Adaptive Authentication Using AI-Driven Password Behavior Clustering: Addressing the Reliability Gaps in Emerging Passkey Systems

Boumedyen Shannaq [1]

[1] *Management of the Information System Department, University of Buraimi, Al Buraimi, Sultanate of Oman*

Abstract **- Recent studies regarding the topic of cybersecurity imply that the issue of password poisoning through AI is rapidly growing in severity, and additional systems of authentication that are more intelligent and behavior-aware are required. Multi-factor authentication (MFA) provides better security but is often more inconvenient for users, and existing authentication systems do not extensively leverage behavioral analysis of password creation and use. Although there has been a recent trend toward Passkey deployments instead of passwords, their effectiveness and widespread adoption have not been tested. The given work, in turn, is more realistic and empirically justified through behavioral password profiling, making it practical and reliable. This paper addresses the gap by exploring the hypothesis that clustering-based password profiling can effectively distinguish a legitimate user from a potential attacker. The password clustering model is a centroid-based model that assumes it enhances authentication accuracy by training on the password patterns users use. In the study, a list of passwords from multiple users was used to determine Centroid Password (CP) profiles via machine learning clustering. The proposed model proved more effective at classifying valid passwords and produced fewer false positives than traditional methods. The results confirm that password behavior can be categorized to enhance the authentication and verification of user identities. The research can be used to develop new, behavior-driven security models to improve the protection of digital identities against emerging AI threats.**

Keywords **- Authentication, security, password pattern, clustering, centroid analysis, Artificial Intelligence (AI).**

DOI: 10.18421/TEM144-04
https://doi.org/10.18421/TEM144-04

Corresponding author: Boumedyen Shannaq,
Management of the Information System Department, University of Buraimi, Al Buraimi, Sultanate of Oman
Email: boumedyen@uob.edu.om

Received: 16 March 2025.
Revised: 16 October 2025.
Accepted: 03 November 2025.
Published: 27 November 2025.

1. Introduction

The legacy password authentication system is now working, but with significant limitations, given the ongoing development of artificial intelligence (AI) that can discern vulnerabilities in password security systems [1], [2]. This analysis, which uses centroid-based analysis along with AI-based password pattern clustering, provides new security improvements to password systems [3].

The use of AI tools has brought significant transformations across various fields, enabling the design of both defensive and offensive solutions to safeguard cybersecurity networks. AI systems have defensive features such as prediction, anomaly detection, and the generation of dynamic passwords, which enhance the overall security infrastructure. Criminal activity can also be carried out with the help of AI, as hackers create advanced security attacks by integrating a sequence of automated password-cracking tools with a 'Deepfake' impersonation plan [4].

Password combination, as defined by security researchers, involves analyzing the organizational patterns of password combinations and the design features of such passwords [5]. Using this method, it is possible to identify ubiquitous trends used by user groups, which poses a potential security threat. Safety nets are more secure when they implement password creation policies to prevent users from creating weak passwords that attackers can easily decipher [6].

In centroid-based analysis, clustering has a spot, called the centroid, which is representative of the cluster [7]. By doing so, technicians will be able to establish the core distribution of regular password patterns within security systems. A system uses centroid analysis to develop new password security by calculating the distance between each password and these core points, then predicting the password's risk level and strength [8].

Moreover, [9] highlight emerging trends and best practices that can inform the development of robust security systems for digital infrastructure in the future. Recent studies indicate that AI has made a revolutionary contribution to cybersecurity, especially in threat detection and the development of flexible defense capabilities [10], [11]. The use of strong passwords is becoming increasingly crucial in the era of AI-based attacks. The issue of password security has become increasingly critical as AI-based technologies continue to advance. Today, in modern applications of AI algorithms, massive datasets are processed in a short period of time to identify patterns, using which their forecasting of passwords is exceptionally accurate [12]. Weak passwords, which are usually built from words or personal data and are easily guessable, are now under major threats from brute-force, dictionary, and machine-learning cracking programs [13], [14].

Since hackers are highly interested in AI technology, they use it to compromise authentication systems with weak security configurations, thereby granting unauthorized users access to internet accounts and altering the original user credentials [15]. An analysis of the security threats is done by [16]. It has proposed an interesting approach to enhance user differentiation using the promising EPSBV01 algorithm [17]. Cases of such security breaches have been experienced in WhatsApp, Facebook and Gmail where attackers get hold of the accounts by altering passwords hence depriving the appropriate owners of their rights. Cases have led to exposure of personal information, economic stability, and business activities [18], [19]. The assessed technology in healthcare security was blockchain [20].

The end-users need to adopt practical password management skills by ensuring that they make their passwords long, complex, and unique to different accounts to fight the threat posed by AI [21]. The multi-factor authentication (MFA) and password manager systems can assist in safety additions by introducing cognitive security and eliminating unauthorized access to a system [22], [23]. The contemporary trend of the development of cybersecurity threats means that password security will be required to defend digital identities and sensitive data against AI-based cyberattacks [24], [25].

The study will use a worst-case analysis methodology, showing that once a user's password is compromised, it may persist despite the absence of all possible multi-factor authentication tools, such as SMS codes, email verification, and biometric authentication.

In this crisis, the attacker gains access to the account of the user, which enables them to alter the original account details, consequently blocking the original owner.

The proposed work compares the risk of the individual who changed the passwords on the compromised account, whether the user is a genuine user or a hacker. The Gmail and WhatsApp account hijacking are the current forms of security violations where an attacker gains access to the personal account of a person.

A cyber attacker will secure entry then edit the account recovery contacts hence preventing the original user to recover access. The suggested system will examine the behavioral trends such as typing speed, password writing patterns, and device interaction trends to differentiate genuine users and possible hackers.

1.1. Problem Statement

Password authentication schemes demand that the stored passwords of users be identical to their present logins [26]. Lockouts of accounts, security breaches, and frustration come when users use small password changes when they update their passwords. The passwords used by users in terms of their patterns are not considered by security policies, and it is imperative that the user changes the passwords on a regular basis. Attackers take advantage of this vulnerability by using phishing, brute-force attacks, and unauthorized intrusions by guessing modified passwords.

1.2. Research Gap

The existing password authentication techniques do not investigate the behavior of each user password [27]. The significance of memorable characters to password security has been comparatively analyzed [28]. Multi-factor authentication (MFA) is more secure, but it also causes usability concerns for user experiences [29]. One of the Face Recognition strategies was machine learning that enhanced security within a smart home [30]. The studies on user specific password profiles show that no research has been done to verify the identity based on the use of established password patterns.

The deployment of AI methods has now become the central issue of study to improve the authentication of cybersecurity [31]. The use of traditional password authentication systems is still in practice, and it is easy to point them but they offer easy targets due to predictable patterns of users and their choice of passwords [32], [33].

The review discusses AI-based password pattern analysis methods, as well as methods of clustering, which results in the proposed method being discussed as follows:

1) Historical Password Protection Problems:
   Authentication by use of passwords is critical in securing security systems. It is due to this practice that users use easy passwords that end up endangering their systems. In a study by [34], trends of password vulnerability were determined, and it is important to establish powerful security mechanisms.
2) AI and Machine Learning in Password Security:
   The development of artificial intelligence and machine learning technology has resulted in advanced password security. In their experimental study, a team of researchers at [35] used machine learning to test password security and hence found standard trends in passwords. LPSE is a machine learning password-strength analysis that was designed by [36] to determine password strength efficiently.
3) Behavioral Biometrics and Keystroke Dynamics:
   Studies have investigated how the behavioral biometric measurements, including the data of keyboard dynamic characteristics, can be used to strengthen security measures. Authors [37] carried out pattern analysis of dynamic keystrokes based on machine learning algorithms to enhance user-level security. The findings of the research show that one can identify the real user amidst the potential attackers using the behavioral biometric techniques.
4) Generation of Passwords by Gesture:
   Several innovation techniques today employ biological actions as a password development approach. The creation system of the password was developed by [38], and it used the data features of the hand gestures together with the security analysis. In their research, 99% accuracy of ensemble learning techniques caused with physiological behaviors into their system was reached [39]. The CNNs-based approach to a multi-factor authentication process is also examined by [40].
5) Password Strength Prediction through Ensemble Learning:
   The predictions of the password strength are more accurate when the ensemble learning techniques are applied. Current studies are directed at the ensemble methods to enhance the ability to predict password strength because each model has certain drawbacks [41]. In the current research methods, there are several classifiers and their arrangement is in such a way that their capability to identify correctly password security levels is achieved [42].
6) Centroid-Based Password Pattern Analysis:
   Centroid-based clustering method allows the identification of common patterns and anomalies in the password patterns [43]. The process uses a statistical approach to determine the focal point (centroid) of groupings of password information and thus forms the standard patterns in passwords. The security threats are identified when information that does not conform to the norms or the central point is analyzed. The [44] has also proposed a relative study of the K-means and fuzzy C-means algorithm.

The standard authentication system has the passwords stored in the form of hashes, and real matching processes are carried out [45]. Studies indicate that users are likely to make weak derivations of their current passwords that can be easily guessed by attackers [46].

1.3. Machine Learning in Password Security

Studies confirm that machine learning algorithms measure the strength of passwords by detecting odd features [47], [48]. Clustering algorithms were used to form password structure clusters used in identifying compromised credentials. These research studies only concentrate on the password recognition but not on the behavioral characteristics of the user.

1.4. Password Similarity Analysis

The identical character sequences are used by the users over and over again, because the studies of the so-called Levenshtein distance and sequence matching have proved [49], [50]. A majority of password management systems are capable of creating unique passwords, and they are usually modified by users into their personal patterns. According to this study, authentication systems that are based on behavioral and also those that are based on tendencies need to be put in place in conjunction with strict systems that verify the passwords.

2. Literature Review

Various attempts have been made regarding password security and machine learning to give individualized profiles of passwords which can be used as effective methods of identity verification. This was a new password clustering model that supports security requirements in accordance with password evolution [51].

This study uses the Centroid Password (CP) algorithm in comparison to the proposed approach to identify unauthorized requests to change the password by analyzing password entries.

CP algorithm was applied to a set of 629 passwords put in by 143 users with an accuracy of precision of 68.88 by correctly identifying 197 of 286 entries. Experimental results have shown that the CR-EPSB method is less accurate by 24.47% than the Centroid Password method. Research works conducted by other researchers have studied various password security factors, although the offered approach stands out due to its ability to integrate centroid-based clustering with AI to improve the process of authentication. The federated system offers new authentication schemes of valid password change requests, which underpins the ongoing cybersecurity fortification efforts. Philosophy: The system of modern authentication is highly advantageous due to the combination of AI and machine learning, and the security of the password. Various security measures that integrate behavioral analytics and ensemble learning systems are an effective way to solve traditional security threats. The suggested centroid-based analysis enables organizations to have a technique of accurately detecting the unapproved password modification, which will improve overall security aspects.

The work is constructed since a password identity profiling system plays a parallel role to various research studies that are currently underway that deal with behavioral biometrics and password security. Behavioral profiling techniques are also presented in [52] which involves the usage of distinct behavioral measurements, like typing rhythms and the movements of a mouse to improve the security of authentication. The user profiling of the proposed work is based on previous password behavior; that is, the analysis is conducted on the password content that is stored and not on the behavior that occurs in the process of entering the passwords. The authentication process by Keystroke Dynamics uses typing patterns and times, thus authenticating users of the system. Even though this is a successful approach, the system must monitor users when entering passwords. The proposed work password analysis system identifies the password structure in the established password assessments that are static, and they do not need real-time data to establish passwords. What the authentication system of the previous related work does is to verify passwords through the dynamic challenge system. The suggested password authentication system creates password centroid profiles using prior user passwords so as to generate password verification based on adaptation using user passwords without incurring extra user input. The other paper explored the behavior of users in order to devise user classification rules depending on both IP addresses and colocation. The proposed work password research, studies the natural passwords patterns in detail which gives even more security to the system. Other literature discusses the behavioral models to promote the protection of user-generated passwords.

The study project on password creation behavior is not similar to the proposed work which examines the current patterns of passwords using user authentication to secure their safety in different manner.

A significant inconsistency in passkey implementation is indicated by an empirical study of a vast amount of web sites, showing inconsistencies and flaws in design that may affect the reliability of actual implementation. Such technical and user- based issues of passkey adoption as account recovery, delegation, synchronization, and user perceptions point to the fact that their validity and universal applicability are yet to be fully validated [53]. A comparison of the device-bound and synced passkey credentials identifies security trade-offs and dependence on passkey providers, and, accordingly, it is a contention that the security assurance of synced passkeys is a point of contention [54]. A general analysis of ‘passwordless’ authentication reveals that, even though passkey advantages are evident, inertia to use, device portability, and absence of device support are some of the deployment requirements that are not fulfilled [55]. There are additional books and papers that offer an extensive analysis of ‘passwordless’ authentication methods [56]. These works validate a provisional assumption that passkey reliability and mass implementation warrant further research.

The given work method contrasts the keystroke dynamics or behavioral biometrics since the given method involves the application of new analysis to the content and structure of past passwords users use, rather than the real-time input information. The analysis of the static passwords allows the adaptive authentication with facilitating the normal evolution of the passwords without generating any more user issues.

2.1. Research Contribution

The study conducted in the research is password identity profiling through machine learning-based techniques of clustering to calculate the password behavioral profile of users. This study provides several significant results.

1) In the development of the model, standard components of previous passwords are identified in the system to create user behavior profiles.
2) The system also improves the security of authentication, whereby new passwords are compared with old historical passwords to identify invalid password changes.
3) The system allows users to make simple adjustments with the help of a secure password procedure.
4) A Scalable Security Layer is the adaptation suggested for large-scale web applications and authentication systems on the enterprise level.
5) The methodology guarantees the convenience of passwords to the authorized persons due to the security of access to the systems.

The suggested work presents a password profiling technique, which takes advantage of user password patterns to complement the existing behavioral authentication techniques, thus offering a feasible security enhancement in dynamic settings.

3. Methodology

This study employs a multi-stage study process in formulating and testing a behavior profile of the user-specific password. The algorithm is based on data collection, feature selection, clustering, and validation to increase the level of authentication and retain its application in cybersecurity systems.

3.1. Step 1: Data Collection

The study retrieves past passwords of different user accounts [19]. Several passwords should be made up of a mixture of symbols, numbers, and capital letters.

3.2. Step 2: Feature Extraction

The stage will be dedicated to estimating the principal characteristics of each password to indicate the unique user behavior. Similarity, variability, and positional patterns of the composing passwords are measured using various textual and structural data.

- Decorative character usage, character length variation, and character use of symbols.
- Through the technique, 'Jaccard' similarity and 'Levenshtein' distance are also calculated along with position weightage in the analysis.

3.3. Step 3: Password Clustering and Centroid Calculation

The third step is password clustering, after which centroid values are determined. The similar password patterns should be classified under either K-means methods or DBSCAN clustering. Equally, the system will generate various user-specific passwords based on patterns.

3.4. Step 4: Verification Mechanism

The tool compares new passwords with the profile using a similarity analysis. A threshold variable of acceptance will decide the acceptable variations of passwords and prevent security attacks.

3.5. Step 5: Implementation and Testing

The model needs to be tested by investigating real password sets [19]. The adopted approach makes it security compatible with the principle of usability, allowing the creation of flexible authentication mechanisms that can respond to the current issues of cybersecurity threats.

The password identity profile is allocated to each user based on investigations of their past passwords. The model developed can be used as a core prototype in identifying the necessary elements of the regular password set up of a user such as the presence of letters, position of numbers and the use and position of symbols. The user has to enter a modified password which is then verified by the system to confirm whether the user is who they say they are in their profile thus establishing it as a proper choice of the user.

4. Experiments

In the experimental stage the proposed centroid-based password profiling model is verified during the experimental stage in a series of controlled experiments and simulations. It is based on defining the problem situation, running the algorithm, and assessing its ability to detect both real and fake password updates.

4.1. Problem Definition for Building Algorithm

Today's password authentication systems authenticate users against stored hashed passwords. Users constantly update their passwords with minimal alterations, making it difficult to tell whether an update was done in an authentic way or an anomaly occurred. The users require a system of password profiles that collates their password tendencies so as to identify them even after minor alterations to their passwords.

4.2. Proposed Solution

A proposed solution of dynamically creating adaptive password profiles in order to increase the level of security in authentication will be introduced. It outlines the derivation of meaningful features, the generation of centroid-based profiles, and the validation of password updates against preset patterns as follows:

1) Retrieve Key Features on Passwords:
   - The users are to be assessed in terms of using common letters, numbers, and symbols,
   - Variations in capturing password length,
   - Examine character sequence and transition.
2) Create Centroid Password Profile:
   - Character frequency analysis to define standard password components should be used in the system,
   - Calculate positional character likelihoods.
   - The system uses different tests of similarity, such as Jaccard similarity, cosine similarity, and 'Levenshtein' distance, among others, to determine the consistency of the passwords.

3) Verify Password Updates:
- Compare centroid profile to new passwords,
- Systems must permit changing of passwords with a similar level under acceptable levels.

4.3. Implementation (Example)

As Figure 1 illustrates, the built-in application takes the input of the dataset, runs password processing on the user passwords, generates an overall representation of a password center, and authenticates renewed passwords with this benchmark. The steps involved in the first step include password collection by the application that is developed:

1) Password Collection
- First, the passwords associated with user1 are retrieved from the dataset:
  user1_passwords = ["muhanad1978@", "MuhaNad!978", "Muh@nad78", "Muh@n@d1978"]

2) Character Position Analysis:
- For each password, the characters are split and stored in a list:
  char_positions = [['m', 'u,' 'h,' 'a', 'n,' 'a', 'd', '1', '9', '7', '8', '@'], ['M ', 'u', 'h', a ', 'N', 'a, 'd', '!', '9', '7', '8'], ['M', 'u', 'h', '@', 'n', a ', d ', '7', '8'], ['M', 'u', 'h', '@', 'n', '@', d ', '1', '9', '7', '8']]

3) Character Frequency Count:
- The Counter function is used to count the frequency of each character across all passwords.
- Updates frequency count for each character.

For the user, after processing all four passwords, the frequency count is as follows:

Common chars = {'m: 1, 'u': 4, 'h': 4, 'a: 4, 'n': 4, d ': 4, '1': 2, '9': 2, '7': 3, '8': 3, '@': 2, 'M': 1, 'N': 1, '!': 1}

4) Centroid Creation:
- The centroid password profile is constructed by selecting the most frequent characters in the password set.
- centroid password = "uhand1978@M!N"

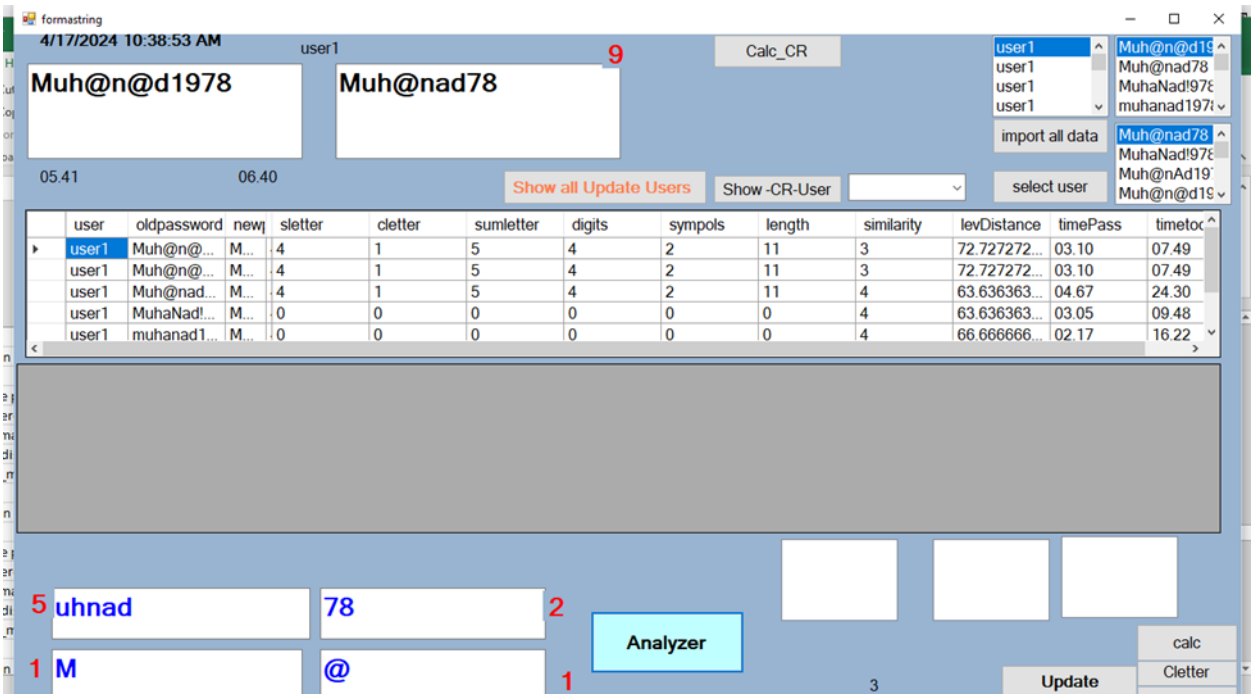

Figure 1. Sample of developed system

4.4. Equation to Create Centroid

This part outlines the process for building a centroid password that models a user's typical password behavior. The centroid is calculated by summing the character frequencies of all passwords and ranking them in order of their significance.

Let C = {c1, c2, ..., ck} be the set of characters across all passwords for a user, and let f(c) be the frequency of character c across the passwords. The centroid password is constructed by arranging the characters c_i_ in the order of *f(c)* from highest to lowest.

Thus, Equation 1:

$$CP = SChf = \sum_{i=1}^{k} Ci\,\Sigma \quad (1)$$

Generated password profile (centroid) for user1: "uhand1978@M!N".

The final centroid password (CP) is a composite profile that reflects the most commonly used characters for a particular user across all their passwords.

Where CP: Centroid Password and SChf: Stored Characters by frequency.

Assume a hacker obtains the user's last password and attempts to update it. The hacker enters" MuhaNad!978." The proposed work will compare" MuhaNad!978" with user 1 CP: "uhand1978@M!N." The similarity will be 58.33%. The similarity function compares two sequences (MuhaNad!978 & uhand1978@M!N) and returns a similarity score between 0 and 1.

Similarity ratio:

$$(r) = N / M \quad (2)$$

Where:

- N is the total number of characters in the combined sequence of both strings.
- M is the total number of matching characters in both strings.

Matching blocks identified where sequences in both strings align well.

Similarity% = r × 100

The similarity is primarily based on how a poor lot of the characters and their positions fit amongst MuhaNad!978 & uhand1978@M!N. as an instance:

- Every MuhaNad!978 & uhand1978@M!N have similar characters like u, h, a, n, d, 1, 9, 7, eight, @, and M, but they're prepared in every other way.
- The positions of characters, much like the @,!, and numbers, affect how the matching subsequences are aligned.

The output of 58.33% suggests that MuhaNad!978 and uhand1978@M!N are reasonably similar but no longer identical.

5. Evaluation and Results

In order to test the proposed algorithm, precision was calculated using experiments that were conducted. The evaluation was done using the last password stored and saved before creating a centroid password profile of any individual. Moreover, to replicate the testing conditions, the study came up with falsified passwords where there was a valid and an invalid (false) password in every test. The data set collected has 143 customers updating their passwords giving 629 data points, 486 of which are training data, 143 of which are testing data and 143 of which are false data. Precision is a typical measure of how well predictions are accurate. It is obtained by the following formula:

$$Precision = (TP) / (TP) + (FP) \quad (3)$$

Where:

(TP) True Positives in cases when the gadget is an efficient identification of a password of the legitimate user.

(FP) False Positives: Cases in which the gadget would mistake a fake password for a legitimate user.

The results of the general performance analysis of the CP (Centroid Password) rule set are displayed in Table 1, where precision represents the primary measure. Real Positives (TP) were 197 times when the rules were able to recognize the proper password of the user. False Positives (FP) were 89. The rules had a false positive error by treating a wrong password as a legitimate user. General Forecasts (TP + FP) were 286 total cases where the set of rules was utilized (correctly and wrongly):

Text {Precision} = \frac{\ text{TP}}{\ text{TP} + \ text{FP}} = \frac{197}{286} = 0.688 \ text{ 88%)}. This finding implies that sixty eight eighty-eight percent of the times the CP set of rules were able to find the actual password and never accept a false one. Though it is a reasonably robust outcome, the fact that there were 89 false positives indicates that it can be improved, probably by enhancing the password profile generation system or adding other security variables. CP is more accurate by 24.47% compared with CR-EPSB, which shows that CP is much more effective in identifying valid passwords correctly and decreases false identifications.

The importance of the proposed work to contemporary cybersecurity is mainly attributed to its better authentication protection against advanced threats. Conventional password authentications are not as safe as AI-based cyberattacks are increasingly becoming. The paper shows that the AI clustering method, in conjunction with the centroid-based evaluation, allows the enhancement of the password authentication security through the identification of the abnormal password requests and the elimination of cases of unauthorized access to the system.

Table 1. Results

Alg.	TP	FP	TP + FP	Precision (TP / (TP + FP))	Precision (%)
CP	197	89	286	0.688	68.88%

5.1. Who Can Use This Work

The results derived in this work will provide the potential end users and beneficiaries of the proposed password profiling system and authentication system with the following.

These IT administrators and cybersecurity analysts can integrate this model with their authentication in the system to curtail unauthorized cases, such as:

- By incorporating AI-powered authentication systems by financial institutions like banks and online payment systems, the two organizations can detect fraud in the process of customer account authentication and protect their accounts. Medical facilities that manage healthcare data like hospitals have an opportunity to implement such authentication procedures to improve the access control procedures and prevent data breaches of patient information.
- The AI-based password authentication ensures the protection of student information and academic assets including intellectual property in learning institutions.
- The security models that AI technology can create will be able to help the government institutions and defense organizations to safeguard key national security data.

5.2. Value of the Research

The cybersecurity of the future is also boosted by this research, with its authentication systems becoming more precise and producing fewer false password alarms. To support the capability of resistance against brute-force attack, credential stuffing, and AI-based hacking, the system uses AI to cluster user passwords and build an understanding of their behavior. The present research opens up new opportunities in the development of AI authentication and thus enhances the level of security in the sectors that use password-based systems. The research design proves the possibility of introducing multi-factor authentication (MFA), which helps to improve the defenses of digital security systems against emerging cyber threats.

5.3. Advantages of AI in Enhancing Authentication Security

As stated in the paper, the primary benefits of the adoption of AI techniques to strengthen authentication tools and improve the assessment of the identity of individuals are as follows:

- AI analyzes massive data quantities to detect irregular patterns within login attempts, enabling it to identify unauthorized entry attempts.
- AI utilizes the study of standard user behavior to recognize abnormal patterns during login, which signifies compromised accounts, thus providing extra security measures.
- AI systems monitor security threats in real time, enabling them to modify security protocols and provide agile protection solutions.

5.4. Disadvantages and Challenges

This section deals with restrictions, risk, and issues related to the introduction of the proposed AI-based authentication system. The following problems are outlined:

- AI-based security systems are costly due to high-cost entry barriers, including expensive technological equipment, on top of a highly trained workforce, which is often beyond the reach of small-scale organizations.
- It is hard to comprehend the inner workings of the decision-making process of AI algorithms, including deep learning models, as they are a black box. There is also little transparency of operators which lead to lack of trust and accountability.
- AI-designed attacks enable the attacker to create sophisticated strategies in their cyber-attack using dynamic malware that responds to existing security mechanisms.

5.5. Future Trends

The use of AI authentication security systems will improve the incorporation of AI technology to establish more identity-like and environment-sensitive security measures. The ability to control the benefits of AI and its risks and ethical implications will determine whether successful security systems will be implemented. With the presence of quantum computing, there are high risks to new cryptographic systems. The current RSA and ECC encryption techniques are highly dependent on the classical computers that have made substantial strides in factoring large prime numbers, and they cannot have any practical solutions within a reasonable time. The conventional security system is now obsolete due to the emergence of quantum algorithms. In particular, the algorithm developed by Shor can decrypt encrypted data in a matter of seconds.

The use of AI-driven methodologies to analyze the patterns of passwords and execute centroid-based analysis has taken the level of authentication security to another level, offering high security to the digital assets. In order to realize the full potential of asset security, it is imperative to eliminate challenges that come with these emerging strategies.

6. Conclusion

The findings of this test indicate that with the CP algorithm, the valid password of a user can be selected with an efficiency of 68.88 percent. Although this result is encouraging, the fact that there are 89 false positives among 286 instances of checks confirms one of the significant weaknesses of the given machine; nevertheless, it still identifies an unauthorized password in approximately 31.12 cases. Such fake positives may be a security threat: An attacker may use them in case the password generated coincidentally matches the centroid profile of passwords. To improve the accuracy, destiny studies must acknowledge the necessity to decrease the level of popularity of fake passwords by improving the password centroid generation algorithm. Virtual authentication by use of passwords can be supplemented with one of the techniques: time-based virtual behavior assessment, keystroke dynamics, or device fingerprinting. Furthermore, the accuracy should be improved with the incorporation of the device analysis models that would be tuned to the consumer-specific password adoption patterns. With the use of similarity measures, anomaly detection strategies, and layered security mechanisms, this work was able to reduce false positives thus improving the reliability of authentication. Simultaneously, since the CP set of policies demonstrates itself to be promising in terms of finding legitimate clients with the help of password profiles alone, developing it further is vital to ensure a greater level of accuracy and protection against the existing AI-based assaults.

Acknowledgments

The University of Buraimi, Research, Innovation and Entrepreneurship Unit supported and funded this work according to the research publication policy IRG/UoB/xxxx-/2024-25.

References:

[1]. Wen, S. F., Shukla, A., & Katt, B. (2025). Artificial intelligence for system security assurance: A systematic literature review. *International Journal of Information Security*, *24*(1), 43. Doi: 10.1007/s10207-024-00959-0.

[2]. Ajayi, A. J., et al. (2025). *The impact of artificial intelligence on cyber security in digital currency transactions.* SSRN.

[3]. Ouamri, M. A., et al. (2025). A comprehensive survey on software-defined wide area network (SD-WAN): principles, opportunities and future challenges. *The Journal of Supercomputing*, *81*(1), 291. Doi: 10.1007/s11227-024-06718-1

[4]. Chawki, M. (2025). Social Engineering in the Era of AI: Unmasking the Changing Face of Cyber Threats. *Cybercrime Unveiled: Technologies for Analysing Legal Complexity*, 1-24. Doi: 10.1007/978-3-031-80557-8_1.

[5]. Hasan, S. S. U., et al. (2025). A Review on Secure Authentication Mechanisms for Mobile Security. *Sensors*, *25*(3), 700. Doi: 10.3390/s25030700.

[6]. Jubur, M., Shrestha, P., & Saxena, N. (2025). An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools. *ACM Computing Surveys*, *57*(5), 1-32. Doi: 10.1145/3711117.

[7]. Adalıoğlu, İ., & Ergün, M. (2025). Empirical Insights into Centroid Optimization in Transportation Planning: A Novel Approach. *Transportation Research Record*. Doi: 10.1177/03611981241308866.

[8]. Djenouri, Y., et al. (2025). Next-Gen Metaverse Security Through Intrusion Detection Enhanced by Transformers and GANs. *IEEE Internet of Things Journal*. Doi: 10.1109/JIOT.2025.3545803.

[9]. Asija, D., & Viral, R. K. (2025). Cyber security: Emerging trends best practices. *Cyber Security Solutions for Protecting and Building the Future Smart Grid*, 161-187. Doi: 10.1016/B978-0-443-14066-2.00011-6.

[10]. Ejjami, R. (2024). Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. *Journal of Next-Generation Research 5.0*. Doi: 10.70792/jngr5.0.v1i1.5.

[11]. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. Doi: 10.1016/j.inffus.2023.101804.

[12]. Raju, N. V. D. S. S. V., & Devi, P. N. (2024). A comparative analysis of machine learning algorithms for big data applications in predictive analytics. *International Journal of Scientific Research and Management (IJSRM)*, *12*(10), 1608-1630. Doi: 10.18535/ijsrm/v12i10.ec09.

[13]. Jamarani, A., et al. (2024). Big data and predictive analytics: A systematic review of applications. *Artificial Intelligence Review*, *57*(7), 176. Doi: 10.1007/s10462-024-10811-5.

[14]. Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. *Applied Sciences*, *13*(12), 7082. Doi: 10.3390/app13127082.

[15]. Aslan, Ö., et al. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333. Doi: 10.3390/electronics12061333.

[16]. Hasan, M. K., et al. (2022). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET communications*, *16*(5), 421-432. Doi: 10.1049/cmu2.12301.

[17]. Shakir, M. (2025). Enhancing User Differentiation in the Electronic Personal Synthesis Behavior (EPSBV01) Algorithm by Adopting the Time Series Analysis. *Emerging Science Journal*, *9*(1), 243–260. Doi: 10.28991/ESJ-2025-09-01-014.

[18]. Okoye, C. C., et al. (2024). Securing financial data storage: A review of cybersecurity challenges and solutions. *International Journal of Science and Research Archive*, *11*(1), 1968-1983. Doi: 10.30574/ijsra.2024.11.1.0267.

[19]. Shannaq, B. (2025). A Novel Algorithm for Differentiating Authorized Users from Fraudsters via Mobile Keypad Input Patterns During Password Updates. *TEM Journal*, *14*(1), 768-778. Doi: 10.18421/TEM141-68.

[20]. Alshar'e, M., et al. (2024). Assessing blockchain's role in healthcare security: a comprehensive review. *Informatica*, *48*(22). Doi: 10.31449/inf.v48i22.6155.

[21]. Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741-759. Doi: 10.1007/s10207-019-00429-y.

[22]. Qin, S., et al. (2025). Practical and veritable threshold multi-factor authentication for mobile devices. *The Computer Journal*, *68*(7), 749-762. Doi: 10.1093/comjnl/bxaf001

[23]. Burton, S. L. (2025). Advancing cybersecurity: Strategic insights into multifactor authentication. *Organizational Readiness and Research: Security, Management, and Decision Making*, 247-282. Doi: 10.4018/979-8-3693-8562-3.ch008.

[24]. George, S. (2025). Artificial Intelligence-Powered Cybersecurity: The Future of How Threats Are Detected and Responded. *Leveraging Large Language Models for Quantum-Aware Cybersecurity*, 247-276. Doi: 10.4018/979-8-3373-1102-9.ch008

[25]. Verma, S. (2025). Harnessing the Strength of Digital Technologies for Cybersecurity. *Cases on Security, Safety, and Risk Management*, 1-20. IGI Global. Doi: 10.4018/979-8-3693-2675-6.ch001.

[26]. Cherekar, R. (2025). Comparative Analysis of Password Alternatives for Enterprise Authentication: A Case Study. *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, 1-8. Doi: 10.1109/ICAIC63015.2025.10849146

[27]. Binbeshr, F., et al. (2025). A systematic review of graphical password methods resistant to shoulder-surfing attacks. *International Journal of Information Security*, *24*(1), 46. Doi: 10.1007/s10207-024-00956-3.

[28]. He, D., et al. (2025). *Evaluating the impact of special characters on password security: A comparative analysis.* IEEE Network. Doi: 10.1109/MNET.2025.3540319.

[29]. Sasikumar, K., & Nagarajan, S. (2025). Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques. *IEEE Open Journal of the Computer Society*. Doi: 10.1109/OJCS.2025.3538557

[30]. Alshar'e, M., et al. (2022). A face recognition method in machine learning (ml) for enhancing security in smart home. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 1081-1086. Doi: 10.1109/ICACITE53722.2022.9823833.

[31]. Pendharkar, S., et al. (2024). *Password strength analysis: A survey.* School of Computer Science and Engineering, Vellore Institute of Technology. Doi: 10.55041/IJSREM17298.

[32]. Sui, Y., Zou, X., & Du, E. Y. (2011). Biometrics-based authentication: A new approach. *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, 1-6. Doi: 10.1109/ICCCN.2011.6005767.

[33]. Juozapavičius, A., et al. (2022). Age and gender impact on password hygiene. *Applied Sciences*, *12*(2), 894. Doi: 10.3390/app12020894.

[34]. Chanda, K. (2016). Password security: an analysis of password strengths and vulnerabilities. *International Journal of Computer Network and Information Security*, *8*(7), 23. Doi: 10.5815/ijcnis.2016.07.04.

[35]. Dell'Amico, M., Michiardi, P., & Roudier, Y. (2010). Password strength: An empirical analysis. *2010 Proceedings IEEE INFOCOM*, 1-9. Doi: 10.1109/INFCOM.2010.5461951.

[36]. Guo, Y., & Zhang, Z. (2018). LPSE: Lightweight password-strength estimation for password meters. *computers & security*, *73*, 507-518. Doi: 10.1016/j.cose.2017.07.012.

[37]. Pirzado, F., et al. (2021). Keystroke dynamics Based Technique to Enhance the Security in Smart Devices: Keystroke dynamics Based Technique to Enhance the Security in Smart Devices. *KIET Journal of Computing and Information Sciences*, *4*(1), 14-14. Doi: 10.51153/kjcis.v4i1.61.

[38]. Mahdi, B. S., Hadi, M. J., & Abbas, A. R. (2022). Intelligent security model for password generation and estimation using hand gesture features. *Big Data and Cognitive Computing*, *6*(4), 116. Doi: 10.3390/bdcc6040116.

[39]. Khodadadi, T., et al. (2015). Security analysis method of recognition-based graphical password. *Jurnal Teknologi (Sciences & Engineering)*, *72*(5). Doi: 10.11113/jt.v72.3941.

[40]. Han, J. (2024). Cnn-based multi-factor authentication system for mobile devices using faces and passwords. *Applied Sciences*, *14*(12), 5019. Doi: 10.3390/app14125019.

[41]. Aziz, E. F., & Baker, M. R. (2024). Enhancing Multi-Class Password Strength Prediction Through Machine Learning and Ensemble Techniques. *International Journal of Safety & Security Engineering*, *14*(5). Doi: 10.18280/ijsse.140530.

[42]. He, Y., Alem, E. E., & Wang, W. (2020). Hybritus: a password strength checker by ensemble learning from the query feedbacks of websites. *Frontiers of Computer Science*, *14*(3), 143802. Doi: 10.1007/s11704-019-7342-y.

[43]. Oti, E. U., et al. (2021). Comprehensive review of K-Means clustering algorithms. *criterion*, *12*(08), 22-23. Doi: 10.31695/IJASRE.2021.34050.

[44]. Ghosh, S., & Dubey, S. K. (2013). Comparative analysis of k-means and fuzzy c-means algorithms. *International Journal of Advanced Computer Science and Applications*, *4*(4). Doi: 10.14569/IJACSA.2013.040406.

[45]. Hatzivasilis, G. (2017). Password-hashing status. *Cryptography*, *1*(2), 10. Doi: 10.3390/cryptography1020010.

[46]. Hong, K. H., & Lee, B. M. (2022). A deep learning-based password security evaluation model. Applied Sciences, 12(5), 2404. Doi: 10.3390/app12052404.

[47]. Gewida, M., & Qu, Y. (2025). Enhancing IoT Security: Predicting Password Vulnerability and Providing Dynamic Recommendations using Machine Learning and Large Language Models. *European Journal of Electrical Engineering and Computer Science*, *9*(1), 8-16. Doi: 10.24018/ejece.2025.9.1.666.

[48]. Zhang, T., et al. (2025). Graph guided local structure propagation for tensorial multi-view subspace clustering. *Intelligent Data Analysis*. Doi: 10.1177/1088467X251315633

[49]. Shannaq, B. (2025). Advancing User Authentication in Cloud Computing: Automated Smart Application as a Multi-Factor Approach Beyond Extended-Levenshtein Distance. *TEM Journal*, *14*(2), 1140-1151. Doi: 10.18421/TEM142-15.

[50]. Raja, R. S. (2025). A Metric for Measuring Distances Between Attack Trees in Cybersecurity. *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, 1-16. Doi: 10.1109/ICAIC63015.2025.10848941.

[51]. 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*, *19*(9). Doi: 10.3991/ijim.v19i09.53793.

[52]. Kumar, N. V., et al. (2025). Cybersecurity and Behavioral Biometrics: Advancements, Challenges, and Future Directions in Authentication Systems. *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, 898-903. Doi: 10.1109/ICCCIT62592.2025.10928063.

[53]. Matzen, A., et al. (2025). Challenges and Potential Improvements for Passkey Adoption—A Literature Review with a User-Centric Perspective. *Applied Sciences*, *15*(8), 4414. Doi: 10.3390/app15084414

[54]. Büttner, A., & Gruschka, N. (2025). Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication. *arXiv preprint arXiv:2501.07380*. Doi: 10.48550/arXiv.2501.07380.

[55]. George, A. S. (2024). The dawn of passkeys: Evaluating a passwordless future. *Partners Universal Innovative Research Publication*, *2*(1), 202-220. Doi: 10.5281/zenodo.10697886

[56]. Yusop, M. I. M., et al. (2025). Advancing passwordless authentication: A systematic review of methods, challenges, and future directions for secure user identity. *IEEE Access*, *13*, 13919–13943. Doi: 10.1109/ACCESS.2025.3528960.