Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 9 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i09.53793

PAPER

Security in Mobile Human-Device Interaction: Leveraging Mobile Keypad Input Patterns for Secure User Recognition and Fraud Detection

Boumedyen Shannaq(✉)

Department of Information Systems, College of Business, University of Buraimi, AL Buraimi, Oman

boumedyen@uob.edu.om

ABSTRACT

This study proposes a novel approach to enhancing mobile security by identifying key parameters of virtual keypad input for user authentication. In particular, the intention is to develop a behavior-based recognition system that uses user behavior during keypad interactions to minimize fraudulent activities. It is necessary to establish an automatic authentication mechanism to identify predictive functional correspondence based on user frailty and distinguish them from intruders. The contingency study design compared several authentication algorithms using a dataset from a company, including 792 users and 4,096 employees who left between 2016 and 2020. The metrics are an average precision of 1.0 and a recall of 1.0, as all models can detect fraud effectively. As for the CR-EPSB algorithm, the precision value was only 0.110, but the proposed TKIP-based algorithms indicated better precision values ranging from 0.516 to 0.723 and F1 scores ranging from 0.681 to 0.839, which contributed to the improvement of the authenticity rate. The outcomes of this work reveal the effectiveness of the proposed keypad-based authentication technique in improving mobile security systems and the security of the various financial transactions for businesses and individuals, as well as the security of their enterprises and personal devices. The study establishes the need to integrate behavioral biometrics as an extra security measure for portable products since other forms of identification might not be sufficient.

KEYWORDS

mobile authentication, mobile interaction security, virtual mobile keypad input patterns, user behavior recognition, fraud detection

1 INTRODUCTION

As most modern people use various applications on their smartphones for communication and personal data processing, the safety of mobile human-device dialogues is of high importance [1], [2], [3], and [4]. Nevertheless, conventional security

Shannaq, B. (2025). Security in Mobile Human-Device Interaction: Leveraging Mobile Keypad Input Patterns for Secure User Recognition and Fraud Detection. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(9), pp. 42–57. https://doi.org/10.3991/ijim.v19i09.53793

Article submitted 2024-12-12. Revision uploaded 2025-02-18. Final acceptance 2025-02-25.

remains intact in terms of password identification and cannot hence ensure user confidence. Presently, cybercriminals use other ways of fraudulence in attacking mobile security, where they use methodologies such as phishing, drive-by downloads, and botnet attacks to install malicious software that compromises personal identifications such as passwords [5], [6], and [7]. The botnet involves compromised devices under a single command center to launch attacks; on the other hand, phishing ambushes the users by sending a link or an email to enter sensitive information on a counterfeit site [8]. Unless the intruder manages to obtain the password, the traditional security measures revolve around this aspect of security [9]. These people can inject scripts into websites, record what is typed, and get the stored passwords from the browsers [10]. These tactics afford the attackers the ability to compromise an account by altering the passwords and thereby be able to stay logged in for an extended duration [11]. The following research proposes a novel behavior-based authentication model that considers how a smartphone's keypad usage changes across different modes. The proposed identification method goes beyond entering credentials, unlike typical identification; therefore, detecting unauthorized access is much easier. This approach helps to neutralize such a threat since even if an attacker acquires the correct login credentials, they cannot use the accounts extensively due to the monitoring process. Taking into consideration the input features identified by users, the described system enhances the credibility of real-time identity confirmation while minimizing various attacks familiar in the world of mobile security.

1.1 Statement of problem

Passwords are often easily cracked or stolen using advanced methods. If an unauthorized user gains access, they can modify the password, posing a serious security risk. Most systems cannot distinguish between legitimate users and intruders, even when the correct password is entered [12]. However, if an organization decides to go the extra measure of incorporating MFA, this risk may be reverted by intruders, and they will change a password. For example, when a user tries to change the password on a particular account, the system fails to determine whether the user is authentic or an intruder. This is the primary issue that arises, and the only work in the literature that has been elaborated to contribute was the Electronic Personal Synthesis Behavior (EPSB) algorithm [13], [14]. While introducing novelties, the system has weaknesses, including time-consuming processes and a low 60% success rate. It struggles with managing password length changes. This study enhances authentication by improving accuracy, reducing selection time, and addressing security gaps to mitigate unauthorized access and cyber threats through advanced algorithms for detecting forged users.

1.2 Proposed solution

To close this gap, we propose a central general algorithm: Transforming Virtual Keypad Input Patterns for Recognizing User Behavior (TKIP-RUB) [15], which is later extended to three more new versions as described in Table 1 and the mobile input patterns depicted in Figure 1. [16] has used the virtual keypad letter substitution encoding to improve text classification accuracy.

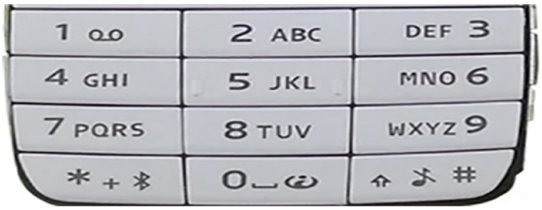

Fig. 1. Mobile input patterns

Table 1 explains the working of the proposed algorithm named as TKIP-RUB.

Table 1. Developed algorithms

Algorithm	Acronym	Example "OMAN@#2040"
Transforming Keypad Input Patterns for Recognizing User Behavior	**TKIP-RUB**	"6666266" Only letters are replaced with number substitution **(*Symbols and numbers are ignored*)**
Transforming Keypad Input Considering Symbols Patterns for Recognizing User Behavior	**TKIP-RUB-SYM**	"6666266 ***SS***" All letters are kept, and all symbols are replaced with "*S*" **(*numbers are ignored*)**
Transforming Keypad Input Considering Numbers Patterns for Recognizing User Behavior	**TKIP-RUB-NUM**	"6666266***NNNN***" All letters are kept, and all Numbers are replaced with "***N***" **(*Symbols are ignored*)**
Transforming Keypad Input considering Numbers & Symbols Patterns for Recognizing User Behavior	**TKIP-RUB-NUM-SYM**	"6666266***SSNNNN***" All letters are kept, all symbols are replaced with "*S*," and all Numbers are replaced with "***N***"

Transforming keypad input patterns for recognizing user behavior along with the expanded sub-level algorithm describes the process of converting key input patterns found in most mobile phone designs into simpler forms of user recognition. From here, it naturally evolves into a project aimed at converting virtual keypad inputs (letters, numbers, symbols) to precise patterns, which can then be used for identification of legitimate users or detection of fraudulent behavior. The following explains how each variant of the algorithm operates: With the TKIP-RUB method, numbers, similar to a mobile phone keypad, replace letters. For example, "OMAN@#2040" was converted into "6666266" because symbols and numbers are ignored. TKIP-RUB-SYM: This version is much the same as the previous one, but it includes symbols as well. Each of the letters is substituted with a corresponding number while 'S' is assigned to the symbols, and numbers are put out of mind. The string "OMAN@#2040" converted into "6666266 SS," for instance. The major distinctive feature of the TKIP-RUB-NUM variant can be marked as the letters' numerical encoding with subsequent replacement of "N" for any number. Every symbol was disregarded. The specific coding was given where "OMAN@#2040" regrouped as 6666266NNNN, for instance. The TKIP-RUB-NUM-SYM version was made with all of the specified transformations with the letters replaced by numbers and symbols replaced by S, and numbers replaced by N and OMAN@#2040 represented as 6666266SSNNNN.

1.3 Significant and novelty

This work is important and unique because it directly fills a major gap in mobile security, namely, that of user authentication, based on the analysis of keypad dynamics. Compared to generic approaches utilizing passwords and PINs, which are prone to various risks including phishing and brute force attacks, this paper advances a new method based on the analysis of user behavior during the selection of passwords. This kind of behavioral analysis also enhances system security a notch higher by denying intruders who already know the proper password a chance to access the system easily. This method of improving security technology elevates the notion of behavior recognition when implemented in mobile authentication systems as superior to conventional fraud detection strategies. Additionally, it enhances the user-friendliness of a website by eliminating certain false alarms to enhance web security for the users and organizations and therefore develops a better, more secure Internet setting for users and organizations.

2 LITERATURE REVIEW

Cybersecurity awareness among vocational students remains limited, highlighting the need for curriculum enhancements and training programs to strengthen their ability to handle cybersecurity threats in professional environments [17]. The rise of the digital economy increases cybersecurity risks, especially in accounting and finance. Mobile learning programs enhance cybersecurity awareness, offering accessibility, engagement, and cost-effectiveness, supporting curriculum integration and future research on long-term impacts [18]. In the past few years, the use of mobile devices to access various information has grown to a factor that requires efficient methods of authenticating an individual [19]. Conventional passwords are very much exposed to phishing, guessing attacks, shoulder surfing, and other forms due to poor password selection and habitual use among users [20], [21]. Recent work carried out in the field stresses identifying user password behavior to improve the reliable and secure authentication models and control the invasion of unauthorized users [22]. In the past, a study was conducted on password behavior to improve security and observed mobile typist behavior as biometric lecturers [23], [24], [25], and [26]. For instance, [14], [27] developed an authentication-based access control algorithm that focuses on passwords entered by the user, typing mistakes, and the time input was done. This was mainly because it depended on user acceptance surveys and a small number of patients, which limited its utility. A similar study assesses student readiness for mobile learning cybersecurity using a survey of 150 engineering students, highlighting the need for enhanced cybersecurity education and training programs [28]. This study examines cyber hygiene among business students, identifying strengths and weaknesses to improve cybersecurity education through targeted curricula and training, ensuring safer digital practices in professional settings [29]. The CR algorithm for developing an EPSB is proposed for user authentication also [13]. Compared to the CR approach, it is effective in tracking password activities, but it fails to balance the difference in password length and have a high computational penalty that excludes it from being in real-time [30], [31], and [15]. There are signs of higher-level tendencies that mobile keypad navigation can be used as identification of users similar to the biometric one [32]. There are ideas and concepts that user identification can be prolonged after the first synchronized password using keystroke dynamics, which was discussed in [33]. However, many previous works involve confined scenarios or possess a small sample set, or the population is studied under the condition that it has prior training in the use of the analyzed tool.

2.1 Electronic personal synthesis behavior algorithm

The possible extension of EPSB algorithm increases password typing duration and choice of an adequate method for user authentication based on the historical behavior data with the help of the Confidence Range (CR) function [12], [13]. But the parameters connected with the password input duration indicator—only six of them—restrain the EPSB algorithm. For better understanding of these six parameters, in this work we proposed the development of an application to simulate the function and working of the EPSB algorithm. The six parameters are explained in Table 2.

Table 2. Six parameters integrated with the EPSB algorithm

Parameter1	Parameter2	Parameter3	Parameter4	Parameter5	Parameter6
Small letters	Capital letters	Sum of Small letters + Capital letters	Numerals	Symbols	Length of the password

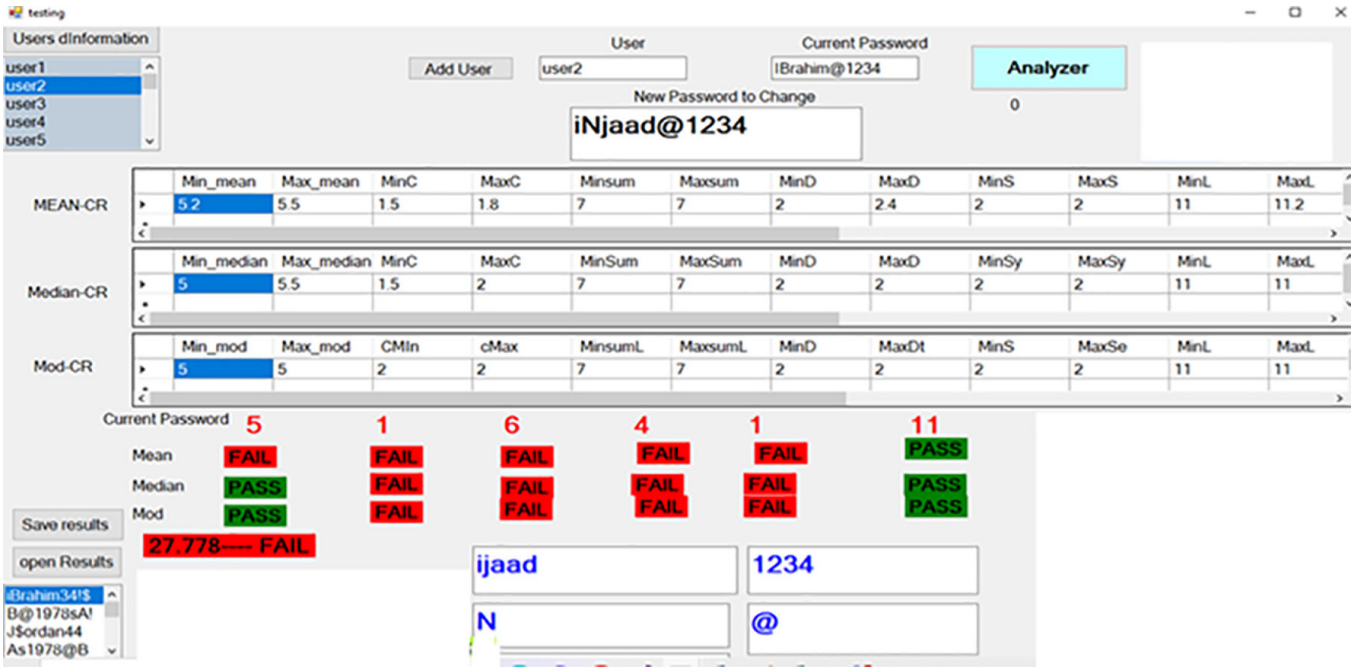

Fig. 2. Screenshot of the developed application implementing the EPSB algorithm

Source: Author's own.

The developed application calculates the most recent password for User 2, who changed her or his password five times in 15 months. It is shown in Figure 2 that the application updates the CR database, which contains data on the minimum and maximum for the mean median and mode of six variables outlined in Table 1. Example: User 2 currently has the password as 'Ibrahim@1234.' The above CR carries calculations for small letters, capital letters, numerals, symbols, and total length. A fake user (F, User) tries to change the password to another one, namely 'iNjaad@1234,' after successfully typing the correct password.

Step 1: For "iNjaad@1234" the simplified CR Calculation is as follows; The targeted value of the CR is as provided below:

- 5 small letters: "ijaad"
- 1 capital letter: "N"

- 6 combined letters: “ijaad + N”
- numerals: “1234”
- 1 symbol: “@”
- 11 total characters: “iNjaad@1234”

Step 2: Comparison with Original User (O-User) CR:

For instance, in the first parameter (small letters), the mean O-User’s CR is 5.2–5.5; the F-User’s CR is 5. As 5 lies out of the range of 5.2–5.5, none of the success points are awarded.

In Figure 2, five successful comparisons are depicted, which yields a then similarity score of 5/18*100 = 27.7%. According to the checklist below, the F-User fails to update the password because the passing score for the test is 66%. In light of the poor detection of unauthorized users by the base EPSB algorithm, explaining its low performance. Consequently, when testing the newly applied algorithm that included more user data in the application during the testing phase, the efficiency of discriminating the EPSB algorithm between unauthorized users was quite low.

Therefore, this study presents TKIP-RUB to address the weakness and low accuracy of the EPSB algorithm. In our technological age, the simplicity of passwords and passphrases continues to be a cause for concern [34]. Research has indicated that a considerable proportion of people use easily guessed passwords, which puts them at risk of being the target of cyberattacks [35]. Secondly, multiple accounts use the same password, making all of the other accounts vulnerable to compromise if one is cracked [36].

3 METHODOLOGY

A comparative experimental research design helps evaluate authentication algorithms using actual data obtained from an IT department of a company. The assessment method analyzes authentication protocol effectiveness by establishing systematic performance evaluation across multiple evaluation criteria.

3.1 Study design and experimental setup

The experimental investigation included analysis between an experimental and control grouping during its performance. The control group used conventional authentication systems, whereas our research methodology served as the experimental group by integrating numeric pattern recognition and behavioral analysis. The research aimed to evaluate authentication precision, recall, accuracy, and F1 score performance when manipulating various system parameters.

The research originated from a cybersecurity problem affecting employees at a company with 792 personnel. Research revealed one Ph.D. work employing the EPSB algorithm, but this study demonstrated insufficient real-world authentication validation. User authentication data was obtained from the IT department of the company following procedures to protect privacy and preserve anonymity.

3.2 Data collection process and selection criteria

The company’s IT logs served as the primary source of information for collecting authentication data related to employee behavior. The method for collecting data consisted of these distinct steps.

Recognized records about handling system logins spanned from 2016 to 2022 and included 2094 records that belonged to 465 workers who moved to different positions during the two years from 2020 to 2022.

Anonymity protection occurred when the IT department used randomly generated user identifiers instead of real user names.

Inclusion Criteria:

- Employees with at least three recorded password updates.
- Users who maintain stable authentication logs through various successive login sessions.

Exclusion Criteria:

- Incomplete authentication records.

Users who did not update their passwords more than three times belong to this category. The research data included three essential components, which were hidden usernames, passwords, and timestamps for password modifications. Verbal analysis was possible through entries in the password logs where users made between 3 and 8 updates for each account. Table 3 presents a sample of the distribution of password changes for all users.

3.3 Dataset splitting and validation

The analysis used these divisions for training data and testing purposes:

- The algorithm training and user profile generation used 1629 records in the training dataset.
- The testing subset consisted of 465 records for algorithm performance assessment.

Several steps were applied to guarantee the validity of the dataset including:

The dataset received verification for completeness by detecting both missing values and inconsistent information.

Verification of anonymization criteria:

- The process successfully replaced actual usernames through a system that generated random user IDs.
- Data quality maintained through the exclusion of the latest user password from model training while securing actual performance assessment during evaluation.

3.4 Comparative analysis of algorithms

A smart application for evaluation purposes integrated multiple algorithmic components to assess authentication effectiveness.

- A system generated individual user profiles by analyzing the behavioral authentication log patterns.
- Multiple authentication algorithms run in the system through the EPSB algorithm and TKIP-RUB.

- Analyzing password evolution required the substitution of letters with numbers using numbers to represent letters for letter-based studies while omitting symbols and numbers.
- Testing of different solutions against each other occurred using precision, recall, and F1 score metrics to pick the best solution.

The developed TKIP-RUB approach proved its versatility by solving weaknesses in password count regulations processing time demands and authentication session reliability. Behavioral-based authentication emerges as a critical method for fighting against cybersecurity threats according to research findings.

Table 3. Distribution of password changes

Number of Password Updates	Number of Employees	Total Records
3	181	543
4	93	372
5	76	380
6	67	402
7	32	224
8	16	128
Total	465	2049

The proposed TKIP-RUB algorithm in this work and its extended sub-algorithms are shown in Figure 3.

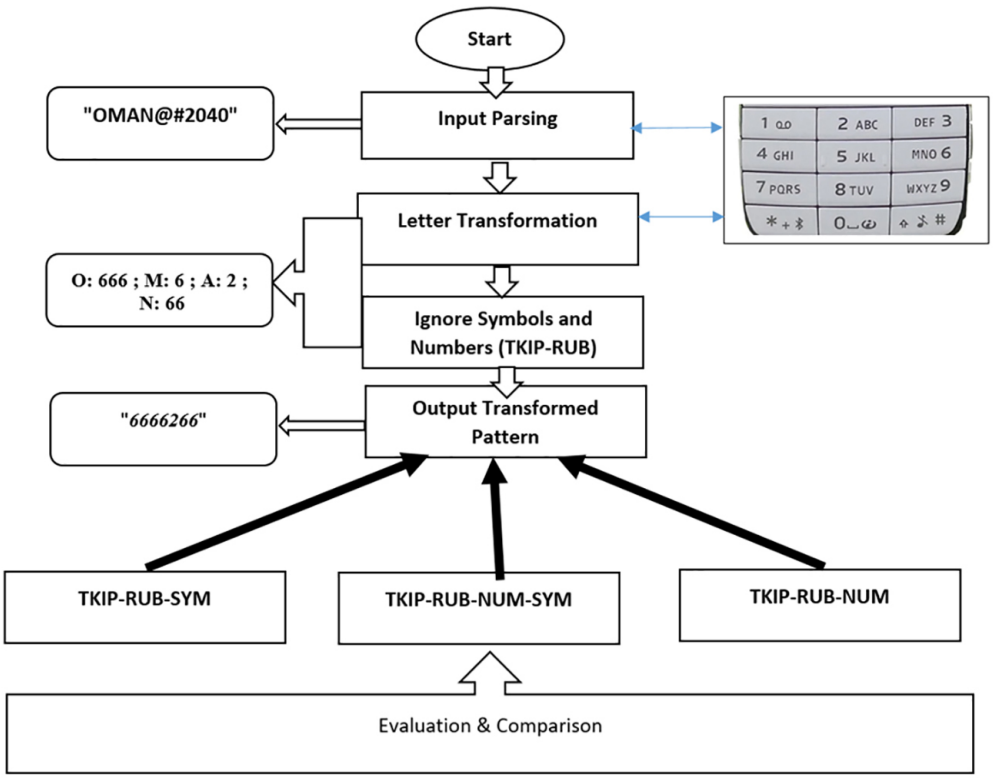

Fig. 3. The proposed algorithm

4 EXPERIMENT AND EVALUATION MEASURES

To conduct the proposed experiments in this work, we first developed a C# code to implement the algorithms. The smart application created profiles for 465 users from the training dataset and then ran experiments to evaluate the performance of each algorithm using the testing dataset. Figure 4 displays a screenshot of the profile of user 151, who has updated their password four times. In the box labeled "Training (DS)," the smart system generates the user profile using four algorithms: TKIP-RUB (highlighted in red), TKIP-RUB-SYM, TKIP-RUB-NUM, and TKIP-RUB-NUM-SYM. The label for each algorithm is placed next to the corresponding generated profile. The first three passwords of user 151 were stored in the training dataset, while the fourth password was stored in the testing dataset. The smart application also ran the EPSB algorithm and calculated the profile of user 151, as shown in Figure 5. For the testing process, each user and their corresponding test password were uploaded to the system. The system then generates a profile based on the relevant algorithm. Figure 6 illustrates the complete scenario of how the proposed algorithms are implemented and tested. As seen in Figure 6, when the command labeled "keyB-Alg" is clicked, the TKIP-RUB algorithm is executed, generating a profile for the tested password. In this case, user 151 entered "Radiologist@U5," and the system generated a profile based on the proposed algorithm. The system then compares the two profiles: one generated from the training dataset and the other from the testing dataset.

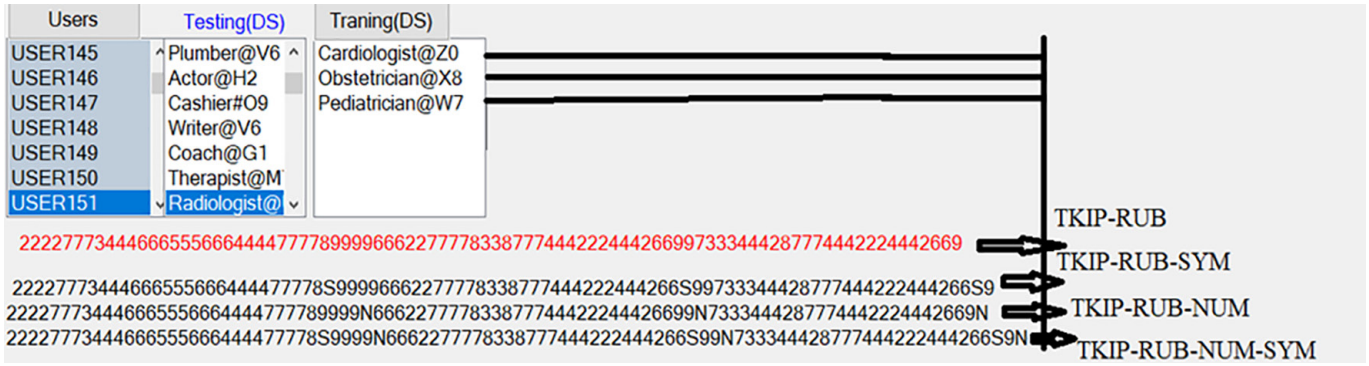

Fig. 4. Generated profile from training dataset for user 151 using all four algorithms

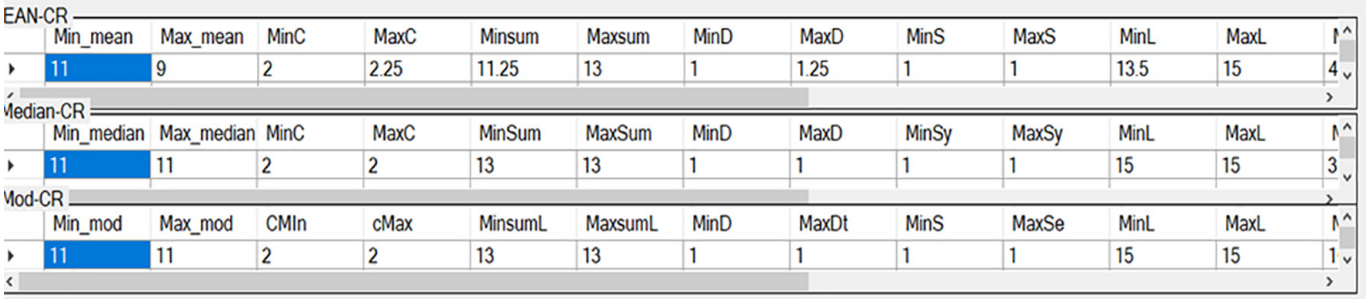

Fig. 5. Generated profile from training dataset for user 151 using EPSB algorithm

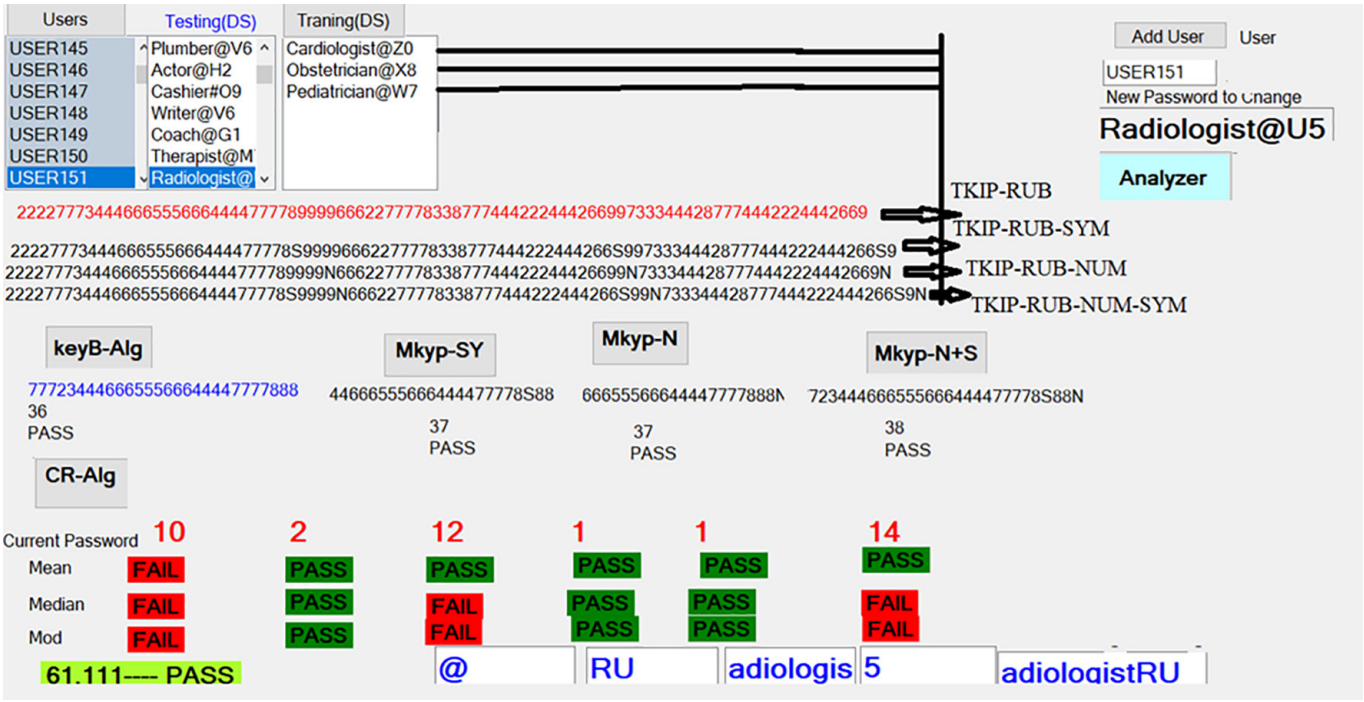

Fig. 6. Comparing the training profile of user 151 to the testing profile "Radiologist@U5"

4.1 Evaluation

The precision-recall and F1 scores used to measure the performance of all algorithms. The obtained results shown in Table 4.

Table 4. Results

Algorithm	Precision	Recall	F1-Score
CR-EPSB	0.11	1	0.198
TKIP-RUB	0.516	1	0.681
TKIP-RUB-NUM	0.723	1	0.839
TKIP-RUB-SYM	0.587	1	0.74
TKIP-RUB-NUM-SYM	0.716	1	0.834

Table 4 presents the compression overall algorithms, and the ranking as follows:

- TKIP-RUB-NUM achieves the highest F1-Score (0.839), indicating its balance between precision and recall.
- TKIP-RUB-NUM-SYM also performs very well with an F1-Score of 0.834.
- CR-EPSB has the lowest F1-Score, showing that while it has high recall, its precision is quite low, leading to less effective performance overall.

This study's outcomes show the effectiveness of using keypad input patterns as a new methodology to recognize and learn about user behaviors and for automated mobile authentication and fraud detection. The recall rate has remained at 1.0 for all algorithms, primarily validating the model's ability to detect only authorized users without any false negatives. This characteristic is highly important in the security of mobile human-device interaction in which the possibility of unauthorized access is threatening.

4.2 Computational complexity and performance overhead

The performance analysis of different algorithms is examined in Table 4 which presents precision, recall, and F1-score results.

Both **CR-EPSB** display the worst precision at the level of 0.11 and F1-score at 0.198 together with perfect recall. Computational simplicity alone does not justify this method because its high number of false positives creates difficulties for applications that require quick response times.

TKIP-RUB enhances accuracy measurements by reaching a 0.681 F1-score but maintains perfect recall through its 0.516 precision rate.

The combination of TKIP-RUB-NUM delivers the best outcomes regarding precision values (0.723) as well as the F1 score measure (0.839) at the cost of higher computational demands for prediction accuracy.

The accuracy performance of TKIP-RUB-SYM and TKIP-RUB-NUM-SYM depends on moderate to high computational requirements. Systems require algorithm choice to fulfill their operational requirements.

5 DISCUSSION

Mobile computing, therefore, makes user authentication one of the most important and sensitive areas of security. The paper also analyzes four types of authentication and discusses their benefits and drawbacks as well as possible usage.

Biometric protection methods are also used, such as face recognition, fingerprint scanning, and voice recognition, and all these strategies are introduced in modern mobile devices for the authentication of unprotected systems. Each method is convenient and has high reliability but exposes its limitations in terms of spoofing the measuring device or environmental conditions. The integration of multiple modalities improves the accuracy and reliability of the approaches because it solves the problem of the lack of effectiveness of separate methods [37], [38], and [39].

The comparison of the results achieved by the given methods, presented in Table 5, provides useful information about the efficiency of the traditional method of password-based authentication, CR Algorithm (EPSB-Based), KDT, and the developed TKIP-RUB approach. Using the password level of security is still common up to the present time because of its easy use by the users. The use of various application programs allows users to control and generate passwords without the need to acquire special hardware and software.

Table 5. Comparative analysis of authentication methods

Algorithm	Strengths	Weaknesses
Password-Based Authentication	Simple and widely used	Vulnerable to phishing and brute-force attacks
CR Algorithm (EPSB-Based)	Tracks typing behavior	Struggles with password variations and high-processing demand
Keystroke Dynamics	Biometric-based, continuous authentication	Requires large datasets and extensive calibration
Proposed TKIP-RUB Approach	Generates unique user profiles, adaptable security	Addresses CR limitations and enhances security monitoring

Nonetheless, some significant weaknesses associated with this method include phishing, brute force, and weak password choice. Unfortunately, these vulnerabilities are often attacked using credential stealing, dictionary attacks, and social engineering techniques, thus making passwords the single factor of authentication unsuitable for use in any highly secured environment. Behavioral tracking along with limitations of the CR algorithm (EPSB-based). The increases in the CR algorithm with the help of EPSB type take the behavior of a particular user into consideration to get improved results in the authentication. This method helps to identify specific keystroke dynamics, patterns, and errors of the users to create a profile. Nevertheless, despite its effectiveness in behavioral tracking, the CR algorithm has its drawbacks: the variance of password length is a problem for the algorithm, in addition to having high computational demand for the immediate recognition of the user. Moreover, the use of regular typing patterns restricts the possibility of application for those users who may modify their typing patterns quite often. Keystroke dynamics authentication is actually an application of biometric signatures that use typing speed, force, and tempo to identify the user from the pseudo one. This means that the current method described in this paper has more security than the regular use of passwords. However, the accuracy greatly depends on the large training dataset, and it undergoes calibration and machine learning models. In addition, the difference in typing behavior due to various reasons such as tiredness, mood, type of keyboard used, or any other related factor might be another limitation. The TKIP-RUB approach deals with the above stated issues encountered in previous studies and designs novel user profiles and modes for security monitoring. It is also different from traditional passwords in that it is not based fully on non-changing authentication. TKIP-RUB is superior to the CR algorithm in terms of adaptation to the user's typing behavior since the user can freely type more variants while using a secured RUB. In addition, it provides real-time security monitoring capability, making it more secure against new forms of security threats. This approach strikes a balance between flexibility and security, enhancing authentication frameworks for mobile security applications. It highlights the need to choose between simplified, secure, or flexible authentication methods. Traditional password systems remain widely used, but their limitations necessitate improved solutions. While the CR algorithm and keystroke dynamics provide behavior-based security, they face challenges like computational complexity and calibration. The proposed TKIP-RUB approach integrates adaptability, security monitoring, and user profiling, making it a promising solution for mobile authentication. Further research should focus on refining TKIP-RUB, incorporating machine learning, and testing it across various devices and platforms. This paper introduces TKIP-RUB alongside the CR approach to develop dynamic user profiles and continuously evaluate password activity. Unlike other models, TKIP-RUB leverages learning capabilities to update passwords, enhancing fraud detection with minimal user inconvenience. This improved security framework makes TKIP-RUB a robust solution for real-world mobile authentication.

6 CONCLUSION

This work is essential and novel since it tackles the problem of identifying user authentication as a significant challenge in mobile security based on analyzing the patterns of keypad inputs. Conventional authentication methods, including passwords and PINs, secure information but are increasingly vulnerable to various risks, such as phishing and brute force attacks. As a result, this research uses a unique approach to identifying human behavior throughout password selection to improve security.

One interesting and often unexplored aspect can be the learning of users' behavior when choosing passwords via their devices. These signatures add another layer of protection so that even if an intruder knows the correct password, he cannot easily penetrate the system. This method seems innovative in dealing with the problem of user authentication since it considers users' behaviors during the actual authentication. In addition, behavior recognition, as part of mobile authentication systems, is considered an improvement in security technology compared to traditional fraud detection. Besides, this approach improves the usability of search engines, removing many frequently found false positives while fortifying web security measures, making the internet environment more secure for users and organizations.

7 ACKNOWLEDGMENTS

The authors express their sincere gratitude to the University of Buraimi, Oman, for their invaluable support throughout the entire process of this research. Their funding and continuous encouragement have been instrumental in the successful completion of this study.

8 REFERENCES

[1] D. Ifenthaler and J. Y.-K. Yau, "Higher education stakeholders' views on learning analytics policy recommendations for supporting study success," *International Journal of Learning Analytics and Artificial Intelligence for Education (iJAI)*, vol. 1, no. 1, pp. 28–42, 2019. https://doi.org/10.3991/ijai.v1i1.10978

[2] M. Shakir, M. J. Al Farsi, I. R. Al-Shamsi, B. Shannaq, and T.-H. Ghilan Al-Madhagy, "The influence of mobile information systems implementation on enhancing human resource performance skills: An applied study in a small organization," *Int. J. Interact. Mob. Technol.*, vol. 18, no. 13, pp. 37–68, 2024. https://doi.org/10.3991/ijim.v18i13.47027

[3] B. Shannaq, "Unveiling the nexus: Exploring TAM components influencing professors' satisfaction with smartphone integration in lectures: A case study from Oman," *TEM Journal*, vol. 13, no. 3, pp. 2365–2375, 2024. https://doi.org/10.18421/TEM133-63

[4] A. Al-Marri *et al.*, "Determinants of using the mobile payment to buy coffee among female college students in Saudi Arabia," *Int. J. Adv. Appl. Sci.*, vol. 8, no. 6, pp. 88–93, 2021. https://doi.org/10.21833/ijaas.2021.06.010

[5] N. A. Mims, "The botnet problem," in *Computer and Information Security Handbook* (Fourth Edition), J. R. Vacca, Ed., Elsevier, 2024, pp. 261–272. https://doi.org/10.1016/B978-0-443-13223-0.00014-X

[6] M. A. Mohd Ariffin, M. Y. Darus, H. Haron, A. Kurniawan, Y. Muliono, and C. R. Pardomuan, "Deployment of Honeypot and SIEM tools for cyber security education model in UITM," *Int. J. Emerg. Technol. Learn.*, vol. 17, no. 20, pp. 149–172, 2022. https://doi.org/10.3991/ijet.v17i20.32901

[7] B. Khamzina, N. Roza, G. Zhussupbekova, K. Shaizhanova, A. Aten, and B. Aigerim Meirkhanovna, "Determination of cyber security issues and awareness training for university students," *Int. J. Emerg. Technol. Learn.*, vol. 17, no. 18, pp. 177–190, 2022. https://doi.org/10.3991/ijet.v17i18.32193

[8] R. K. Ayeni, A. A. Adebiyi, J. O. Okesola, and E. Igbekele, "Phishing attacks and detection techniques: A systematic review," in *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*, Omu-Aran, Nigeria, 2024, pp. 1–17. https://doi.org/10.1109/SEB4SDG60871.2024.10630203

[9] N. Ravichandran, T. Tewaraja, V. Rajasegaran, S. S. Kumar, S. K. L. Gunasekar, and S. R. Sindiramutty, "Comprehensive review analysis and countermeasures for cybersecurity threats: DDoS, ransomware, and Trojan horse attacks," *Preprints*, 2024. https://doi.org/10.20944/preprints202409.1369.v1

[10] M. Maceiras *et al.*, "Know their customers: An empirical study of online account enumeration attacks," *ACM Trans. Web*, vol. 18, no. 3, pp. 1–36, 2024. https://doi.org/10.1145/3664201

[11] A. Cherry, "A secure password manager governance framework for web user authentication," Research Thesis, University of York, 2024. Accessed: Oct. 19, 2024. [Online]. Available: https://etheses.whiterose.ac.uk/35281/

[12] B. Shannaq and M. Shakir, "Enhancing security through multi-factor user behavior identification: Moving beyond the use of the longest common subsequence (LCS)," *Informatica*, vol. 48, no. 16, pp. 73–82, 2024. https://doi.org/10.31449/inf.v48i19.6270

[13] M. Shakir, A. Abubakar, Y. Yusoff, M. Al-Emran, and M. Hammood, "Application of confidence range algorithm in recognizing user behavior through EPSB in cloud computing," *Journal of Theoretical and Applied Information Technology*, vol. 94, pp. 416–427, 2016.

[14] M. Shakir, M. Hammood, and A. Kh. Muttar, "Literature review of security issues in saas for public cloud computing: A meta-analysis," *International Journal of Engineering and Technology*, vol. 7, no. 3, pp. 1161–1171, 2018. https://doi.org/10.14419/ijet.v7i3.13075

[15] B. Shannaq, "Novel algorithm for differentiating authorized users from fraudsters by analyzing mobile keypad input patterns during password updates," *TEM Journal*, vol. 14, no. 1, pp. 768–778, 2025. https://doi.org/10.18421/TEM141-68

[16] B. Shannaq, "Development of a new encoding algorithm using virtual keypad letter substitutions for improved text classification," *Journal of Theoretical and Applied Information Technology*, vol. 103, no. 2, pp. 714–724, 2025.

[17] R. Fadli, H. D. Surjono, R. C. Sari, Y. Hidayah, and F. Eliza, "Assessing cybersecurity awareness among vocational students in office administration," *International Journal of Safety and Security Engineering*, vol. 14, no. 4, pp. 1115–1123, 2024. https://doi.org/10.18280/ijsse.140410

[18] F. Eliza *et al.*, "Assessing student readiness for mobile learning from a cybersecurity perspective," *Online J. Commun. Media Technol.*, vol. 14, no. 4, p. e202452, 2024. https://doi.org/10.30935/ojcmt/15017

[19] M. L. Shuwandy *et al.*, "Sensor-based authentication in smartphone: A systematic review," *Journal of Engineering Research*, p. S2307187724000300, 2024. https://doi.org/10.1016/j.jer.2024.02.003

[20] V. Tsoukas, A. Gkogkidis, and A. Kakarountas, "A survey on mobile user perceptions of sensitive data and authentication methods," in *24th Pan-Hellenic Conference on Informatics*, Athens, Greece, 2020, pp. 346–349. https://doi.org/10.1145/3437120.3437337

[21] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023. https://doi.org/10.3390/electronics12061333

[22] M. Yıldırım and I. Mackie, "Encouraging users to improve password security and memorability," *Int. J. Inf. Secur.*, vol. 18, no. 6, pp. 741–759, 2019. https://doi.org/10.1007/s10207-019-00429-y

[23] A. Shaji George, "The dawn of passkeys: Evaluating a passwordless future," *Partners Universal Innovative Research Publication (PUIRP)*, vol. 2, no. 1, pp. 202–220, 2024. https://doi.org/10.5281/ZENODO.10697886

[24] M. A. Khan, I. U. Din, and A. Almogren, "Securing access to internet of medical things using a graphical-password-based user authentication scheme," *Sustainability*, vol. 15, no. 6, p. 5207, 2023. https://doi.org/10.3390/su15065207

[25] A. Mahfouz, A. Hamdy, M. A. Eldin, and T. M. Mahmoud, "B2auth: A contextual fine-grained behavioral biometric authentication framework for real-world deployment," *Pervasive and Mobile Computing*, vol. 99, p. 101888, 2024. https://doi.org/10.1016/j.pmcj.2024.101888

[26] J. Swisher, "How weak passwords expose you to serious security risks," *Jetpack*, 2024. Accessed: May 06, 2024. [Online]. Available: https://jetpack.com/blog/weak-passwords/

[27] M. T. Shakir, "User authentication in public cloud computing through adoption of electronic personal synthesis behavior," PhD Thesis, 2020. https://doi.org/10.13140/RG.2.2.35475.71202

[28] F. Eliza *et al.*, "Enhancing cybersecurity awareness through mobile learning: A study on vocational accounting and finance students," *International Journal of Advanced Technology and Engineering Exploration (IJATEE)*, vol. 11, no. 121, pp. 1714–1731, 2024. https://doi.org/10.19101/IJATEE.2024.111101097

[29] F. Eliza *et al.*, "Building a secure digital future: Investigating cyber hygiene levels of accounting, finance, and business students," *Data and Metadata*, vol. 3, no. 544, pp. 1–13, 2024. https://doi.org/10.56294/dm2024.554

[30] M. Al-Hashimi, R. Tawafak, M. Alnaseri, M. Shakir, and M. Sheker, "Users acceptance of electronic personal synthesis behavior (EPSB): An exploratory study," in *Recent Advances in Technology Acceptance Models and Theories.* in Studies in Systems, Decision and Control, vol. 335, M. Al-Emran and K. Shaalan, Eds., Springer, Cham, 2021, pp. 509–520. https://doi.org/10.1007/978-3-030-64987-6_30

[31] B. Shannaq, "Improving security in intelligent systems: How effective are machine learning models with TF- IDF vectorization for password-based user classification," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 22, pp. 8340–8355, 2024.

[32] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Computer Networks*, vol. 170, p. 107118, 2020. https://doi.org/10.1016/j.comnet.2020.107118

[33] R. Shadman, A. A. Wahab, M. Manno, M. Lukaszewski, D. Hou, and F. Hussain, "Keystroke dynamics: Concepts, techniques, and applications," *arXiv preprint arXiv:2303.04605*, 2023. https://doi.org/10.48550/ARXIV.2303.04605

[34] B. Shannaq, M. A. Talab, M. Shakir, M. T. Sheker, and A. M. Farhan, "Machine learning model for managing the insider attacks in big data," in *The Second International Conference on Emerging Technology Trends in Internet of Things and Computing*, Ramadi, Iraq, 2023, p. 020013. https://doi.org/10.1063/5.0188358

[35] Z. M. Saadi, A. T. Sadiq, O. Z. Akif, and A. K. Farhan, "A survey: Security vulnerabilities and protective strategies for graphical passwords," *Electronics*, vol. 13, no. 15, p. 3042, 2024. https://doi.org/10.3390/electronics13153042

[36] S. Chakraborty, C. Jackson, M. Frazier, and K. Clark, "A study on password protection and encryption in the era of cyber attacks," in *SoutheastCon 2024*, Atlanta, GA, USA, 2024, pp. 460–465. https://doi.org/10.1109/SoutheastCon52093.2024.10500214

[37] A. Sarkar and B. K. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," *Multimed. Tools Appl.*, vol. 79, nos. 37–38, pp. 27721–27776, 2020. https://doi.org/10.1007/s11042-020-09197-7

[38] E. Al. Jegede, "Cancelable and hybrid biometric cryptosystems: Current directions and open research issues," *Int. J. Adv. Appl. Sci.*, vol. 4, no. 11, pp. 65–77, 2017. https://doi.org/10.21833/ijaas.2017.011.010

[39] A. M. Alodaynan and A. A. Alanazi, "A survey of cybersecurity vulnerabilities in healthcare systems," *Int. J. Adv. Appl. Sci.*, vol. 8, no. 12, pp. 48–55, 2021. https://doi.org/10.21833/ijaas.2021.12.007

9 AUTHOR

Dr. Boumedyen Shannaq is an Associate Professor in Smart Information Systems specializing in AI, Machine Learning, and Data Analytics. With over 13 years as a Program Chair, he advances research in Information Systems, Knowledge Management, and HCI. His work integrates AI-driven solutions to enhance education and workplace productivity. Scopus ID: 57214330239, 0000-0001-5867-3986. Research Project(HCI): https://taerproject.com/