Enhancing Security with Multi-Factor User Behavior Identification Via Longest Common Subsequence Analysis

Boumedyen Shannaq, Mohanaad Shakir*
Management Information System, College of Business (CoB), University of Buraimi (UoB), Buraimi, Oman
E-mail: boumedyen@uob.edu.om, mohanaad.t@uob.edu.om, mohanaadshakir@gmail.com
*Corresponding author

Keywords: machine learning, longest common subsequence (LCS), authentication, confidence range algorithm (CR), electronic personal synthesis behavior (EPSB), smart Information security application**.**

Received: June 2, 2024

The proposed approach comprises a set of strategies and tools to protect user-sensitive data, such as passwords, from unauthorized access, misuse, or loss. It aims to identify unauthorized users, often attackers who have obtained passwords, attempting to change authorized user passwords. By employing the Longest Common Subsequence (LCS) algorithm, the proposed method compares the current user password (AUP) with the unauthorized user's intended password update (UUP). The methodology involved a smart security application analyzing a dataset from user authentication attempts. It included 68 users who updated their passwords, totaling 617 records (467 in the training dataset and 141 in the test dataset. Focusing on password modification patterns and comparing user actions during these changes. To compare and evaluate the accuracy of the algorithms, we utilized the precision measure (P) to gauge their effectiveness. This comparison reveals shared patterns between the two passwords, aiding in detecting unauthorized access attempts. For example, recurring patterns in password updates could serve as biometric security factors, allowing for the identification of user actions when updating sensitive data like passwords. This study enhances the CR approach associated with Electronic Personal Synthesis Behavior (EPSB) by introducing the Utilized Longest Common Subsequence (LCS) to address challenges such as the unavailability of user password history and password length. Our experiments indicate that the CR fails to identify the authorized user in 75 attempts and succeeds only 52% of cases when unauthorized users attempt to change the password. In contrast, our proposed method fails only 28.66% and succeeds with 102% of the time out of 141 data tests. The results from the test collection reveal the weaknesses of Alg1-CR in distinguishing authorized users from false ones, achieving a precision of only 53.191%. In contrast, Alg2-LCS achieved a precision of 72.34%. Thus, the proposed algorithm is more effective to implement and could improve security levels significantly.

Povzetek: Študija je razvila nov pristop, ki uporablja algoritem najdaljše skupne zaporedne podvrste (LCS) za izboljšanje varnosti pri identifikaciji uporabniškega vedenja pri spremembi gesla. Metoda izboljšuje točnost prepoznave nepooblaščenih uporabnikov, dosega boljše rezultate od prejšnjih metod ter izboljšuje varnostne protokole.

1 Introduction

Nowadays, information systems hold utmost significance owing to their substantial influence on the uninterrupted operation, advancement, and expansion of firms[1]. The pervasive and broad use of information systems has given rise to corresponding requirements, such as the significance of implementing secure methodologies, procedures, and processes to safeguard the security and confidentiality of information[2]. Consequently, many researchers have focused on developing and innovating new and innovative security methods to maintain information security[3]. With the revolution of artificial intelligence and the immense capabilities it offers, the adoption of intelligent systems that apply artificial intelligence principles has become an exemplary choice for providing high-efficiency capabilities and methods in information security[4]. These solutions include advanced features such intelligent authentication mechanisms that combine passwords with specific user behavior. What are the methods of authentication that exhibit high degrees of intelligence? Information security measures consist of a range of tools and tactics designed to establish secure and efficient methods for users of information systems to obtain the required data or information. These solutions depend on understanding user behavior and assessing it to ascertain the suitable amount of access for each individual[5]. The main objective of these solutions is to mitigate the hazards linked to illegal information retrieval and avert security breaches[6] . The fundamental methods of intelligent authorization encompass:
a) Two-Factor Authentication: Users must provide two forms of identification to get access to the system[4],[7].
b) Multifactor Authentication: These methods enable users to provide supplementary credentials, in addition to a password, in order to get access to the system[8],
c) User activity Analysis: The research aimed at counting

the typical patterns of the individual user behaviors, e.g., typing on keyboards and setting color preferences[9] The intelligent authorization, which combines the user behavior analysis and password authentication, stands a remarkable difference in both security and the convenience of accessing information, due to this dual upgrade[10].

Nevertheless, in an alternative situation, several experts have carried out thorough investigations on various approaches for predicting time series data[11]. Temporal data approaches encompass the analysis of time series data to derive various statistical measures and other characteristics [12]. Time series prediction entails utilizing models to analyze past data and make predictions about future values[13]. Regression analysis is a useful method for detecting connections between different time series. Nevertheless, it is seldom regarded as a form of "time series" research inside a certain framework [14]. Discrete-time series analysis can be employed to detect changes in the pattern of a time series. This analysis considers any possible activities that may affect the underlying variable[15]. This also suggests the capacity to predict future likelihood for any variable based on historical data. Mohanaad's proposed EPSB algorithm aims to improve user authentication by studying previous data in certain situations[16],[17]. EPSB employs a duration index that is calculated by analyzing the user's past data to improve the differentiation between legitimate and illegal users[16], [17]. The EPSB algorithm-imposed authorization layer records information on the length of the user's password input, the method employed to select it (either graphical or random), and any common failures. This data is stored to safeguard against password theft [16], [17], [18]. The Electronic Personal Synthesis Behavior (EPSB) improves the accuracy of confirming an authorized user by taking into account three attributes - EPSBERROR, EPSBTime, and EPSBStyle. The EPSB algorithm, includes a duration index derived by analyzing a user's historical data. The primary goal of developing the EPSB algorithm is to enhance the differentiation between authorized users and unauthorized ones. This enhancement is accomplished by gathering and classifying data on authorized user behavior, including their password, across several parameters such as password entry time, password selection technique, and common errors committed. The EPSB approach is utilized to enhance the authentication layer's resilience against password theft by examining the user's historical password-related behavior [14]. The EPSB approach utilizes the Confidence Range (CR) function to evaluate user historical data. This function integrates the equations for median, mean, and mode to establish significant benchmarks for distinguishing authorized users from unauthorized ones [14], [15].

User behavior analysis is becoming increasingly vital in Data loss prevention (DLP) systems. The recent technologies survey underscored the importance of identifying critical insiders. User behavior analytics (UBA) is experiencing rapid growth, and it is integrated with a dedicated module to meet this demand. This UBA module focuses on detecting anomalous behavior, which enhances threat identification processes. Additionally, formalized behavior patterns have simplified threat detection, with over two dozen patterns already identified. As a result, the process of identifying the genie user from the fake user are expanding beyond mere information security to address broader corporate security concerns. In our investigation in the literature we could found last work in this path ,In [17] [19]have been proposed security application system which include many calculations and procedures to identify the genie user from the fake user. Based on ‘Confidence Range ‘(CR). The CR is calculated by considering the MIN and MAX for the MEAN, MEDIAN and MODE Factors respectively. The selected password of the genie user is processed as follow

1-The password is extracted to generate 6 patterns: the capital letters, small letters, capital latter and small letters, numbers, symbols, and the length of the password.
2- Calculate the length of each pattern

3- For each pattern the MIN and MAX of MEAN, MEDIAN and MODE are calculated
4-Repeate step 1 each time when the genie user updated password.

4-Generate Confidence Range for each user
According to the consideration of each part of the password, the EPSB algorithm failed to consider the nature of the user who selects the sequences of letters, symbols, or numbers that constitute a password, then the style of use that the user applies to the arrangement of other components of a password. Additionally, when implementing the EPSB algorithm, the success rate of the tests was 52%, indicating a risk level of 48%. The proposed EPSB algorithm needs ample user records to learn and function effectively without risk. In Figure 1 from [20], each user could update their password with minimal changes per year, according to organizational policies. Approximately 70% of users change their password at least once a year, and 40% change it three times a year. The EPSB algorithm analyzes the components of a legitimate user's password by examining its basic elements (uppercase and lowercase letters, numbers, symbols, and word length). The research gap in this study is that the EPSB method neglects the analysis of the sequence of password components. As a result, in this study, the researchers will employ the LCS technique to investigate the sequence of password components and compare the algorithm's overall performance with and without LCS. We need to enhance the current EPSB algorithm by concentrating on minimizing the existing flaws in the proposed algorithm to attain enhanced performance. Using the results of the analysis and sorting of previous studies, researchers concluded that LCS is able to replace the present method and overcome the existing problems. Hence, this study enhances it by introducing the utilized Longest Common Subsequence (LCS) to address challenges like the unavailability of user password history and password length. As a result, the algorithm will be more effective at distinguishing between authorized and illegitimate users.

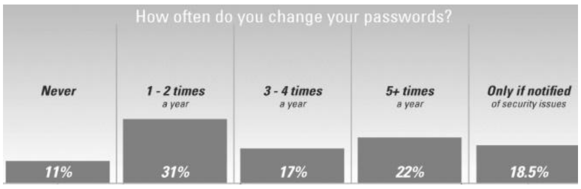


Figure 1. Frequency of password changes by users

2 Literature review

In this current part of the literature study, the labeling of 'intelligent authentication method' will be explained fully to the reader, so as to comprehend each component of the phrase. This does not require lengthy introduction and the subsequent discussion will be devoted to the analysis of the EPSB technique where every component will be described, the roots of the technique described, its benefits carefully outlined, and the weaknesses of the method defining the limited perspective of using this technique discussed. In the following part, this research will give a better understanding of the Longest Common Subsequence and give a brief description on how could it be used.

2.1 Intelligent authentication methods

Intelligent authentication techniques use state-of-the-art approaches like biometrics, machine learning, and artificial intelligence to increase the accuracy and resilience of authentication systems [21],[22]. Thanks to technological improvements, traditional authentication methods like passwords and personal identification numbers (PINs) are becoming more vulnerable to security breaches[23]. Very smart authentication made use of high-level skills such as biometrics machine learning and artificial intelligence to improve authentication systems accuracy and resilience[24], [25]. Researchers made their best to make biometric data processing algorithms and systems that are very precise and capable of giving high authentication rates of [18], [26], [27].Given the substantial advancements in artificial intelligence, intelligent systems that integrate AI and authentication techniques must be developed in order to improve authentication accuracy[28],[29]. Machine learning is one of the most widely used techniques in this field[30], [31]. However, the technology of machine learning that being used in artificial intelligence today has not been pushed to the limit[32]. The latter group of nonprofits sticks out by resorting to the latest technologies which utilize sophisticated algorithms to mine data and patterns and thus obtain results with a high degree of accuracy[33]. Researchers can now create many authentication models of increased complexity through advanced machine learning algorithms of a type such as decision trees, neural networks, and support vector machines[34]. These models work incredibly well when evaluating contextual cues, device attributes, and user behavior to determine authenticity[35]. The adaption ability of machine learning algorithms is great if it comes to defending against even sophisticated threats and therefore these algorithms are a great help fighting with authentication assaults. The basic purpose of behavior-based authentication (BBA) is to verify a user identity by considering his or her characteristics that can be manifested during typical behavior pattern. These patterns include but are not limited to, keyboard rhythm, mouse motions, touchscreen gestures, and navigational behavior. Intelligent authentication systems are able to verify user identities and identify a significant amount of anomalous activity by continuously observing and evaluating user behavior patterns. The researchers have investigated several machine learning and statistical techniques to determine the most effective ways to model user activities for the validation process, which would yield effective, discrete authentication solutions. This is consistent with those techniques. Although, intelligent authentication methods are the main point, several worries are left unanswered [36]. Universal adoption of the technology related to end-users will only be possible if barriers can be effectively resolved, e.g. privacy, data security, interoperability, and friendliness of use[37]. Establishing efficient algorithms along with their practical implementation in the systems intends to tackle adversarial attacks and impersonation attacks is considered the core issue of research[38]. Future research needs to be aimed on increasing the identification accuracy, the system efficacy and the user satisfaction by deeper exploring the advanced technologies in blockchain, for example, powerful computing, deep learning, and so on. [39], [40] Intelligent authentication technologies turns out to be tremendously be effective to protect the authentication of systems[41]. By the use of biometric, machine learning, continuous multi-factor authentication, and behavioral-based authentication, more advanced approaches taking place nowadays result in better accuracy and security in comparison with the old tactics[42], [43]. Intelligent methods and algorithms offer one of the most favored approaches in the sense of where they can revolutionize authentication systems per a banking environment, a medical health care setting, and an e-commerce platform[38],[39],[46]. Continuous multi-factor authentication is a continual and persistent process that uses many factors to consistently verify the identity of a user. Typically, these elements comprise two known pieces of information (such as a password and a verification code) along with a unique third factor related to the user (such as a fingerprint or facial recognition) [47].

Two modern techniques for continuous multi-factor authentication, OneSpan and Zighra, rely on spotting unusual usage patterns[26]. However, these systems only offer limited opportunities to track modifications in user habits that lead to behavioral record modifications [26]. People may have to edit their profiles regularly as a result, which could be inconvenient[48]. Utilizing application and physical activity monitoring for contextual information analysis is a helpful method to increase access control system (ACS) accuracy[49],[50]. By making it more difficult for hackers to change data acquired from contextual sources, these reduce the effectiveness of spoofing attempts[51]. Samsung HYPR[52], NuData Security, TwoSense.AI[53], Secured Touch (purchased by Ping Identity[54]), and Samsung HYPR[52] are examples of context-based ACS solutions. These systems enable continuous tracking of behavior-related features and contextual data, such as the user's location through banking apps. Even with the accuracy and anti-spoofing power of the authentication procedure, there may be better choices available for clients who are concerned about privacy violations, excessive battery usage, and account resource consumption[55].

Identification of users via the use of deep learning algorithms and analysis of human activities. Mobile sensor data plays a

crucial role in the field of user authentication, especially for devices that are shared among several users[56],[57]. The research was evaluated to demonstrate a wide range of methodologies, including physical biometric authentication and behavioral features obtained from human activity identification. Deep learning models, using Long Short-Term Memory classifiers on time-series data collected from

mobile sensors, have shown a maximum accuracy of 90% in recognizing people by analyzing their body motions and everyday activities [42]. Moreover, an extensive examination of non-intrusive active user authentication in biometrics elucidates the advantages and disadvantages of several techniques such as speech recognition, keystroke analysis, and mouse dynamics. Key management and authentication procedures play a crucial role in safeguarding smart grids from unauthorized access in smart metering systems[43]. The use of AI-powered User Behavior Analytics (UBA) in Zero Trust security frameworks and cloud settings demonstrates how ongoing monitoring and adaptive algorithms may improve Identity and Access Management (IAM) [58], [41]. Furthermore, the application of the Apriori optimization approach for assessing library user activity and large data, as well as artificial intelligence for detecting irregularities in user behavior, demonstrates the technology' flexibility in different sectors[59],[60],[61]. Finally, emerging techniques such as behavior-based sensor access control on smartphones and user behavior modelling for AR personalized recommendations emphasize the necessity of integrating user behavior into security and customization. These studies highlight the need of incorporating user activity data, especially password data, in order to develop more robust and comprehensive authentication systems[62], [63]. The table below summarizes some related studies on authorization that applies intelligent standards based on user behavior with the system's authorization layer. The table 1 shows that most systems neglected password analysis, with only a few studies addressing this topic. For more information regarding with intelligent methods you can see[17],[64], [65], [66].

Table 1: Summarizes related studies

Study Title	Strengths	Neglected Analysis
User identification using deep learning and human activity mobile sensor data [42]	High accuracy (up to 90%) in user identification using mobile sensor data; effective use of LSTM classifier.	Password component analysis
A broad review on non-intrusive active user authentication in biometrics[43]	Detailed analysis of various authentication methods (voice recognition, keystroke, mouse dynamics) and their pros/cons.	Password component analysis
A Survey on Key Management and Authentication Approaches in Smart Metering Systems[41]	Comprehensive overview of key management and authentication in smart grids; critique of proposed techniques.	Password component analysis
Leveraging Artificial Intelligence for Enhanced Identity and Access Management within Zero Trust Security Architectures: A Focus on User Behavior Analytics and Adaptive Authentication[67]	Effective use of AI for user behavior analytics and adaptive authentication within Zero Trust frameworks.	Password component analysis
AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems[58]	Comprehensive study on the integration of AI in IAM, focusing on user authentication, authorization, and access control.	Password component analysis
Analysis and research on library user behavior based on Apriori algorithm[59]	Application of Apriori optimization algorithm for analyzing library user behavior and improving book recommendations.	Password component analysis
User Behavior Analysis Based on Big Data and Artificial Intelligence[60]	Development of a big data analysis model for user behavior and abnormal behavior detection in libraries.	Password component analysis

Enhanced User Authentication Algorithm Based on Behavioral Analytics in Web-Based Cyberphysical Systems[61]	Proposes an anomaly detection algorithm for improving user authentication in web-based systems using machine learning.	Password component analysis
A Behavior-based Scheme to Block Privacy Leakage on Smartphone Sensors When You Exercise[62]	Novel behavior-based sensor access control scheme to prevent privacy leakage in smartphone fitness apps.	Password component analysis
User behavior modeling for AR personalized recommendations in spatial transitions[63]	Proposes a user behavior model for personalized AR content recommendations, addressing cold-start problems.	Password component analysis
Application of confidence range algorithm in recognizing user behavior through EPSB in cloud computing[16]	The Electronic Personal Synthesis Behavior (EPSB) improves the accuracy of confirming an authorized user by taking into account three attributes - EPSBERROR, EPSBTime, and EPSBStyle. (EPSB) (Electronic Personal Synthesis Behavior) algorithm includes a duration index derived by analyzing a user's historical data.	The EPSB algorithm analyzes the components of a legitimate user's password by examining its basic elements (uppercase and lowercase letters, numbers, symbols, and word length) and neglects the analysis of the sequence of password components

All of the studies that were examined did not take into account user behavior in relation to passwords throughout the authentication process. This is a significant omission, since passwords continue to be a major aspect of user authentication. In addition, important data on user password interactions, such as typing patterns, tendencies to repeat passwords, and common mistakes, is ignored, therefore failing to take advantage of a chance to enhance security processes. While user behavior analytics is relevant to the topic, its primary focus is on behaviors that are unrelated to passwords.

Incorporating password behavior within this environment might provide a more complete security architecture. By incorporating password behavior analysis, it is possible to enhance the security of IAM systems by detecting irregularities in password use patterns, hence improving their overall effectiveness. Subsequent investigations should focus on filling these deficiencies by integrating user password-related behavior into the authentication procedure. Conducting longitudinal research on the effects of technical improvements and demographic-specific reactions to AI-integrated Identity and Access Management (IAM) systems might provide more profound understanding.

To address these problems, Mahanaad proposes the EPSB algorithm [17] .This method logs the user's behavior with the password in order to facilitate authentication. This method doesn't require any material improvements; hence it saves money. It also doesn't require any training and is easy to use [8][48]The EPSB algorithm analyzes the components of a legitimate user's password by examining its basic elements (uppercase and lowercase letters, numbers, symbols, and word length). Therefore, the researchers in this study will enhance the EPSB technique by analyzing the structure of the algorithm and finding the best way to improve it. In the next section, the focus will be on the EPSB algorithm from all structural aspects, including definition and application method.

2.2 Electronic personal synthesis behavior (EPSB)

The EPSB method incorporates three crucial factors, namely EPSBStyle, EPSBTime, and EPSBError, to enhance the precision of distinguishing authorized users from unauthorized ones and mitigate the risk of password theft [8],[22],[48]. The key considerations are the user's password selection method, the speed of password typing, and permissible user errors. EPSBDecision reviews the findings and makes a determination on whether to grant or deny system access. This method depends on capturing the actions of authorized users in these variables and creating a range of certainty for the user linked to the password during the verification procedure while entering the system.

CR stands for the Confidence Range which means it is a series of data points created while strong password creation by something real like behavior and real actions that are close to inputting, deleting, and redoing passwords in real life. This is like the user's willingness to use a stronger password, password mistakes that they do and an average of typing speed of the user. EPSBStyle logs both successful and unsuccessful password attempts made by the authorized user. Consequently, when a user modifies their password, the algorithm stores the previous passwords as historical user data. The system evaluates user behaviors secondary to the introduction of the newest efficient password in order to identify and analyze the patterns of passwords they select. The method gathers information about the accuracy margins of the legitimate users' credentials values in the version called EPSBStyle that is characterized by few key elements. These signs comprise of the type of letters (capital and lowercase), the number and stick length of letters, digits content, and full number of special characters in the given password. Through diligently analyzing those facets, the algorithm builds up an implied cognition of user's likes in creating passwords

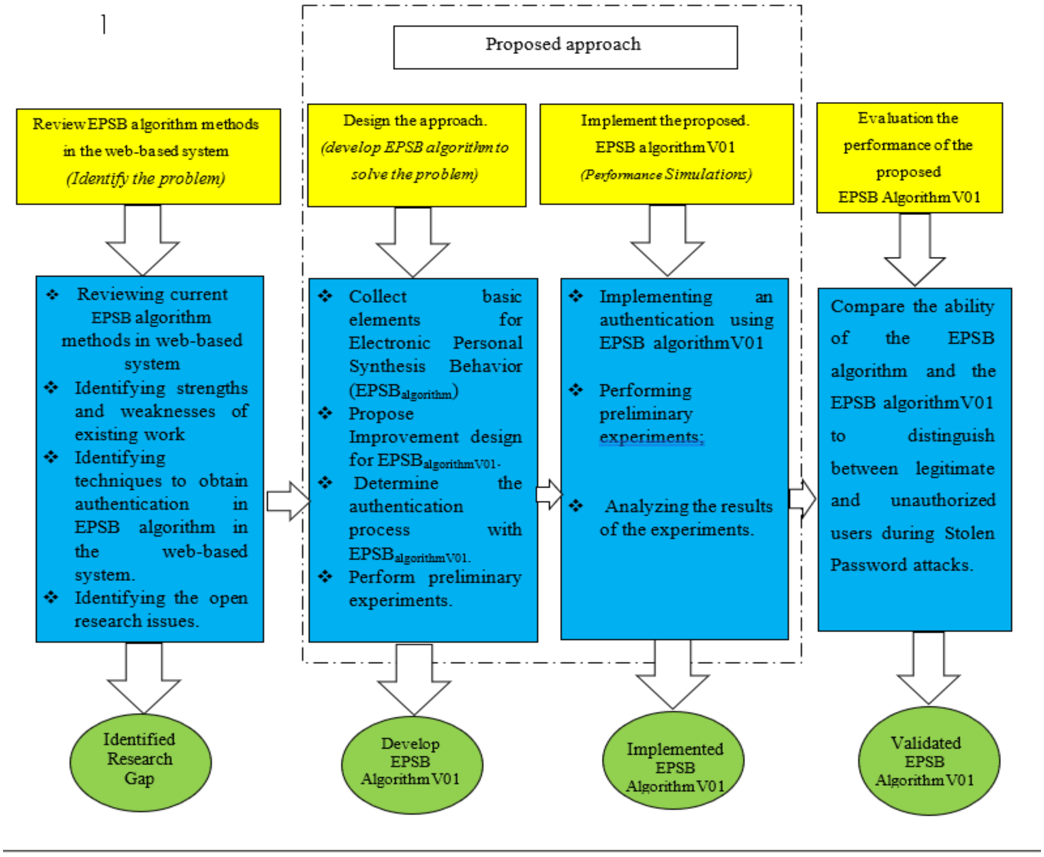

1
Proposed approach
Review EPSB algorithm methods in the web-based system (Identify the problem)
Design the approach. (develop EPSB algorithm to solve the problem)
Implement the proposed. EPSB algorithm V01 (Performance Simulations)
Evaluation the performance of the proposed EPSB Algorithm V01
❖ Reviewing current EPSB algorithm methods in web-based system
❖ Identifying strengths and weaknesses of existing work
❖ Identifying techniques to obtain authentication in EPSB algorithm in the web-based system.
❖ Identifying the open research issues.
❖ Collect basic elements for Electronic Personal Synthesis Behavior (EPSBalgorithm)
❖ Propose Improvement design for EPSBalgorithmV01.
❖ Determine the authentication process with EPSBalgorithmV01.
❖ Perform preliminary experiments.
❖ Implementing an authentication using EPSB algorithm V01
❖ Performing preliminary experiments;
❖ Analyzing the results of the experiments.
Compare the ability of the EPSB algorithm and the EPSB algorithm V01 to distinguish between legitimate and unauthorized users during Stolen Password attacks.
Identified Research Gap
Develop EPSB Algorithm V01
Implemented EPSB Algorithm V01
Validated EPSB Algorithm V01

Figure 2: Research methodology

and, therefore, it helps a lot in the assessment of user's password-related habits. In addition, EPSBTime collects and evaluates past data concerning the duration it takes for an authorized user to input a password into the system. It calculates a confidence interval for the authorized user, indicating the minimum and maximum amount of time they require to handle the password for accessing the system. EPSBError logs data pertaining to authorized users who input erroneous passwords. Occasionally, authorized users may unintentionally input a password without being aware of the selected language, whether they have chosen uppercase or lowercase letters, whether they have made a single or double-character error, or if they are using an outdated password. The process of analyzing and creating confidence intervals for incorrect passwords used by valid users in EPSBError relies on the following indicators: The process of analyzing and creating confidence intervals for incorrect passwords used by valid users in EPSBError. During authentication, the password analysis revealed: that firstly, the count of capital and lowercase letters utilized in the incorrect password. In addition, the length of the wrong password and the total characters used in the erroneous password. In a related context, the digit count in the wrong password and unique characters in the erroneous password. Finally, Whether the incorrect password is in the list of old passwords.

When analyzing historical data for legitimate users, the EPSBalgorithm generates a Confidence Range (CR) associated with the password based on the equation below [16].

Confidence Range (CR)=L + h $\frac{\mathrm{fm}-\mathrm{f1}}{(2\mathrm{fm}-\mathrm{f1}-\mathrm{f2})}, \sum_i \frac{xi}{n}, L + \frac{h1}{f}$((n/2)-C

The confidence level for each of the indicators mentioned above is determined by calculating six essential metrics: the minimum and maximum average, the minimum and maximum median, and the minimum and maximum mode. Therefore, the algorithm produces the subsequent points, the number of confidence range points for EPSBStyle turns out to be equal to 6*n indicators, with n values ranging from 6 to 36. This yields 18 bands with the lower limit as 18 minimum and the upper limit as maximum. The course EPSBError comprises of 7 indicators costing 6 confidence points each therefore resulting in a total of 42 confidence points. Consequently, 21 top and 21 bottom possess the highest and lowest confidence interval ranges. Under the numbers of indicators, confidence range for EPSBTime is calculated by merely multiplying them to six, thus, attaining six confidence points. Which implies the availability of lower and upper bounds of confidences in each and every case.

The EPSB algorithm, once an authorized user password is provided, the algorithm functions through 45 confidence range points for authorized users.

The processes for verification of these points are obtained together with the user ID with the password by using EPSB Decision-making method to decide if the user is allowed to gain access to the system. The EPSB algorithm has set a threshold of 60% success rate as the minimum acceptable match ratio for users in EPSB Decision. This ratio determines whether users are granted access to the system [49]. In addition, In EPSB Algorithm is high consuming of time, as we have seen from our experimental data while changing the password length. It's some weaknesses are, too.

To pass significantly, an algorithm has to be served ample training users records, so without risk it cannot operate effectively. In Figure 1 [20], each user could update their password with minimal changes per year, according to Organizational Policies. Figure it this way: on average 70 percent of users change their passwords once a year, whereas 40 percent of users do it three times a year. So, it is important to enhance this particular algorithm through addressing some main systems' weaknesses implied in the presented algorithm that would guarantee a better performance. Conducting a comparative study and a sorting of researches, researchers came to the conclusion that LCS may be a sole method of the previous one and the problems existing now could be overcome. Thus, the latter study is tried to upgrade by using the existing Longest Common Subsequence (LCS) method to overcome the limitations where the unknown password history and restricted password lengths are considered[69].

2.3 Longest common subsequence (LCS)

The Longest Common Subsequence (LCS) is the central concept in computing and bio-informatics used to find the longest sequence of characters or elements from two or

More sequence of characters or elements, which are the common ones. The LCS binds the elements as they are not continuous, and this very feature makes it an even more useful tool across many applications ranging from text comparison, DNA sequence analysis to data differencing. The LCS methodological approach to sequences identification allows one to get an understanding of similarities and dissimilarities, which is very helpful for tasks like plagiarism detection, aiding version control and genetic alignment.

3 Research methodology

At the start of the research, numerous articles on smart security technologies were reviewed to understand the topic, aiding in defining the research problem and formulating objectives and methods. The EPSB algorithm was developed by adopting a new approach in analyzing data related to legitimate users. In this research, the developed smart security application and then tested on a group of users to assess the algorithm's ability to surpass the limitations in the algorithm prior to the proposed development in this study. Finally, the performance of the algorithm before and after the developed model was compared to determine the extent of improvement in performance after adopting the latest development in the EPSB algorithm. This allows us to decide whether the research problem, for which the research was designed, has been addressed. Figure 2 illustrates the details of the research methodology[70],[71].

3.1 Data collection

In the experiment, a dataset was created from user authentication attempts. It included 68 users who updated their passwords, totaling 617 records (467 in the training dataset and 141 in the test dataset.

3.1.1 The structure of the test collection is as follows

1. Five records were produced, one test password being used by each of the five individuals.
2. A bigger sample of 54 individuals generated 108 entries, with each person using two test passwords.
3. Eight additional individuals each used three test passwords for a total of 24 records.
4. Ultimately, four test passwords were used by one person, yielding four records.
5. The dataset had 141 entries in total, gathered from different user-password interactions.

3.2 Preprocessing steps

The preprocessing steps involved:

1. Developing the database (with all related tables) as
described in Figure 2.

1. Writing the code to implement the Confidence Range (CR) algorithm and Electronic Personal Synthesis Behavior (EPSB) for the training dataset of 467 records (Figures 3, 4, and 5).

2. Writing the code to implement the LCS algorithm. Integrating steps 2 and 3.

3. Uploading the test data to the developed application, which consists of 141 records (Figure 7).

4. Entering the test collection.

5. Saving the results (Table 5)

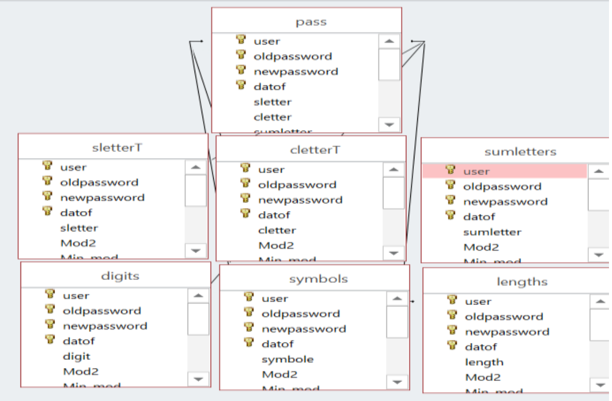
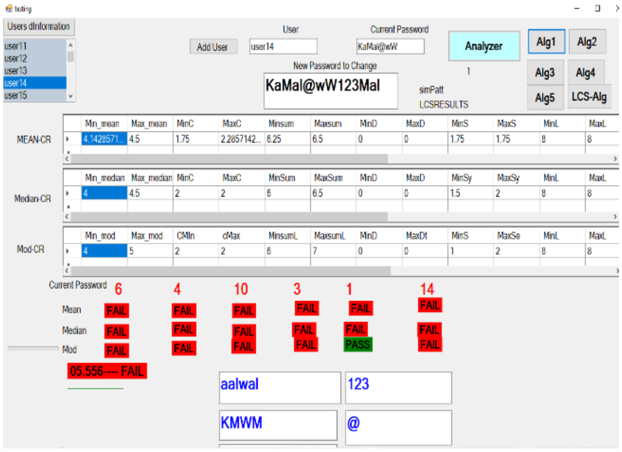


Figure 3: Main screen to update password



user14

KaMal@wW

KaMal@wW123Mal

	Min_mean	Max_mean	MinC	MaxC	Minsum	Maxsum	MinD	MaxD	MinS	MaxS	MinL	MaxL
MEAN-CR	4.1428571...	4.5	1.75	2.2857142...	6.25	6.5	0	0	1.75	1.75	8	8

	Min_median	Max_median	MinC	MaxC	MinSum	MaxSum	MinD	MaxD	MinSy	MaxSy	MinL	MaxL
Median-CR	4	4.5	2	2	6	6.5	0	0	1.5	2	8	8

	Min_mod	Max_mod	CMIn	cMax	MinsumL	MaxsumL	MinD	MaxDt	MinS	MaxSe	MinL	MaxL
Mod-CR	4	5	2	2	6	7	0	0	1	2	8	8

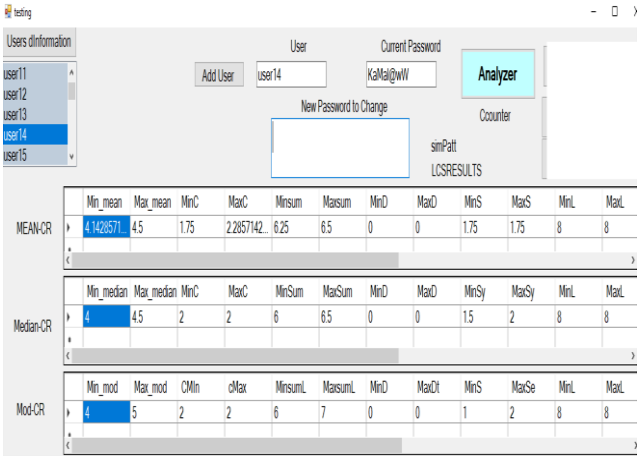
Current Password	6	4	10	3	1	14
Mean	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Median	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Mod	FAIL	FAIL	FAIL	FAIL	PASS	FAIL

05.556---- FAIL

aalwal 123

KMWM @

Figure 4: EPSB for user 14 updating password



user14

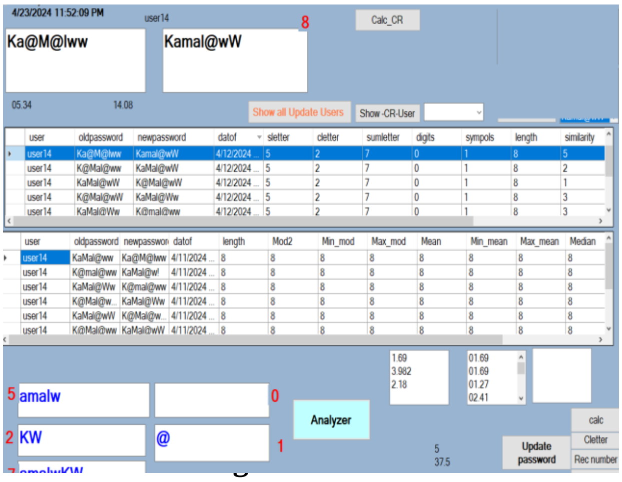
KaMal@wW

	Min_mean	Max_mean	MinC	MaxC	Minsum	Maxsum	MinD	MaxD	MinS	MaxS	MinL	MaxL
MEAN-CR	4.1428571...	4.5	1.75	2.2857142...	6.25	6.5	0	0	1.75	1.75	8	8

	Min_median	Max_median	MinC	MaxC	MinSum	MaxSum	MinD	MaxD	MinSy	MaxSy	MinL	MaxL
Median-CR	4	4.5	2	2	6	6.5	0	0	1.5	2	8	8

	Min_mod	Max_mod	CMIn	cMax	MinsumL	MaxsumL	MinD	MaxDt	MinS	MaxSe	MinL	MaxL
Mod-CR	4	5	2	2	6	7	0	0	1	2	8	8

Figure 5: EPSB calculated for user 14



4/23/2024 11:52:09 PM user14

Ka@M@lww Kamal@wW 8

05.34 14.08

user	oldpassword	newpassword	datof	sletter	cletter	sumletter	digits	sympols	length	similarity
user14	Ka@M@lww	Kamal@wW	4/12/2024 ...	5	2	7	0	1	8	5
user14	K@Mal@ww	KaMal@wW	4/12/2024 ...	5	2	7	0	1	8	2
user14	KaMal@wW	K@Mal@wW	4/12/2024 ...	5	2	7	0	1	8	1
user14	K@Mal@wW	KaMal@Ww	4/12/2024 ...	5	2	7	0	1	8	3
user14	KaMal@Ww	K@mal@ww	4/12/2024 ...	5	2	7	0	1	8	3

user	oldpassword	newpasswon	datof	length	Mod2	Min_mod	Max_mod	Mean	Min_mean	Max_mean	Median
user14	KaMal@ww	Ka@M@lww	4/11/2024 ...	8	8	8	8	8	8	8	8
user14	K@mal@ww	KaMal@w!	4/11/2024 ...	8	8	8	8	8	8	8	8
user14	KaMal@Ww	K@mal@ww	4/11/2024 ...	8	8	8	8	8	8	8	8
user14	K@Mal@w...	KaMal@Ww	4/11/2024 ...	8	8	8	8	8	8	8	8
user14	KaMal@wW	K@Mal@w...	4/11/2024 ...	8	8	8	8	8	8	8	8
user14	K@Mal@ww	KaMal@wW	4/11/2024 ...	8	8	8	8	8	8	8	8

1.69
3.982
2.18

01.69
01.69
01.27
02.41

5 amalw 0

2 KW @ 1

7 amalwKW

5
37.5

Figure 6: CR with LCS in ESPB

We assessed and contrasted the Confidence Range (CR) and Longest Common Subsequence (LCS) algorithms. The algorithm known as Longest Common Subsequence, or LCS: Without changing the character order, the LCS method finds the longest subsequence shared by the current and previous passwords. Because it catches the sequential patterns and similarities in user behavior while establishing and updating passwords, this algorithm is very successful in our environment. Based on these patterns, the LCS algorithm is able to reliably differentiate between users who are permitted and those who are not based on the password sequences they employ.

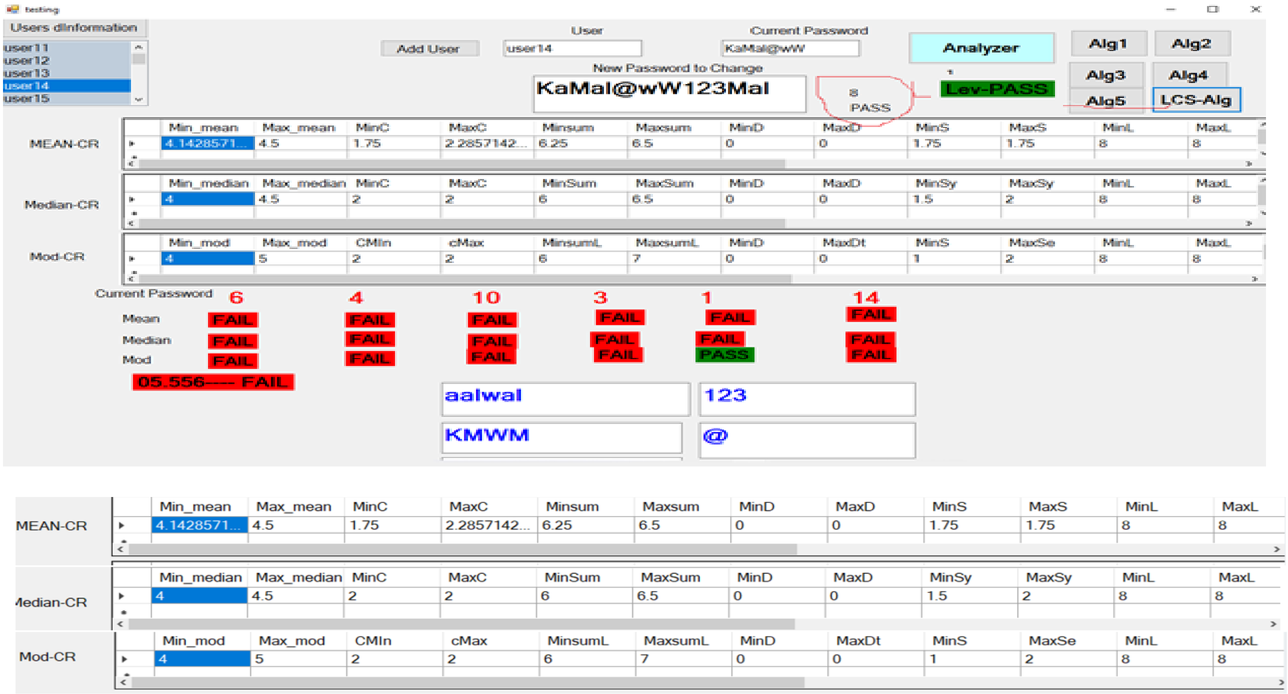
3.4 Confidence range (CR) method

In its earlier iteration, the CR method relied on statistical metrics such the password change median, mean, and mode. Even while it is thorough, it could overlook complex behaviors and patterns that the LCS algorithm can identify.

3.5 Why LCS is more effective

The LCS algorithm is more effective because it can:

1. Capture Sequential Patterns: LCS is more adept at detecting recurring behaviors in password updates because it is more focused on the order and sequence of characters than CR, which uses aggregate statistical measures.
2. Adapt to Variations: LCS can manage variations in password lengths and modifications more skillfully by taking into account the complete sequence of characters in the password.
3. Increase Precision: Our tests showed that LCS outperformed the CR algorithm, which had a precision of 53.191%, with a precision of 72.34%. This demonstrates how reliable LCS is at differentiating between users who are permitted and those who are not, with fewer false positives and negatives.
To sum up, the LCS algorithm is a more practical and effective method than the CR algorithm because of its emphasis on character sequences and flexibility in handling various password settings. This thorough methodological justification highlights the benefits of our suggested approach in improving security via multi-factor user behavior identification.



user11
user12
user13
user14
user15

User
user14

Current Password
KaMal@wW

New Password to Change
KaMal@wW123Mal

MEAN-CR	Min_mean	Max_mean	MinC	MaxC	Minsum	Maxsum	MinD	MaxD	MinS	MaxS	MinL	MaxL
	4.1428571...	4.5	1.75	2.2857142...	6.25	6.5	0	0	1.75	1.75	8	8

Median-CR	Min_median	Max_median	MinC	MaxC	MinSum	MaxSum	MinD	MaxD	MinSy	MaxSy	MinL	MaxL
	4	4.5	2	2	6	6.5	0	0	1.5	2	8	8

Mod-CR	Min_mod	Max_mod	CMIn	cMax	MinsumL	MaxsumL	MinD	MaxDt	MinS	MaxSe	MinL	MaxL
	4	5	2	2	6	7	0	0	1	2	8	8

Current Password	6	4	10	3	1	14
Mean	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Median	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Mod	FAIL	FAIL	FAIL	FAIL	PASS	FAIL

05.556---- FAIL

aalwal

123

KMWM

@

MEAN-CR	Min_mean	Max_mean	MinC	MaxC	Minsum	Maxsum	MinD	MaxD	MinS	MaxS	MinL	MaxL
	4.1428571...	4.5	1.75	2.2857142...	6.25	6.5	0	0	1.75	1.75	8	8

Median-CR	Min_median	Max_median	MinC	MaxC	MinSum	MaxSum	MinD	MaxD	MinSy	MaxSy	MinL	MaxL
	4	4.5	2	2	6	6.5	0	0	1.5	2	8	8

Mod-CR	Min_mod	Max_mod	CMIn	cMax	MinsumL	MaxsumL	MinD	MaxDt	MinS	MaxSe	MinL	MaxL
	4	5	2	2	6	7	0	0	1	2	8	8

Figure 7: CR for old password

4 Experiment process

The developed EPSBalgorithm, adopting the Longest Common Subsequence (LCS), was constructed using Python. The algorithm was designed and subjected to multiple tests to ensure its functionality aligns with the intended structure.

During this phase, the algorithm will be applied to a sample consisting of 141 users to test its performance. Subsequently, the performance of the developed algorithm will be compared with that of the

algorithm without LCS. Then, the algorithm's capability to achieve the intended objectives will be demonstrated.

4.1 Experimental method

The Confidence Range (CR) algorithm, responsible for generating Electronic Personal Synthesis Behavior (EPSB), was previously introduced and explained in [1]. However, this study provides a more practical demonstration of its functionality. Our newly developed simulator, depicted in Figures 2, 3, 4, and 5, offers a detailed example illustrating the process from start to finish in calculating CR. For instance, Table 1 demonstrates the relationship of user log history within the security system log file for all users. The average user updated their password six times. Each update was analyzed by the Smart application monitor, which considered factors such as the length of capital letters, small letters, digits, symbols, and the length of the password.

The security analyzer software developed in this study demonstrates the steps in which the CR is utilized to distinguish between authorized and unauthorized users. In this example, the last updated password by User 14, as shown in Figure 4 and Figure 5, was: Old password of the authorized user: 'KaMal@wW' In EPSB$_{\text{algorithm}}$ Figure 3 shows the total

calculated CR for 'KaMal@wW' across three grid view objects. The first set of grids shows the average outcome which is the CR-Mean while the second set of grid shows the median outcome which is the CR-Median. The third grid view was further divided into CR-Mode and the correspondent lowest and highest values. In conclusion, based on the aggregate sum of CR, it represents the amount of the earnings per share balance of User 14. Through this EPSB, the CR values are more effectively used in determining User 14's password security level. In the present approach, the cumulative CR from a sequence of consecutive grid views is calculated and analyzed in order to assess the quality of the password that is likely to have been used by either an authorized or an unauthorized user.

Additionally, the new password entered for the update is: 'KaMal@wW123Mal'.

The CR calculation for this new password is detailed in Table 2:

Table 2: CR for the new password

C-Letter	S-Letter	C + S	Digits	Symbols	Length
6	4	10	3	1	14

The compression is as follows:
All CR values fail to match between the Min and Max, except for the CR-Mod for symbols, highlighted in green, as shown in Figure 3. Figure 3 results of comparing CR: 'KaMal@wW' and CR: 'KaMal@wW123Mal'.
Figure 3 also illustrates this information from Table 2 under the grid view, all marked in red. This example highlights the weakness of the CR algorithm in its ability to distinguish between authorized and unauthorized users. As discussed in the introduction, the CR requires extensive historical records for each user to learn effectively.

4.2 Longest common subsequence (LCS)

The Longest Common Subsequence (LCS) involves comparing two strings, patterns, or sequences of objects. Your task is to identify the longest sequence of elements that appear in the same order within both strings and patterns.
Let's consider the following scenarios:
Assuming:
Pattern_1 /old Password = 'KaMal@wW'
Pattern_2 / new password = KaMal@wW123Mal'
• From Pattern_1, sequences like "Kamal", "aMal" "Mal", "wW", @wW, etc… can be generated. These sequences maintain the relative position of each character within the string.
• From Pattern_2, sequences such as "Kamal", "MwW ","aMal", "Mal", W123", etc… can be formed, preserving the relative order of characters in the original string.
Here, relative position refers to the order of appearance.
For instance, " MwW " is a valid sequence since, in
Pattern_2, "w" precedes "M", followed by "W". Conversely, if the sequence is "mka", it is invalid. This is because "k" is not the first character in the original Pattern_2 string as demonstrated in table 3.

Table 3: The LCS Length of 8

K	a	M	a	l	@	w	W						
K	a	M	a	l	@	w	W	1	2	3	M	a	l

Figure 6 displays the results calculated after entering the two string patterns, as demonstrated by the red circles manually added in Figure 8.
Figure 6 and Figure 8 illustrate the functionality of the LCS and its effectiveness in distinguishing between authorized and unauthorized users based on their behavior, particularly in pattern sequence style. Therefore, we can conclude that it is much easier to achieve better results with just a few lines of code to calculate the LCS compared to the entire process of calculating the CR, as demonstrated in Figures 2, 3, 4, and 5.

4.3. Test collection

Examining a test dataset containing 141 authentic records from 68 individuals at a chosen company between 2021 and 2022, encompassing a span of two years, we scrutinized user actions during password modifications. Upon reviewing historical log in password database, it becomes apparent that about 68 users altered their passwords multiple times within the two-year span. The test collection entries were as follows: the last 5 passwords belonged to 5 users, 108 entries belonged to 54 users (2 entries per user), 24 entries belonged to 8 users (3 entries per user), and 4 entries belonged to 1 user. The selection of users for the study was based on available log data used by the IT department for various tests and experiments.

4.4. Evaluation measure

To evaluate the CR algorithm presented in [5] (Alg1) alongside the Longest Common Subsequence (LCS) algorithm (Alg2), we have utilized the precision measure to gauge their effectiveness, defined as follows:
Precision (P) indicates the ratio of accurately classified passwords that are deemed successful.
Precision (P) = # (relevant password Matched [Pass]) / # (All test items). Table 4 illustrates the concept behind precision calculation.

Table 4: Evaluation measure

	Matched Password	Not Matched Password
Pass	true positives (TP)	false positives (FP)
Fail	false negatives (FN)	true negatives (TN)

Where:
Relevant passwords = number of all matched Password = 141 for 68 users
P = TP/ (TP + FP)

4.5. Experiment

In the Experiment, the test collection comprising 68 users was uploaded to the smart security application developed in [5] to compute the Alg1 (CR) algorithm developed in [5] and Alg2 (LCS) for all 68 users with 141 records. The experiment's results are presented in Table 5, and more details are in Table 6.

Table 5. Results after experiment.

Algorithm(R-DB=68)	TP	FP	TP +FP	TP/(TP + FP)
Alg1- (CR)	75	66	75 + 66	53.191
Alg2-L(Longest Common Subsequence (LCS))	102	39	102 + 39	72.34

The LCS algorithm, has shown promising results compared to Alg1 (CR). However, the results from test collection reveal the weaknesses of Alg1-CR in distinguishing authorized user users from false ones, achieving a recognition rate of only 53.191%. In contrast, Alg2-LCS achieved a precision of 72.34%. Further details can be found in Table 10, which provides a sample of the evaluation process.

Table 6: Sample of details for experiment.

Activity	User	last Password	Current Pass	Alg_CR(EPSB)Results	LCS	Number of matching patterns using LCS
change pass	user28	Aish#2002	Aish2002#	100.000---- PASS	fail	1
change pass	user36	Honda2009@	@Honda2009	100.000---- PASS	fail	1
change pass	user48	Tamer22Yq	TamerY22q	100.000---- PASS	fail	1
change pass	user15	Salim1978!	$alim1978	38.889---- FAIL	fail	2
change pass	user22	HammEr#1	HammEr#11#	55.556---- FAIL	fail	2
change pass	user1	Muh@nAd1978	Muh@nad!978	72.222---- PASS	fail	2
change pass	user18	GAs6677@	Fat77@	27.778---- FAIL	PASS	4
change pass	user18	GAs6677@	6677G@S	44.444---- FAIL	PASS	4
change pass	user3	1978BAs@	B@1978sA!	50.000---- FAIL	PASS	4
change pass	user36	Honda2009@	Hyundai2008#	50.000---- FAIL	PASS	4
change pass	user61	ooUU300B@	300B@UUoo	100.000---- PASS	PASS	6
change pass	user26	@qwe22Ahmad	@asd33Muhamad	50.000---- FAIL	PASS	6
change pass	user32	DSA@44Asd	Asd44@DSA	77.778---- PASS	PASS	6
change pass	user27	Muhamad$$1980	Muha1980mad$$	83.333---- PASS	PASS	7
change pass	user67	3333rT$$	rT$$3333	83.333---- PASS	PASS	7
change pass	user2	IBrahim@1234	@12himalaya4	00.000---- FAIL	PASS	7
change pass	user15	Salim1978!	K@m@l@ww	38.889---- FAIL	PASS	7
change pass	user11	omAN#Uob123@	syrIA@Squ123@	50.000---- FAIL	PASS	7
change pass	user26	@qwe22Ahmad	Ahm@dqwe22	50.000---- FAIL	PASS	7
change pass	user25	JJYYhh45@N	hN@45JJYYhh	55.556---- FAIL	PASS	7
change pass	user32	DSA@44Asd	CXZ#66Zxc	77.778---- PASS	PASS	8
change pass	user16	J2005Hud@	Huda@J2005	94.444---- PASS	PASS	8

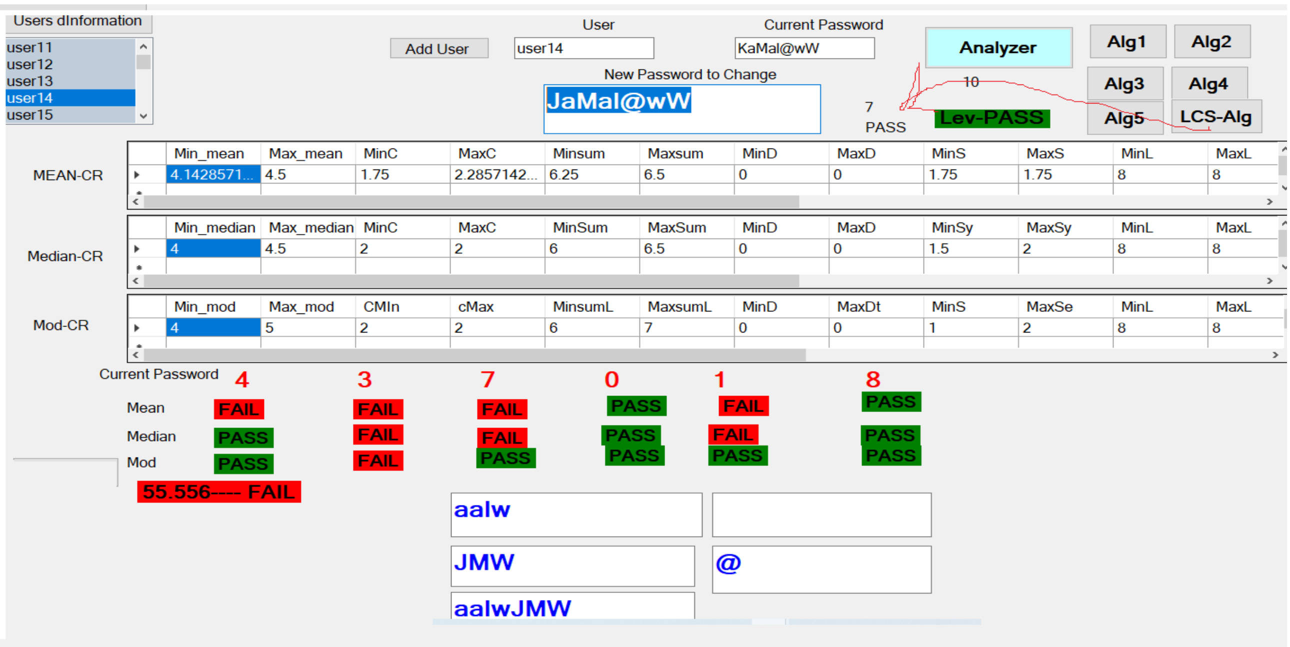
5 Discussion

The evaluation results underscore the limitations of the CR algorithm in discerning between authorized and unauthorized users. As outlined in the introduction, the EPSB algorithm mechanism in such a lengthy process is time-consuming, as shown by our experiments when altering the password length. In contrast, the functionality of the LCS and its efficacy in distinguishing between authorized and unauthorized users based on their behavior, particularly in pattern sequence style, offers a more practical and efficient approach. Consequently, achieving superior results with minimal code for LCS computation proves substantially easier compared to the complex CR calculation process. To highlight the shortcomings of the CR algorithm proposed by Mohanaad, we developed an application and simulator to implement the algorithm. Various experiments conducted on a test collection revealed overlooked aspects unaddressed by the reference authors [5]. Experiment two corroborated the weaknesses observed in Alg1 (CR), showing that the CR algorithm identified unauthorized users in only 53.191% of cases when unauthorized users attempted password changes. Our proposed method, in contrast, encountered failure in only 39 cases out of 141, achieving a success rate of 72.34%.

Compared to the 53.191% precision obtained using the CR algorithm, our LCS-based technique attained a precision of 72.34%. This enhancement demonstrates the effectiveness of the LCS approach in accurately distinguishing between authorized and unauthorized users. The higher accuracy rate of LCS suggests it is more successful at minimizing false positives and negatives. The CR method's complexity lies in its time-consuming computation of the median, mean, and mode for every user pattern, while the LCS method simplifies this by concentrating on password update sequence patterns, offering a more scalable real-time solution and improving computational efficiency. The CR algorithm assesses user behavior using pre-established statistical metrics, which may not adequately represent individual nuances in update and password-choosing behavior. The LCS algorithm, however, excels in character sequence analysis, spotting recurring patterns and providing an in-depth behavioral study essential for identifying significant yet subtle changes in user behavior.

The LCS algorithm's primary strength is finding the longest common subsequences between current and prior passwords, considering typical password-creation behavior and providing a realistic representation of user habits. The CR method, relying on aggregate statistical metrics, may miss complex patterns despite its thoroughness. Our approach skillfully handles the issue of different password lengths and the unavailability of user password histories by focusing on character sequences rather than individual features, ensuring consistent performance across various datasets.

This work offers a unique contribution by integrating the LCS algorithm into our intelligent security application, greatly enhancing the detection of unwanted access attempts. Analyzing and comparing password sequences adds a robust layer of protection, making multi-factor authentication solutions more reliable. By integrating LCS, our method improves the Electronic Personal Synthesis Behavior (EPSB), addressing drawbacks of earlier models and advancing intelligent authentication techniques through a detailed understanding of user behavior. The simplicity and efficacy of the LCS method make it highly suitable for practical implementation in various security applications, ensuring scalability and effective user activity



User user14

Current Password KaMal@wW

New Password to Change JaMal@wW

MEAN-CR

Min_mean	Max_mean	MinC	MaxC	Minsum	Maxsum	MinD	MaxD	MinS	MaxS	MinL	MaxL
4.1428571...	4.5	1.75	2.2857142...	6.25	6.5	0	0	1.75	1.75	8	8

Median-CR

Min_median	Max_median	MinC	MaxC	MinSum	MaxSum	MinD	MaxD	MinSy	MaxSy	MinL	MaxL
4	4.5	2	2	6	6.5	0	0	1.5	2	8	8

Mod-CR

Min_mod	Max_mod	CMIn	cMax	MinsumL	MaxsumL	MinD	MaxDt	MinS	MaxSe	MinL	MaxL
4	5	2	2	6	7	0	0	1	2	8	8

Current Password	4	3	7	0	1	8
Mean	FAIL	FAIL	FAIL	PASS	FAIL	PASS
Median	PASS	FAIL	FAIL	PASS	FAIL	PASS
Mod	PASS	FAIL	PASS	PASS	PASS	PASS

55.556---- FAIL

aalw

JMW

@

aalwJMW

Figure 8: Implement of the LCS in EPSB

analysis for organizations looking to strengthen their information security frameworks. To summarize, the suggested LCS-based approach shows notable improvements over the CR algorithm, offering increased accuracy, efficiency, and deeper behavioral insights. Our research provides a fresh approach to multi-factor user behavior identification security enhancement by addressing current method drawbacks and offering a scalable, practical solution.

6 Conclusion

The EPSB algorithm discussed by Mohannad considers numerous aspects of distinctive users' behavior while interacting with passwords, including password style, entry errors, and time spent inputting passwords. The method has three primary parameters: In order to define these styles, I have created three regular expressions: EPSBStyle, EPSBError, and EPSBTime. However, when the EPSB algorithm was being implemented, its flaws in terms of the user's serial choices of sequences of letters, symbols, or numbers were also observed. Furthermore, the method, when implemented, had a risk margin of around 48%. However, the longest common sequence (LCS) is a fundamental idea in the fields of computing and bioinformatics. It is used in determining the set of characters or components that are found in two or more sequences and are of the longest alternative. The limitations of modality the researchers of this work tackled EPSB in the procedure of implementing this approach in the algorithm. This technique uses a combined evaluation of characters and not each character in a distinct manner; this reduces the risk in the traditional EPSB algorithm.

Acknowledgement

This work is a part of project submitted to University of Buraimi (UoB), al Buraimi, Oman, Under No. IRG/UoB/CoB-005/2022-23 I would like to thank UoB for providing me the facility for completing this work.

References

[1] A. Szymkowiak, B. Melović, M. Dabić, K. Jeganathan, and G. S. Kundi, "Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people," *Technology in Society*, vol. 65, p. 101565, May 2021, doi: 10.1016/j.techsoc.2021.101565.

[2] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework," *Inf Syst Front*, vol. 24, no. 2, pp. 393–414, Apr. 2022, doi: 10.1007/s10796-020-10044-1.

[3] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-Driven IoT for Food Traceability With an Integrated Consensus Mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019, doi: 10.1109/ACCESS.2019.2940227.

[4] V. Papaspirou, L. Maglaras, M. A. Ferrag, I. Kantzavelou, H. Janicke, and C. Douligeris, "A novel Two-Factor HoneyToken Authentication Mechanism," in *2021 International Conference on Computer Communications and Networks (ICCCN)*, Jul. 2021, pp. 1–7. doi: 10.1109/ICCCN52240.2021.9522319.

[5] M. Hazratifard, F. Gebali, and M. Mamun, "Using Machine Learning for Dynamic Authentication in Telehealth: A Tutorial," *Sensors*, vol. 22, no. 19, Art. no. 19, Jan. 2022, doi: 10.3390/s22197655.

[6] X. Guo, J. Yang, and L. Yang, "Retrieval and Analysis of Multimedia Data of Robot Deep Neural Network Based on Deep Learning and Information Fusion," *Informatica*, vol. 48, no. 13, Art. no. 13, Sep. 2024, doi: 10.31449/inf.v48i13.6063.

[7] H. Albazar, A. Abdel-Wahab, M. Alshar'e, and A. Abualkishik, "An Adaptive Two-Factor Authentication Scheme Based on the Usage of Schnorr Signcryption Algorithm," *Informatica*, vol. 47, no. 5, Art. no. 5, May 2023, doi: 10.31449/inf.v47i5.4627.

[8] S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating User Perception of Multi-Factor Authentication: A Systematic Review," Aug. 16, 2019, *arXiv*: arXiv:1908.05901. doi: 10.48550/arXiv.1908.05901.

[9] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Behavioral biometrics & continuous user authentication on mobile devices: A survey," *Information Fusion*, vol. 66, pp. 76–99, Feb. 2021, doi: 10.1016/j.inffus.2020.08.021.

[10] J. He and J. Yang, "Network security situational level prediction based on a double-feedback Elman model," *Informatica*, vol. 46, no. 1, Art. no. 1, Mar. 2022, doi: 10.31449/inf.v46i1.3775.

[11] F. Guarracino *et al.*, "Noninvasive Ventilation for Awake Percutaneous Aortic Valve Implantation in High-Risk Respiratory Patients: A Case Series.," *Journal of cardiothoracic and vascular anesthesia*, vol. 294, no. 24, pp. 3124–3130, 2010, doi: 10.1053/j.jvca.2010.06.032.

[12] S. Ahmed, I. E. Nielsen, A. Tripathi, S. Siddiqui, R. P. Ramachandran, and G. Rasool, "Transformers in time-series analysis: A tutorial," *Circuits, Systems, and Signal Processing*, vol. 42, no. 12, pp. 7433–7466, 2023.

[13] A. Zeng, M. Chen, L. Zhang, and Q. Xu, "Are transformers effective for time series forecasting?," in *Proceedings of the AAAI conference on artificial intelligence*, 2023, pp. 11121–11128.

[14] H. A. Jeng *et al.*, "Application of wastewater-based surveillance and copula time-series model for COVID-19 forecasts," *Science of The Total Environment*, vol. 885, p. 163655, 2023.

[15] M. Soltani, M. Khashei, and N. Bakhtiarvand, "A Novel Discrete Deep Learning--Based Cancer Classification Methodology," *Cognitive*

Computation, pp. 1–19, 2023.

[16] M. Shakir, “User Authentication In Public Cloud Computing Through Adoption Of Electronic Personal Synthesis Behavior,” Uniten, 2020.

[17] M. Shakir, A. B. Abubakar, Y. Yousoff, 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, no. 2, p. 416, 2016.

[18] M. Shakir, “Applying Human Behaviour Recognition in Cloud Authentication Method—A Review,” in *International Conference on Emerging Technologies and Intelligent Systems*, 2021, pp. 565–578.

[19] M. Shakir, M. Hammood, and A. Kh. Muttar, “Literature review of security issues in saas for public cloud computing: a meta-analysis,” *IJET*, vol. 7, no. 3, p. 1161, Jun. 2018, doi: 10.14419/ijet.v7i3.13075.

[20] C. S. Lee and Y. Wang, “Typology of Cybercrime Victimization in Europe: A Multilevel Latent Class Analysis,” *Crime & Delinquency*, vol. 70, no. 4, pp. 1196–1223, Apr. 2024, doi: 10.1177/00111287221118880.

[21] E. Al Alkeem *et al.*, “An enhanced electrocardiogram biometric authentication system using machine learning,” *IEEE Access*, vol. 7, pp. 123069–123075, 2019.

[22] A. H. A. Alattas, M. A. Al-Shareeda, S. Manickam, and M. A. Saare, “Enhancement of NTSA Secure Communication with One-Time Pad (OTP) in IoT,” *Informatica*, vol. 47, no. 1, Art. no. 1, Feb. 2023, doi: 10.31449/inf.v47i1.4463.

[23] M. Papathanasaki, L. Maglaras, and N. Ayres, “Modern Authentication Methods: A Comprehensive Survey,” *AI, Computer Science and Robotics Technology*, Jun. 2022, doi: 10.5772/acrt.08.

[24] D. Tirfe and V. K. Anand, “A Survey on Trends of Two-Factor Authentication,” in *Contemporary Issues in Communication, Cloud and Big Data Analytics*, H. K. D. Sarma, V. E. Balas, B. Bhuyan, and N. Dutta, Eds., Singapore: Springer Singapore, 2022, pp. 285–296.

[25] B. Shannaq, R. Adebiaye, T. Owusu, and A. Al-Zeidi, “An intelligent online human-computer interaction tool for adapting educational content to diverse learning capabilities across Arab cultures: Challenges and strategies,” *Journal of Infrastructure, Policy and Development*, vol. 8, no. 9, Art. no. 9, Sep. 2024, doi: 10.24294/jipd.v8i9.7172.

[26] D. Progonov, V. Cherniakova, P. Kolesnichenko, and A. Oliynyk, “Behavior-based user authentication on mobile devices in various usage contexts,” *EURASIP Journal on Information Security*, vol. 2022, no. 1, p. 6, 2022.

[27] M. Shakir, R. Abood, M. Sheker, M. Alnaseri, M. Al-hashimi, and R. M. Tawafak, “Users Acceptance of Electronic Personal Synthesis Behavior (EPSB): An Exploratory Study,” *Recent Advances in Technology Acceptance Models and Theories, Part of the Studies in Systems, Decision and Control book series*, vol. 135, pp. 509–520, 2021.

[28] H. Wu, H. Han, X. Wang, and S. Sun, “Research on artificial intelligence enhancing internet of things security: A survey,” *Ieee Access*, vol. 8, pp. 153826–153848, 2020.

[29] M. SHAKIR, A. ABUBAKAR, Y. YOUSOFF, M. WASEEM, and M. AL-EMRAN, “MODEL OF SECURITY LEVEL CLASSIFICATION FOR DATA IN HYBRID CLOUD COMPUTING.,” *Journal of Theoretical & Applied Information Technology*, vol. 94, no. 1, 2016.

[30] S. Roopashree, J. Anitha, T. R. Mahesh, V. V. Kumar, W. Viriyasitavat, and A. Kaur, “An IoT based authentication system for therapeutic herbs measured by local descriptors using machine learning approach,” *Measurement*, vol. 200, p. 111484, 2022.

[31] S. Sivaslioglu, F. O. Catak, and K. Şahinbaş, “A Generative Model based Adversarial Security of Deep Learning and Linear Classifier Models,” *Informatica*, vol. 45, no. 1, Art. no. 1, Mar. 2021, doi: 10.31449/inf.v45i1.3234.

[32] P. H. Basha, G. Prathyusha, D. N. Rao, V. Gopikrishna, P. Peddi, and V. Saritha, “AI-Driven Multi-Factor Authentication and Dynamic Trust Management for Securing Massive Machine Type Communication in 6G Networks,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 1s, pp. 361–374, 2024.

[33] T. Bin Shams, M. S. Hossain, M. F. Mahmud, M. S. Tehjib, Z. Hossain, and M. I. Pramanik, “EEG-based Biometric Authentication Using Machine Learning: A Comprehensive Survey,” *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, vol. 20, no. 2, pp. 225–241, 2022.

[34] M. Srinivasan and N. C. Senthilkumar, “Machine Learning-Based Security Enhancement in Heterogeneous Networks Using an Effective Pattern Mining Framework,” *INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING*, vol. 12, pp. 244–257, 2024.

[35] A. Ashtari, B. Alizadeh, and others, “A comparative study of machine learning classifiers for secure RF-PUF-based authentication in internet of things,” *Microprocessors and Microsystems*, vol. 93, p. 104600, 2022.

[36] P. C. Golar, “INTELLIGENT SYSTEMS AND APPLICATIONS IN Security Analysis of the Graphical Password-Based Authentication Systems with Different Attack Proofs,” vol. 11, pp. 155–165, 2023.

[37] "Sensors | Free Full-Text | Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare." Accessed: Dec. 17, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/21/8944

[38] H. Alqahtani and G. Kumar, "Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems," *Engineering Applications of Artificial Intelligence*, vol. 129, p. 107667, Mar. 2024, doi: 10.1016/j.engappai.2023.107667.

[39] K. A. Shastry and A. Shastry, "An integrated deep learning and natural language processing approach for continuous remote monitoring in digital health," *Decision Analytics Journal*, vol. 8, p. 100301, Sep. 2023, doi: 10.1016/j.dajour.2023.100301.

[40] M. Alabadi and A. Habbal, "Next-generation predictive maintenance: leveraging blockchain and dynamic deep learning in a domain-independent system," *PeerJ Comput. Sci.*, vol. 9, p. e1712, Dec. 2023, doi: 10.7717/peerj-cs.1712.

[41] M. S. Abdalzaher, M. M. Fouda, A. Emran, Z. M. Fadlullah, and M. I. Ibrahem, "A Survey on Key Management and Authentication Approaches in Smart Metering Systems," *Energies*, vol. 16, no. 5, Art. no. 5, Jan. 2023, doi: 10.3390/en16052355.

[42] L. Alawneh, M. Al-Zinati, and M. Al-Ayyoub, "User identification using deep learning and human activity mobile sensor data," *Int. J. Inf. Secur.*, vol. 22, no. 1, pp. 289–301, Feb. 2023, doi: 10.1007/s10207-022-00640-4.

[43] P. A. Thomas and K. Preetha Mathew, "A broad review on non-intrusive active user authentication in biometrics," *J Ambient Intell Human Comput*, vol. 14, no. 1, pp. 339–360, Jan. 2023, doi: 10.1007/s12652-021-03301-x.

[44] B. Vyas and M. Nawaz, *Java in Action : AI for Fraud Detection and Prevention*. 2023. doi: 10.13140/RG.2.2.20929.33125.

[45] H. Jebamikyous, M. Li, Y. Suhas, and R. Kashef, "Leveraging machine learning and blockchain in E-commerce and beyond: benefits, models, and application," *Discov Artif Intell*, vol. 3, no. 1, p. 3, Jan. 2023, doi: 10.1007/s44163-022-00046-0.

[46] S. Nasiri, F. Sadoughi, A. Dehnad, M. H. Tadayon, and H. Ahmadi, "Layered Architecture for Internet of Things-based Healthcare System: A Systematic Literature Review," *Informatica*, vol. 45, no. 4, Art. no. 4, Dec. 2021, doi: 10.31449/inf.v45i4.3601.

[47] B. Yang *et al.*, "AI-Oriented Two-Phase Multifactor Authentication in SAGINs: Prospects and Challenges," *IEEE Consumer Electronics Magazine*, vol. 13, no. 1, pp. 79–90, Jan. 2024, doi: 10.1109/MCE.2023.3262904.

[48] P. Zhou, H. Xu, L. H. Lee, P. Fang, and P. Hui, "Are you left out? an efficient and fair federated learning for personalized profiles on wearable devices of inferior networking conditions," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 6, no. 2, pp. 1–25, 2022.

[49] A. Rehman *et al.*, "CTMF: Context-aware trust management framework for internet of vehicles," *IEEE Access*, vol. 10, pp. 73685–73701, 2022.

[50] B. Roumaissa and B. Rachid, "An IoT-Based Pill Management System for Elderly," *Informatica*, vol. 46, no. 4, Art. no. 4, Dec. 2022, doi: 10.31449/inf.v46i4.4195.

[51] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep learning for phishing detection: Taxonomy, current challenges and future directions," *IEEE Access*, vol. 10, pp. 36429–36463, 2022.

[52] E. Koster, "Why Samsung NEXT and HYPR believe the future will be passwordless.," Samsung Newsroom USA. [Online]. Available: https://news.samsung.com/us/samsung-next-hypr-believe-future-will-passwordless/

[53] TwoSense.AI, "Continuous multifactor authentication." [Online]. Available: https://www.twosense.ai/.

[54] Kristin Miller, "Ping Identity Announces the Acquisition of SecuredTouch to Accelerate Identity Fraud Capabilities," *Ping Identity Holding Corp*.

[55] B. Noë, L. D. Turner, D. E. J. Linden, S. M. Allen, B. Winkens, and R. M. Whitaker, "Identifying indicators of smartphone addiction through user-app interaction," *Computers in human behavior*, vol. 99, pp. 56–65, 2019.

[56] B. Shannaq, "Enhancing Human-Computer Interaction: An Interactive and Automotive Web Application - Digital Associative Tool for Improving Formulating Search Queries," in *Advances in Information and Communication*, K. Arai, Ed., Cham: Springer Nature Switzerland, 2024, pp. 511–523. doi: 10.1007/978-3-031-54053-0_35.

[57] A. S. Gaafar, J. M. Dahr, and A. K. Hamoud, "Comparative Analysis of Performance of Deep Learning Classification Approach based on LSTM-RNN for Textual and Image Datasets," *Informatica*, vol. 46, no. 5, Art. no. 5, Mar. 2022, doi: 10.31449/inf.v46i5.3872.

[58] S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye, and T. O. Oladoyinbo, "AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems," Jan. 25, 2024, *Rochester, NY*: 4706726. doi: 10.2139/ssrn.4706726.

[59] X. Zhang and J. Zhang, "Analysis and research on library user behavior based on apriori algorithm," *Measurement: Sensors*, vol. 27, p. 100802, Jun. 2023, doi: 10.1016/j.measen.2023.100802.

[60] "IOS Press Ebooks - User Behavior Analysis Based

on Big Data and Artificial Intelligence." Accessed: Jun. 27, 2024. [Online]. Available: https://ebooks.iospress.nl/doi/10.3233/FAIA230881

[61] A. Yu. Iskhakov, M. V. Mamchenko, and S. P. Khripunov, "Enhanced User Authentication Algorithm Based on Behavioral Analytics in Web-Based Cyberphysical Systems," in *2023 International Russian Smart Industry Conference (SmartIndustryCon)*, Mar. 2023, pp. 253–258. doi: 10.1109/SmartIndustryCon57312.2023.10110791.

[62] L. Yang, X. Zhang, and Q. Wang, "A Behavior-based Scheme to Block Privacy Leakage on Smartphone Sensors When You Exercise," *Sensors and Materials*, vol. 35, no. 2, p. 579, Feb. 2023, doi: 10.18494/SAM4173.

[63] "User behavior modeling for AR personalized recommendations in spatial transitions | Virtual Reality." Accessed: Jun. 27, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10055-023-00852-6

[64] B. Shannaq, I. A. Shamsi, and S. N. A. Majeed, "Management Information System for Predicting Quantity Martials," vol. 8, no. 4.

[65] B. Shannaq, "Digital Formative Assessment as a Transformative Educational Technology," in *Advances in Information and Communication*, K. Arai, Ed., Cham: Springer Nature Switzerland, 2024, pp. 471–481. doi: 10.1007/978-3-031-54053-0_32.

[66] 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," *AIP Conference Proceedings*, vol. 3015, no. 1, p. 020013, Dec. 2023, doi: 10.1063/5.0188358.

[67] M. Shaik, L. Gudala, and A. K. R. Sadhu, "Leveraging Artificial Intelligence for Enhanced Identity and Access Management within Zero Trust Security Architectures: A Focus on User Behavior Analytics and Adaptive Authentication," *Australian Journal of Machine Learning Research & Applications*, vol. 3, no. 2, Art. no. 2, Jul. 2023.

[68] M. Shakir, A. B. Abubakar, Y. Yousoff, 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, no. 2, 2016.

[69] L. Wang and B. Zhu, "Algorithms and Hardness for the Longest Common Subsequence of Three Strings and Related Problems," in *String Processing and Information Retrieval*, F. M. Nardini, N. Pisanti, and R. Venturini, Eds., Cham: Springer Nature Switzerland, 2023, pp. 367–380. doi: 10.1007/978-3-031-43980-3_30.

[70] M. Shakir, M. J. Al Farsi, I. R. Al-Shamsi, B. Shannaq, and G. A.-M. Taufiq-Hail, "The Influence of Mobile Information Systems Implementation on Enhancing Human Resource Performance Skills: An Applied Study in a Small Organization. | International Journal of Interactive Mobile Technologies | EBSCOhost." Accessed: Sep. 19, 2024. [Online]. Available: https://openurl.ebsco.com/contentitem/doi:10.3991%2Fijim.v18i13.47027?sid=ebsco:plink:crawler&id=ebsco:doi:10.3991%2Fijim.v18i13.47027

[71] M. Shakir, "Applying Human Behaviour Recognition in Cloud Authentication Method—A Review," in *Proceedings of International Conference on Emerging Technologies and Intelligent Systems*, M. Al-Emran, M. A. Al-Sharafi, M. N. Al-Kabi, and K. Shaalan, Eds., Cham: Springer International Publishing, 2022, pp. 565–578. doi: 10.1007/978-3-030-85990-9_45.