A Secure and Scalable Behavioral Dynamics Authentication Model

Idowu Dauda Oladipo[1], Mathew Nicho[2], Joseph Bamidele Awotunde[3],
Jemima Omotola Buari[4], Muyideen Abdulraheem[5], Tarek Gaber[6]
Department of Computer Science, University of Ilorin, Ilorin, Nigeria[1, 3, 4, 5]
Research and Innovation Center, Rabdan Academy, Abu Dhabi[2]
School of Science, Engineering & Environment, University of Salford, Manchester, United Kingdom[6]

***Abstract*—Various authentication methods have been proposed to mitigate data breaches. However, the increasing frequency of data breaches and users' lack of awareness have exposed traditional methods, including single-factor password-based systems and, two-factor authentication systems, to vulnerabilities against attacks. While behavioral authentication holds promise in tackling these issues, it faces challenges concerning interoperability between operating systems, the security of behavioral data, accuracy enhancement, scalability, and cost. This research presents a scalable dynamic behavioral authentication model utilizing keystroke typing patterns. The model is constructed around five key components: human-computer interface devices, encryption of behavioral data, consideration of the authenticator's emotional state, incorporation of cross-platform features, and proposed implementation solutions. It addresses potential typing errors and employs data encryption for behavioral data, achieving a harmonious blend of usability and security by leveraging keyboard dynamics. This is accomplished through the implementation of a web-based authentication system that integrates Convolutional Neural Networks (CNNs) for advanced feature engineering. Keystroke typing patterns were gathered from participants and subsequently employed to evaluate the system's keystroke timing verification, login ID verification, and error handling capabilities. The web-based system uniquely identifies users by merging their username-password (UN-PW) credentials with their keyboard typing patterns, all while securely storing the keystroke data. Given the achievement of a 100% accuracy rate, the proposed Behavioral Dynamics Authentication Model (BDA) introduces future researchers to five scalable constructs. These constructs offer an optimal combination, tailored to the device and context, for maximizing effectiveness. This achievement underscores its potential applications in the realm of authentication.**

Keywords*—Behavioral authentication; keystroke dynamics; human-computer interface; two-factor authentication

I. INTRODUCTION

Stolen credentials remain the most frequent means by which hackers commit data breaches. In general, 80% of hacking-related breaches involve brute force or stolen credentials, and 37% of all breaches involve the use or theft of credentials [1]. Ensuring data protection and privacy through effective and efficient authentication methods is not only a priority for individuals, organizations, and countries but also a context for promoting incremental and radical innovation. Data-protection authorities must acquire new technologies and use them effectively to regulate personal information practices so as to meet present and future challenges, for the technology advances in step with the security threats [2-3]. Hence, cybersecurity attacks have been increasing exponentially and rendering existing detection mechanisms insufficient [4]. Cyber-criminals exploit security flaws to access users' data and privileges [5], and, in turn, tactics such as authentication serve to restrict and control access to unauthorized users [6].

More than 555 million passwords have been obtained through data breaches and exposed in the public domain [7]. Some 27% of those surveyed in a Google poll admitted attempting to guess the passwords of others, 17% of whom claimed to have succeeded [8], and, according to one report, 80% of hacking incidents are enabled by stolen and reused login information, 81% of which at the company level are caused by the many poor passwords among the 300 billion in use [9]. Verizon's 2022 Data Breach Investigations Report identified passwords as a frequent weak link in cybersecurity, with 80% of all data breaches worldwide again being associated with passwords [10].

Multifactor authentication (MFA) can block more than 99.9% of account compromise attacks [11], and two-factor authentication (2FA) is currently among the primary mechanisms for defending against password attacks [12], especially those involving phishing and password reuse [13]. Biometric authentication (BA) based on keystrokes is considered more reliable than these traditional means of authentication because of its novelty and low intrusiveness [14]. A National Bureau of Standards study found keystroke dynamics (KD) to be a reliable and accurate BA method, achieving at least 98% accuracy [15].

The overwhelming focus in the scholarship for several decades has been on the legal and technological dimensions of the challenges associated with data protection [2]. Among the world's privacy and security laws, the European Union General Data Protection Regulation (GDPR), adopted in 2016 and enacted on May 25, 2018, is the strongest [16], and a crucial aspect of compliance with this regulation is adequate authentication and authorization [17]. Accordingly, biometrics generated through KD has become a viable option to authenticate users for both security and surveillance purposes [18] given the minimal implementation cost of KD and lack of a need for special hardware since the gathering of typing data

is reasonably straightforward, requiring no additional effort by the user [19].

Accordingly, we propose a scalable dynamic behavioral authentication model incorporating future trends in information systems, specifically, trends in or toward (1) devices, (2) dynamic encryption standards, (3) assessing the emotional state of the authenticator, (4) the ubiquitous access to and usage of devices, and the option to (5) incorporate emerging technologies and solutions for low cost and increased functionality. The result, validated based on these five constructs, is a cost-effective and non-intrusive MFA system method to augment users' authentication and ensure data security while efficiently handling their typing errors [19]. The use of keystrokes itself validates the model owing to its simplicity and its ability to integrate seamlessly with passwords. Simply put, KD is an extremely useful method for BA because it is extremely difficult to impersonate [20].

The main contributions of this paper are:

- a dynamic behavioral authentication model incorporating five scalable constructs namely HCI devices, encryption, user profiles, ubiquitous, and the options for cost effective applications,
- scalability in all five constructs of the model that offers multiple avenues for future research on combinations of the components of the constructs,
- a secure and efficient authentication system based on users' unique key-typing patterns with an error-correction feature,
- a cost-effective way to implement BA compared with other methods (which may require a combination of hardware and software),
- alignment of the proposed system with the relevant data protection and privacy regulations (e.g., the GDPR) to assist organizations with compliance.

In the remainder of the paper, Section II presents our justification for using 2FA and MFA and our analysis of attacks followed by a review of the research on the application of behavioral authentication in KD. Section III presents the methodology and Section IV discusses the application of KD and the resulting model. We discuss our conclusions in Section V.

II. Literature Review

The following discussion surveys current issues relating to password authentication, the use and usability of multifactor authentication, the ease of password attacks, and behavioral authentication methods.

A. Challenges in Password Authentication

Password-based authentication has been fraught with multiple issues. Firstly, the resilience of diverse operating environments is considered a significant technical challenge for future biometric systems. [21]. Secondly, the endeavor to develop efficient and secure biometric authentication systems that can withstand impersonation attacks, guarantee the non-reversibility of biometric templates, and safeguard the privacy of personal information is critical [22]. Thirdly, the challenge lies in establishing appropriate policies and laws to prevent the indiscriminate use of biometric data [23]. From a keystroke recognition perspective, there is a necessity for the development of technology to enhance accuracy [24]. Lastly, a majority of the current research on keystroke dynamics revolves around free text (emphasizing n-graphs). This not only poses challenges in improving accuracy but also frequently requires a substantial amount of time to construct user models [25]. The suggested research surmounts these constraints by achieving a 100% accuracy enhancement and employing the Homomorphic Public Key Encryption technique for training and predicting encrypted data. This approach guarantees privacy while expediting training without sacrificing usability.

However, this can be enhanced through multifactor authentication systems that combine passwords, biometrics, and OTP verification [26]. The study [27] observed that, to control access to data, most systems rely on usernames and passwords for authentication, which are both convenient and insecure because they can be quickly entered into an online application or service [28]. Since the human capacity for information processing is limited, users face difficulties in remembering and matching their passwords and, therefore, often use either easy-to-guess passwords or complex passwords that are hard to remember [29]. Many internet applications, such as remote logins, for government organizations, private corporations, database management systems, and school systems are based on password authentication, but the current internet environment is vulnerable to replay, guessing, modification, stolen verifier, and other types of attacks [30]. Regardless of the complexity of a password string, passwords are considered a weak form of authentication because they can be shared, stolen, forgotten, or hacked [31]. Despite several major problems that have been identified with alphanumeric passwords, they are still used to protect both low-sensitivity and highly sensitive information [29] and remain the most widely used method of end-user authentication [32] Since password-based user authentication methods provide only partial protection from hackers and intruders, additional authentication should be applied [33].

B. Multifactor Authentication (MFA)

MFA has emerged as a substitute mechanism to increase security by demanding that users provide more than one factor of authentication (i.e., in addition to a password) [32]. This layered approach to authentication provides more robust protections for users and minimizes the risks of breaching security [5] because a hacker must penetrate multiple layers of security to gain access to an MFA-enabled system. The various types of MFA present various security issues but combining them with password-based authentication systems can greatly improve the credibility of a user's login and complicate access for intruders [34].

Factors such as "what the user knows" (inherent), "what the user has" (possession), and "what the user is" (biometric) have served as additional authentication methods [32]. In this regard, biometric features unique to individuals, ranging from physiological characteristics (e.g., fingerprints and iris, hand, and face patterns) to behavioral characteristics (e.g., KD,

mouse movements, gait, and handwriting), have served to identify users [3]. Many such biometric approaches tend either to be expensive or to place heavy demands on computer hardware, making them inappropriate for most users [35].

C. Review of Authentication Methods

Human interface devices such as keyboards and mouse have been used extensively to help users interact with computer devices to increase their productivity. In this respect, the analysis of computer users' typing behavior (i.e., KD) is described as a behavioral biometric (BB) that can be analyzed and measured to improve cyber defenses [36]. The analysis of KD through BB (Fig. 1) focus on human-computer interaction (HCI) involving mouse movements and keyboard strokes [37]. The method proposed concentrates on a subcategory of HCI, wherein the innovative secure authentication approach relies on users' behavioral patterns manifested through keystrokes.

While extensive and valuable research on KD has facilitated authentication systems, challenges relating to the current user-authentication features include: -

- the increased use and introduction of HCI devices,
- the need to secure a behavioral and biometric database through relevant encryption standards,
- the ubiquitous and universal nature of devices that require cross-platform functionality,
- users' input errors during UN and PW entry linked to emotional states and secure web forms that restrict genuine access after a limited set of related errors,
- the availability of machine learning- and web-based solutions and hardware for authentication mechanisms, and
- biometric systems that can be forced on victims (unconsciously or under duress).

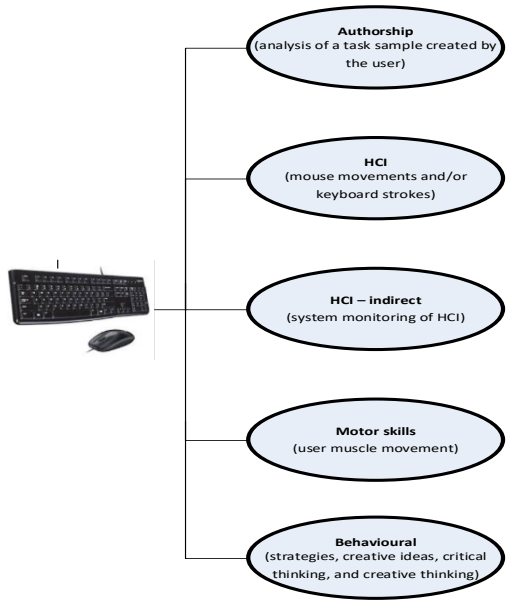

Fig. 1. Classifcation of behavioral biometrics [adapted from 37].

A lightweight, web-based secure authentication system that can be seamlessly integrated into multiple browsers based on behavioral KD meets these challenges. Research on KD using the keyboard and/or mouse in the literature includes authentication studies using ML, a combination of machine learning (ML) and web-based solutions, and hardware tokens. A Google Scholar title search using "keyboard dynamics" and "user authentication" generated seven relevant results, and a further search for these phrases anywhere in articles published since 2016 generated 62 results. These search results indicate that academic researchers exploring the application of KD in systems and device authentication (Table I) have been focusing on:

- the use of ML techniques for enrollment and verification with KD from live users and publicly available datasets based on keyboard and/or mouse dynamics with a near-zero error rate,
- proposing and experimenting with web-based applications that incorporate KD, mouse dynamics, a combination thereof, a combination of KD and biometrics, and behavioral features to achieve an accuracy of 97.96%,
- methodologies and experimental applications using KD and a combination of KD and mouse dynamics with hardware and software to achieve an accuracy of 97%, and
- Client-server KD systems requiring both hardware and software, along with peripherals like sensors, cameras, and hardware tokens.

D. Behavioral Authentication using ML

Several studies have described the successful or near-successful use of keystroke and/or mouse dynamics for authentication with public data sets as well as live users, mostly from a back-end server perspective. The author in [38] created a system using an ML classifier beginning with a support vector machine (SVM) room for each user that accesses data from 34 user environments and was able to accept real users with an extremely low error rate (nearly 0%). These findings demonstrate that a one-class SVM may serve as a tool for the continuous user analysis and validation of button dynamics through the formulation of plans and the choice of the proper kernel parameter. With histogram gradient boosting as the primary classifier for the training and testing phase on a keystroke benchmark dataset, [19] achieved 97.96% average accuracy and an average equal error rate (EER) of 0.014 across all subjects, thus outperforming all previous advances in both ML and deep learning approaches. The researcher in [39] used the confidence interval and k-means clustering to demonstrate the success of trajectory dissimilarity, achieving a higher accuracy rate, 96%, than other techniques. While trajectory dissimilarity uses KD for the usernames confidence interval and k-means clustering uses KD for passwords, another significant finding from the study is the use of the former to protect users from account lockout attacks (i.e., exploiting the lock-out of accounts after a defined number of incorrect password attempts).

TABLE I. REVIEW OF EXPERIMENTAL RESEARCH USING KEYBOARD AND / OR MOUSE DYNAMICS

		Author	ML	Live users	Public dataset	Error-correction method	Web-based	Accuracy (%)	Error rate
		Ibrahim et al., 2023	Yes	No	Yes	No	No	97.96	X
		Anusas-amornkul & Wangsuk, 2015	Yes	No	Yes	No	No	96.00	X
		Quimatio, Njike, & Nkenlifack, 2022	Yes	No	Yes	No	No	95.65	X
		Raul, Shankarmani, & Joshi, 2020	Yes	Yes	No	No	No	90.50	X
		Kar, Bamotra, Duvvuri, & Mohanan, 2023	Yes	Yes	No	No	No	95.05	X
		Phadol, 2022	Yes	No	Yes	No	No	X	Near 0
	Machine Learning focus	Shi, Wang, Zheng, & Cao, 2022	Yes	Yes	No	No	No	89.22	FAR of 11.27%; FRR of 10.25%
		X. Wang et al., 2022	Yes	Yes	No	No	No	84.00	X
		Jadhav et al., 2017	Yes	Yes	No	No	No	X	FAR of 1%; FRR 4%
		Stragapede et al., 2022	Yes	No	Yes	No	No	X	EER 03.25%
		Piugie, Di Manno, Rosenberger, & Charrier, 2022	Yes	No	Yes	No	No	X	EER of 04.49%
		Gupta et al., 2015	Yes	Yes	No	No	?	X	FAR of 05.4%; FRR of 09.2%
		Alshanketi et al., 2016	Yes	Yes	Yes	Yes	No	X	X
Web-based focus		Bhattacharya et al., 2022	Yes	Yes	No	No	Yes	87.00	X
		Yang et al., 2023	Yes	No	Yes	No	No	X	X
		(Shekhawat & Bhatt, 2022)	Yes	No	Yes	No	No	97.00	X
		Zaidan et al., 2017	No	Yes	No	No	Yes	Positive results	EER of 2.3%
		Boakye Osei, Opanin Gyamfi, & Okoe Alhassan, 2020	No	Yes	No	No	Yes	X	FER of 4%; FRR of 6%; FAR of 1%
		Kang & Kim, 2023	No	Yes	No	No	Yes	X	Low FAR and FRR values.
		Siti Rahayu et al., 2020	No	Yes	No	No	Yes	X	Low ERR
		Rahman, Neupane, Zaiter, & Hossain, 2019	No	Yes	Yes	No	Yes	X	EER of 10.50%
		Vasyl, Sharapova, Ivanova, Denis, & Yuliia, 2017	No	Yes	No	No	Yes	X	X
		Cockell & Halak, 2020	**	Yes	No	No	No	X	Error rate of 4.5%
		Proposed Study	YES	Yes	No	Yes	Yes	100	X

**Natural language processing; **Portable hardware token. EER = equal error rate; FAR = false accept rate; FRR = false reject rate; FER = failure to enroll rate*

Quimatio, Njike, and Nkenlifack [40] proposed an authentication method based on three bagging ensembles formed by an SVM, K-nearest neighbor (KNN), and decision tree classifiers, the outputs of which were merged using the CMU dataset to achieve 95.65% accuracy. Kar, Bamotra, Duvvuri, and Monahan [41] proposed KD for authentication by taking a dataset of 51 users who typed a password in eight sessions on alternate days to record fluctuations in their moods and implemented anomaly-detection algorithms based on distance metrics and ML algorithms, such as artificial neural networks (ANNs) and convolutional neural networks (CNNs), to classify the users with 95.05% accuracy with an ANN with Negative Class.

Other studies of these issues include that of Raul, Shankarmani, and Joshi [42], who proposed combining non-conventional features with the conventional time-based features for user identification in static KD using ML classifiers and observed improvements in the false reject rate (FRR), false accept rate (FAR), and EER; their five ML algorithms determined that the logistic regression method

achieved 90.50% accuracy. Shi, X. Wang, Zheng, and Cao [43] proposed a user authentication method based on KD and mouse dynamics involving comparison of all of the representative time windows and dimensionality-reduction targets of the KD features to determine the parameters for ensuring the robustness of the algorithm and, using real-world setting, the HCI dataset achieved 89.22% accuracy in authenticating users, thus demonstrating the effectiveness of the algorithm. X. Wang, Shi, Zheng, Zhang, Hong, and Cao [44] presented a user authentication method that relies on scene-related and user-related features for user identification: first, features are extracted based on keystroke and mouse movement data; next, scene-related features are obtained that have a low correlation with scenes; lastly, scene-related and user-related features are fused to ensure their integrity. This proposed method has the advantage of improving user authentication accuracy in hybrid scenes, with an accuracy of 84%. Alshanketi, Traore, and Ahmed [31] presented an algorithm for handling typing errors in mobile keystroke BA combining timing- and pressure-based features. They used the random forest algorithm to classify and differentiate between trusted users and impostors based on a profile built for each user.

Researchers have also used ML to measure the error rates as success factors in authentication. Piugie, Di Manno, Rosenberger, and Charrier [45] proposed an approach based on the transformation of behavioral biometrics data (i.e., time series) into a 3D image that retains all of the characteristics of the behavioral signal and assists in training images based on CNNs and evaluates the performance of the system in terms of the EER based on a significant dataset, and they demonstrated the efficiency of the proposed approach on a multi-instance system. Mao, Wang, and Ji [46] combined keystroke content with keystroke time as the feature vector using a CNN to process the feature vectors and then input the normalized vector into the bi-LSTM network for training; they then tested this approach on an open data set and achieved an FRR, FAR, and EER of 3.09%, 3.03%, and 4.23%, respectively. Stragapede, Delgado-Santos, Tolosana, Vega-Rodriguez, Guest, and Morales [47] took into account the emotional and physical state of the authenticator and proposed a novel transformer architecture to model free-text KD performed on mobile devices using a publicly available Aalto mobile keystroke database, and they achieved experimental results that outperformed the current state-of-the-art systems, with an EER of 3.25% from only five enrollment sessions of 50 keystrokes each.

Jadhav Kulkami, Shelar, Shinde, and Dharwadkar [3] proposed an ML-based authentication model that uses the static approach of keystroke dynamics to recognize and authenticate users accessing the system based on their unique keystroke profiles with respect to the flight, dwell, press, press-to-press, and release-to-release time and achieved an FAR and an FRR of 1% and 4%, respectively. Gupta, Khanna, Jagetia, Sharma, Alekh, and Chouldhary [35] proposed a high-efficiency authentication system combining two methods to make keystroke biometrics less susceptible to forgery and more usable and reported that the system efficiently implemented secure authentication with the advantage of ease of implementation since all that is required is the installation of software on any workstation. Yang et al. [55] focused on the text entered by the user and proposed contents and keystroke dual attention networks (ML) with pre-trained models for continuous authentication to address user-inputted "text" during keystrokes as an important asset beyond traditional KD characteristics, and their model achieved state-of-the-art performance on two datasets.

E. Web-based Behavioral Authentication

The research on various aspects of authentication systems has included web-based authentication, web-based keystroke authentication, portable tokens, and parametric approaches. Beginning with the first of these, to date, researchers have looked at web-based authentication. Thus, Bhattacharya, Trivedi, Obaidat, Patel, Tawar, and Hsiao [48] constructed a 2FA scheme for web users based on real-time KD by employing the KNN classification algorithm and achieved 87% accuracy over 146 testing samples and a recall value of 0.95, thus addressing the false-negative issue. Kang and Kim [49] used mouse dynamics and KD to identify personalized repeated user interface (UI) sequences with an Apriori algorithm based on the keystroke-level model of the HCI domain and validated the effectiveness of the system in complementing normal authentication through access testing with commercial applications that require intensive UI interactions.

Siti Rahayu, Guan, and Yusof [33] proposed an authentication system using KD in three stages—enrollment, verification/retraining, and client/server connection—and achieved a low error rate with just five users. Rahman [50] introduced a novel method utilizing KD as an additional validation layer in web-based applications such that users were prompted to type five words after registering their username and password (UN-PW), with the extracted features stored as a JSON object in the database. Vasyl, Sharapova, Ivanova, Denis, and Yulia [51] developed a web-based authentication system based on users' keystroke features and suggested merging KD with other human features to achieve greater precision in authenticating users. Zaidan, Salem, Swidan, and Saifan [27] developed a web-based application for use in the study of the factors affecting KD in mobile systems that extracts and stores features such as the characters typed, key-hold latency, up-down latency, down-down latency, and overall latency; they then tested factors such as the device used for typing, the knowledge of the text, the mood of the user, and the complexity of the password on this dataset and achieved positive results. Boakye Osei, Opanin Gyamfi, and Okoe Alhassan [52] proposed a web-based keystroke login system using features such as dwell, flight, and locate to minimize error rates. Though the system achieved lower error rates than previous systems, it was limited to web-based formats and QWERTY keyboards. Alieksieiev, Strelnitskiy, Gavva, Gorelov, and Synytsia [53] used a web-based application to gather and analyze users' keystroke information based on a calculation of digraph timings and employed a non-parametric test to compare multiple datasets for situations in which distribution is difficult to determine and the sample is small.

From a cloud environment perspective, [54] used a combination of static authentication, click color-based dynamic authentication, and behavioral biometrics (keystroke with cryptographic encryption and a hashing technique) to achieve 96% accuracy and a decrease in false positives with an error rate of 3%. In [18] author developed a unique way to perform KD-based authentication with a keyboard and an array of pressure sensors that serves to develop unique user profiles that improve the suggested system's efficiency and, using a real-world dataset, achieved a 97% success rate in experiments. Using a natural language processing method, [56] introduced a portable hardware token for MFA using keystrokes to enhance authentication, but the proposed algorithm, though simple, achieved relatively low accuracy, but with a relatively high error rate. So, they suggested applying ML and considering close keystrokes to reduce authentication errors. ML techniques, especially CNN, have been effectively employed in behavioral authentication using gait recognition to extract high-level features from the input data [57]. Likewise, the random forest classifier and support vector machine have been utilized in behavioral authentication involving touch behavior (such as finger pressure, size, and pressure time) while tapping keys on smartphones. This approach achieved an accuracy of 97.80% employing just 25 features [58].

This review of the literature on KD reveals two major aspects of authentication, namely the use of multiple devices (KD and/or mouse dynamics, including touch screens) and the extensive use of ML and web-based solutions in authentication. However, there is a lack of emphasis on the applicability of Behavioral Authentication (BA) across different devices, the potential for scalability in encryption standards, the influence of various emotional states of users on behavioral data errors, cross-platform compatibility, and the need to incorporate upcoming applications and solutions for cost efficiencies. In this regard, a validated secure and scalable model can offer multiple alternatives for the five constructs.

The experiment phase of research centers on keystroke dynamics as a behavioral biometric, propelled by both the user's frequent utilization of this parameter and their proximity to the computing device. While biometric parameters can encompass both physiological and behavioral traits, behavioral aspects, such as the user's gait, interaction with the graphical user interface, haptic responses, programming style, registry access, system call logs, and mouse dynamics, offer advantages like persistent security, post-login authentication, ease of behavioral data collection, and the absence of a requirement for specialized hardware [37]. The evaluation metrics, namely FAR, FRR, ERR, and FER, are all zero due to the 100% acceptance rate. As a result, these evaluation metrics are not elaborated upon in the subsequent section. Additionally, the experimental results establish a foundation for the forthcoming model, which can be employed for future research endeavors. In terms of the number of users, researchers have extensively used ML classifiers on publicly available databases for error reduction and conducted experiments using live keystrokes with numbers of users ranging from five to hundreds in which the data revealed no change in effectiveness, even with few users.

III. METHODOLOGY

The discussion of the research methodology here includes the proposed framework (Fig. 2) and the methods employed during the development of the proposed system.

A. KD Authentication Framework

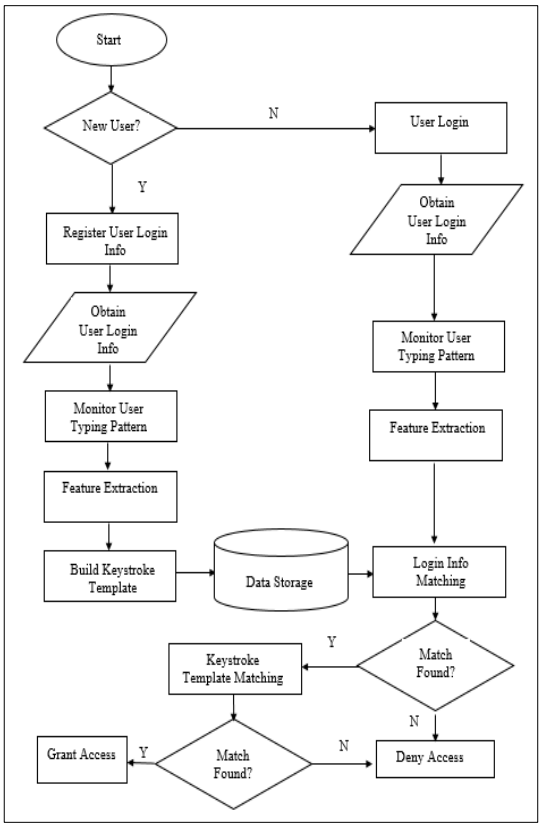

Fig. 2. Proposed framework.

B. Methods Employed

The method is a static approach that involves checking users' data during authentication. The experimental process starts with the training and testing phase and concludes with measures to handle errors. This section describes the environment under which our system was developed and evaluated.

1) Experiment environment: The system was developed using Python Programming 3.12 prerelease (2028-10 PEP 6932028-10 PEP 693) windows version running on a Laptop with specification (Core i5 with Intel Processor and 16 GB of RAM with Window 10 Operating version (Box 1).

2) Dataset description: The data were collected from five users. Each one was asked to type in the word "P@ssw0rd" in 10 trials. From each trail, four features (key press, key release, the characters typed by the user, and the total number of keys typed by the user) were extracted. Then three statistical features (average, mean and standard division) were added to each user's features. So, the total dataset used consists of 800 features (5x10x4x3).

3) Classifier description: In the classification phase, the CNN algorithm was used as follows. The features, extracted above, have been added at the fully connected layer of the CNN model. This further improved the classification accuracy.

Box 1 Python parameters

Python-CNN parameters tuning Learning rate = 0.01, 0.001, 0.0001 Neuron count= 8, 16, 12, Layer depth = 1, 2, 3, Kernel size = 8, 16, 12, Loss function = L2 loss, Binary cross-entropy, Epoch = 20, 50, 100 Number of Hidden layers =2 Output layer=1 Total number of layers =3

4) Security of the data: Since the behavioral keystroke data from the five users is stored on a server, users are unable to modify the application due to encryption. The system utilizes keystrokes to ascertain whether a user is a legitimate individual or an imposter, both during the session and even after logging into the program. The Paillier cryptosystem algorithm, that comes under the category of the Homomorphic Public Key Encryption technique was utilized in the keystroke analysis training to predict encrypted data, ensure both privacy and accelerate training without compromising usability. It assumes a public key encryption technique that supports the following homomorphic property, as demonstrated by the equation: E(m_1).E(m_2). This property can be stated as E(m)^k=E(k .m) for various identical ciphertexts. For notation, we use the letter E to designate an encrypted value. For example, E(x) stands for the encryption of x, and (C) represents the encryption of the distance indication C.

a) Training phase: The training phase incorporates the enrollment and registration of new users, who are prompted to a sign-up page, thus enabling the system to acquire and store their data. This phase includes the following processes:

- Registering and Obtaining Users' Login Information: Every unique user signs up with a preferred UN-PW (with a minimum length) that is stored in the database.
- Monitoring Users' Typing Patterns: After registration, users are required to type a sequence of characters three times at various speeds while the system monitors their typing rhythm.
- Feature Extraction: Once users register, specific features are extracted while they are typing, including key press (how long a key is held down), key release (how quickly a pressed key is released), the characters typed, and the total number of keys typed.
- Building a Keystroke Template: After extraction of the behavioral features, the data are structured in an array to store the extracted features of each character independently of the other characters. To build a keystroke template, the fastest keystroke data typed serve as the upper bound and the slowest as the lower bound.
- Data Storage: After these features have been extracted and the template has been built, they are stored in the database along with users' UN-PWs for deployment to authenticate them when they try to log into the system.

b) Testing phase: The testing phase occurs during the login of existing users using the credentials registered in the enrollment process through the sign-up interface. This phase includes the following processes:

- Obtaining Users' Login Information: Each user must type in the previously chosen UN-PW, and the data are collected mainly for matching with the stored behavioral characteristics.
- Monitoring Users' Typing Patterns and Feature Extraction: As in the training phase, users are prompted to type a sequence of characters twice so that the system can extract matching keystroke data.
- Login Information and Keystroke Template-matching: The system matches the UN-PW to the pre-registered data stored in the database. If the data do not match, the user is given three more tries and then, if still unsuccessful, locked out. Authentication is ensured only after matching of the username, password, and behavioral keystroke data. If the average keystroke provided does not fall within the bounds described in 3.2.1, the user is prompted to try again in like manner as in the case of the UN-PW.

c) Error handling: Users may make mistakes when entering their passwords, thereby compromising the accuracy of the authentication system. To prevent this outcome, the keystroke data for each letter are gathered and stored separately based on how the letter is typed. This information is then organized into an array and stored in the database. If a user attempts to correct a mistake by deleting a character using the backspace key, the keystroke datum for the last letter entered is removed from the array.

IV. Implementation, Results and Model

A. Implementation

A web-based application served to implement the system, the main components of which are (1) a server-side programming language (NodeJs) for back-end functions, (2) a front-end language (HTML and CSS) for user interface, (3) a database (MongoDB) for storing users' profiles and keystroke data, (4) JavaScript for extracting keystroke data, and (5) a web browser. As the flow chart (Fig. 2) shows, the proposed system consists of two phases, registration (training) and login (testing). The following discussion describes each of these phases in turn.

1) User registration: As discussed, access to the system requires a login ID for every user (Fig. 3). The login data are collected and stored during the registration process. In this phase, data such as first and last name, username, email, and password are collected, as the figure shows, and then stored in the database.

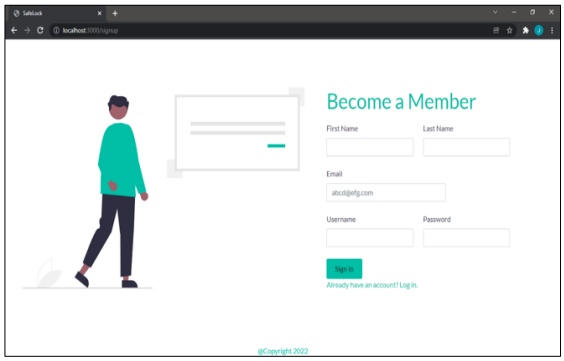

Fig. 3. User registration page.

2) Generation of the keystroke template: Once the login ID has been documented and stored in the database, the user is prompted through a screen as shown (Fig. 4).

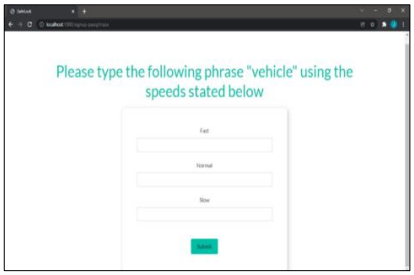

Fig. 4. Keystroke collection page.

Users are asked to type a randomly generated word in order to build a keystroke template. The features described above, such as the press and release of keys, which letters are typed, and the total number of characters typed, are extracted while the user types the word and stored independently in separate arrays. The keystroke data for the first letter occupy the first index of the array, the data for the second letter occupy the second index, and so on, as shown (Fig. 5).

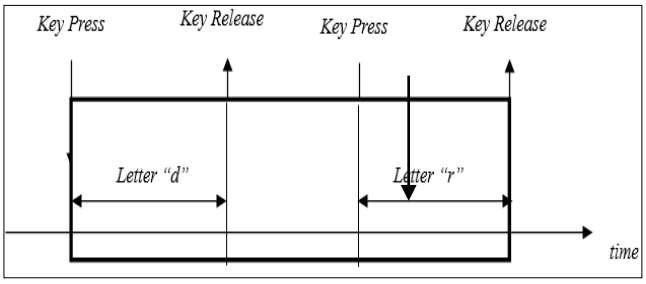

Fig. 5. Keystroke parameters.

The keystroke time KT, also referred to as the dwell time, is based on the user's typing rhythm for each letter of the randomly generated word and computed as

$$KT = K_{release} - K_{press}$$

where K_{press} is how long the user presses a key, $K_{release}$ is the time the user releases the pressed key, and $KT_{average}$, is the keystroke time of the phrase typed computed as the summation of the difference between the key press and key release times divided by the overall number of characters typed:

$$KT_{average} = \sum(K_{release} - K_{press}) \,/\, \textit{total number of letters typed}$$

Users are required to type the randomly generated word at various speeds as shown (Fig. 5) so that the system can collect their keystroke data at various speeds. The keystroke data at these speeds provide the bounds for each user's keystroke values, with the fastest keystroke serving as the lower bound and the slowest as the upper bound.

3) Data storage: Users' login ID and keystroke data are collected and stored in the database as shown (Fig. 6).

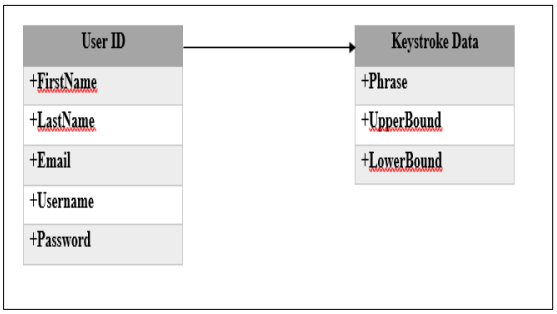

Fig. 6. Database model.

After users enter their login information on the registration page, the data are saved in the database, including the upper bound, the cumulative keystroke data, and the phrase used to log in. To minimize security risks, sensitive data, such as users' passwords and keystroke timing, are encrypted before storage in the database.

4) User verification: This process consists of the verification of users' login ID and keystroke timing as shown (Fig. 7).

a) Login ID verification: Once users try to access the system after registration, they are required to type in the credentials that they previously supplied, including the UN-PW, as shown in Fig. 7. Once the mandatory login data have been provided, the system matches the username and encrypted password by decrypting the latter to cross-check with the stored password hash for successful authentication, after which users are directed to the keystroke verification page.

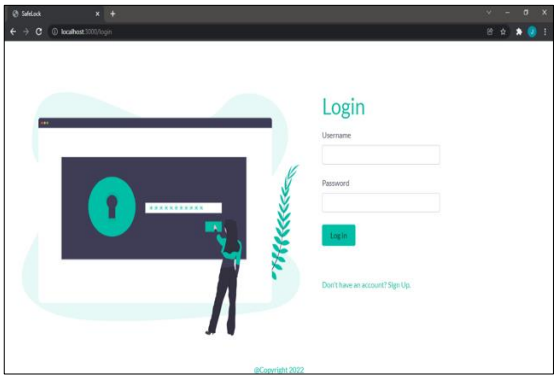

Fig. 7. Login ID verification.

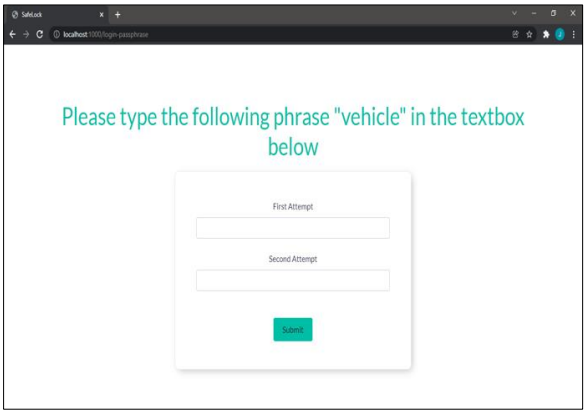

Fig. 8. Keystroke verification page.

b) Keystroke timing verification: On this form (Fig. 8), the user is required to enter the given phrase twice. During this process, the system computes the keystroke data for each letter typed and, once the user completes typing the first word or phrase, the average keystroke data. The process is then repeated with a second word or phrase. Once the user submits these data, the average of the keystroke data of the two words or phrases is computed and compared with the upper and lower keystroke bounds stored in the database, and the user is given access only if the average falls between them.

5) Error handling: Users are bound to make mistakes when typing. In keystroke-based systems, these mistakes can affect the accuracy of the system, but they can be managed efficiently. For example, in a situation in which a user types a sequence of characters, accidentally types a wrong character, and attempts to correct the error by tapping the backspace key. However, this attempt does not solve the problem of the mistyped character because the backspace key can be considered a character as well and the keystroke timing can be computed together with other characters. The proposed system incorporates an error-handling feature that deletes the last keystroke data accumulated after the backspace key is typed (Fig. 9).

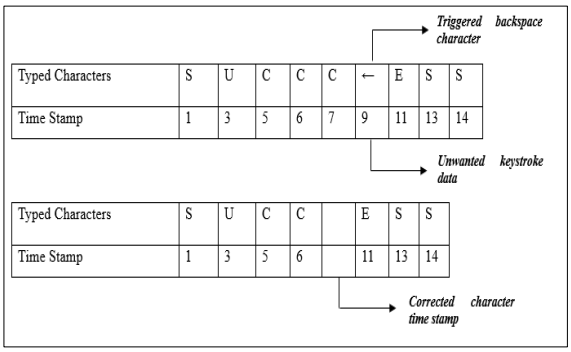

Fig. 9. Error handling using backspace.

B. Results and Discussion

To enroll in the system, each user types three words or phrases at fast, normal, and slow speeds. Taking into account the emotional state of authenticators, a rapid typing speed indicates that they are in a hurry or excited, while a slow speed indicates feelings of tiredness or illness. This approach, then, establishes ranges of possible values for users' keystroke timing in order to authenticate them regardless of their emotional state. During the typing process, event listeners (key down and key up) served to capture the key press and the key release times. The system is designed so that, when users make mistakes and press the backspace character, instead of adding the last character typed, it deletes the last character from the array as shown (Fig. 10). This feature renders our system privacy-protected, as personal behavioral data is deleted when no longer required.

In the experiment, the system grants access to all users who have connected to it provided that their typing times fall within their ranges. Conversely, if the keystroke time is not within their ranges, users are not granted access. However, the system can also grant access to another entity if the stored behavioral values fall within the range (using the same UN-PW), and this feature can be enhanced by increasing the number of words/phrases (Fig. 8) entered into the systems as shown in Table II. Based on these features of our model, it can be noted that there is a time limit imposed on the storage of personal data, fulfilling one of the privacy protection requirements.

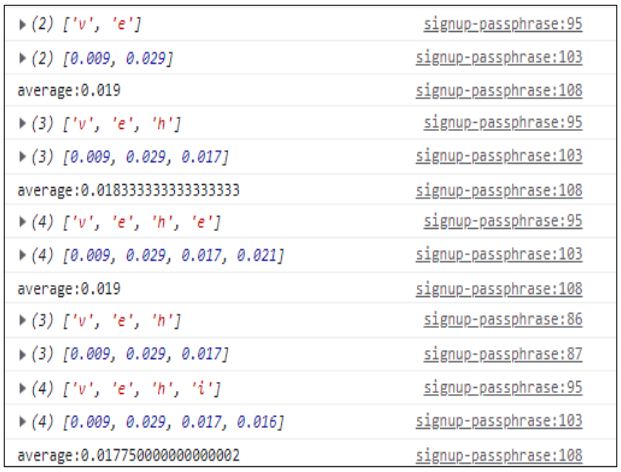

Fig. 10. Error handling using backspace.

The example presented in the figure is of the lower-bound keystroke values and corresponding upper-bound values for five users. User_a is granted access as long as the keystroke values provided at login fall within the range of 0.019 to 0.022, and this applies to other selected users as well. However, if user_c logs into the system as user_a, access is still granted because the keystroke times for user_a and user_c are similar. This method should always complement the usual UN-PW authentication method.

TABLE II. KEYSTROKE TIME VARIATION

User	User_a	User_b	User_c	User_d	User_e
Lower Bound	0.019	0.015	0.019	0.023	0.016
Upper Bound	0.022	0.020	0.023	0.026	0.019

In the error-handling approach, the last character typed and its corresponding keystroke are deleted once the backspace key is pressed. However, in rare cases, a user holds a character down for too long and causes it to duplicate, resulting in a key down time for each duplicated character but only one key up time for all of them. This arrangement renders the algorithm inefficient because the user's effort to delete the duplicated characters removes the data for other characters typed as well. Therefore, the user is required to delete all of the characters and start typing over again or refresh the page.

C. The Behavioral Dynamics Authentication Model

Five major constructs that directly influence the security of the authentication mechanism were developed based on the comprehensive review of the literature and were validated in the authentication experiment: the HCI devices, the encryption standard for the behavioral data, users' emotional state at the time of data entry, the seamless cross-platform transferability of the authentication mechanism, and the cost-effectiveness of the authentication mechanism (Fig. 11). Since the emergence of the keyboard, the HCI interface domain has advanced to support specialized devices that incorporate virtual or augmented reality and wearable technologies. Similarly, any authentication mechanism must take into account emerging trends in cryptology, including encryption algorithms. The accuracy of authentication depends on the emotional state of the authenticator as reflected in login errors. In other words, consideration of users' dominant emotional state during authentication can mitigate unauthorized authentication as well as authentication errors and recourse to the "forget your password?" option. For security of authentication mechanisms in a cross-platform domain, incorporating options for multiple operating systems authentications into the mechanism ensure seamless and secure operations. With the rapid application of AI in securing information system entities, and the emergence of innovative web applications taking into account the dynamic adoption of these into authentication mechanisms can ensure a balanced cost-security feature.

The system achieved 100% model validation with just five users by taking into account only one feature of each of the five constructs. This result demonstrates the economic feasibility and potential scalability of the model for future research involving experiments with various combinations of the constructs.

The main findings of the present study include:

1) The introduction of five constructs that offer an optimal combination ensuring efficient and effective behavioral authentication across all computer usage contexts.

2) The assessment of KD simulation to showcase the capability of KD in accurately authenticating even with just five users,

3) The demonstration of achieving a 0% rate for both FAR and FRR, and

4) The feasibility of encrypting behavioral data to enhance data protection.

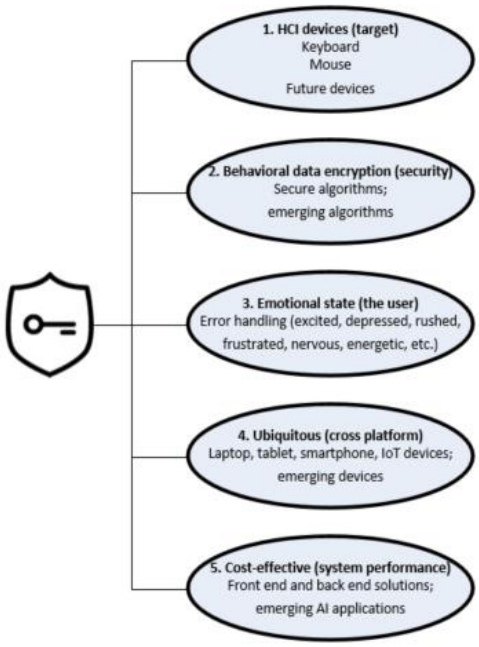

Fig. 11. The behavioral dynamics authentication model (BDAM).

V. Conclusion

Authentication processes that employ behavioral dynamics can ensure seamless and secure authentication through an optimal combination of HCI devices, data encryption, users' emotional states, cross-platform functionality, and the appropriate selection of solutions. We demonstrated the feasibility of constructing a secure, scalable, and dynamic behavioral authentication model, as described in this study. Our experimental results involved keystroke behavioral data collected from a computer system utilizing a web-based solution. We employed a CNN classifier and incorporated an error-correction feature. Remarkably, we achieved 100% accuracy in our authentication model with just five users. The web-based keystroke authentication system uniquely identifies users by integrating the UN-PW with their keyboard typing patterns, storing the keystroke data for each character typed independently, based on the bound value of the largest and smallest keystroke values recorded. For error handling, once the backspace key is triggered during typing, the keystroke data for the last character typed is deleted, and, when the keystroke data acquired during the process do not fall within the bounds established for a user, access to the system is denied; otherwise, access is granted.

The limitations of the research described here, also present avenues for future study to improve authentication systems. First, regarding the error-detection phase, the researchers considered only the backspace key, though some users also use the delete key, and taking this additional feature into account could enhance the speed of genuine authentication. Second, the system receives input in the form of mouse dynamics and touchscreen dynamics for laptops, tablets, and smartphones, but, while the focus here is on KD, the addition of touchscreen dynamics along with KD can add an additional security layer (potentially as an option) to touchscreen-enabled devices.

Third, changes in the environment and variation in the emotional state of the authenticator can render authentication challenging.

Future research can address the limitations by considering the following aspects. Firstly, researchers could replicate the study across various contexts, encompassing diverse environmental conditions similar to those encountered during authentication. Secondly, by accounting for users' cultural differences, extending the research to encompass subjects from multiple cultural backgrounds can enhance the robustness of the findings. Thirdly, given the substantial potential of ML in this domain, experimenting with different classifiers can yield those that ensure efficiency and effectiveness. Lastly, since the proposed model's versatility allows replication with diverse construct combinations and its scalability accommodates future trends in devices, security concerns, user behavior, and technologies, researchers could strive to pinpoint the optimal set of construct variables for enhancing authentication security and performance.

REFERENCES

[1] Crawley, K.: A deep dive into the Verizon 2020 data breach investigations report. https://spycloud.com/blog/a-deep-dive-into-the-verizon-2020-data-breach-investigations-report/ (2020). Accessed 22nd november 2022

[2] Raab, C., Szekely, I.: Data protection authorities and information technology. Comput. Law Secur. Rev. 33, 421–433 (2017)

[3] Jadhav, C., Kulkami, S., Shelar, S., Shinde, K., Dharwadkar, N.V.: Biometric authentication using keystroke dynamics. Paper presented at the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). (2017)

[4] Ben Fredj, O., Mihoub, A., Krichen, M., Cheikhrouhou, O., Derhab, A.: CyberSecurity attack prediction: a deep learning approach. Paper presented at the 13th International Conference on Security of Information and Networks. (2020)

[5] Aldwairi, M., Aldhanhani, S.: Multi-factor authentication system. Paper presented at the 2017 International Conference on Research and Innovation in Computer Engineering and Computer Sciences (RICCES 2017), Malaysia Technical Scientist Association. (2017)

[6] Pagar, V.R., Pise, R.G.: Password security mechanisms: comparative study. Paper presented at the International Conference on Research in Intelligent and Computing in Engineering (RICE 2017).

[7] Shankland, S.: Two-factor authentication helps but isn't as secure as you might expect. Retrieved from https://www.cnet.com/tech/services-and-software/two-factor-authentication-isnt-as-secure-as-you-might-expect-world-password-day/ (2017). Accessed 1st December, 2022

[8] Baig, E.C.: Google will warn you when your passwords are too simple to guess and used too often. Retrieved from https://techxplore.com/news/2019-10-google-passwords-simple.html (2019). Accessed 7th january 2023

[9] Verizon Inc.: Verizon data breach investigation report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/ (2018). Accessed 3rd February, 2023

[10] The Healthy Journal: How many people get hacked due to weak passwords? https://www.thehealthyjournal.com/frequently-asked-questions/how-many-people-get-hacked-due-to-weak-passwords#:~:text=Passwords%20are%20often%20identified%20as,to%20practice%20good%20password%20hygiene (2023). Accessed 3rd march 2023

[11] Maynes, M.: One simple action you can take to prevent 99.9 percent of attacks on your accounts. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ (2019). Accessed 3rd March 2023

[12] Wang, D., He, D., Wang, P., Chu, C.-H.: Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans. on Dependable Secure Computing 12, 428–442 (2014)

[13] Golla, M., Ho, G., Lohmus, M., Pulluri, M., Redmiles, E.M.: Driving 2FA adoption at scale: optimizing two-factor authentication notification design patterns. Paper presented at the 30th USENIX Security Symposium. (2021)

[14] Bhattasali, T., Saeed, K.: Two factor remote authentication in healthcare. Paper presented at the 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI). (2014)

[15] Sridhar, S.: Mitigating snoop-forge-replay attack by integrating text-based and language-based traits with the keystroke verification system. Int. J. Sci. Eng. Res. 5, 56–60. (2014)

[16] Council of the EU and the European Council.: The general data protection regulation. Retrieved from https://www.consilium.europa.eu/en/ (2022). Accessed 6th March, 2023

[17] ElShekeil, S.A., Laoyookhong, S.: GDPR privacy by design. Ph. D. dissertation, master's thesis. Stolkhom University (2017)

[18] Shekhawat, K., Bhatt, D.P.: A novel approach for user authentication using keystroke dynamics. J. Discrete Math. Sci. and Cryptogr. 25, 2015–2027. (2022)

[19] Ibrahim, M., AbdelRaouf, H., Amin, K.M., Semary, N.: Keystroke dynamics based user authentication using Histogram Gradient Boosting. Int. J. Computers and Inf. 10, 36–53. (2023)

[20] Chandok, R., Bhoir, V., Chinnaswamy, S.: Behavioural biometric authentication using keystroke features with machine learning. Paper presented at the 2022 IEEE 19th India Council International Conference (INDICON). (2022)

[21] S. M. S. Ahmad, B. M. Ali, and W. A. W. Adnan.: Technical issues and challenges of biometric applications as access control tools of information security. International Journal of Innovative Computing, Information and Control, 8 (11), 7983-7999, (2012)

[22] E. Pagnin and A. Mitrokotsa.: Privacy-preserving biometric authentication: challenges and directions. Security and Communication Networks, 2017, 1-9, (2017)

[23] N. Memon.: How biometric authentication poses new challenges to our security and privacy [in the spotlight]. IEEE Signal Processing Magazine, 34(4), 196-194, (2017)

[24] S. S. Harakannanavar, P. C. Renukamurthy, and K. B. Raja.: Comprehensive study of biometric authentication systems, challenges and future trends. International Journal of Advanced Networking and Applications, 10(4), 3958-3968, (2019)

[25] Z. Gao, W. Diao, Y. Huang, R. Xu, H. Lu, and J. Zhang.: Identity authentication based on keystroke dynamics for mobile device users. Pattern Recognition Letters, 148, 61-67, (2021)

[26] Hassan, M.A., Shukur, Z.: A secure multi factor user authentication framework for electronic payment system. Paper presented at the 2021 Third International Cyber Resilience Conference (CRC). (2021)

[27] Zaidan, D., Salem, A., Swidan, A., Saifan, R.: Factors affecting keystroke dynamics for verification data collecting and analysis. Paper presented at the 2017 Eighth International Conference on Information Technology (ICIT). (2017)

[28] Kuka, E., Bahiti, R.: Information security management: password security issues. Acad. J. Interdiscip. Stud. 7(2), 43. (2018)

[29] Hoonakker, P., Bornoe, N., Carayon, P.: Password authentication from a human factors perspective: results of a survey among end-users. Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting. (2009)

[30] Liao, I.-E., Lee, C.-C., Hwang, M.-S.: A password authentication scheme over insecure networks. J. Comput. and Syst. Sci. 72, 727–740. (2006)

[31] Alshanketi, F., Traore, I., Ahmed, A.A.: Improving performance and usability in mobile keystroke dynamic biometric authentication. Paper presented at the 2016 IEEE Security and Privacy Workshops (SPW). (2016)

[32] De Cristofaro, E., Du, H., Freudiger, J., Norcie, G.: A comparative usability study of two-factor authentication. arXiv preprint arXiv:1309.5344. (2013)

[33] Siti Rahayu, S., Guan, T.T., Yusof, R.: Enhanced authentication for web-based security using keystroke dynamics. Int. J. Netw. Secur. and Its Appl. (IJNSA) 12, 1–16. (2020)

[34] Williamson, J., Curran, K.: The role of multi-factor authentication for modern day security. Semicond. Sci. and Inf. Devices 3(1), 16–23. (2021)

[35] Gupta, A., Khanna, A., Jagetia, A., Sharma, D., Alekh, S., Choudhary, V.: Combining keystroke dynamics and face recognition for user verification. Paper presented at the 2015 IEEE 18th International Conference on Computational Science and Engineering. (2015)

[36] Banerjee, S.P., Woodard, D.L.: Biometric authentication and identification using keystroke dynamics: a survey. J. Pattern Recognit. Res. 7, 116–139. (2012)

[37] Oak, R.: A literature survey on authentication using behavioural biometric techniques. Paper presented at the Intelligent Computing and Information and Communication: Proceedings of 2nd International Conference, ICICC (2018)

[38] Phadol, N.B.: Keystroke dynamics for user authentication using SCM. Master's thesis, National College of Ireland, Dublin. (2022)

[39] Anusas-amornkul, T., Wangsuk, K.: A comparison of keystroke dynamics techniques for user authentication. Paper presented at the 2015 International Computer Science and Engineering Conference (ICSEC). (2015)

[40] Quimatio, B.M.A., Njike, O.F.Y., Nkenlifack, M.: User authentication through keystroke dynamics based on ensemble learning approach. Paper presented at the CARI 2022-Colloque Africain sur la Recherche en Informatique et en Mathémathiques Appliquées. (2022)

[41] Kar, S., Bamotra, A., Duvvuri, B., Mohanan, R.: KeyDetect: detection of anomalies and users based on keystroke dynamics. arXiv preprint arXiv:2304.03958. (2023)

[42] Raul, N., Shankarmani, R., Joshi, P.: Non-conventional factors for keystroke dynamics as a support factor for authenticating users. Int. J. Innov. Tech. and Exploring Eng. (IJITEE), 9, 474–479. (2020)

[43] Shi, Y., Wang, X., Zheng, K., Cao, S.: User authentication method based on keystroke dynamics and mouse dynamics using HDA. Multimed. Syst. 1–16. (2022)

[44] Wang, X., Shi, Y., Zheng, K., Zhang, Y., Hong, W., Cao, S.: User authentication method based on keystroke dynamics and mouse dynamics with scene-irrelated features in hybrid scenes. Sensors 22, 6627. (2022)

[45] Piugie, Y.B.W., Di Manno, J., Rosenberger, C., Charrier, C.: Keystroke dynamics based user authentication using deep learning neural networks. Paper presented at the 2022 International Conference on Cyberworlds (CW). (2022)

[46] Mao, R., Wang, X., Ji, H.: ACBM: attention-based CNN and Bi-LSTM model for continuous identity authentication. Paper presented at the Journal of Physics Conference Series. (2022)

[47] Stragapede, G., Delgado-Santos, P., Tolosana, R., Vera-Rodriguez, R., Guest, R., Morales, A.: TypeFormer: transformers for mobile keystroke biometrics. arXiv preprint arXiv:2212.13075. (2022)

[48] Bhattacharya, P., Trivedi, C., Obaidat, M.S., Patel, K., Tanwar, S., Hsiao, K.-F.: BeHAutH: A KNN-based classification scheme for behavior-based authentication in Web 3.0. Paper presented at the 2022 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI). (2022)

[49] Kang, S.J., Kim, S.K.: User interface-based repeated sequence detection method for authentication. Intell. Autom. and Soft Computing 35, 2573–2588. (2023)

[50] Rahman, K.A., Neupane, D., Zaiter, A., Hossain, M.S.: Web user authentication using chosen word keystroke dynamics. Paper presented at the 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA). (2019)

[51] Vasyl, A., Sharapova, E., Ivanova, O., Denis, G., Yuliia, S.: Web-based application to collect and analyze users' data for keystroke biometric authentication. Paper presented at the 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON). (2017).

[52] Boakye Osei, M., Opanin Gyamfi, E., Okoe Alhassan, M.: Keystroke dynamics algorithm for securing web-based password driven systems. Asian J. Res. in Comput. Sci. 4, 1–26. (2020)

[53] Alieksieiev, V., Strelnitskiy, A., Gavva, D., Gorelov, D., Synytsia, Y.: Studying keystroke dynamics statistical properties for biometric user authentication. Paper presented at the 2018 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). (2018)

[54] Saravanan, A., Bama, S. S.: CloudSec (3FA): a multifactor with dynamic click colour-based dynamic authentication for securing cloud environment. Int. J. Inf. and Comput. Secur. 20, 269–294. (2023)

[55] Yang, H., Meng, X., Zhao, X., Wang, Y., Liu, Y., Kang, X., . . . Huang, W.: CKDAN: Content and keystroke dual attention networks with pre-trained models for continuous authentication. Comput. and Secur. 128, 103159. (2023)

[56] Cockell, R., Halak, B.: On the design and analysis of a biometric authentication system using keystroke dynamics. Cryptogr., 4(2), 12. (2020)

[57] M. S. Sayeed, P. P. Min, and M. A. Bari.: Deep Learning Based Gait Recognition Using Convolutional Neural Network in the COVID-19 Pandemic. Emerging Science Journal, 6(5), 1086-1099, (2022)

[58] M. W. A. 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, 60(1), 273-283, (2021)