. Wang, Y. Li, L. Li, W. T. Zhu, and L. Song, "EvoPass: Evolvable graphical password against shoulder-surfing attacks," *Computers and Security*, 2017.

[24] C. Giuffrida, K. Majdanik, M. Conti, and H. Bos, "I sensed it was you: Authenticating mobile users with sensor-enhanced keystroke dynamics," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8550 LNCS, pp. 92–111, 2014.

[25] S. Singh, A. Inamdar, A. Kore, and A. Pawar, "Analysis of Algorithms for User Authentication using Keystroke Dynamics," in *Proceedings of the 2020 IEEE International Conference on Communication and Signal Processing, ICCSP 2020*, 2020.

[26] N. Raul, R. Shankarmani, and P. Joshi, "Non-Conventional Factors for Keystroke Dynamics as a Support Factor for Authenticating User," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 4, 2020.

[27] G. J. Krishna, H. Jaiswal, P. S. R. Teja, and V. Ravi, "Keystroke based User Identification with XGBoost," in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, vol. 2019-Octob, 2019.

[28] S. Roy, U. Roy, and D. Sinha, "Analysis of typing pattern in identifying soft biometric information and its impact in user recognition," in *Advances in Intelligent Systems and Computing*. Springer, Singapore, 2019, vol. 699.

[29] S. Roy, U. Roy, and D. D. Sinha, "Deep Learning Approach in Predicting Personal Traits Based on the Way User Type on Touchscreen," in *Advances in Intelligent Systems and Computing*, vol. 999, 2020.

[30] I. Tsimperidis, G. Peikos, and A. Arampatzis, "Classifying Users Through Keystroke Dynamics," in *Studies in Classification, Data Analysis, and Knowledge Organization*, vol. 5, 2021.

[31] V. Udandarao, M. Agrawal, R. Kumar, and R. R. Shah, "On the Inference of Soft Biometrics from Typing Patterns Collected in a Multi-device Environment," in *Proceedings - 2020 IEEE 6th International Conference on Multimedia Big Data, BigMM 2020*. Institute of Electrical and Electronics Engineers Inc., sep 2020, pp. 76–85.

[32] E. A. Sağbaş, S. Korukoglu, and S. Balli, "Stress Detection via Keyboard Typing Behaviors by Using Smartphone Sensors and Machine Learning Techniques," *Journal of Medical Systems*, vol. 44, no. 4, 2020.

[33] R. Giot, A. Ninassi, M. El-Abed, and C. Rosenberger, "Analysis of the acquisition process for keystroke dynamics," in *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG - Proceedings of the International Conference of the*, 2012, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6313543

[34] S. Rajput and P. Vijayavargiya, "Objective of Keystroke Dynamics for Identifying Emotional State," *International Journal of Computer Science and Information Technologies*, vol. 6, no. 1, 2015.

[35] R. E. Mastoras, D. Iakovakis, S. Hadjidimitriou, V. Charisis, S. Kassie, T. Alsaadi, A. Khandoker, and L. J. Hadjileontiadis, "Touchscreen typing pattern analysis for remote detection of the depressive tendency," *Scientific Reports*, 2019.

[36] A. Ntracha, D. Iakovakis, S. Hadjidimitriou, V. S. Charisis, M. Tsolaki, and L. J. Hadjileontiadis, "Detection of Mild Cognitive Impairment Through Natural Language and Touchscreen Typing Processing," *Frontiers in Digital Health*, vol. 2, no. October, pp. 1–13, 2020.

[37] D. Iakovakis, K. R. Chaudhuri, L. Klingelhoefer, S. Bostantjopoulou, Z. Katsarou, D. Trivedi, H. Reichmann, S. Hadjidimitriou, V. Charisis, &. Leontios, and J. Hadjileontiadis, "Screening of parkinsonian subtle fine-motor impairment from touchscreen typing via deep learning," *Scientific Reports*, vol. 10, no. 12623, pp. 1–13, 2020. [Online]. Available: https://doi.org/10.1038/s41598-020-69369-1

[38] S. Roy, U. Roy, and D. Sinha, "Identifying age group and gender based on activities on touchscreen," *International Journal of Biometrics*, vol. 14, no. 1, p. 61, 2022.

[39] M. N. Yaacob, S. Z. S. Idrus, W. N. A. W. Ali, W. A. Mustafa, M. A. Jamlos, and M. H. A. Wahab, "Soft Biometrics and Its Implementation in Keystroke Dynamics," *Journal of Physics: Conference Series*, 2020.

[40] S. Roy, U. Roy, and D. Sinha, "Analysis of Typing Pattern in Identifying Soft Biometric Information and Its Impact in User Recognition," in *Information Technology and Applied Mathematics, Advances in Intelligent Systems and Computing*. Springer, Singapore, 2019, pp. 69–83.

[41] S. Roy, U. Roy, and D. Sinha, "Efficacy of Typing Pattern Analysis in Identifying Soft Biometric Information and Its Impact in User Recognition," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10590 LNCS, 2017, pp. 320–330.

[42] S. Earl, J. Campbell, and O. Buckley, "Identifying Soft Biometric Features from a Combination of Keystroke and Mouse Dynamics," in *Lecture Notes in Networks and Systems*, vol. 268, 2021.

[43] H. Crawford, "Keystroke dynamics: Characteristics and opportunities," *PST 2010: 2010 8th International Conference on Privacy, Security and Trust*, pp. 205–212, 2010.

[44] S. P. Banerjee and D. Woodard, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey," *Journal of Pattern Recognition Research*, vol. 7, no. 1, pp. 116–139, 2012.

[45] P. H. Pisani and A. C. Lorena, "A systematic review on keystroke dynamics," *Journal of the Brazilian Computer Society*, vol. 19, no. 4, pp. 573–587, 2013.

[46] P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," 2013.

[47] P. S. Teh, N. Zhang, A. B. J. Teoh, and K. Chen, "A survey on touch dynamics authentication in mobile devices," *Computers and Security*, 2016.

[48] M. L. Ali, J. V. Monaco, C. C. Tappert, and M. Qiu, "Keystroke Biometric Systems for User Authentication," *Journal of Signal Processing Systems*, pp. 1–16, 2016.

[49] L. Yang and S.-F. Qin, "A Review of Emotion Recognition Methods From Keystroke, Mouse, and Touchscreen Dynamics," *IEEE Access*, vol. 9, pp. 162 197–162 213, 2021.

[50] M. Mohlala, A. R. Ikuesan, and H. S. Venter, "User attribution based on keystroke dynamics in digital forensic readiness process," *2017 IEEE Conference on Applications, Information and Network Security, AINS 2017*, 2018.

[51] E. Kochegurova, E. Luneva, and E. Gorokhova, "On continuous user authentication via hidden free-text based monitoring," in *Advances in Intelligent Systems and Computing*, 2019.

[52] M. Koistinen, "Tolerance for Typographical Errors on Password Authentication Securely via Keystroke Dynamics," 2021.

[53] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "Continuous Authentication using Deep Neural Networks Ensemble on Keystroke Dynamics," *PeerJ Computer Science*, vol. 7, pp. 1–27, 2021.

[54] W. L. Bryan and N. Harter, "Studies in the physiology and psychology of the telegraphic language," *Psychological Review*, vol. VI, no. 4, pp. 345–375, 1899.

[55] R. J. Spillane, "Keyboard Apparatus for Personal Identification," 1975.

[56] G. Forsen, M. Nelson, and R. J. Staron, "Personal attributes authentication techniques," Rome Air Development Center, Tech. Rep., 1977.

[57] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by Keystroke Timing: Some Preliminary Results," in *Technical Report R-2526-NSF*, may ed. Rand Corporation, 1980.

[58] J. D. Garcia, "PERSONAL IDENTIFICATION APPARATUS," 1986.

[59] J. Leggett and G. Williams, "Verifying identity via keystroke characteristics," *International Journal of Man-Machine Studies*, vol. 28, no. 1, pp. 67–76, 1988.

[60] J. Duprez, "Synchronization between keyboard typing and neural oscillations Abbreviated title: Neural oscillations and synchronization with typing Corresponding author," *bioRxiv*, 2020.

[61] M. Ehatisham-ul Haq, M. A. Azam, J. Loo, K. Shuang, S. Islam, U. Naeem, and Y. Amin, "Authentication of smartphone users based on activity recognition and mobile sensing," *Sensors (Switzerland)*, 2017.

[62] Z. Chen, H. Cai, L. Jiang, W. Y. Zou, W. Zhu, and X. Fei, "Keystroke Dynamics Based User Authentication and its Application in Online Examination," *Proceedings of the 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2021*, pp. 649–654, may 2021.

[63] A. Mhenni, E. Cherrier, C. Rosenberger, and N. Essoukri Ben Amara, "Analysis of Doddington zoo classification for user dependent template update: Application to keystroke dynamics recognition," *Future Generation Computer Systems*, 2019.

[64] A. K. Kumar M, K. B. R, S. B. R, and S. J. Victor, "A Multimodal Approach To Detect User's Emotion," *Procedia Computer Science*, vol. 70, pp. 296–303, 2015.

[65] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in *Proceedings of the International Conference on Dependable Systems and Networks*, 2009, pp. 125–134.

[66] K. Killourhy and R. Maxion, "The effect of clock resolution on keystroke dynamics," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5230 LNCS, pp. 331–350, 2008.

[67] Y. M. Lim, A. Ayesh, and M. Stacey, "Exploring direct learning instruction and external stimuli effects on learner's states and mouse/keystroke behaviours," *Proceedings - 2016 4th International Conference on User Science and Engineering, i-USEr 2016*, 2017.

[68] L. Xiaofeng, Z. Shengfei, and Y. Shengwei, "Continuous authentication by free-text keystroke based on CNN plus RNN," *Procedia Computer Science*, 2019.

[69] S. Roy, U. Roy, and D. Sinha, "Protection of kids from internet threats: A machine learning approach for classification of age-group based on typing pattern," *Lecture Notes in Engineering and Computer Science*, 2018.

[70] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, S. Mondal, and P. Bours, "Keystroke dynamics performance enhancement with soft biometrics," in *2015 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2015*, 2015.

[71] Y. Uzun, K. Bicakci, and Y. Uzunay, "Could We Distinguish Child Users from Adults Using Keystroke Dynamics?" Middle East Technical University, Ankara, Turkey, Tech. Rep., 2014. [Online]. Available: http://arxiv.org/abs/1511.05672

[72] R. Giot, M. El-Abed, and C. Rosenberger, "Web-Based Benchmark for Keystroke Dynamics Biometric Systems: A Statistical Analysis," *Intelligent information hiding andmultimedia signal processing (IIH-MSP)*, pp. 11–15, 2012. [Online]. Available: http://arxiv.org/abs/1207.0784

[73] K. S. Killourhy, "A Scientific Understanding of Keystroke Dynamics," Ph.D. dissertation, 2012.

[74] I. Tsimperidis, P. D. Yoo, K. Taha, A. Mylonas, and V. Katos, "R2BN: An Adaptive Model for Keystroke-Dynamics-Based Educational Level Classification," *IEEE Transactions on Cybernetics*, 2018.

[75] M. Antal and G. Nemes, "Gender recognition from mobile biometric data," *SACI 2016 - 11th IEEE International Symposium on Applied Computational Intelligence and Informatics, Proceedings*, pp. 243–248, 2016.

[76] A. Kolakowska, A. Landowska, P. Jarmolkowicz, M. Jarmolkowicz, and K. Sobota, "Automatic recognition of males and females among web browser users based on behavioural patterns of peripherals usage," *Internet Research*, vol. 26, no. 5, pp. 1093–1111, 2016. [Online]. Available: http://dx.doi.org/10.1108/IntR-04-2015-0100

[77] Z. J., A. P., R. M., E. R., B. P., L. S., M. M., A. O., N. P., R. K., and L. A., "Predicting mood disturbance severity in bipolar subjects with mobile phone keystroke dynamics and metadata," *Biological Psychiatry*, vol. 81, no. 10, 2017.

[78] P. R. Borj and P. Bours, "Detecting liars in chats using keystroke dynamics," *ACM International Conference Proceeding Series*, 2019.

[79] H. R. Lv, Z. L. Lin, W. J. Yin, and J. Dong, "Emotion recognition based on pressure sensor keyboards," in *2008 IEEE International Conference on Multimedia and Expo, ICME 2008 - Proceedings*, 2008.

[80] A. Kołakowska, "Towards detecting programmers' stress on the basis of keystroke dynamics," *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems*, 2016.

[81] L. M. Vizer and A. Sears, "Detecting cognitive impairment using keystroke and linguistic features of typed text: Toward an adaptive method for continuous monitoring of cognitive status," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7058 LNCS, pp. 483–500, 2011.

[82] T. Committee, R. Maxion, T. Mitchell, D. Siewiorek, A. R. Reserved, L. M. Vizer, L. Zhou, A. Sears, D. R. Dacunhasilva, Z. Wang, R. Gutierrez-Osuna, A. Sultanov, K. Kogos, S. V. Hoecke, R. Van, W. Counsellor, O. J. Master, I. Systems, R. Van, P. B. Pankajavalli, G. S. Karthick, R. Sakthivel, Y. M. Lim, A. Ayesh, M. Stacey, J. Hernandez, P. Paredes, A. Roseway, and M. Czerwinski, "Detecting emotional stress during typing task with time pressure," *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*, vol. 36, no. 4, pp. 256–265, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.ijhcs.2009.07.005

[83] D. Iakovakis, S. Hadjidimitriou, V. Charisis, S. Bostanjopoulou, Z. Katsarou, L. Klingelhoefer, S. Mayer, H. Reichmann, S. B. DIas, J. A. DIniz, D. Trivedi, R. K. Chaudhuri, and L. J. Hadjileontiadis, "Early Parkinson's Disease Detection via Touchscreen Typing Analysis using Convolutional Neural Networks," in *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, 2019.

[84] A. Milne, K. Farrahi, and M. A. Nicolaou, "Less is More: Univariate Modelling to Detect Early Parkinson's Disease from Keystroke Dynamics," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11198 LNAI, 2018.

[85] S. Ghosh, S. Sahu, N. Ganguly, B. Mitra, and P. De, "EmoKey: An Emotion-aware Smartphone Keyboard for Mental Health Monitoring," *2019 11th International Conference on Communication Systems and Networks, COMSNETS 2019*, 2019.

[86] L. Van Waes, M. Leijten, P. Mariën, and S. Engelborghs, "Typing competencies in Alzheimer's disease: An exploration of copy tasks," *Computers in Human Behavior*, vol. 73, pp. 311–319, 2017.

[87] K. Lam, K. Meijer, F. Loonstra, E. Coerver, J. Twose, E. Redeman, B. Moraal, F. Barkhof, V. de Groot, B. Uitdehaag, and J. Killestein, "Real-world keystroke dynamics are a potentially valid biomarker for clinical disability in multiple sclerosis," *Multiple Sclerosis Journal*, p. 135245852096879, 2020.

[88] J. Twose, G. Licitra, H. McConchie, K. H. Lam, and J. Killestein, "Early-warning signals for disease activity in patients diagnosed with multiple sclerosis based on keystroke dynamics," *Chaos*, vol. 30, no. 11, 2020.

[89] K. A. Hubel, E. W. Yund, T. J. Herron, and D. L. Woods, "Computerized measures of finger tapping: Reliability, malingering and traumatic brain injury," *Journal of Clinical and Experimental Neuropsychology*, vol. 35, no. 7, pp. 745–758, 2013.

[90] F. Gao, X. Mei, and A. C. Chen, "Delayed finger tapping and cognitive responses in preterm-born male teenagers with mild spastic diplegia," *Pediatric Neurology*, vol. 52, no. 2, pp. 206–213, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.pediatrneurol.2014.04.012

[91] BioPassword, "BioPassword 4.5: Hardware-Free Biometrics," 2001. [Online]. Available: http://www.pcmag.com/article2/0,2817,38615,00.asp

[92] AuthenWare, "The Rhythm of Security," 2010. [Online]. Available: www.authenware.com

[93] D. Security, "Deepnet Security Two?factor authentication for Windows computers," 2021. [Online]. Available: http://www.deepnetsecurity.com/desktop/windows/

[94] Behaviosec, "Continuous Authentication with Behavioral Biometrics," 2012. [Online]. Available: https://www.behaviosec.com

[95] I. Control, "KeystrokeID," 2017.

[96] TypingDNA, "Typing Biometrics Auth . API for Two-Factor Authentication Based on Keystroke Dynamics," 2016. [Online]. Available: http://typingdna.com

[97] A. Das, C. Galdi, H. Han, R. Ramachandra, J.-l. Dugelay, S. Antipolis, and S. Antipolis, "Recent Advances in Biometric Technology for Mobile Devices," *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–11, 2020.

[98] H. Lee, J. Y. Hwang, D. I. Kim, S. Lee, S.-H. Lee, and J. S. Shin, "Understanding Keystroke Dynamics for Smartphone Users Authentication and

Keystroke Dynamics on Smartphones Built-In Motion Sensors," *Security and Communication Networks*, vol. 2018, 2018.

[99] P. S. Teh, S. Yue, and A. B. Teoh, "Feature Fusion Approach on Keystroke Dynamics Efficiency Enhancement," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 1, no. 1, pp. 20–31, 2012.

[100] R. Kumar, V. V. Phoha, and A. Serwadda, "Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns," *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*, 2016.

[101] M. Pleva, P. Bours, S. Ondáš, and J. Juhár, "Improving static audio keystroke analysis by score fusion of acoustic and timing data," *Multimedia Tools and Applications*, 2017.

[102] P. Baynath, K. M. Soyjaudah, and M. H. M. Khan, "Machine Learning Algorithm on Keystroke dynamics Fused pattern in biometrics," *2nd International Conference on Next Generation Computing Applications 2019, NextComp 2019 - Proceedings*, 2019.

[103] A. Muthuramalingam, J. Gnanamanickam, and R. Muhammad, "Optimum Feature Selection Using Firefly Algorithm for Keystroke Dynamics," in *Advances in Intelligent Systems and Computing*, vol. 736, 2018.

[104] D. El Zein and A. Kalakech, "Feature Selection for Android Keystroke Dynamics," *ACIT 2018 - 19th International Arab Conference on Information Technology*, 2018. [Online]. Available: http://www.mendeley.com/research/feature-selection-android-keystroke-dynamics

[105] E. Ivannikova, G. David, and T. Hamalainen, "Anomaly detection approach to keystroke dynamics based user authentication," *Proceedings - IEEE Symposium on Computers and Communications*, 2017.

[106] J. V. Monaco, "Robust Keystroke Biometric Anomaly Detection," *arXiv preprint arXiv:1606.09075*, 2016.

[107] A. K. Belman and V. V. Phoha, "DoubleType: Authentication Using Relationship between Typing Behavior on Multiple Devices," in *2020 International Conference on Artificial Intelligence and Signal Processing, AISP 2020*, 2020.

[108] P. Smriti, S. Srivastava, and S. Singh, "Keyboard Invariant Biometric Authentication," *International Conference on "Computational Intelligence and Communication Technology", CICT 2018*, 2018.

[109] Y. Zeng, A. Pande, J. Zhu, and P. Mohapatra, "WearIA: Wearable device implicit authentication based on activity information," *18th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2017 - Conference*, 2017.

[110] Y. Wang, C. Wu, K. Zheng, and X. Wang, "Improving reliability: User authentication on smartphones using keystroke biometrics," *IEEE Access*, 2019.

[111] Z. Yu, H. Du, D. Xiao, Z. Wang, Q. Han, and B. Guo, "Recognition of Human Computer Operations Based on Keystroke Sensing by Smartphone Microphone," *IEEE Internet of Things Journal*, 2018.

[112] Y. Sun, H. Ceker, and S. Upadhyaya, "Shared Keystroke Dataset for Continuous Authentication," in *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2016, pp. 0–5.

[113] A. Pentel, "Emotions and user interactions with keyboard and mouse," *2017 8th International Conference on Information, Intelligence, Systems and Applications, IISA 2017*, 2018.

[114] Neha and K. Chatterjee, "Continuous User Authentication System: A Risk Analysis Based Approach," *Wireless Personal Communications*, 2019.

[115] S. Roy, U. Roy, and D. Sinha, "Password Recovery Mechanism Based on Keystroke Dynamics', in Information Systems Design and Intelligent, ed. by Poland Janusz Kacprzyk, Polish Academy of Sciences, Warsaw (Springer, 2015), cccxxxix, 245–59ssword," in *Information Systems Design and Intelligent*, P. Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Ed., vol. 339. Springer, 2015, pp. 245–259.

[116] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, and D. Moher, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, mar 2021. [Online]. Available: https://www.bmj.com/content/372/bmj.n71 https://www.bmj.com/content/372/bmj.n71.abstract

[117] C. C. Loy, C. P. Lim, and W. K. Lai, "Pressure-based typing biometrics user authentication using the fuzzy ARTMAP neural network," in *International Conference on Neural Information Processing (ICONIP)*, 2005.

[118] R. Giot, M. El-abed, C. Rosenberger, R. Giot, M. El-abed, C. Rosenberger, G. Keystroke, C. Rosenberger, and M. El-abed, "GREYC Keystroke : a Benchmark for Keystroke Dynamics Biometric Systems," in *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2009)*, I. C. Society, Ed., Washington, United States., 2009.

[119] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics database: A benchmark for keystroke dynamics biometric systems," in *Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the*, no. September, 2013, pp. 1–8.

[120] A. Morales, J. Fierrez, R. Tolosana, J. Ortega-Garcia, J. Galbally, M. Gomez-Barrero, A. Anjos, and S. Marcel, "Keystroke Biometrics Ongoing Competition," *IEEE Access*, vol. 4, pp. 7736–7746, 2016.

[121] Y. Li, B. Zhang, Y. Cao, S. Zhao, Y. Gao, and J. Liu, "Study on the BeiHang keystroke dynamics database," *2011 International Joint Conference on Biometrics, IJCB 2011*, 2011.

[122] Y. Sun, H. Ceker, and S. Upadhyaya, "Shared keystroke dataset for continuous authentication," in *8th IEEE International Workshop on Information Forensics and Security, WIFS 2016*, 2017.

[123] L. Bello and M. Bertacchini, "Collection and publication of a fixed text keystroke dynamics dataset," *CACIC 2010 - XVI CONGRESO ARGENTINO DE CIENCIAS DE LA COMPUTACIÓN*, pp. 822–831, 2010. [Online]. Available: http://sedici.unlp.edu.ar/handle/10915/19357

[124] E. Vural, J. Huang, D. Hou, and S. Schuckers, "Shared research dataset to support development of keystroke authentication," in *IJCB 2014 - 2014 IEEE/IAPR International Joint Conference on Biometrics*, 2014.

[125] J. R. Montalva and E. O. Freire, "On the equalization of keystroke timing histograms," *Pattern Recognition Letters*, vol. 27, pp. 1440–1446, 2006.

[126] E. P. Calot, J. S. Ierache, and W. Hasperue, "Document Typist Identification by Classification Metrics Applying Keystroke Dynamics Under Unidealised Conditions," in *2019 International Conference on Document Analysis and Recognition Workshops (ICDARW)*, 2019.

[127] L. Giancardo, A. Sánchez-Ferro, T. Arroyo-Gallego, I. Butterworth, C. S. Mendoza, P. Montero, M. Matarazzo, J. A. Obeso, M. L. Gray, and R. S. J. Estépar, "Computer keyboard interaction as an indicator of early Parkinson's disease," *Scientific Reports*, vol. 6, pp. 1–10, 2016. [Online]. Available: http://dx.doi.org/10.1038/srep34468

[128] A. L. Goldberger, L. A. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C. K. Peng, and H. E. Stanley, "PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals." *Circulation*, vol. 101, no. 23, 2000.

[129] M. Monaro, C. Galante, R. Spolaor, Q. Q. Li, L. Gamberini, M. Conti, and G. Sartori, "Covert lie detection using keyboard dynamics," *Scientific Reports*, 2018.

[130] M. El-Abed, M. Dafer, and R. E. Khayat, "RHU Keystroke: A mobile-based benchmark for keystroke dynamics systems," *2014 International Carnahan Conference on Security Technology (ICCST)*, pp. 1–4, 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6986984/

[131] M. Antal and L. Nemes, "The MOBIKEY keystroke dynamics password database: Benchmark results," *Advances in Intelligent Systems and Computing*, 2016.

[132] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG : New Behavioral Biometric Features for Continuous Authentication of Smartphone Users *," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2016.

[133] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, 2013.

[134] M. Antal, Z. Bokor, and L. ZsoltSzabó, "Information revealed from scrolling interactions on mobile devices," *Pattern Recognition Letters*, 2015.

[135] P. Teh, N. Zhang, A. Teoh, and K. Chen, "Recognizing Your Touch: Towards Strengthening Mobile Device Authentication via Touch Dynamics Integration," *13th International Conference on Advances in Mobile Computing and Multimedia, MoMM 2015 - Proceedings*, 2015.

[136] M. J. Coakley, J. V. Monaco, and C. C. Tappert, "Keystroke biometric studies with short numeric input on smartphones," *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*, 2016.

[137] J. Kim and P. Kang, "Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features," *Pattern Recognition*, vol. 108, 2020.

[138] M. El-Abed, M. Dafer, and C. Rosenberger, "RHU keystroke touchscreen benchmark," *Proceedings - 2018 International Conference on Cyberworlds, CW 2018*, 2018.

[139] V. Dhakal, A. M. Feit, P. O. Kristensson, and A. Oulasvirta, "Observations on Typing from 136 Million Keystrokes," *Proc. of CHI*, 2018.

[140] K. S. Killourhy and R. A. Maxion, "Free vs. transcribed text for keystroke-dynamics evaluations," in *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results - LASER '12*. New York, New York, USA: ACM Press, 2012, pp. 1–8. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2379616.2379617

[141] M. S. Obaidat and B. Sadoun, "Keystroke Dynamics Based Authentication," *Biometrics*, pp. 213–229, 1996. [Online]. Available: http://link.springer.com/10.1007/0-306-47044-6_10

[142] R. A. J. Everitt and P. W. McOwan, "Java-based internet biometric authentication system," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1166–1172, 2003.

[143] L. Cai and H. Chen, "TouchLogger: inferring keystrokes on touch screen from smartphone motion," *Proceedings of the 6th USENIX Conference on Hot Topics in Security*, pp. 1–6, 2011. [Online]. Available: https://www.usenix.org/events/hotsec11/tech/final_files/Cai.pdf

[144] J. Angulo and E. Wästlund, "Exploring touch-screen biometrics for user identification on smart phones," *IFIP Advances in Information and Communication Technology*, vol. 375 AICT, pp. 130–143, 2012.

[145] M. Antal, L. Z. Szabó, and I. László, "Keystroke Dynamics on Android Platform," *Procedia Technology*, vol. 19, pp. 820–826, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S221201731500119X

[146] D. Zaidan, A. Salem, A. Swidan, and R. Saifan, "Factors affecting keystroke dynamics for verification: Data collecting and analysis," *ICIT 2017 - 8th International Conference on Information Technology, Proceedings*, 2017.

[147] A. Vasyl, E. Sharapova, O. Ivanova, G. Denis, and S. Yuliia, "Web-based application to collect and analyze users data for keystroke biometric authentication," *2017 IEEE 1st Ukraine Conference on Electrical and Computer Engineering, UKRCON 2017 - Proceedings*, 2017.

[148] W. Xu, N. Bergmann, C. Javali, G. Revadigar, C. Luo, and W. Hu, "Gait-Key: A Gait-Based Shared Secret Key Generation Protocol for Wearable Devices," *ACM Transactions on Sensor Networks*, 2017.

[149] A. Darabseh, S. Siami-Namini, and A. Siami Namin, "Continuous Authentications Using Frequent English Terms," *Applied Artificial Intelligence*, 2018.

[150] G. Zhao, J. Yang, J. Chen, G. Zhu, Z. Jiang, X. Liu, G. Niu, Z. L. Wang, and B. Zhang, "Keystroke Dynamics Identification Based on Triboelectric Nanogenerator for Intelligent Keyboard Using Deep Learning Method," *Advanced Materials Technologies*, 2019.

[151] J. R. Young, R. S. Davies, J. L. Jenkins, and I. Pfleger, "Keystroke Dynamics: Establishing Keyprints to Verify Users in Online Courses," *Computers in the Schools*, 2019.

[152] M. Boakye Osei, E. Opanin Gyamfi, and M. Okoe Alhassan, "Keystroke Dynamics Algorithm for Securing Web-based Password Driven Systems," *Asian Journal of Research in Computer Science*, 2020.

[153] N. Raul, R. D'mello, and M. Bhalerao, "Keystroke dynamics authentication using small datasets," in *Communications in Computer and Information Science*, vol. 939, 2019.

[154] V. Loboda and G. Kolaczek, "Sound and Keystroke Dynamics Analysis for User Authenticity Verification," in *Proceedings of IEEE 14th International Conference on Intelligent Systems and Knowledge Engineering, ISKE 2019*, 2019.

[155] A. Foresi and R. Samavi, "User Authentication Using Keystroke Dynamics via Crowdsourcing," in *2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings*, 2019.

[156] C. J. Tsai and K. J. Shih, "Mining a new biometrics to improve the accuracy of keystroke dynamics-based authentication system on free-text," *Applied Soft Computing Journal*, 2019.

[157] R. Manandhar, S. Wolf, and M. Borowczak, "One-class classification to continuously authenticate users based on keystroke timing dynamics," *Proceedings - 18th IEEE International Conference on Machine Learning and Applications, ICMLA 2019*, 2019.

[158] R. Conijn, J. Roeser, and M. van Zaanen, "Understanding the keystroke log: the effect of writing task on keystroke features," *Reading and Writing*, 2019.

[159] T. Y. Chang, C. J. Tsai, J. Y. Yeh, C. C. Peng, and P. H. Chen, "New soft biometrics for limited resource in keystroke dynamics authentication," *Multimedia Tools and Applications*, vol. 79, no. 31-32, 2020.

[160] S. Rahayu Selamat, T. Teck Guan, and R. Yusof, "Enhanced Authentication for Web-Based Security using Keystroke Dynamics," *International Journal of Network Security & Its Applications*, vol. 12, no. 4, 2020.

[161] D. Escobar Grisales, J. C. Vásquez-Correa, J. F. Vargas-Bonilla, and J. R. Orozco-Arroyave, "Identity Verification in Virtual Education Using Biometric Analysis Based on Keystroke Dynamics," *TecnoLógicas*, vol. 23, no. 47, 2020.

[162] O. Alpar, "Biometric keystroke barcoding: A next-gen authentication framework," *Expert Systems with Applications*, vol. 177, no. April 2020, p. 114980, 2021. [Online]. Available: https://doi.org/10.1016/j.eswa.2021.114980

[163] A. Rahman, M. E. Chowdhury, A. Khandakar, S. Kiranyaz, K. S. Zaman, M. B. I. Reaz, M. T. Islam, M. Ezeddin, and M. A. Kadir, "Multimodal EEG and Keystroke Dynamics Based Biometric System Using Machine Learning Algorithms," *IEEE Access*, vol. 9, pp. 94 625–94 643, 2021.

[164] S. Unni, S. S. Gowda, and A. F. Smeaton, "An Investigation into Keystroke Dynamics and Heart Rate Variability as Indicators of Stress," pp. 379–391, 2022.

[165] I. Lamiche, G. Bin, Y. Jing, Z. Yu, and A. Hadid, "A continuous smartphone authentication method based on gait patterns and keystroke dynamics," *Journal of Ambient Intelligence and Humanized Computing*, 2019.

[166] E. Klieme, C. Tietz, and C. Meinel, "Beware of SMOMBIES: Verification of Users Based on Activities while Walking," *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 2018.

[167] A. Buriro, S. Gupta, B. Crispo, and F. Frari, "Dialerauth: A motion-assisted touch-based smartphone user authentication scheme," 2018.

[168] S. J. Alghamdi and L. A. Elrefaei, "Dynamic Authentication of Smartphone Users Based on Touchscreen Gestures," *Arabian Journal for Science and Engineering*, 2018.

[169] S. H. Lee, J. H. Roh, S. H. Kim, and S. H. Jin, "Feature subset for improving accuracy of keystroke dynamics on mobile environment," *Journal of Information Processing Systems*, 2018.

[170] Y. Fang, Z. Zhao, Z. Wang, G. Min, Y. Cao, H. Huang, and H. Yin, "Eavesdrop with PoKeMon: Position free keystroke monitoring using acoustic data," *Future Generation Computer Systems*, 2018.

[171] Y. Zhang, M. Yang, Z. Ling, Y. Liu, and W. Wu, "FingerAuth: 3D magnetic finger motion pattern based implicit authentication for mobile devices," 2018.

[172] A. Jain and V. Kanhangad, "Gender classification in smartphones using gait information," *Expert Systems with Applications*, 2018.

[173] H. Cao and K. C. C. Chang, "Nonintrusive Smartphone User Verification Using Anonymized Multimodal Data," *IEEE Transactions on Knowledge and Data Engineering*, 2017.

[174] C. Shen, Y. Chen, and X. Guan, "Performance evaluation of implicit smartphones authentication via sensor-behavior analysis," *Information Sciences*, vol. 430-431, 2018.

[175] M. Smith-Creasey and M. Rajarajan, "A novel word-independent gesture-typing continuous authentication scheme for mobile devices," *Computers and Security*, 2019.

[176] M. D. Papamichail, K. C. Chatzidimitriou, T. Karanikiotis, N.-C. I. Oikonomou, A. L. Symeonidis, and S. K. Saripalle, "BrainRun: A Behavioral Biometrics Dataset towards Continuous Implicit Authentication," *Data*, 2019.

[177] T. Anusas-Amornkul, "Strengthening password authentication using keystroke dynamics and smartphone sensors," *ACM International Conference Proceeding Series*, 2019.

[178] B. S. Saini, P. Singh, A. Nayyar, N. Kaur, K. S. Bhatia, S. El-Sappagh, and J. W. Hu, "A Three-Step Authentication Model for Mobile Phone User Using Keystroke Dynamics," *IEEE Access*, vol. 8, 2020.

[179] C. Vesel, H. Rashidisabet, J. Zulueta, J. P. Stange, J. Duffecy, F. Hussain, A. Piscitello, J. Bark, S. A. Langenecker, S. Young, E. Mounts, L. Omberg, P. C. Nelson, R. C. Moore, D. Koziol, K. Bourne, C. C. Bennett, O. Ajilore, A. P. Demos, and A. Leow, "Effects of mood and aging on keystroke dynamics metadata and their diurnal patterns in a large open-science sample: A BiAffect iOS study," *Journal of the American Medical Informatics Association : JAMIA*, vol. 27, no. 7, 2020.

[180] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "Stealing PINs via mobile sensors: actual risk versus user perception," *International Journal of Information Security*, 2018.

[181] H. Lee, J. Y. Hwang, S. Lee, D. I. Kim, S. H. Lee, J. Lee, and J. S. Shin, "A parameterized model to select discriminating features on keystroke

dynamics authentication on smartphones," *Pervasive and Mobile Computing*, 2019.

[182] F. Alshanketi, I. Traoré, and A. Awad, "Multimodal mobile keystroke dynamics biometrics combining fixed and variable passwords," *Security and Privacy*, vol. 2, no. 1, 2019.

[183] S. Lee, J. Y. Hwang, H. Lee, D. I. Kim, S.-H. Lee, and J. S. Shin, "Distance-Based Keystroke Dynamics Smartphone Authentication and Threshold Formula Model," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 28, no. 2, 2018.

[184] A. Huang, S. Gao, J. Chen, L. Xu, and A. Nathan, "High Security User Authentication Enabled by Piezoelectric Keystroke Dynamics and Machine Learning," *IEEE Sensors Journal*, vol. 20, no. 21, 2020.

[185] P. M. Koh and W. K. Lai, "Keystroke Dynamics Identification System using ABC Algorithm," *2019 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2019 - Proceedings*, 2019.

[186] N. Benjapatanamongkol and P. Bhattarakosol, "A Preliminary Study of Finger Area and Keystroke Dynamics Using Numeric Keypad with Random Numbers on Android Phones," in *ICSEC 2019 - 23rd International Computer Science and Engineering Conference*, 2019.

[187] D. Iakovakis, S. Hadjidimitriou, V. Charisis, S. Bostantzopoulou, Z. Katsarou, and L. J. Hadjileontiadis, "Touchscreen typing-pattern analysis for detecting fine motor skills decline in early-stage Parkinson's disease," *Scientific Reports*, vol. 8, no. 1, pp. 1–13, 2018. [Online]. Available: http://dx.doi.org/10.1038/s41598-018-25999-0

[188] F. J. Zareen, C. Matta, A. Arora, S. Singh, and S. Jabin, "An authentication system using keystroke dynamics," *International Journal of Biometrics*, vol. 10, no. 1, pp. 65–76, 2018.

[189] M. Nakakuni and H. Dozono, "User authentication method for computer-based online testing by analysis of keystroke timing at the input of a family name," in *Proceedings - 2018 International Conference on Computational Science and Computational Intelligence, CSCI 2018*, 2018.

[190] A. Acar, H. Aksu, A. S. Uluagac, and K. Akkaya, "WACA: Wearable-assisted continuous authentication," *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, 2018.

[191] D. Cilia and F. Inguanez, "Multi-model authentication using keystroke dynamics for smartphones," *IEEE International Conference on Consumer Electronics - Berlin, ICCE-Berlin*, 2018.

[192] Z. Farou and K. Buza, "The warping window size effects the accuracy of person identification based on keystroke dynamics," in *CEUR Workshop Proceedings*, vol. 2473, 2019.

[193] A. Salem and M. S. Obaidat, "A novel security scheme for behavioral authentication systems based on keystroke dynamics," *Security and Privacy*, vol. 2, no. 2, 2019.

[194] A. M. Gedikli and M. Ö. Efe, "A simple authentication method with multilayer feedforward neural network using keystroke dynamics," in *Communications in Computer and Information Science*, vol. 1144 CCIS, 2020.

[195] A. Daribay, M. S. Obaidat, and P. V. Krishna, "Analysis of authentication system based on keystroke dynamics," *CITS 2019 - Proceeding of the 2019 International Conference on Computer, Information and Telecommunication Systems*, 2019.

[196] S. Krishnamoorthy, L. Rueda, S. Saad, and H. Elmiligi, "Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning," in *ICBEA '18*, 2018.

[197] Y. Patel, K. Ouazzane, V. T. Vassilev, I. Faruqi, and G. L. Walker, "Keystroke dynamics using auto encoders," in *2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019*, 2019.

[198] R. Giot and A. Rocha, "Siamese Networks for Static Keystroke Dynamics Authentication," in *2019 IEEE International Workshop on Information Forensics and Security, WIFS 2019*, 2019.

[199] M. Guerar, A. Merlo, and M. Migliardi, "Completely Automated Public Physical test to tell Computers and Humans Apart: A usability study on mobile devices," *Future Generation Computer Systems*, 2018.

[200] H. Zhu, J. Hu, S. Chang, and L. Lu, "ShakeIn: Secure User Authentication of Smartphones with Single-Handed Shakes," *IEEE Transactions on Mobile Computing*, 2017.

[201] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales, "Benchmarking Touchscreen Biometrics for Mobile Authentication," *IEEE Transactions on Information Forensics and Security*, 2018.

[202] A. B. A. Ali, V. Ponnusamay, and A. Sangodiah, "User Behaviour-Based Mobile Authentication System," *Advances in Intelligent Systems and Computing*, 2019.

[203] A. I. Filippov, A. V. Iuzbashev, and A. S. Kurnev, "User authentication via touch pattern recognition based on isolation forest," *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018*, 2018.

[204] N. Karakaya, G. I. Alptekin, and Ö. D. İncel, "Using behavioral biometric sensors of mobile phones for user authentication," *Procedia Computer Science*, 2019.

[205] N. Ali and Y. Yang, "Game Authentication Based on Behavior Pattern," 2018.

[206] S. A. Alsuhibany, M. Almushyti, N. Alghasham, and F. Alkhudhayr, "The impact of using different keyboards on free-text keystroke dynamics authentication for Arabic language," *Information and Computer Security*, 2019.

[207] M. Monaro, I. Zampieri, G. Sartori, P. Pietrini, and G. Orrù, "The detection of faked identity using unexpected questions and choice reaction times," *Psychological Research*, 2020.

[208] E. P. Calot, J. S. Ierache, and W. Hasperué, "Robustness of keystroke dynamics identification algorithms against brain-wave variations associated with emotional variations," in *Advances in Intelligent Systems and Computing*, vol. 1037, 2020.

[209] G. Wu, J. Wang, Y. Zhang, and S. Jiang, "A Continuous Identity Authentication Scheme Based on Physiological and Behavioral Characteristics," *Sensors*, 2018.

[210] T. Nguyen and N. Memon, "Tap-based user authentication for smartwatches," *Computers and Security*, 2018.

[211] M. Noorulfakhri Yaacob, S. Zulkarnain Syed Idrus, W. Azani Mustafa, M. Aminudin Jamlos, and M. Helmy Abd Wahab, "Multiple Fusions Approach for Keystroke Dynamics Verification System with Soft Biometrics," in *IOP Conference Series: Materials Science and Engineering*, vol. 917, no. 1, 2020.

[212] C. J. Tsai and P. H. Huang, "Keyword-based approach for recognizing fraudulent messages by keystroke dynamics," *Pattern Recognition*, vol. 98, 2020.

[213] T. Mokoena and D. Sabatta, "User classification by keystroke dynamics using text retrieval methods," *2020 International SAUPEC/RobMech/PRASA Conference, SAUPEC/RobMech/PRASA 2020*, pp. 1–6, 2020.

[214] S. Rasnayaka and T. Sim, "Who wants continuous authentication on mobile devices?" *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems, BTAS 2018*, pp. 1–9, 2018.

[215] A. Pentel, "Predicting user age by keystroke dynamics," in *Advances in Intelligent Systems and Computing*, R. S. (Ed.), Ed. Springer Nature, 2019.

[216] P. Baynath, K. M. Soyjaudah, and M. H. M. Khan, "Pattern representation using Neuroevolution of the augmenting topology (NEAT) on Keystroke dynamics features in Biometrics," in *2nd International Conference on Next Generation Computing Applications 2019, NextComp 2019 - Proceedings*, 2019.

[217] M. L. Bernardi, M. Cimitile, F. Martinelli, and F. Mercaldo, "Keystroke Analysis for User Identification using Deep Neural Networks," in *Proceedings of the International Joint Conference on Neural Networks*, 2019.

[218] F. Tomas, I. Tsimperidis, S. Demarchi, and F. El Massioui, "Keyboard dynamics discrepancies between baseline and deceptive eyewitness narratives," *Applied Cognitive Psychology*, 2020.

[219] Y. Yang, B. Guo, Z. Wang, M. Li, Z. Yu, and X. Zhou, "BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics," *Ad Hoc Networks*, vol. 84, 2019.

[220] Q. Li and H. Chen, "CDAs: A continuous dynamic authentication system," *ACM International Conference Proceeding Series*, 2019.

[221] Z. Syed, J. Helmick, S. Banerjee, and B. Cukic, "Touch gesture-based authentication on mobile devices: The effects of user posture, device size, configuration, and inter-session variability," *Journal of Systems and Software*, 2019.

[222] M. Gadaleta and M. Rossi, "IDNet: Smartphone-based gait recognition with convolutional neural networks," *Pattern Recognition*, 2018.

[223] S. Alotaibi, A. Alruban, S. Furnell, and N. Clarke, "A novel behaviour profiling approach to continuous authentication for mobile applications," *ICISSP 2019 - Proceedings of the 5th International Conference on Information Systems Security and Privacy*, 2019.

[224] S. Amini, S. Gupte, V. Noroozi, P. S. Yu, A. Pande, and C. Kanich, "Deepauth: A framework for continuous user re-authentication in mobile apps," *International Conference on Information and Knowledge Management, Proceedings*, 2018.

[225] M. J. Hooman Oroojeni, J. Oldfield, and M. A. Nicolaou, "Detecting early Parkinson's disease from keystroke dynamics using the tensor-train decomposition," in *European Signal Processing Conference*, vol. 2019-Septe, 2019.

[226] G. Li, P. R. Borj, L. Bergeron, and P. Bours, "Exploring keystroke dynamics and stylometry features for gender prediction on chat data," in *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2019 - Proceedings*, 2019.

[227] A. Buriro, B. Crispo, and M. Conti, "ANSWERAUTH: A bimodal behavioral biometric-based user authentication scheme for smartphones," *Journal of Information Security and Applications*, vol. 44, 2019.

[228] I. Hazan, O. Margalit, and L. Rokach, "Keystroke dynamics obfuscation using key grouping," *Expert Systems with Applications*, 2020.

[229] K. Benzekki, A. El Fergougui, and A. E. B. Elalaoui, "A context-aware authentication system for mobile cloud computing," *Procedia Computer Science*, 2018.

[230] A. Acar, H. Aksu, A. S. Uluagac, and K. Akkaya, "A Usable and Robust Continuous Authentication Framework using Wearables," *IEEE Transactions on Mobile Computing*, 2020.

[231] A. Das, S. K. Mohapatra, and L. P. Mishra, "Biometric detection using stroke dynamics," in *Lecture Notes in Networks and Systems*, 2020, vol. 109.

[232] H. Mostafa, A. M. Elkorany, M. El-Ramly, and H. Shaban, "Behavio2Auth: Sensor-based behavior biometric authentication for smartphones," *ACM International Conference Proceeding Series*, 2019.

[233] P. Slipenchuk and A. Epishkina, "Practical User and Entity Behavior Analytics Methods for Fraud Detection Systems in Online Banking: A Survey," in *Advances in Intelligent Systems and Computing*, vol. 948, 2020.

[234] N. Whiskerd, N. Körtge, K. Jürgens, K. Lamshöft, S. Ezennaya-Gomez, C. Vielhauer, J. Dittmann, and M. Hildebrandt, "Keystroke biometrics in the encrypted domain: a first study on search suggestion functions of web search engines," *Eurasip Journal on Information Security*, vol. 2020, no. 1, 2020.

[235] S. Batool, A. Hassan, N. A. Saqib, and M. A. Khattak, "Authentication of Remote IoT Users Based on Deeper Gait Analysis of Sensor Data," *IEEE Access*, vol. 8, pp. 101 784–101 796, 2020.

[236] C. Wu, W. Ding, R. Liu, J. Wang, A. C. Wang, J. Wang, S. Li, Y. Zi, and Z. L. Wang, "Keystroke dynamics enabled authentication and identification using triboelectric nanogenerator array," *Materials Today*, 2018.

[237] Y. Chen, C. Shen, Z. Wang, and T. Yu, "Modeling interactive sensor-behavior with smartphones for implicit and active user authentication," *2017 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2017*, 2017.

[238] A. Alshehri, F. Coenen, and D. Bollegala, "Iterative Keystroke Continuous Authentication: A Time Series Based Approach," *KI - Kunstliche Intelligenz*, 2018.

[239] A. Alshehri, F. Coenen, and D. Bollegala, "Spectral analysis of keystroke streams: Towards effective real-time continuous user authentication," *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018.

[240] A. Alshehri, F. Coenen, and D. Bollegala, "Behavioural biometric continuous user authentication using multivariate keystroke streams in the spectral domain," *Communications in Computer and Information Science*, 2019.

[241] L. Chen, Y. Zhong, and D. Zhang, "Continuous authentication based on user interaction behavior," *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, 2019.

[242] I. Hazan, O. Margalit, and L. Rokach, "Securing keystroke dynamics from replay attacks," *Applied Soft Computing Journal*, vol. 85, 2019.

[243] A. Acien, A. Morales, R. Vera-Rodriguez, J. Fierrez, and R. Tolosana, "Multi lock: Mobile active authentication based on multiple biometric and behavioral patterns," *MULEA 2019 - 1st International Workshop on Multimodal Understanding and Learning for Embodied Applications, co-located with MM 2019*, 2019.

[244] S. Hriez, N. Obeid, and A. Awajan, "User authentication on smartphones using keystroke dynamics," in *ACM International Conference Proceeding Series*, 2019.

[245] A. Mhenni, E. Cherrier, C. Rosenberger, and N. E. B. Amara, "User dependent template update for keystroke dynamics recognition," *Proceedings - 2018 International Conference on Cyberworlds, CW 2018*, 2018.

[246] M. P. Centeno, Y. Guan, and A. van Moorsel, "Mobile Based Continuous Authentication Using Deep Features," *Proceedings of the 2nd International Workshop on Embedded and Mobile Deep Learning - EMDL'18*, 2018.

[247] A. Mhenni, E. Cherrier, C. Rosenberger, and N. Essoukri Ben Amara, "Double serial adaptation mechanism for keystroke dynamics authentication based on a single password," *Computers and Security*, vol. 83, 2019.

[248] A. Tharwat, A. Ibrahim, T. Gaber, and A. E. Hassanien, "Personal Identification Based on Mobile-Based Keystroke Dynamics," in *Advances in Intelligent Systems and Computing*, vol. 845, 2019.

[249] M. Montgomery, P. Chatterjee, J. Jenkins, and K. Roy, "Touch Analysis: An Empirical Evaluation of Machine Learning Classification Algorithms on Touch Data," 2019.

[250] T. Wu, K. Zheng, G. Xu, C. Wu, and X. Wang, "User identification by keystroke dynamics using improved binary particle swarm optimisation," *International Journal of Bio-Inspired Computation*, vol. 14, no. 3, 2019.

[251] A. Mhenni, D. Migdal, E. Cherrier, C. Rosenberger, and N. Essoukri Ben Amara, "Vulnerability of adaptive strategies of keystroke dynamics based authentication against different attack types," in *Proceedings - 2019 International Conference on Cyberworlds, CW 2019*, 2019.

[252] D. K. Purwar, D. Vishwakarma, N. Singh, and V. Khemchandani, "One v/s All SVM Implementation for Keystroke based Authentication System," in *2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019*, 2019.

[253] H. R. Lv and W. Y. Wang, "Biologic verification based on pressure sensor keyboards and classifier fusion techniques," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 3, 2006.

[254] D. A. T. Tran, W. Ma, G. Chetty, and D. Sharma, "Fuzzy and Markov Models for Keystroke Biometrics Authentication," *New Advances in Simulation, Modelling and Optimization (Smo '07)*, pp. 89–94, 2007.

[255] R. Kumar, P. P. Kundu, D. Shukla, and V. V. Phoha, "Continuous user authentication via unlabeled phone movement patterns," *IEEE International Joint Conference on Biometrics, IJCB 2017*, 2018.

[256] F. Rahman, M. O. Gani, G. M. T. Ahsan, and S. I. Ahamed, "Seeing beyond visibility: A four way fusion of user authentication for efficient usable security on mobile devices," *Proceedings - 8th International Conference on Software Security and Reliability - Companion, SERE-C 2014*, 2014.

[257] K. S. Killourhy and R. A. Maxion, "Why Did My Detector Do That?!" *Recent Advances in Intrusion Detection*, pp. 256–276, 2010.

[258] Y. Deng and Y. Zhong, "Keystroke Dynamics User Authentication Based on Gaussian Mixture Model and Deep Belief Nets," *ISRN Signal Processing*, vol. 2013, pp. 1–7, 2013.

[259] M. P. Centeno, A. Van Moorsel, and S. Castruccio, "Smartphone continuous authentication using deep learning autoencoders," *Proceedings - 2017 15th Annual Conference on Privacy, Security and Trust, PST 2017*, 2018.

[260] J. V. Monaco and M. M. Vindiola, "Crossing domains with the inductive transfer encoder: Case study in keystroke biometrics," *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*, 2016.

[261] G. Zhao, Z. Wu, Y. Gao, G. Niu, Z. L. Wang, and B. Zhang, "Multi-layer Extreme Learning Machine-Based Keystroke Dynamics Identification for Intelligent Keyboard," *IEEE Sensors Journal*, 2020.

[262] V. Vapnik, "The Nature of Statistical Learning Theory," *Springer-Verlag, New York, NY*, 1995.

[263] C.-c. Chang and C.-j. Lin, "LIBSVM : A Library for Support Vector Machines," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 2, pp. 1–39, 2001.

[264] C. Bo, L. Zhang, X. Y. Li, Q. Huang, and Y. Wang, "SilentSense: Silent user identification via touch and movement behavioral biometrics," *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, pp. 187–189, 2013.

[265] Y. Li, H. Hu, and G. Zhou, "Using Data Augmentation in Continuous Authentication on Smartphones," *IEEE Internet of Things Journal*, 2019.

[266] N. Amraoui, A. Besrour, R. Ksantini, and B. Zouari, "Implicit and Continuous Authentication of Smart Home Users," *Advances in Intelligent Systems and Computing*, 2020.

[267] P. H. Pisani, A. C. Lorena, and A. C. De Carvalho, "Adaptive algorithms applied to accelerometer biometrics in a data stream context," *Intelligent Data Analysis*, vol. 21, no. 2, 2017.

[268] J. Hatin, E. Cherrier, J. J. Schwartzmann, and C. Rosenberger, "Privacy preserving transparent mobile authentication," *ICISSP 2017 - Proceed-*

ings of the 3rd International Conference on Information Systems Security and Privacy, 2017.

[269] R. Toosi and M. A. Akhaee, "Time–frequency analysis of keystroke dynamics for user authentication," *Future Generation Computer Systems*, vol. 115, 2021.

[270] H. Jawed, Z. Ziad, M. M. Khan, and M. Asrar, "Anomaly detection through keystroke and tap dynamics implemented via machine learning algorithms," *Turkish Journal of Electrical Engineering and Computer Sciences*, 2018.

[271] S. Haider, A. Abbas, and A. K. Zaidi, "A multi-technique approach for user identification through keystroke dynamics," *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, vol. 2, pp. 1336–1341 vol.2, 2000.

[272] S. Roy, U. Roy, and D. Sinha, "Comparative Study of Various Features-Mining-Based Classifiers in Different Keystroke Dynamics Datasets," in *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems*, Springer, Ed., vol. 2, 2016, pp. 155–164.

[273] D. Buschek, A. De Luca, and F. Alt, "Evaluating the Influence of Targets and Hand Postures on Touch-based Behavioural Biometrics," *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, 2016.

[274] U. Mahbub, S. Sarkar, V. M. Patel, and R. Chellappa, "Active user authentication for smartphones: A challenge data set and benchmark results," *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*, 2016.

[275] C. Ferrari, D. Marini, and M. Moro, "An adaptive typing biometric system with varying users model," *Proceedings - 32nd IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2018*, 2018.

[276] G. Fenu and M. Marras, "Controlling user access to cloud-connected mobile applications by means of biometrics," *IEEE Cloud Computing*, 2018.

[277] X. Liu, Y. Li, R. H. Deng, B. Chang, and S. Li, "When Human cognitive modeling meets PINs: User-independent inter-keystroke timing attacks," *Computers and Security*, 2019.

[278] M. S. Obaidat and W. L. Branch, "Chapter 10 - Keystroke Dynamics Based Authentication," *Biometrics - Personal Identification in Networked Society*, 1996.

[279] W.-H. Lee, X. Liu, Y. Shen, H. Jin, and R. B. Lee, "Secure Pick Up: Implicit Authentication When You Start Using the Smartphone," in *SACMAT'17*, 2017.

[280] C. Shen, Z. Cai, X. Guan, Y. Du, and R. A. Maxion, "User authentication through mouse dynamics," *IEEE Transactions on Information Forensics and Security*, 2013.

[281] J. V. Monaco and C. C. Tappert, "The partially observable hidden Markov model and its application to keystroke dynamics," *Pattern Recognition*, 2018.

[282] S. Roy, U. Roy, and D. D. Sinha, "Performance Perspective of Different Classifiers on Different Keystroke Datasets," *International Journal of New Technologies in Science and Engineering*, vol. 2, no. October, pp. 64–73, 2015.

[283] T. Sim and R. Janakiraman, "Are digraphs good for free-text keystroke dynamics?" in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, no. November, 2007.

[284] R. Janakiraman and T. Sim, "Keystroke dynamics in a general setting," *Advances in Biometrics*, vol. 4642, pp. 584–593, 2007.

[285] P. Kang, S.-S. Hwang, and S. Cho, "Continual Retraining of Keystroke Dynamics based Authenticator.pdf," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4642 LNCS, pp. 1203–1211, 2007.

[286] S. Mandujano and R. Soto, "Deterring password sharing: User authentication via fuzzy c-means clustering applied to keystroke biometric data," in *Proceedings of the Fifth Mexican International Conference in Computer Science, ENC 2004*, 2004.

[287] M. Rathi and A. V. Senthil Kumar, "Euler movement firefly algorithm and fuzzy kernel support vector machine classifier for keystroke authentication," *International Journal of Innovative Technology and Exploring Engineering*, 2019.

[288] M. Monaro, M. Businaro, R. Spolaor, Q. Q. Li, M. Conti, L. Gamberini, and G. Sartori, "The online identity detection via keyboard dynamics," in *Advances in Intelligent Systems and Computing*, vol. 881, 2019.

[289] D. Soni, M. Hanmandlu, and H. C. Saini, "A machine learning approach for user authentication using touchstroke dynamics," in *Smart Innovation, Systems and Technologies*, vol. 79, 2018.

[290] N. Murali and K. Appaiah, "Keyboard Side Channel Attacks on Smartphones Using Sensor Fusion," *2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings*, 2018.

[291] X. Liang, F. Zou, L. Li, and P. Yi, "Mobile terminal identity authentication system based on behavioral characteristics," *International Journal of Distributed Sensor Networks*, 2020.

[292] W. Meng, Y. Wang, D. S. Wong, S. Wen, and Y. Xiang, "TouchWB: Touch behavioral user authentication based on web browsing on smartphones," *Journal of Network and Computer Applications*, 2018.

[293] W. Meng, W. Li, and D. S. Wong, "Enhancing touch behavioral authentication via cost-based intelligent mechanism on smartphones," *Multimedia Tools and Applications*, 2018.

[294] J. Blomqvist and J. Blomqvist, "Using XGBoost to classify the Beihang Keystroke Dynamics Database Dynamics Database," *UPTEC F 18049*, 2018.

[295] C. Dwivedi, D. Kalra, D. Naidu, and S. Aggarwal, "Keystroke dynamics based biometric authentication: A hybrid classifier approach," *Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence, SSCI 2018*, 2019.

[296] B. Li, W. Wang, Y. Gao, V. V. Phoha, and Z. Jin, "Wrist in Motion: A Seamless Context-Aware Continuous Authentication Framework Using Your Clickings and Typings," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 2, no. 3, 2020.

[297] K. W. Tse and K. Hung, "User Behavioral Biometrics Identification on Mobile Platform using Multimodal Fusion of Keystroke and Swipe Dynamics and Recurrent Neural Network," *ISCAIE 2020 - IEEE 10th Symposium on Computer Applications and Industrial Electronics*, 2020.

[298] Y. Cai, H. Jiang, D. Chen, and M. C. Huang, "Online learning classifier based behavioral biometrie authentication," *2018 IEEE 15th International Conference on Wearable and Implantable Body Sensor Networks, BSN 2018*, 2018.

[299] E. Maiorana, H. Kalita, and P. Campisi, "Deepkey: Keystroke Dynamics and CNN for Biometric Recognition on Mobile Devices," in *Proceedings - European Workshop on Visual Information Processing, EUVIP*, vol. 2019-Octob, 2019.

[300] K. W. Tse and K. Hung, "Behavioral biometrics scheme with keystroke and swipe dynamics for user authentication on mobile platform," *ISCAIE 2019 - 2019 IEEE Symposium on Computer Applications and Industrial Electronics*, 2019.

[301] O. Alpar, "Biometric touchstroke authentication by fuzzy proximity of touch locations," *Future Generation Computer Systems*, 2018.

[302] S. X. C. Loh, H. Y. Ow-Yong, H. Y. Lim, W. K. Lai, and L. L. Lim, "Fuzzy inference for user identification of pressure-based keystroke biometrics," *IEEE Student Conference on Research and Development: Inspiring Technology for Humanity, SCOReD 2017 - Proceedings*, 2017.

[303] A. Bhatia and M. Hanmandlu, "Keystroke Dynamics Based Authentication Using Possibilistic Renyi Entropy Features and Composite Fuzzy Classifier," *Journal of Modern Physics*, vol. 09, no. 02, 2018.

[304] J. Yadav, K. Pandey, S. Gupta, and R. Sharma, "Keystroke dynamics based authentication using fuzzy logic," *2017 10th International Conference on Contemporary Computing, IC3 2017*, 2018.

[305] W. G. De Ru and J. H. P. Eloff, "Enhanced password authentication through fuzzy logic," *IEEE Expert-Intelligent Systems and their Applications*, vol. 12, no. 6, pp. 38–45, 1997.

[306] M. Ulinskas, M. Woźniak, and R. Damaševičius, "Analysis of keystroke dynamics for fatigue recognition," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10408 LNCS, 2017.

[307] P. H. Pisani, A. Mhenni, R. Giot, E. Cherrier, N. Poh, A. C. P. D. L. F. De Carvalho, C. Rosenberger, and N. E. B. Amara, "Adaptive biometric systems: Review and perspectives," *ACM Computing Surveys*, 2019.

[308] George Kofi Gagbla, "Applying Keystroke Dynamics for Personal Authentication," *Degree of Master of Science in Electrical Engineering Supervisors: Thesis*, 2005.

[309] P. H. Pisani, A. C. Lorena, and A. C. de Carvalho, "Adaptive Positive Selection for Keystroke Dynamics," *Journal of Intelligent and Robotic Systems: Theory and Applications*, 2015.

[310] R. Giot, C. Rosenberger, and B. Dorizzi, "Hybrid template update system for unimodal biometric systems," *2012 IEEE 5th International Conference on Biometrics: Theory, Applications and Systems, BTAS 2012*, pp. 1–7, 2012.

[311] P. H. Pisani, A. C. Lorena, and A. C. P. L. F. De Carvalho, "Adaptive approaches for keystroke dynamics," *Proceedings of the International Joint Conference on Neural Networks*, vol. 2015-Septe, 2015.

[312] H. Çeker and S. Upadhyaya, "Adaptive Techniques for Intra-User Variability in Keystroke Dynamics," *IEEE Eighth International Conference on Biometrics: Theory, Applications, and Systems (BTAS 2016)*, 2016.

[313] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *Computers and Security*, 2016.

[314] A. Mhenni, E. Cherrier, C. Rosenberger, and N. E. B. Amara, "Adaptive Biometric Strategy using Doddington Zoo Classification of User's Keystroke Dynamics," *2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018*, no. June, pp. 488–493, 2018.

[315] M. El Abed, "Usability assessment of keystroke dynamics systems," *International Journal of Computer Applications in Technology*, 2017.

[316] a. J. Mansfield and J. L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices ver 2.01," *National Physics Laboratory*, pp. 1–36, 2002. [Online]. Available: https://www.biometricscatalog.org/2003gbw/downloads/Best_Practice.pdf

[317] R. Work, "Chapter 2 BIOMETRICS MEASUREMENTS," *Biometrics*, 2005.

[318] R. Giot, A. Ninassi, M. El-Abed, and C. Rosenberger, "Analysis of the acquisition process for keystroke dynamics," *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG - Proceedings of the International Conference of the*, pp. 1–6, 2012. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6313543

[319] A. Buriro, B. Crispo, F. Del Frari, J. Klardie, and K. Wrona, "ITSME: Multi-modal and unobtrusive behavioural user authentication for smartphones," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016.

[320] CENELEC, "Alarm systems - Access control systems for use in security applications – Part 1," in *System requirements, EN 50133-1 edition*, 1996.

[321] D. I. Kim, S. Lee, and J. S. Shin, "A New Feature Scoring Method in Keystroke Dynamics-Based User Authentications," *IEEE Access*, vol. 8, 2020.

[322] A. Salem, A. Sharieh, A. Sleit, and R. Jabri, "Enhanced authentication system performance based on keystroke dynamics using classification algorithms," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 8, 2019.

[323] A. Andrean, M. Jayabalan, and V. Thiruchelvam, "Keystroke Dynamics Based User Authentication using Deep Multilayer Perceptron," *International Journal of Machine Learning and Computing*, vol. 10, no. 1, pp. 134–139, 2020.

[324] E. A. Kochegurova and Y. A. Martynova, "Aspects of Continuous User Identification Based on Free Texts and Hidden Monitoring," *Programming and Computer Software*, vol. 46, no. 1, 2020.

[325] P. Y. O. Amoako and I. O. Osunmakinde, "Emerging bimodal biometrics authentication for non-venue-based assessments in open distance e-learning (OdeL) environments," *International Journal of Technology Enhanced Learning*, vol. 12, no. 2, 2020.

[326] A. B. Baban, A. M. Alkababji, and M. S. Oassab, "Real - Time biometric authentication based on key stroke dynamics," 2020.

[327] M. S. Obaidat, I. Traore, and I. Woungang, "Biometric-Based Physical and Cybersecurity Systems," *Biometric-Based Physical and Cybersecurity Systems*, 2018.

[328] D. R. Chandranegara, H. Wibowo, and A. E. Minarno, "Combined scaled manhattan distance and mean of horner's rules for keystroke dynamic authentication," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 2, pp. 770–775, 2020.

[329] K. S. Balagani, P. Gasti, A. Elliott, A. Richardson, and M. O'Neal, "The impact of application context on privacy and performance of keystroke authentication systems," *Journal of Computer Security*, 2018.

[330] S. Modi and S. J. Elliott, "Keystroke dynamics verification using a spontaneously generated password," *Proceedings - International Carnahan Conference on Security Technology*, pp. 116–121, 2006.

[331] P. Bours and S. Brahmanpally, "Language dependent challenge-based keystroke dynamics," *Proceedings - International Carnahan Conference on Security Technology*, 2017.

[332] R. Raghavendra and C. Busch, "A low cost wrist vein sensor for biometric authentication," *IST 2016 - 2016 IEEE International Conference on Imaging Systems and Techniques, Proceedings*, 2016.

[333] S. Roy, U. Roy, and D. Sinha, "The probability of predicting personality traits by the way user types on touch screen," *Innovations in Systems and Software Engineering*, pp. 1–8, dec 2018.

[334] A. Bangor, P. Kortum, and J. Miller, "Determining What Individual SUS Scores Mean: Adding an Adjective Rating ScaleJUS," *Journal of Usability studies*, vol. 4, no. 3, 2009. [Online]. Available: https://uxpajournal.org/determining-what-individual-sus-scores-mean-adding-an-adjective-rating-scale/

[335] S. Maheshwary and V. Pudi, "Mining keystroke timing pattern for user authentication," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017.

[336] A. Bhatia, M. Hanmandlu, S. Vasikarla, and B. K. Panigrahi, "Keystroke Dynamics Based Authentication Using GFM," *2018 IEEE International Symposium on Technologies for Homeland Security, HST 2018*, 2018.

[337] A. Khodabakhsh, E. Haasnoot, and P. Bours, "Predicted Templates: Learning-curve Based Template Projection for Keystroke Dynamics," *2018 International Conference of the Biometrics Special Interest Group, BIOSIG 2018*, 2018.

[338] M. Li, B. Wu, and Z. Qin, "Anomaly User Detection via Comprehensive Keystroke Features Optimization," *Proceedings of the International Joint Conference on Neural Networks*, 2018.

[339] G. J. Krishna and V. Ravi, "Keystroke based User Authentication using Modified Differential Evolution," in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, vol. 2019-Octob, 2019.

[340] M. Liakat Ali and C. C. Tappert, "POHMM/SVM: A hybrid approach for keystroke biometric user authentication," *2018 IEEE International Conference on Real-Time Computing and Robotics, RCAR 2018*, 2019.

[341] K. Bicakci, O. Salman, Y. Uzunay, and M. Tan, "Analysis and Evaluation of Keystroke Dynamics as a Feature of Contextual Authentication," *2020 International Conference on Information Security and Cryptology, ISCTURKEY 2020 - Proceedings*, pp. 11–17, 2020.

[342] I. Hazan, O. Margalit, and L. Rokach, "Supporting unknown number of users in keystroke dynamics models," *Knowledge-Based Systems*, vol. 221, p. 106982, 2021. [Online]. Available: https://doi.org/10.1016/j.knosys.2021.106982

[343] N. Sae-Baeid and N. Memon, "Distinguishability of keystroke dynamic template," *PLoS ONE*, vol. 17, no. 1, 2022. [Online]. Available: https://doi.org/10.1371/journal.pone.0261291

[344] M. M. Al-Jarrah, G. M. Khalaf, and S. Amin, "PIN Authentication Using Multi-Model Anomaly Detection in Keystroke Dynamics," in *2019 2nd International Conference on Signal Processing and Information Security, ICSPIS 2019*, 2019.

[345] S. A. Alsuhibany and A. S. Almuqbil, "Analyzing the Effectiveness of Touch Keystroke Dynamic Authentication for the Arabic Language," *Wireless Communications and Mobile Computing*, vol. 2021, p. 15, 2021. [Online]. Available: https://doi.org/10.1155/2021/9963129

[346] M. Choi, S. Lee, M. Jo, and J. S. Shin, "Keystroke dynamics-based authentication using unique keypad," *Sensors*, vol. 21, no. 6, pp. 1–19, 2021.

[347] B. Ayotte, M. Banavar, D. Hou, and S. Schuckers, "Fast Free-text Authentication via Instance-based Keystroke Dynamics," 2020.

[348] X. Lu, S. Zhang, P. Hui, and P. Lio, "Continuous authentication by free-text keystroke based on CNN and RNN," *Computers and Security*, vol. 96, p. 101861, 2020. [Online]. Available: https://doi.org/10.1016/j.cose.2020.101861

[349] A.-c. Iapa and V.-i. Cretu, "Shared Data Set for Free-Text Keystroke Dynamics Authentication Algorithms," *Preprints*, no. May, 2021.

[350] N. González, E. P. Calot, J. S. Ierache, and W. Hasperué, "Towards liveness detection in keystroke dynamics: Revealing synthetic forgeries," *Systems and Soft Computing*, vol. 4, p. 200037, 2022. [Online]. Available: https://doi.org/10.1016/j.sasc.2022.200037

[351] A. Morales, J. Fierrez, A. Acien, R. Tolosana, and I. Serna, "SetMargin loss applied to deep keystroke biometrics with circle packing interpretation," *Pattern Recognition*, vol. 122, p. 108283, feb 2022. [Online]. Available: https://doi.org/10.1016/j.patcog.2021.108283

[352] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. Nyang, "AUToSen: Deep-learning-based implicit continuous authentication using smartphone sensors," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5008–5020, jun 2020.

[353] H. Kalita, E. Maiorana, and P. Campisi, "Keystroke Dynamics for Biometric Recognition in Handheld Devices," in *2020 43rd International Conference on Telecommunications and Signal Processing, TSP 2020*, 2020.

[354] S. Keykhaie and S. Pierre, "Mobile Match on Card Active Authentication Using Touchscreen Biometric," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 4, pp. 376–385, nov 2020.

[355] O. D. Incel, S. Gunay, Y. Akan, Y. Barlas, O. E. Basar, G. I. Alptekin, and M. Isbilen, "DAKOTA: Sensor and Touch Screen-Based Continuous Authentication on a Mobile Banking Application," *IEEE Access*, vol. 9, pp. 38 943–38 960, 2021.

[356] P. Baynath, K. M. Sunjiv Soyjaudah, and M. Heenaye-Mamode Khan, "Machine Learning Algorithm on Keystroke Dynamics Pattern," in *Proceedings - 2018 IEEE Conference on Systems, Process and Control, ICSPC 2018*, 2018.

[357] C. H. Lin, J. C. Liu, and K. Y. Lee, "On neural networks for biometric authentication based on keystroke dynamics," *Sensors and Materials*, vol. 30, no. 3, 2018.

[358] X. Wang, Q. Tan, J. Shi, S. Su, and M. Wang, "Insider threat detection using characterizing user behavior," *Proceedings - 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018*, 2018.

[359] P. Baynath, S. Soyjaudah, and M. H. M. Khan, "Feature selection and representation of evolutionary algorithm on keystroke dynamics," *Intelligent Automation and Soft Computing*, vol. 25, no. 4, 2019.

[360] Neha and K. Chatterjee, "Biometric re-authentication: an approach towards achieving transparency in user authentication," *Multimedia Tools and Applications*, vol. 78, no. 6, 2019.

[361] A. Ferhatovic, A. A. Almisreb, S. Turaev, and M. A. Saleh, "Implementation Of Long Short-Term Memory (LSTM) For User Authentication Based On Keystroke Dynamics," *Southeast Europe Journal of Soft Computing*, vol. 9, no. 1, 2020.

[362] A. Darabseh and D. Pal, "Performance analysis of keystroke dynamics using classification algorithms," in *Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020*, 2020.

[363] M. Rathi, A. V. S. Kumar, A. Alrabea, and A. Amine, "A Unified Neutrosophical Identification of Authenticated Users with Continuous A Unified Neutrosophical Identification of Authenticated Users with Continuous Keystroke Dynamics," *International Journal of Advanced Science and Technology*, vol. 29, no. 3, 2020.

[364] I. Bhardwaj, N. D. Londhe, and S. K. Kopparapu, "Performance Evaluation of Fingerprint Dynamics in Machine Learning and Score Level Fusion Framework," *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)*, 2019.

[365] R. Rocha, D. Carneiro, R. Costa, and C. Analide, "Continuous authentication in mobile devices using behavioral biometrics," *Advances in Intelligent Systems and Computing*, 2020.

[366] L. De-Marcos, J.-J. Martínez-Herráiz, J. Junquera-Sánchez, C. Cilleruelo, and C. Pages-Arévalo, "Comparing Machine Learning Classifiers for Continuous Authentication on Mobile Devices by Keystroke Dynamics," *Electronics*, vol. 10, 2021. [Online]. Available: https://doi.org/10.3390/electronics10141622

[367] I. Stylios, A. Skalkos, S. Kokolakis, and M. Karyda, "BioPrivacy : Development of a Keystroke Dynamics Continuous Authentication System BioPrivacy : Development of a Keystroke Dynamics Continuous Authentication System," no. November, 2021.

[368] R. Abinaya and R. Sowmiya, "Soft biometric based keystroke classification using PSO optimized neural network," *Materials Today: Proceedings*, no. xxxx, pp. 1–4, 2021. [Online]. Available: https://doi.org/10.1016/j.matpr.2021.01.733

[369] M. N. Yaacob, S. Z. Syed Idrus, W. A. Wan Mustafa, M. A. Jamlos, and M. H. Abd Wahab, "Identification of the exclusivity of individual's typing style using soft biometric elements," *Annals of Emerging Technologies in Computing*, vol. 5, no. Special issue 5, pp. 10–26, 2021.

[370] I. Tsimperidis, S. Rostami, and V. Katos, "Age Detection Through Keystroke Dynamics from User Authentication Failures," *International Journal of Digital Crime and Forensics*, 2017.

[371] D. R. Dacunhasilva, Z. Wang, and R. Gutierrez-Osuna, "Towards Participant-Independent Stress Detection Using Instrumented Peripherals," *IEEE Transactions on Affective Computing*, pp. 1–18, 2021.

[372] I. Tsimperidis, C. Yucel, and V. Katos, "Age and gender as cyber attribution features in keystroke dynamic-based user classification processes," *Electronics (Switzerland)*, vol. 10, no. 7, pp. 1–14, 2021.

[373] I. Tsimperidis, S. Rostami, K. Wilson, and V. Katos, "User Attribution Through Keystroke Dynamics-Based Author Age Estimation," in *Lecture Notes in Networks and Systems*. Springer, Cham, sep 2021, pp. 47–61. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-64758-2_4

[374] E. Davarci, B. Soysal, I. Erguler, S. O. Aydin, O. Dincer, and E. Anarim, "Age Group Detection Using Smartphone Motion Sensors," *2017 25th European Signal Processing Conference (EUSIPCO)*, pp. 2265–2269, 2017.

[375] O. Oyebola and A. O. Adesina, "Predicting Age Group and Gender of Smartphone Users Using Keystroke Biometrics," *Malaysian Journal of Science and Advanced Technology*, vol. 1, no. 4, pp. 124–128, 2021.

[376] P. Bours and S. Mondal, "Performance evaluation of continuous authentication systems Performance evaluation of continuous authentication systems," *IET Biometrics*, vol. 4, no. 4, pp. 1–7, 2015.

[377] C. Shen, Y. Zhang, Z. Cai, T. Yu, and X. Guan, "Touch-interaction behavior for continuous user authentication on smartphones," *Proceedings of 2015 International Conference on Biometrics, ICB 2015*, pp. 157–162, 2015.

[378] A. Alsultan, K. Warwick, and H. Wei, "Free-text keystroke dynamics authentication for Arabic language," *IET Biometrics*, vol. 5, no. February, pp. 164–169, 2016.

[379] E. Yu and S. Cho, "Keystroke dynamics identity verification - Its problems and practical solutions," *Computers and Security*, vol. 23, no. 5, pp. 428–440, 2004.

[380] S. Roy, U. Roy, and D. Sinha, "Security Enhancement of Knowledge-based User Authentication through Keystroke Dynamics," in *MATEC Web of Conferences*, vol. 57, 2016.

[381] A. Acar, W. Liu, R. Beyah, K. Akkaya, and A. S. Uluagac, "A privacy-preserving multifactor authentication system," *Security and Privacy*, vol. 2, no. 5, 2019.

[382] A. Selcuk Uluagac, W. Liu, and R. Beyah, "A multi-factor re-authentication framework with user privacy," *2014 IEEE Conference on Communications and Network Security, CNS 2014*, 2014.

[383] M. Nauman, T. Ali, and A. Rauf, "Using trusted computing for privacy preserving keystroke-based authentication in smartphones," *Telecommunication Systems*, vol. 52, no. 4, pp. 2149–2161, 2013.

[384] T. Eude and C. Chang, "One-class SVM for biometric authentication by keystroke dynamics for remote evaluation," *Computational Intelligence*, 2018.

[385] L. H. Lorena, A. C. Carvalho, and A. C. Lorena, "Filter Feature Selection for One-Class Classification," *Journal of Intelligent and Robotic Systems: Theory and Applications*, 2015.

[386] H. Khan, A. Atwater, and U. Hengartner, "Itus : An Implicit Authentication Framework for Android," *In Proceedings of the 20th annual international conference on Mobile computing and networking*, pp. 507–518, 2014.

[387] Z. Sitova, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, 2016.

[388] W. H. Lee and R. B. Lee, "Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning," *Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017*, 2017.

[389] A. A. Alariki, A. A. Manaf, and S. M. Mousavi, "Features extraction scheme for behavioural biometric authentication in touchscreen mobile devices," *International Journal of Applied Engineering Research*, 2016.

[390] A. S. Yuksel, F. A. Senel, and I. A. Cankaya, "Classification of Soft Keyboard Typing Behaviors Using Mobile Device Sensors with Machine Learning," *Arabian Journal for Science and Engineering*, 2019.

[391] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Computers and Security*, vol. 39, no. PART B, 2013.

[392] L. Li, X. Zhao, and G. Xue, "Unobservable Re-authentication for Smartphones," in *20th annual network & distributed system security symposium*. The Internet Society, 2013, pp. 1–16.

[393] M. L. Ali, J. V. Monaco, and C. C. Tappert, "Hidden Markov Models in Keystroke Dynamics," in *Proceedings of Student-Faculty Research Day, CSIS*, 2015.

[394] S. I. Hassan, M. S. Mazen, and H. H. Zayed, "User Authentication with Adaptive Keystroke Dynamics," *IJCSI International Journal of Computer Science Issues*, vol. Vol. 10, no. Issue 4, pp. 127–134, 2013.

[395] H. Crawford and E. Ahmadzadeh, "Authentication on the Go: Assessing the Effect of Movement on Mobile Device Keystroke Dynamics," *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, 2017.

[396] H. Ceker, "Keystroke Dynamics for Enhanced User Recognition in Active Authentication," *ProQuest Dissertations and Theses*, 2017.

SOUMEN ROY was born in Bagnan, Howrah, India in 1985. Now he has been doing research at the University of Calcutta, Kolkata for the last 10 years on keystroke dynamics, machine learning, access control, etc. He is also working with Bagnan College, Bagnan, Howrah, India for the last 12 years as a lecturer. He has more than a year of experience in software development. He has more than 30 international publications in the form of journals, edited books, and conference proceedings. He is a reviewer for various SCI-indexed journals.

JITESH PRADHAN is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Faculty of Engineering and Technology (ITER), Sikhsha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha. He has completed his PhD and M.Tech. from the Department of Computer Science and Engineering, Indian Institute of Technology (ISM) Dhanbad, in the years 2021 and 2015, respectively. He has done his B.Tech. from Chhattisgarh Swami Vivekananda Technical University Bhilai in the year 2012. He is a reviewer for various IEEE, Elsevier, Springer, ACM, and Scopus journals. He has published more than 20 research papers in different journals and international conferences. His research areas include content-based image retrieval, image processing, computer vision, machine learning, DNA computing for image retrieval, etc.

ABHINAV KUMAR is currently working as an Assistant Professor, Department of Computer Science and Engineering, Siksha 'O' Anusandhan, Deemed to be University, Bhubaneswar, Odisha-751030. He has obtained a PhD degree in Computer Science and Engineering from the Department of Computer Science and Engineering of the National Institute of Technology, Patna, India. His research interests include machine learning, deep learning, crisis informatics, natural language processing, and social networks. He has published articles in different journals, including Applied Soft Computing, Annals of Operation Research, Sustainable Cities and Society, Information Systems Frontiers, International Journal of Disaster Risk Reduction, Multimedia Tools and Applications, and others. He has also published many conference proceedings at prestigious international conferences.

DIBYA RANJAN DAS ADHIKARY is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha-751030. He has completed his PhD and M.Tech. from the Department of Computer Science and Engineering, Birla Institute of Technology Mesra, Ranchi in the years 2019 and 2011, respectively. His research interests include machine learning, deep learning, natural language processing, wireless sensor networks, and pattern matching. He is a reviewer for various journals and conferences. He has published more than 10 research papers in different journals and international conferences.

UTPAL ROY After the completion of his masters and PhD from the Department of Mathematics, Visva-Bharati in the year 1994, he joined the University LAVAL, Quebe, CANADA from 1994 to 1996. Later, he joined the Indian Association for the Cultivation of Science (IACS), Jadavpur Calcutta as a scientist pool and, subsequently, he accepted the job of Assistant Professor in computer science in the Visva-Bharati in 1997. Furthermore, he worked as a visiting faculty at the Academia Sinica, Taipei, Taiwan, during the period 2002-2003. The department of IT, Assam University Silchar, Silchar, Assam, appoint him as a Professor in Feb. 2008. Presently, he is a professor and former head of the Department of Computer and System Sciences, Siksha-Bhavana, Visva-Bharati with 28 years of teaching and research experience. During this period, he published more than one hundred papers in journals of National and International repute. During this academic tenure, he guided five PhD students who are well placed in India and abroad. As a Principal supervisor, he has handled externally (UGC, DAE) and internally funded (Visva-Bharati) scientific projects. In recognition of his academic field, India International Society, an NGO, in New Delhi, awarded him the Bharat Gourav Award in 2017.

DEVADATTA SINHA has more than forty of experience in the field of Computer Science and Engineering in research and teaching. He worked as a Faculty member in BIT Mesra, Ranchi, Jadavpur University, University of Calcutta. He has written many research papers in National and International Journals, Conference Proceedings. He has also written many expository articles in periodicals, books, and monographs. He has research interests include Software Engineering, Parallel and Distributed Algorithms, Bioinformatics, Computational Intelligence, Computer Education, Mathematical Ecology, and Networking. He guided research students for PhD, in Computer Science and Engineering and M.Tech., B.Tech. and M.Sc. students for their dissertations. He performed as Sectional President, Section of Computer Science, Indian Science Congress Association (1994). He is a Fellow of the Computer Society of India.

RAJAT KUMAR PAL (Member, IEEE) received his B.E. degree in Electrical Engineering from Bengal Engineering College, Shibpur, under the University of Calcutta, India, the M.Tech. degree in Computer Science and Engineering from the University of Calcutta, India, in 1985 and 1988, respectively, and the PhD degree from the Indian Institute of Technology, Kharagpur, India, in 1996. Since 1994, he has been working as a faculty with the Department of Computer Science and Engineering, University of Calcutta. He took a leave of absence to become a Professor with the Department of Information Technology, Assam University, India, from 2010 to 2012. Presently, he is working as a professor with the Department of Computer Science and Engineering, University of Calcutta, India. His major research interests include VLSI design, graph theory and its applications, perfect graphs, logic synthesis, design and analysis of algorithms, computational geometry, and parallel computation and algorithms. He has published nearly 250 research articles and has authored and co-authored two books. He also holds several international patents.