IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133105

KEYSTROKE RHYTHM ANALYSIS FOR IDENTITY VERIFICATION

Rajesh N Kamath[1], Swathi.K.L.[2], Vijetha Pai[3], Sneha C M[4], Lakshitha K Salian[5]

Student, Dept. of Information Science & Engineering, Mangalore Institute of Technology & Engineering, Moodabidre, India[2,3,4,5]

Senior Assistant Professor, Dept. of Information Science & Engineering, Mangalore Institute of Technology & Engineering, Moodabidre, India[1]

Abstract: Analysing behavioural biometrics involves examining various user behaviours, such as the dominant hand used on a phone, the angle of device holding, typing speed and style, including keystroke rhythm and pressure applied, along with swipe and scroll patterns. Gait analysis further contributes by assessing an individual's walking pattern. Continuously monitoring these biometric traits and comparing them against established user profiles can significantly bolster security against identity theft and online fraud. However, it's paramount to strike a delicate balance between the security benefits and privacy concerns, ensuring the responsible use and safeguarding of user data. Our multi-modal authentication system harnesses both facial features and typing patterns, employing cutting-edge algorithms and real-time processing to deliver a seamless user authentication experience. Anti-spoofing measures are integrated to enhance system integrity, while comprehensive testing validates its effectiveness across a wide range of applications, from cybersecurity to access control. Continuous monitoring and updates are implemented to maintain optimal system performance, adapting to evolving security threats and user needs. By leveraging the distinctiveness of these behavioural biometrics, our system stands as a pioneering solution in enhancing security measures while prioritizing user privacy and usability.

Keywords: Behavioural biometrics, Keystroke rhythm, Finger pressure, Swipe patterns, Gait analysis.

I. INTRODUCTION

The integration of keystroke dynamics classifiers employing long short-term memory (LSTM) layers marks a significant stride forward in authentication system development. This paper endeavours to offer an exhaustive elucidation of the classifier implementation process while presenting a methodology for ascertaining the optimal number of test samples per individual necessary for ensuring the security and sustainability of the system. By capitalizing on LSTM layers, renowned for their ability to capture temporal dependencies within data, keystroke dynamics classifiers present a robust solution for user authentication. A central aim of this paper is to advocate for the incorporation of keystroke dynamics as a ubiquitous authentication mechanism. Rather than supplanting conventional password systems, keystroke dynamics can serve as a complementary layer, augmenting security measures without imposing additional burdens on users. Through seamless integration into existing authentication frameworks, users stand to benefit from heightened security without necessitating significant alterations in behaviour. The paper delves into the potential of keystroke dynamics as an authentication modality, evaluating its accuracy and efficacy. Crucial considerations encompass its capacity to mitigate prevalent security threats like keyloggers, which pose substantial risks to password-based authentication schemes. By mandating a typing rhythm vector alongside a password, accounts can be shielded from unauthorized access, even in scenarios of password compromise.

Moreover, keystroke recognition exhibits promise in addressing concerns related to account sharing, a longstanding issue for service providers. By scrutinizing typing rhythms, it becomes feasible to detect instances of account sharing and implement corresponding policies. Leveraging publicly accessible datasets and advanced machine learning methodologies, keystroke recognition systems can play a pivotal role in upholding the integrity and security of online platforms.

In summation, this paper serves as a comprehensive examination of keystroke dynamics classifiers, spotlighting their potential to fortify authentication systems across diverse domains. Through empirical analyses and theoretical discourse, it underscores the significance of integrating keystroke dynamics analysis into everyday applications, thereby fortifying security measures and safeguarding user accounts against unauthorized access.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133105

II. LITERATURE SURVEY

In [1] Fabian Monrose and Aviel D. Rubin (2000) introduced keystroke dynamics as a biometric for authentication, leveraging unique typing patterns for user verification. Their research established the viability of using keystroke dynamics to enhance security in digital systems, pioneered keystroke dynamics as a biometric for authentication, demonstrating its potential in secure systems. paving the way for further advancements in biometric authentication methods.

In [2] Kenneth Revett and Johnathan M. Dale (1992), "Keystroke dynamics: considerations and implications," delved into keystroke dynamics, emphasizing its significance and implications for user authentication. By examining keystroke patterns, they aimed to develop more secure authentication systems, contributing valuable insights to the field of cybersecurity and biometrics.

In [3]. Francesco Bergadano, Daniele Gunetti, and Claudia Picardi, "User authentication through keystroke dynamics,"(2002) proposed a novel approach to user authentication based on keystroke dynamics. Their research focused on analysing individual typing patterns to create robust authentication mechanisms, improving security measures in digital environments and addressing the growing need for reliable user verification methods.

In [4] Ferdous Kawsar and Dimitrios Hristu-Varsakelis, "Learning-based keystroke dynamics for continuous authentication in IoT,"(2020) The researchers proposed a learning-centric strategy for keystroke dynamics to enable continuous authentication in IoT devices. Through the utilization of machine learning methodologies, their objective was to elevate authentication precision and flexibility, tackling the distinctive hurdles presented by IoT environments and fostering progress in secure IoT systems.

In [5] Kevin S. Killourhy and Roy A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics,"(2009). The researchers conducted an in-depth examination of anomaly detection algorithms tailored for keystroke dynamics. Their study concentrated on identifying and assessing efficient techniques for recognizing unauthorized access through keystroke patterns, offering valuable perspectives on enhancing the security of authentication systems against insider threats and cyber assaults.

In [6] Daniele Gunetti and Claudio Picardi, "Keystroke analysis of free text,"(2001)conducted a thorough investigation into keystroke analysis in free text. By studying natural typing behaviors, they aimed to develop more accurate and reliable authentication systems based on keystroke dynamics, contributing to the ongoing efforts to enhance security measures in digital environments.

In [7] M. S. Obaidat and A. M. Agbaria, "Keystroke dynamics-based authentication for cloud computing," 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, 2015. introduced keystroke dynamics-based authentication for cloud computing, addressing the need for secure authentication methods in cloud-based systems. Their research focused on leveraging keystroke patterns to enhance the security of user authentication processes, ensuring robust protection against unauthorized access and data breaches in cloud environments.

In [8] Ankit Kalra and Rajesh Kumar, "A comparative study of different classification algorithms for keystroke dynamics,"(2019) conducted a comparative study of classification algorithms for keystroke dynamics. Their research aimed to identify the most effective algorithms for analyzing and verifying keystroke patterns, optimizing authentication accuracy and reliability in digital systems, and providing valuable insights into improving authentication mechanisms based on keystroke dynamics.

In [9] Benjamin Fabian et al., "User authentication through keystroke dynamics and its evaluation on a mobile device," (2015) evaluated user authentication through keystroke dynamics on mobile devices, addressing the unique challenges and opportunities presented by mobile computing environments. Their research aimed to develop reliable authentication mechanisms tailored to mobile devices, ensuring secure user verification processes and enhancing the overall security posture of mobile computing platforms.

In [10] Peter J. Kilpatrick, Fabian Monrose, and Aviel D. Rubin, "Biometric authentication using time-dependent Gaussian mixture models,"(2007.) proposed biometric authentication using time-dependent Gaussian mixture models, leveraging advanced statistical techniques to enhance authentication accuracy and robustness. Their research contributed to the development of more secure and reliable authentication methods based on keystroke dynamics, paving the way for advancements in biometric authentication technologies.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133105

III. SCOPE AND METHODOLOGY

Aim of the project

The goal of the Keystroke Rhythm Analysis for Identity Verification project is to create robust technologies or systems proficient in scrutinizing keystroke patterns to authenticate user identities with precision. Through the utilization of sophisticated machine learning algorithms, the system endeavors to grasp distinctive keystroke rhythms linked to individual users, facilitating dependable identity verification. Its core aim is to elevate security protocols by harnessing biometric data extracted from typing behavior, furnishing an extra layer of authentication alongside conventional methods such as passwords or PINs. Additionally, the project aims to enhance user experience by delivering smooth and user-friendly identity verification procedures, all the while upholding stringent security standards.

Existing system

Conventional password-based authentication methods are widely employed to safeguard user accounts, typically comprising combinations of alphanumeric characters selected by users. However, this approach harbors several shortcomings. Traditional passwords remain static and fail to adapt to evolving user behavior, rendering them susceptible to exploitation. Furthermore, the prevalence of weak password choices or their reuse across multiple accounts exacerbates security vulnerabilities.

Consequently, regular password updates become necessary to mitigate these risks. Additionally, traditional passwords are vulnerable to various threats, including phishing attacks, where malicious entities attempt to deceive users into disclosing their credentials, and brute-force attacks, which entail systematically guessing passwords until the correct one is uncovered. These limitations underscore the imperative for more resilient and adaptable authentication mechanisms to bolster security and safeguard user accounts.

Proposed system

The prevailing issue with current approaches and implementations regarding keystroke authentication based on static text lies in the lack of accessibility and compatibility between the chosen statistics and the constructed models. Hence, we advocate for a more straightforward and accessible model and metric to attain the desired classification, offering improved interpretability.

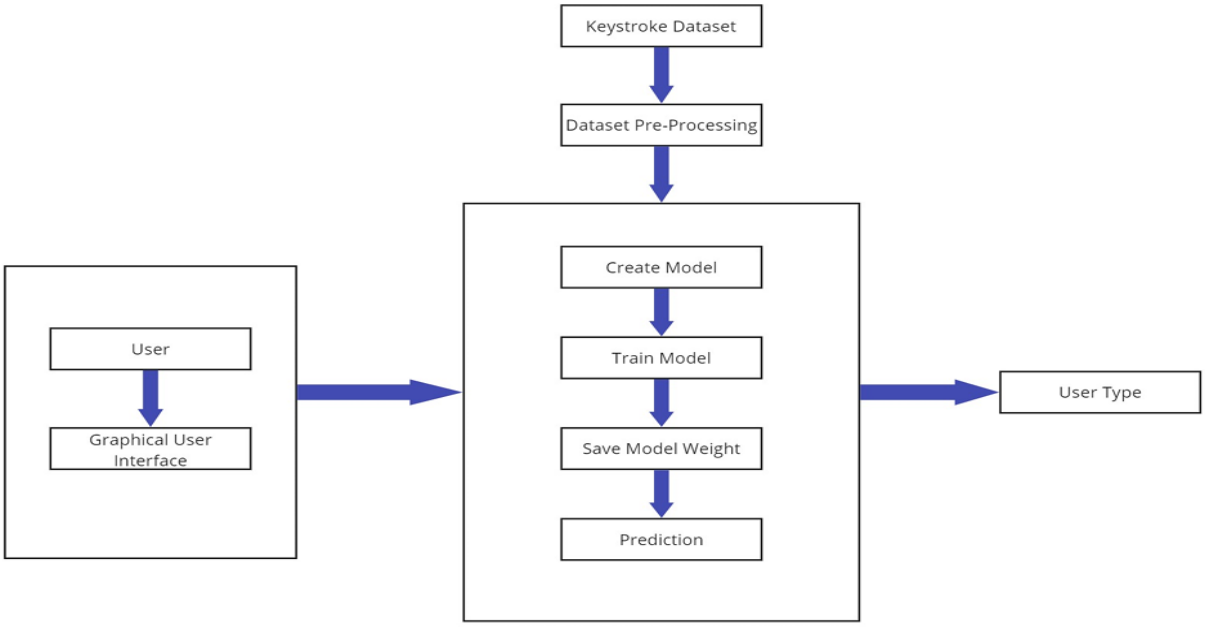

Fig 1. Proposed system

The user's score is juxtaposed against a predetermined threshold to determine the decision. If the Euclidean measure derived from the test sample surpasses a certain threshold in comparison to the training set, the user is categorized as an imposter.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133105

Dataset

In keystroke dynamics analysis, each typing session captures a range of attributes associated with users' typing behavior. These attributes encompass metrics like hold time, flight time, and up-down duration for specific key transitions. For example, "Hold time" denotes the duration a key remains pressed during typing, while "Flight time" signifies the interval between releasing one key and pressing the next key. Additionally, "Up-down duration" measures the time between releasing a key and pressing it again. These metrics play a pivotal role in understanding the unique typing patterns and behaviors of individuals. Through the analysis of these attributes, valuable insights can be gleaned into the distinctiveness of each user's typing behavior, potentially serving as a biometric identifier for authentication and identification purposes. The dataset furnishes a comprehensive overview of these metrics across multiple typing sessions, enabling thorough examination of keystroke dynamics and its diverse applications, spanning realms such as cybersecurity and human-computer interaction.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	subject	sessionInd	rep	H.period	DD.period	UD.period	H.t	DD.t.i	UD.t.i	H.i	DD.i.e	UD.i.e	H.e	DD.e.five	UD.e.five	H.five	DD.five.Sh	UD.five.Sh	H.Shift.r	DD.Shift.r.	UD.Shift.r.	H.o	DD.o.a
2	s002	1	1	0.1491	0.3979	0.2488	0.1069	0.1674	0.0605	0.1169	0.2212	0.1043	0.1417	1.1885	1.0468	0.1146	1.6055	1.4909	0.1067	0.759	0.6523	0.1016	0.2136
3	s002	1	2	0.1111	0.3451	0.234	0.0694	0.1283	0.0589	0.0908	0.1357	0.0449	0.0829	1.197	1.1141	0.0689	0.7822	0.7133	0.157	0.7877	0.6307	0.1066	0.1684
4	s002	1	3	0.1328	0.2072	0.0744	0.0731	0.1291	0.056	0.0821	0.1542	0.0721	0.0808	1.0408	0.96	0.0892	0.6203	0.5311	0.1454	0.7195	0.5741	0.1365	0.2931
5	s002	1	4	0.1291	0.2515	0.1224	0.1059	0.2495	0.1436	0.104	0.2038	0.0998	0.09	1.0556	0.9656	0.0913	1.2564	1.1651	0.1454	0.755	0.6096	0.0956	0.153
6	s002	1	5	0.1249	0.2317	0.1068	0.0895	0.1676	0.0781	0.0903	0.1589	0.0686	0.0805	0.8629	0.7824	0.0742	0.8955	0.8213	0.1243	0.7632	0.6389	0.043	0.1975
7	s002	1	6	0.1394	0.2343	0.0949	0.0813	0.1299	0.0486	0.0744	0.1412	0.0668	0.0863	0.9373	0.851	0.0942	1.0896	0.9954	0.1681	0.3716	0.2035	0.1154	0.1287

Fig 2. Dataset

As suggested, the optimal approach to represent a typing rhythm for an individual is through a time series. Essentially, a time series is a vector comprising time measurements of specific actions. In the context of keystroke dynamics, these actions can be delineated into key presses, as well as the constituent elements of key presses, and the transition times between these elements.

System Architecture

An architectural explanation serves as a structured depiction and formal delineation of a system, designed to facilitate understanding of the system's structure. It encompasses various aspects including the system components, the discernible properties of these components, their interactions, and offers a blueprint from which products can be sourced and systems can be developed. This plan ensures that the components work cohesively to realize the system's overarching objectives.

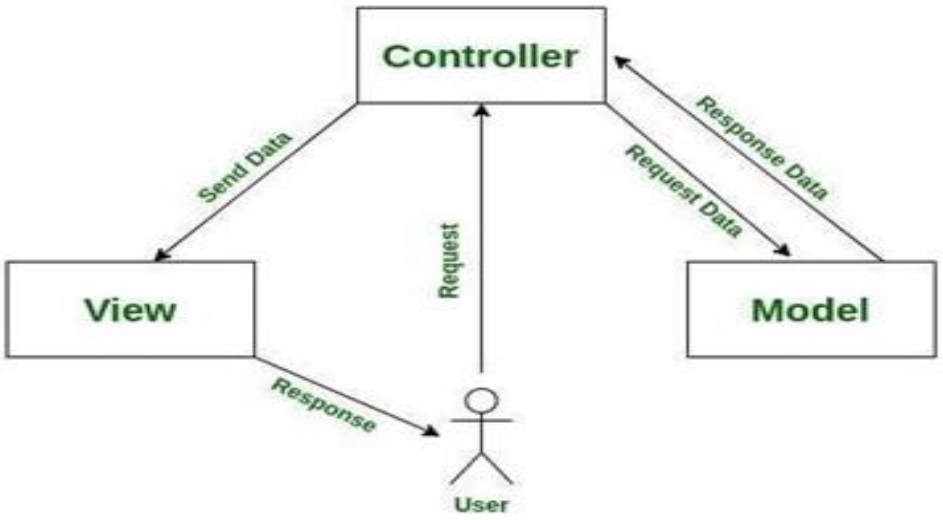

Fig 3. System Architecture

The Model component encompasses all data-related logic utilized by the user. It handles data transfer between the View and Controller components, as well as any other business logic-associated data. The View component manages the user interface (UI) logic of the application. Controllers serve as intermediaries between the Model and View components, managing business logic and incoming requests. They manipulate data using the Model component and interact with Views to generate the final output.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133105

IV. RESULTS

The objective of the tests was to illustrate that training and retraining neural network models are no longer excessively resource-intensive in terms of computational power and time. By demonstrating the efficient execution of training neural network models, particularly emphasizing the crucial aspect of time, the goal is to promote the widespread acceptance and integration of such models into standard software development procedures. It is observed that the accuracy peaks at over 80% with the training data.

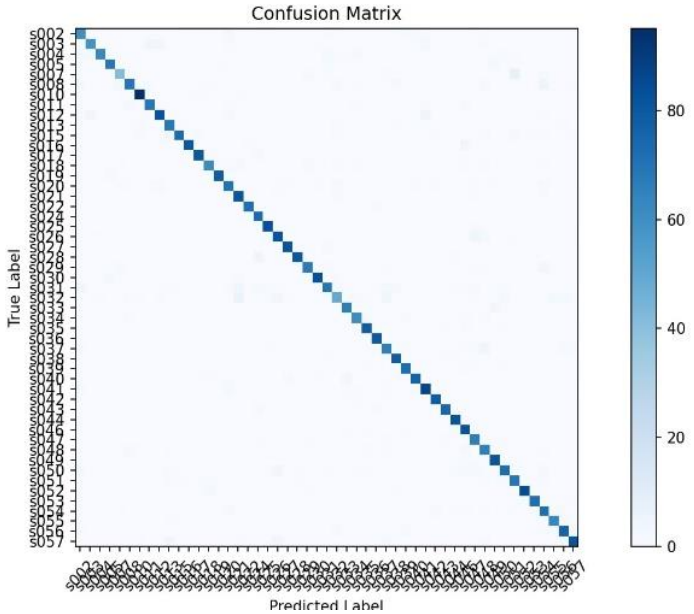

Fig 4.1. Results

Implementing the earlier proposed strategy, which involves utilizing clusters, each equipped with its own model, would facilitate the periodic retraining of clusters needing updates to uphold accuracy. This method proves cost-effective as the probability of errors during the designated retraining period is minimal, and the retraining of models does not demand downtime for the e-commerce system.

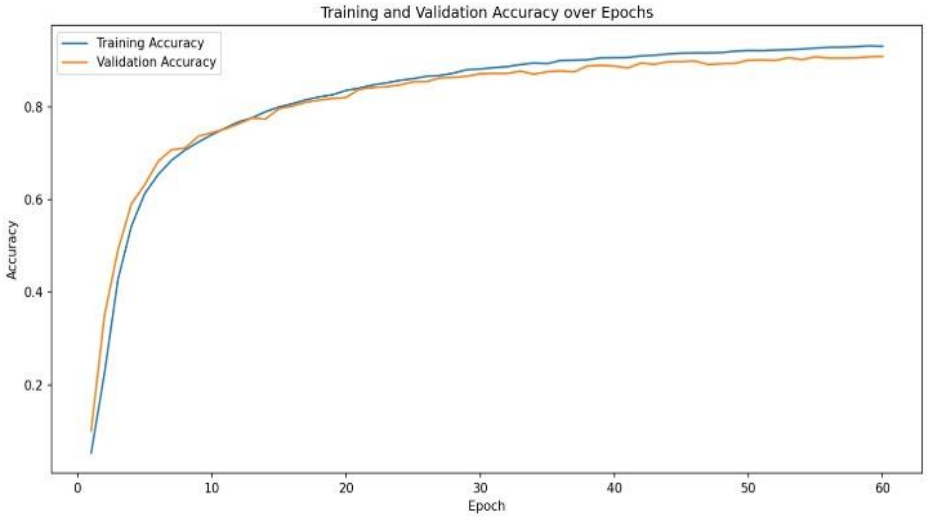

Fig 4.2. Results

DOI: 10.17148/IJARCCE.2024.133105

V. CONCLUSION

In summary, this paper has conducted a comprehensive investigation into keystroke dynamics classifiers utilizing long short-term memory (LSTM) layers. Through the utilization of advanced machine learning techniques, notably LSTM, the study has underscored the efficacy of keystroke dynamics analysis as a feasible authentication system. Throughout the paper, we have emphasized the potential advantages of integrating keystroke dynamics analysis into various applications. Rather than replacing conventional password systems, keystroke dynamics can function as an additional authentication mechanism, augmenting security measures without imposing substantial user burdens. Additionally, the paper has addressed pertinent considerations concerning the implementation and deployment of keystroke dynamics classifiers. By delving into topics such as determining the optimal number of test samples per person for a secure and sustainable system, practical insights have been provided for the real-world deployment of keystroke dynamics analysis.

REFERENCES

[1] Bartneck, C., Kulic, D., Croft, E., & Zoghbi, S. (2009). Measurement instruments for the anthropomorphism, animacy, likeability, perceived intelligence, and perceived safety of robots. International Journal of Social Robotics, 1(1), 71-81.

[2] Bellovin, S. M. (2008). Security implications of typical email address syntax. Proceedings of the 17th conference on Security symposium, 15-28.

[3] Birhanu, T. M., & Kang, D. K. (2020). Keystroke dynamics-based continuous authentication for wearable IoT devices. Sensors, 20(11), 3084.

[4] Feng, J., Zhang, X., & Su, J. (2019). Research on keystroke dynamics based on deep learning. Journal of Physics: Conference Series, 1221(1), 012044.

[5] Giot, R., El-Abed, M., & Rosenberger, C. (2017). An efficient and robust biometric system for real-time authentication based on keystroke dynamics. IEEE Transactions on Information Forensics and Security, 12(4), 844-859.

[6] Giot, R., El-Abed, M., & Rosenberger, C. (2018). A hybrid approach for keystroke dynamics-based authentication using multiple sources of constraints. Computers & Security, 77, 383-397.

[7] Nguyen, T. H., Nguyen, T. H., & Kim, D. S. (2021). Continuous authentication using keystroke dynamics based on a deep neural network. Sensors, 21(2), 478.

[8] Nitzan, D., & Tavabi, N. (2019). Continuous user authentication using keystroke dynamics and mouse dynamics. Future Generation Computer Systems, 90, 155-167.

[9] Revett, K., & Dale, J. M. (1994). A continuous authentication scheme for cryptographic systems based on keyboard dynamics. Computers & Security, 13(3), 255-267.

[10] Yao, Y., Liu, Y., Wang, Z., Zhang, J., & Wang, G. (2019). User authentication on smartphones using keystroke dynamics and swipe gestures. Future Generation Computer Systems, 95, 471-478