Grenze International Journal of Engineering and Technology, Jan Issue

Security Enhancement in Social Media Users using Keystroke Biometrics

D. Kavitha[1] and Thejas S[2]
[1-2]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India
Email: kavitha.d@vit.ac.in, thejas.s2023@vitstudent.ac.in

***Abstract*— As social media platforms continue to grow in popularity, ensuring the security and privacy of users' accounts has become a critical concern. Traditional authentication methods, such as passwords and PINs, are vulnerable to various attacks, including password guessing, phishing, and brute force attacks. To address these challenges, researchers have turned to keystroke dynamics as a promising solution. Keystroke dynamics, also known as keystroke biometrics, leverages the unique typing patterns and behavioral characteristics of individuals to authenticate their identities. This approach analyzes various keystroke attributes, such as key press duration, flight time, and typing rhythm, to create a user's unique typing profile. By continuously monitoring and comparing these patterns, social media platforms can verify the authenticity of users in real-time. This paper explores the potential of keystroke dynamics in enhancing security for social media users. It discusses the advantages of this approach, including its non-intrusive nature, continuous authentication capabilities, and resistance to common attacks. Additionally, the paper examines the challenges associated with implementing keystroke dynamics, such as user acceptance, system performance, and potential privacy concerns.**

***Index Terms*— phishing, brute force attacks, keystroke dynamics, flight time, typing rhythm.**

I. INTRODUCTION

The way individuals interact, communicate, and exchange information has changed dramatically in recent years due to the increasing usage of social media platforms. On the other hand, serious worries about user privacy and security have also been raised by this quick expansion. Password guessing, phishing, and brute force assaults are just a few of the ways that traditional authentication techniques, such passwords and PINs, have shown to be susceptible to. Keystroke dynamics has emerged as a viable approach to improve security on social media sites in response to these issues. Utilising each person's own typing habit and behavioural traits, keystroke dynamics, commonly referred to as keystroke biometrics, is a behavioural biometric authentication technique. Key press duration, flight time (the interval between releasing one key and hitting the next), typing rhythm, and other characteristics indicate the unique typing style of each individual. One may construct a unique typing profile for a user by analysing these patterns.

The concept behind keystroke dynamics is that individuals have consistent and distinguishable typing patterns that can be used to verify their identities. This strategy has a number of benefits over conventional authentication techniques. Firstly, it is non-intrusive, as users do not need to remember or disclose any additional information

Grenze ID: 01.GIJET.10.1.186

beyond their typing behavior. Secondly, it provides continuous authentication capabilities, allowing for real-time monitoring of user activity. Lastly, keystroke dynamics is resistant to common attacks such as password guessing, as an attacker would need to replicate the precise typing patterns of the legitimate user. The objective of this paper is to explore the potential of keystroke dynamics in enhancing security for social media users. We will discuss the advantages and challenges associated with implementing this approach, as well as the techniques and algorithms used in keystroke dynamics. Additionally, we will examine the implications of keystroke dynamics in social media platforms, including improved account security, reduced risk of unauthorized access, and enhanced user experience. By leveraging the unique typing patterns of individuals, keystroke dynamics offers a promising avenue for strengthening security in social media platforms. This research aims to contribute to the understanding and adoption of keystroke dynamics as an effective and reliable method of user authentication, ultimately ensuring a safer and more secure social media environment for users.

II. Related Works

[1]The essay exposes the vulnerabilities of knowledge-based authentication, exemplified by personal identification numbers (PINs), to spoofing attacks, emphasizing the importance of user authentication in a man-machine system. While suggesting the use of heredity factors like fingerprints for enhanced security, it introduces the WiPass device-free authentication system. WiPass utilizes existing Wi-Fi infrastructure to analyze keyboard dynamics recorded via channel state information, aiming to distinguish authentic users from impostors.Deciphering nuanced human keystroke behavioral characteristics poses a challenge, prompting the authors to introduce a signal augmentation model based on the Ricean distribution. They further develop a hybrid learning model for user authentication, combining support vector machines (SVM) and convolutional neural networks (CNN) for feature extraction and classification. Visualizing channel responses as time-series pictures aids in learning behavioral traits in energy and spectrum domains. The WiPass system comprises two closely related modules. The Ricean Fading-Based Signal Enhancement module magnifies keyboard dynamics through a signal amplification model. This model improves Wi-Fi Channel State Information (CSI) data and generates a filtered data profile with enhanced keystroke-induced trace descriptions. The second module uses a CNN for feature extraction and user authentication, leveraging time-series pictures to capture behavioral characteristics. Support Vector Machine (SVM) is then employed for user authentication based on the retrieved characteristics.WiPass's key advantage lies in eliminating the need for additional devices or hardware, utilizing existing Wi-Fi infrastructures for keystroke sensing. This approach addresses privacy concerns, allowing users to authenticate themselves without feeling monitored. The system's cost-effectiveness, relying on the current Wi-Fi infrastructure, positions it favorably compared to methods requiring additional hardware. WiPass streamlines authentication by enabling users to use a single, memorable phrase instead of complex passwords, enhancing user experience and reducing the burden of password management.Despite these merits, WiPass has its share of disadvantages. Dependency on Wi-Fi signals makes it susceptible to environmental factors like scattering, multipath fading, and signal blockage, potentially introducing noise and affecting keystroke recognition accuracy. Keystroke dynamics, influenced by individual typing habits, may result in variations leading to false rejections or acceptances, impacting system accuracy. WiPass primarily relies on knowledge-based authentication (a user's awareness of a phrase or password), potentially lacking the security level provided by multi-factor authentication methods incorporating biometrics. Users may need to adapt to WiPass's specific requirements, such as typing speed and input rhythm, requiring initial practice and adjustment, possibly leading to a learning curve.

In conclusion, while WiPass offers a practical and cost-effective solution leveraging existing Wi-Fi infrastructure for keystroke sensing, its effectiveness depends on overcoming challenges related to environmental factors and individual typing variations. The trade-off between convenience and security necessitates careful consideration in its adoption.

[2] Using Long Short-Term Memory (LSTM) networks for keystroke biometric authentication is investigated in the study "Short-Term Memory Networks for Keystroke Biometric Authentication at Large Scale in Free-Text Scenarios". The research concentrates on free-text situations—writing an email or message, for example—where the keystroke order is random, as opposed to fixed-text situations—entering a login or password.A variety of scenarios are used to assess the performance of the LSTM networks, including comparisons with cutting-edge methods and the use of four public datasets. The study's findings show that the suggested strategy beats earlier methods in the circumstances it was tested, suggesting that it has the potential to be authenticated in free-text situations.The intricacy and diversity of text entry, which lead to intra-subject behavioural variances, make it difficult to identify individuals in free-text settings, as the research emphasises. Although the performance of free-

text algorithms is often lower than that of fixed-text situations, previous research have demonstrated encouraging results utilising digraph algorithms and other strategies. LSTM networks trained with a reasonable amount of keystrokes per identity are used in the suggested method. Experiments with as many as 100,000 test subjects demonstrate competitive performance in large-scale authentication. The findings imply that individuals may be successfully authenticated in free-text keystroke dynamics using the suggested strategy.The research also addresses the effects of variables including keystroke sequence length, desktop or mobile device type, and text type dependence. The performance and generalisation ability of the suggested TypeNet models are revealed by the trials, underscoring the possibility for more advancements and uses.Finally, proof of the large-scale competitive performance of free-text keystroke biometric authentication is shown in the study. When creating efficient authentication systems, it is crucial to take into account the unique difficulties and features of free-text scenarios, as the findings show. LSTM networks have a lot of promise.

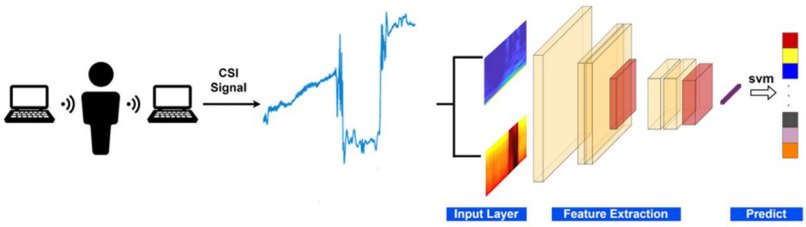

Fig. 1. Architecture of the adopted neural network.

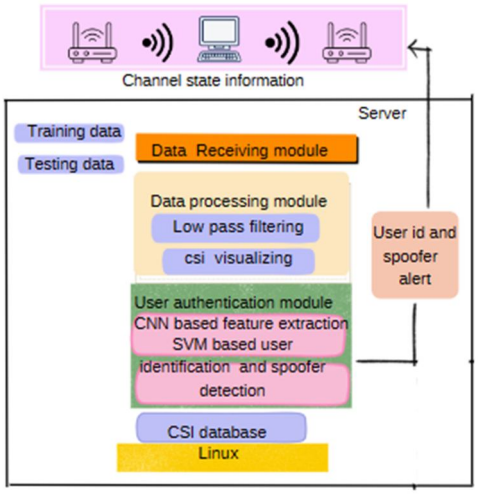

Fig. 2. WifiPass System architecture.

[3] Within the context of textual password authentication techniques that combine biometrics and textual passwords, the authors of this research especially address the shoulder-surfing resistance of mobile user authentication methods. With regard to these hybrid password strategies, there is a research gap that needs to be filled.Touch-gesture-based passwords and keystroke-based passwords are two hybrid password techniques that are compared in the study. Passwords entered by touch gestures on a mobile device's screen are required to be authenticated by users using the touch-gesture-based password technique. The keystroke-based password technique examines key hold times, down and up timings, pressure, and finger area measurements.The design of shoulder-surfing resistance techniques and password entering tactics are examined by the writers for these two approaches. The authors examine how input mistakes affect the resistance to shoulder-surfing and suggest novel efficiency measures to assess real-world situations involving time-sensitive shoulder-surfing attacks. In addition, the study addresses the experimentation approach, lists important literature, and examines comparable works in the subject.In this study, a statistical distance-to-median anomaly detector is integrated into a keystroke dynamics system designed for personal mobile devices. The system uses a particular feature set that blends touch screen capabilities like pressure and finger area with keyboard timing elements like hold and delay. Training and testing

are the two parts that make up the system. During the training phase, the user repeatedly enters the password; the data records of all those typing attempts are gathered and kept in a CSV file for further statistical analysis. During this step, a template with upper and lower criteria for every feature element is also developed and saved in a database.When a login attempt is performed during the testing phase, the input's keystroke and touch screen characteristics are recorded by the system. The resultant test vector of feature items is then compared to the user's saved template. The authenticity of a login attempt is determined by a predetermined passmark.In order to enhance user authentication on mobile devices, the suggested system functions as a research tool. It illustrates how keyboard dynamics and touch screen characteristics may be used to improve security and authentication.

[4] The study suggests a brand-new multi-user identification approach for fixed text keystroke behavioural dynamics that is based on non-linear transformation. The authors employ keystroke dynamics to categorise and identify multiple users who are using the same application in a unique way. To do this, the suggested method makes use of the quantile transform and localization strategies. The algorithm is referred to as UNLOC, or ordinal Unfolding based Localization. The study describes the suggested algorithm in detail, demonstrates how it was implemented, and provides benchmark keystroke dataset results that demonstrate the suggested algorithm's superiority over competing techniques. A multi-user identification technique for fixed text keystroke behavioural dynamics is the system that is suggested in this study. The approach employs a non-linear transformation that draws inspiration from localization techniques and the quantile transform. The term for it is UNLOC, or ordinal Unfolding based Localization. The suggested system uses keyboard dynamics to categorise and identify numerous users who are accessing the same application in a unique way. The system is tested using benchmark keystroke datasets and is intended to outperform existing techniques. This study uses a suggested technique known as ordinal Unfolding based Localization, or UNLOC. This approach for multi-user identification makes use of ideas from the following domains: data preparation, dimensionality reduction, clustering, embedding, and localization. Using just ordinal data derived by comparing distance proxies, the system analyses users' typing habits to "locate" them in a simplified PCA/Kernel-PCA/t-SNE space. The benchmark keystroke datasets are used to validate the proposed algorithm, which is intended to outperform existing techniques.The suggested strategy has the following benefits: The suggested algorithm is made to be more accurate and efficient than existing techniques. Because the technique just utilises ordinal data gathered by comparing distance proxies, noise and variances in typing behaviour are better tolerated. The suggested system uses keystroke dynamics to distinguish and categorise numerous users who are accessing the same application in a unique way. The suggested method has several drawbacks, including: To get high accuracy, the suggested method needs a lot of training data. Because of its computational complexity, the approach might not be appropriate for real-time applications. It's possible that the suggested technique won't work well against complex assaults that aim to imitate the typing patterns of real users. In terms of accuracy and efficiency, the suggested algorithm is intended to outperform alternative techniques. Because the technique just utilises ordinal data gathered by comparing distance proxies, noise and variances in typing behaviour are better tolerated. However, owing to its computational complexity, the suggested technique might not be appropriate for real-time applications and needs a significant quantity of training data in order to reach high accuracy. It's possible that the suggested technique won't work well against complex assaults that aim to imitate the typing patterns of real users.

[5] This study introduces a novel method utilizing keystroke dynamics from free-text for user identification authentication. To surpass previous research, a hybrid model, comprising a CNN and an RNN, employs a unique feature engineering approach to construct image-like transition matrices. The report meticulously examines hyperparameters, including keystroke sequence length and cutout regularization, presenting not only the methodology but also background information, learning strategies, and datasets. It also discusses relevant prior studies and suggests potential avenues for future research.The proposed method tackles the crucial cybersecurity challenge of ensuring accuracy and effectiveness in keystroke dynamics-based authentication. Using a feature engineering approach, it creates a five-channel transition matrix known as the Keystroke Dynamics Image (KDI). This matrix, resembling an image, incorporates characteristics arranged by channels, rows, and columns representing keys on a keyboard. The CNN and hybrid models then process the KDI, enhancing user identification based on keyboard dynamics.The hybrid model, combining CNNs and RNNs, operates by initially analyzing the KDI with a CNN to extract spatial information. Multiple layers within the CNN architecture generate a feature vector representing the spatial data. Subsequently, an RNN captures temporal dependencies within keystroke dynamics, producing a feature vector combining both spatial and temporal information. User classification as real or imposter is based on this final feature vector.Key benefits of the suggested strategy include a novel feature engineering approach, increased precision, and robustness suitable for real-world applications. However, drawbacks include limited datasets, computational complexity due to training both an RNN and a CNN, and

potential user resistance to inputting specific quantities of text. In summary, the suggested method, utilizing free-text keystroke dynamics for user identification, demonstrates promising results but requires further investigation to address constraints and validate its efficacy in practical scenarios.

[6] This study aims to enhance free-text keystroke biometric systems, addressing challenges posed by unpredictable text circumstances, user states, and in-use applications. It introduces a unique technique based on Transformers, a deep learning architecture renowned for natural language processing tasks. Remarkably, the proposed Transformer architecture outperforms existing deep learning techniques, including recurrent and convolutional neural networks, along with conventional machine learning methods. The study, recognizing the difficulty of free-text situations, makes its experimental framework and methodology open to the research community. The proposed keystroke verification method for free-text mobile scenarios leverages Transformers and their self-attention mechanism to function seamlessly over extended input sequences. Handling each sample simultaneously from the time series without summarizing earlier data, the model retrieves characteristics from two independent perspectives: the time and channel modules. To overcome challenges posed by unregulated text conditions, user mental and physical states, and diverse applications, the suggested Transformer design incorporates a self-attention mechanism. By simultaneously treating multiple ranges and using Gaussian range encoding with a multi-scale keystroke CNN, the model acquires a viewpoint on each sample in various situations. Impressively, with just five enrollment sessions, the suggested methodology surpasses existing state-of-the-art methods, achieving an Equal Error Rate (EER) of 3.84%. The study emphasizes the limitations of traditional machine learning techniques in addressing the complexity of free-text situations. The suggested Transformer architecture excels due to its advantages over recurrent and convolutional neural networks, offering parallel processing, efficient training, and the ability to handle long-distance sequences. Despite focusing on user verification, the article does not delve into potential applications for the system. However, the increasing demand for secure digital authentication methods in industries such as banking, financial services, healthcare, e-commerce, and government suggests potential uses for this technology. Further investigation and development are needed to explore these possibilities fully. Drawing on the Transformer architecture, the study presents a novel approach to free-text mobile keystroke biometrics, outperforming existing techniques. Utilizing data from over 260,000 participants in the Aalto mobile keystroke database, the suggested method showcases superior performance compared to alternative deep learning and conventional machine learning techniques. The study concludes by suggesting the method's applicability across various industries, including government, e-commerce, healthcare, banking, financial services, and insurance (BFSI), as well as mobile devices. It highlights the potential to enhance the security and reliability of digital authentication methods, indicating the broader impact of the suggested Transformer-based approach in real-world applications.

[7] This research introduces a groundbreaking multimodal biometric identification system that integrates keyboard dynamics and EEG (brain waves), potentially revolutionizing the biometrics industry. The study is organized into six sections, starting with an overview of contributions and research challenges. It proposes a system seamlessly integrated into password/PIN-based authentication, reducing user inconvenience. The multimodal system combines behavioral patterns from input data for user identification, using passwords for authorization.Machine learning algorithms process pre-processed data, selecting models with optimal accuracy. Unique custom models for each user further enhance recognition performance. A binary template matching technique for rapid identification and authentication is also presented. The study contends that EEG and keyboard dynamics are complementary, forming a robust biometric identification method. EEG waves, unique and challenging to fake, enhance trustworthiness, while keystroke dynamics offer high recognition rates.The paper highlights the system's advantages, including novelty, high accuracy, anti-spoofing capability, efficiency, personalization, and real-time authentication. However, it acknowledges limitations, such as susceptibility to attacks and potential incompatibility with certain individuals or ethical concerns about data use. The report emphasizes the need for robust security measures, ethical considerations, and individual data control.While the study lacks a direct comparison with conventional techniques, it asserts superior performance, achieving an identification accuracy of 98.5% and an equal error rate (EER) of 0.5%. The suggested system proves resilient against various attacks, reinforcing its reliability and security. In summary, the research proposes a multimodal biometric system merging EEG and keystroke dynamics, outperforming individual modalities significantly. The algorithmic approach addresses limitations, and the system demonstrates promising results in varied scenarios. It introduces an efficient method for real-time authentication, showcasing potential as a reliable and secure biometric authentication system.

[8] In this study, a unique method for improving user authentication using convolutional neural networks is proposed. The performance and constraints of the present biometric systems are examined by the authors in order to solve the shortcomings of those systems, and they also suggest a model that might improve the precision and

functionality of those systems. In addition to the experimental findings, which include the dataset, assessment measures, and outcomes, the study provides a thorough overview of the suggested technique and the preprocessing and learning methods employed. The authors also recommend possible directions for more research. In this paper, the authors present an efficient convolutional neural network-based system designed to enhance user authentication through keystroke dynamics. This system incorporates effective preprocessing methods, a deep learning architecture, and a boosting classifier to elevate the accuracy and overall performance of biometric systems. The authors also introduce an innovative data augmentation technique that effectively increases the dataset by manipulating standard deviation and reduces anomalies and extreme values through quantile transformation, thereby transforming any distribution into a uniform one. The custom convolutional neural network is specifically crafted to mitigate overfitting and underfitting issues. In essence, the proposed system seeks to overcome the shortcomings of existing systems and improve the accuracy and performance of biometric authentication systems. The presented system achieves remarkable results, with an average accuracy of 99.95%, an average equal error rate (EER) of 0.65%, and an average area under the curve (AUC) of 99.99%. These outcomes surpass recent advancements made on the Carnegie Mellon University (CMU) dataset. The system relies on effective preprocessing techniques, a deep learning architecture, and a boosting classifier to enhance the accuracy and overall performance of biometric systems. The authors also introduce an innovative data augmentation method, leveraging standard deviation, and employ quantile transformation to mitigate anomalies and extreme data values, converting distributions into uniform ones. The custom convolutional neural network is intentionally designed to handle overfitting and underfitting issues. It's important to note that the proposed system's evaluation is based solely on the CMU dataset and may not generalize effectively to other datasets. Additionally, acquiring a substantial amount of training data may pose challenges in certain situations. The system could be susceptible to attacks aimed at mimicking legitimate users' keystroke patterns. In summary, this paper concludes that the proposed system, based on an efficient convolutional neural network approach for improving user authentication through keystroke dynamics, achieves impressive accuracy and performance when tested on the CMU dataset. The authors tackle the limitations of existing biometric systems by thoroughly examining their performance and shortcomings, and they put forward a model designed to enhance the accuracy and overall effectiveness of such systems. The system introduces a novel data augmentation method, deals with anomalies and extreme data values, and features a customized convolutional neural network that's resilient to overfitting and underfitting challenges. The authors suggest that the system has the potential to be adapted for use with other datasets and could prove valuable for improving the accuracy and performance of biometric systems in various applications.

[9] In order to develop a more reliable and secure method of user authentication, this article investigates the usage of keyloggers in conjunction with keystroke dynamics. Keyloggers and keystroke dynamics are defined first, followed by a discussion of how they might be combined to enhance authentication. We also address prospective uses of this technology and give an outline of the current research in this field.This study presents a sophisticated keylogger with keystroke dynamics. In order to identify a user, this system records keystrokes performed on a computer keyboard and analyses their distinct patterns and rhythms. Compared to conventional keyloggers, the system is more advanced as it records not just keystrokes but also the user's whole activity, including system and application information. The system also has capabilities that let it determine which user, out of several, is utilising the system at that moment and which programme is open in the target system. This is accomplished by scrutinising the user's typing pattern, including the duration of time spent hitting the subsequent key on the keyboard after pressing a previous key. Eventually, the system stores all of the data it collects as data logs, which are then forwarded as log files to the admin email ID. The suggested technology has potential uses in sensitive applications like online banking, e-commerce, and other sectors since it is generally more precise and secure than conventional keyloggers.

Compared to conventional keyloggers, the suggested solution is more precise and safe. In addition to recording keystrokes, the system also records the user's whole activity, including system and application specifics. The system can determine which user, out of several, is utilising the target system at the moment and which application is open in that system. A more advanced and secure method of authentication is used by the system to identify users using keystroke dynamics. Limitations: Users with physical limitations or disabilities that impact their typing habits may find the suggested system difficult to utilise. Because it records and stores extensive information about the user's activities on the target system, the system may not function well in noisy environments or with users who have irregular typing patterns. Adoption may be hampered by the need to install additional hardware or software on the target system.This research concludes by proposing a sophisticated keylogger with keystroke dynamics that is intended to record keystrokes performed on a computer keyboard and identify a user based on

their own keystroke patterns and rhythms. Online banking, e-commerce, and other sensitive applications might benefit from the use of the suggested method, which is more secure and accurate than conventional keyloggers. The suggested system's drawbacks are also noted in the study, including possible problems for users with impairments or irregular typing styles and privacy issues with recording and storing extensive user activity. Overall, the suggested technique is a significant advancement towards the creation of more precise and safe user authentication methods, and it may prove to be a useful instrument for enhancing security across a range of apps.

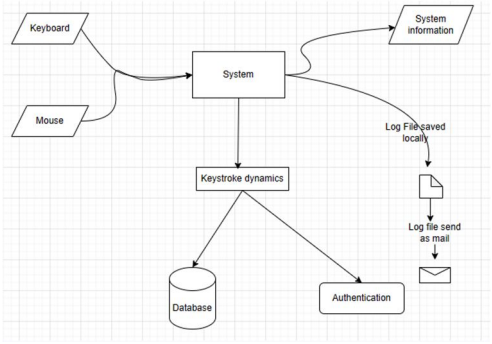

Fig. 3. Proposed block diagram

[10] An approach for lowering the number of keystrokes needed for user authentication is proposed in the paper "Fast and Accurate Continuous User Authentication by Fusion of Instance-based, Free-text Keystroke Dynamics". Using characteristics that are often utilised, including digraphs and monographs, the technique builds a fused classifier. The algorithm's performance is assessed and contrasted for varying quantities of graphs inside the testing dataset. With EERs of 7.9%, 5.7%, 3.4%, and 2.7% for test samples of 50, 100, 200, and 500 keystrokes, the fused classifier beats the state-of-the-art. In order to enhance an existing system and more effectively detect attackers, the article intends to speed up authentication and give an extra layer of protection.An instance-based graph comparison technique is the solution that is suggested in the study to improve user authentication efficiency using keystroke dynamics. This system's primary goal is to minimise the amount of keystrokes needed for authentication while keeping a high degree of security.The programme compares each graph time between the reference profile and the test sample using instance-based techniques. It looks at frequently used characteristics like digraphs and monographs and determines the significance of each feature in order to build a fused classifier. Using detection error tradeoff (DET) curves with varying keystroke counts, the algorithm's performance is assessed. With the use of an innovative instance-based algorithm and keystroke dynamics, the study provides encouraging findings for improving account security. Its limitations, nevertheless, such as the particular dataset it employed and the requirement for more study, should be taken into account when evaluating its wider application. By utilising instance-based authentication techniques and keystroke dynamics, the suggested approach presents a viable way to improve user account security. The system can effectively strike a balance between security requirements and user ease, according to the findings, which makes it a significant advancement in the field of biometrics and security.

III. CONCLUSIONS

In conclusion, the examined papers collectively illuminate the challenges and advancements in user authentication, particularly focusing on keystroke dynamics and its integration with various technologies. The vulnerabilities of knowledge-based authentication, such as PINs, underscore the need for more secure alternatives. WiPass emerges as a practical solution, leveraging existing Wi-Fi infrastructure, yet it grapples with challenges like environmental factors and typing variations, emphasizing the delicate balance between convenience and security. The studies exploring LSTM networks, hybrid password strategies, and multimodal biometric systems showcase the evolving landscape of authentication methods, addressing complexities in free-text scenarios and introducing innovative approaches.The CNN-based models and the UNLOC algorithm contribute to enhancing accuracy in user identification, though considerations of training data and real-time applicability persist. Integrating keyloggers with keystroke dynamics presents a novel approach, emphasizing precision and security but requiring attention to user limitations and privacy concerns. The proposal for continuous user authentication through a fused classifier demonstrates a promising stride, improving efficiency and security. Collectively, these studies shed light on the

multifaceted nature of user authentication, emphasizing the ongoing pursuit of secure, user-friendly methods with broader implications for the evolving landscape of digital security.

REFERENCES

[1] Y. Gu et al., "Secure User Authentication Leveraging Keystroke Dynamics via Wi-Fi Sensing," in IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2784-2795, April 2022, doi: 10.1109/TII.2021.3108850.

[2] A. Acien, A. Morales, J. V. Monaco, R. Vera-Rodriguez and J. Fierrez, "TypeNet: Deep Learning Keystroke Biometrics," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 1, pp. 57-70, Jan. 2022, doi: 10.1109/TBIOM.2021.3112540.

[3] L. Zhou, K. Wang, J. Lai and D. Zhang, "A Comparison of a Touch-Gesture- and a Keystroke-Based Password Method: Toward Shoulder-Surfing Resistant Mobile User Authentication," in IEEE Transactions on Human-Machine Systems, vol. 53, no. 2, pp. 303-314, April 2023, doi: 10.1109/THMS.2023.3236328.

[4] C. Sahu, M. Banavar and S. Schuckers, "A Novel Non-Linear Transformation Based Multi User Identification Algorithm for Fixed Text Keystroke Behavioral Dynamics," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 5, no. 2, pp. 277-287, April 2023, doi: 10.1109/TBIOM.2022.3212958.

[5] Li, Jianwei, "Keystroke Dynamics for User Authentication with Fixed and Free Text" (2021). Master's Projects. 1004. DOI: https://doi.org/10.31979/etd.ku7u-v7s4

[6] G. Stragapede, P. Delgado-Santos, R. Tolosana, R. Vera-Rodriguez, R. Guest and A. Morales, "Mobile Keystroke Biometrics Using Transformers," 2023 IEEE 17th International Conference on Automatic Face and Gesture Recognition (FG), Waikoloa Beach, HI, USA, 2023, pp. 1-6, doi: 10.1109/FG57933.2023.10042710.

[7] A. Rahman et al., "Multimodal EEG and Keystroke Dynamics Based Biometric System Using Machine Learning Algorithms," in IEEE Access, vol. 9, pp. 94625-94643, 2021, doi: 10.1109/ACCESS.2021.3092840.

[8] AbdelRaouf, Hussien, Samia Allaoua Chelloug, Ammar Muthanna, Noura Semary, Khalid Amin, and Mina Ibrahim. 2023."Efficient Convolutional Neural Network Based Keystroke Dynamics for Boosting UserAuthentication" Sensors 23,no.10:4898.https://doi.org/10.3390/s23104898.

[9] J. Sabu, A. S, A. Gopan, G. S and S. Murali, "Advanced Keylogger with Keystroke Dynamics," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 1598-1603, doi: 10.1109/ICICT57646.2023.10134044.

[10] B. Ayotte, M. K. Banavar, D. Hou and S. Schuckers, "Fast and Accurate Continuous User Authentication by Fusion of Instance-based, Free-text Keystroke Dynamics," 2019 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2019, pp. 1-6.