Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 9, No. 1, February, 2025

Enhancing User Differentiation in the Electronic Personal Synthesis Behavior (EPSBV01) Algorithm by Adopting the Time Series Analysis

Mohanaad Shakir [1*]

[1] *Management Information System (MIS), College of Business (CoB), University of Buraimi (UoB), Buraimi, Oman.*

Abstract

The progress of contemporary technology has rendered information systems essential in our everyday existence, underscoring the crucial necessity to safeguard information security and privacy. In password authentication, the Electronic Personal Synthesis Behaviour (EPSB) heightens the accuracy of authorizing an authenticated user based on three parameters: $EPSB_{ERROR}$, $EPSB_{Time}$, and $EPSB_{Style}$. $EPSB_{Time}$ suffers from a lack of indicators associated with the legitimate user; containing only six indicators, there arose the need to adopt methods for generating additional reliable indicators by analyzing old indicators and generating new indicators related to the legitimate user. Therefore, this study aims to test the impact of adopting time series analysis in the EPSB time indicator on improving the differentiation of user legitimacy in the case of password-stolen attacks. The research methodology, which involves analyzing and evaluating existing authentication methods in web-based systems, is a key component of this study. The study is divided into stages, with the first phase focusing on enhancing the existing EPSB model, the second phase implementing $EPSB_{algorithmV01}$, and the final stage ensuring validation. Thus, two preliminary experiments were conducted with 22 users from January 13 to February 1, 2024. The final phase involved comparing EPSBV01's accuracy in determining unauthorized users before and after using the ARIMA method. Thus, the $EPSB_{V01}$ algorithm successfully identified 17 unauthorized users during a stolen password attack simulation, outperforming the normal EPSB by 22.73%.

Keywords:

Authentication; Intelligent Authentication;
EPSB; ARIMA; MFA;
Time Series Analysis;
Cybersecurity; AI;
Stolen Password Attack;
Implicit Authentication;
Human Behavior Recognition.

Article History:

Received:	02	October	2024
Revised:	11	December	2024
Accepted:	17	January	2025
Published:	01	February	2025

1- Introduction

Intelligent authentication is one of the modern trends in information technology, providing a higher level of authentication than traditional methods like password use [1]. Many researchers have proposed various Intelligent authentication methods that rely on building systems capable of learning from user behavior, and the EPSB algorithm is one of them [2-4]. The EPSB algorithm works by identifying user behavior based on recording legitimate user data, storing it, analyzing it, and deriving indicators associated with the legitimate user in order to distinguish them from an unauthorized user in the event of stolen password attack [5]. The Electronic Personal Synthesis Behavior (EPSB) heightens the accuracy of authorizing an authenticated user based on three parameters - $EPSB_{ERROR}$, $EPSB_{Time}$, and $EPSB_{Style}$ [5, 6].

The $EPSB_{algorithm}$ (Electronic Personal Synthesis Behavior) algorithm integrates a duration index from analyzing a user's historical data. The $EPSB_{algorithm}$ is introduced to fortify the authorization layer during password theft by scrutinizing the user's historical behavior with the password [5]. In the $EPSB_{algorithm}$, analyzing user historical data is pivotal via employing the Confidence Range (CR) function, which integrates median, mean, and mode equations to define crucial reference points for distinguishing authorized users from unauthorized ones [5, 6]. $EPSB_{Time}$ suffers from

* **CONTACT**: mohanaad.t@uob.edu.om; mohanaadshakir@gmail.com

DOI: http://dx.doi.org/10.28991/ESJ-2025-09-01-014

a lack of indicators associated with the legitimate user, containing only six indicators. The researcher in this study pointed out the need for future development of this indicator to improve its performance during the authorization process. Since the acceptance rate when comparing the behavior of the user attempting to log in with the historical data of the legitimate user is at least 60%, there arose the need to adopt methods for generating additional reliable indicators related to the legitimate user [5]. Many established equations use available data for future prediction, and one of the commonly used methods is Time Series Analysis.

Time series prediction uses models applied to past observation data to predict future values [7]. Regression analysis, however practical it is in determining relationships between different time series, isn't usually designated as a form of "time series" (i.e., within the exact timetable) analysis [8]. This also suggests predicting future probabilities for any variable from historical data. As for processing historical data, Shakir [5] and Shakir et al. [6] proposed that the EPSB algorithm can improve user authentication according to specific conditions. EPSB incorporates a duration index based on analyzing the user's historical data to improve differentiation between legal and illegal users. Data about how long the user typed in their password, what type of method they used to select it (either graphic or random), and standard errors are stored by EPSB-algorithm enforced authorization layer against obtaining stolen passwords. In this paper, we introduce a time series analysis equation, which enhances the outcomes generated by the previously mentioned functions in $EPSB_{Time}$. This augmentation yields fresh data points that serve as distinctive markers for authorized users. The enhancements made to the EPSB algorithm greatly boost its ability to discriminate and improve its security capability. We will prioritize comprehending their execution and assessing their efficacy in protecting sensitive data inside modern information systems. Therefore, this study aims to test the impact of adopting time series analysis in the EPSB time indicator on improving the differentiation of user legitimacy in the case of a password-stolen attack (PSA).In addition, time series analysis is still not widely used in information systems, particularly in authorization systems, despite being widely used in many different fields. The main objective of this paper is to employ time series analysis to improve the precision of differentiating authorized users from unauthorized ones. This study will examine and evaluate the feasibility of combining time series analysis with EPSB to enhance the precision of recognizing authorized users in information systems when faced with a password-stolen attack (PSA).

2- Literature Review

A number of papers and case studies have been published in the field of the authentication of information systems. A comprehensive study of single-factor and multi-factor validation systems, and especially the requirements of the human user's memory, was performed [9-12]. The effectiveness of graphical passwords was developed in an empirical cycle study in the laboratory focusing on usability and security, conducted for a large number of users with a variety of websites. Improvements to machine heuristics were described [13, 14]. An automatic method for face recognition was presented, using unique features that appear during the presentation of different expressions as the expression-based face [15, 16].

Passwords have been and still are the most widely used security method in the context of computer systems and network applications [17]. This situation has resulted in a great focus on the development and implementation of intelligent authentication systems [18]. These systems try to address either the weaknesses of password-based systems or offer an alternative security credential that is independent of the password [19]. Intelligent authentication systems are complex and involve related issues, such as unimodal, multimodal, and multi-channel design methodologies; the use of techniques based on the field of biometrics; and the application of machine learning in developing these systems [20]. There are numerous studies that provide different perspectives on the aforementioned research, conceptual frameworks, and contributions in the field of biometric authentication [21-23]. These include the construction of a conceptual framework to investigate the usability aspects of user authentication and the user-friendly support for the design and application of user-centered principles in authentication systems, as well as the background and motivation to explore the various methodologies used in the development of intelligent authentication systems [24, 25].

Many studies have focused on intelligent authorization in information systems. Chen et al. conducted one of these studies in 2021. This research has shown advancements in biometric multi-factor authentication (MFA) systems, which combine fingerprint, facial, and iris recognition technologies with other traditional authentication methods. This layered approach effectively increases security by adding biometric uniqueness to traditional MFA systems [26]. In addition, Kim & Park (2022) suggest authentication methods for behavioral biometrics. Intelligent authentication involves the use of behavioral biometrics, such as keystroke dynamics, mouse movements, and touchscreen gestures [27]. These systems record and assess distinctive user behavioral patterns in real time, complicating the replication of these patterns by attackers. Research indicates that behavioral biometrics might decrease false-positive rates when used with machine learning techniques. Context-aware authentication systems assess parameters such as location, time, and device attributes to determine the probability of an access request being valid. An authentication attempt from a new geographical coordinate or that is made at a time considered incongruous by the system may require further authentications. This technique, called context-aware authentication, where AI is applied for contextual analysis, has been shown to lower the attempts of unauthorized access [28].

In continuous authentication, which is different from the login authentication, the user's identity is checked over and over again in the activity session; aspects such as typing rhythm, pressure on the screen, and gaze follow [29, 30]. Patel et al. [31] proved that extending the rate of standard continuous authentication can minimize session hijacking, especially in the highest-risk setting. In a related context, face recognition has improved due to deep learning and may be used as a primary or secondary form of biometrics. CNN improves face recognition in different lighting conditions and view angles, which are important aspects for successful user identification [32]. However, different strategies, such as the utilization of deep neural networks (DNNs) to control background noise, have increased reliability in the application of voice recognition systems under adverse situations. Noise robustness facilitates precise voice authentication in difficult conditions, including crowded or loud settings [33]. In addition, blockchain technology offers a decentralized authentication framework that diminishes reliance on a singular authority and bolsters data security. The blockchain's immutability safeguards authentication records against manipulation, providing a secure and verifiable record of access occurrences [29]. Studies demonstrate that blockchain is particularly beneficial for systems necessitating transparency and robust security [34].

2-1- Intelligent Authentication

Intelligent authentication methods utilize advanced techniques, including biometrics, machine learning, and artificial intelligence, to enhance the accuracy and strength of authentication systems [35]. Technological advancements have made traditional authentication methods, such as passwords and personal identification numbers (PINs), vulnerable to security breaches [36]. Modern solutions for authentication, such as OneSpan and Zighra, rely on detecting unusual usage patterns [37]. However, these solutions offer limited opportunities to track behavioral record changes resulting from user habit shifts [37]. Consequently, users may be required to update their profiles, which can be inconvenient regularly [38]. A practical method to enhance the accuracy of access control systems (ACS) involves contextual information analysis through monitoring user interactions with applications and physical activities [39]. These make it challenging for intruders to manipulate data extracted from contextual sources, reducing the effectiveness of spoofing attempts [40]. Examples of context-based ACS solutions include Secured Touch (acquired by Ping Identity [41]), Samsung HYPR [42], NuData Security, and TwoSense.AI [43]. These systems enable continuous tracking of behavior-related features and contextual information, such as the user's location using banking applications. Despite the precision and anti-spoofing strength of the authentication process, there may be better solutions for users with concerns about privacy violations, account resource consumption, and high battery usage [44-46]. To avoid these problems, Mahanaad proposes the $EPSB_{algorithm}$ (Electronic Personal Synthesis Behavior) model [6]. This algorithm stores the user's behavior when interacting with the password and the password for authentication purposes. This method is cost-effective as it does not require any physical additions. It is also easy to implement and requires no training.

The EPSB algorithm uses three essential factors to increase the accuracy of discriminating between authorized and unauthorized users: EPSBStyle, EPSBTime, and EPSBError. These variables take into account user behavior in password-choosing style, time required to enter a password, and real user mistakes while inputting a password. The results are sent to EPSBDecision to grant or deny system access. The algorithm records the activities of legitimate users in these variables and generates a confidence range for the user associated with the password during the legitimate user verification process upon system entry. Confidence Range (CR) is defined as a set of points recorded based on actual user behavior, such as the user's nature in choosing the password, common mistakes made by the user, and the user's speed in typing the password. EPSBTime records and analyzes historical data related to the time it takes for a legitimate user to enter a password into the system. It generates confidence ranges for the shortest and most prolonged time they need to deal with the password for system access. With reference to a valid password, EPSBalgorithm produces 45 confidence range points for real users, which are concurrently scrutinized with the username and password by EPSBDecision to grant or deny a real user access to the system [5]. However, like many other indicators, EPSBTime has less success in experimental tests than other indexes do. This research focuses on the time series analysis in order to identify new confidence points that were founded in past and present data so as to compare test results to previous ones.

Time Series Analysis is a statistical and mathematical approach that examines data gathered over a given time period to identify patterns, trends, and probable forecasts [47]. It is critical in predicting future trends and identifying hidden elements that influence the dataset. Approaches such as regression, variance analysis, time series transformation, and dynamic regression analysis help the study provide a longitudinal view of the flow of events within the data-gathering period and the estimation of similar values within the future periods. It is commonly used in fields like economics, meteorology, loaning, wellbeing, data sciences, etc. [48]. The advantages of using time series include the identification of long-term trends, clarification of temporal correlations, and future trends. This has made a major contribution to the anticipation of future economic incidences as well as the identification of variables to the level of economic development. When applied in economic studies, time series will produce accurate models for forecasting economic variables. Time-related variables incorporate Moving Average Model, Dynamic Regression Model, Autoregressive Conditional Heteroskedasticity (ARCH), Fourier, Autoregressive Integrated Moving Average (ARIMA) [49-52]. This kind of model is preferable for economics, weather forecasting, and financial time series data prediction. This work extended the EPSB algorithm to incorporate the ARIMA model within it, incorporating CR outputs as new inputs into the algorithm, and was successfully designed to enhance the system performance of detecting unauthorized users in stolen password attacks.

2-2- Password Stolen Attacks (PSA)

One of the most fundamental threats that can befall a user's accounts is the scenario in which an adversary gains direct access to a user's login credentials, particularly the password [53]. This can be accomplished through several well-known online and offline attacks, including client-side malware, phishing via a spoofed website, and eavesdropping on password transmission [54]. The implementation of these attack methods can result in the compromise of a user's account for a particular site, as well as any associated personal information. According to Pallivalappil & Jagadeesha [55], Facebook experienced an estimated 272 million stolen password attacks in just one month. However, in recent years, various defenses against this threat have emerged. This includes the utilization of multi-factor authentication, such as SMS, Smartcard, and Biometric, in addition to a password [56]. Nevertheless, there are limitations to these models due to the additional hardware required for their implementation, which can become expensive if an entire organization opts to use this feature for user authentication. Furthermore, if both the user's authentication factor and password are stolen simultaneously, there is no way to prevent an attacker from impersonating the user. In a related context, many researchers are advocating for the incorporation of behavior recognition as an authenticating factor alongside the password during the authentication process [2]. Consequently, in this study, we have chosen behavior recognition, especially EPSB combined with a password, to enhance the accuracy in authenticating an authorized user when facing a stolen password attack. I constructed my research assumptions based on a password-stolen attack. In this study, all experimental procedures were developed around the assumption that an intruder has obtained an active password and is attempting to access the system remotely.

3- Research Methodology

In this section, a literature review has been conducted to identify the business intelligence challenges of authenticated users. These questions are relevant for both practitioners and the academic world. The question was addressed through the collection of multiple studies that examined the issue of using intelligent user verification and supporting intelligence from user activity measurements. After the detailed literature review carried out in Section 2, some findings were obtained, followed by a broad discussion. At the end of the paper, the final remarks are shared. Section 3 consists of three parts: Explain a new $EPSB_{Timev01}$ structure, Implement the new $EPSB_{Timev01}$ in $EPSB_{Algorithmv01}$, and $EPSB_{TimeV01}$ Experimental and Evaluation.

The research methodology is formulated in accordance with the study objectives. The researcher will gather and analyze cutting-edge findings and evaluate the advantages and disadvantages of the existing authentication methods in web-based systems. The research project is segmented into multiple stages, as depicted in Figure 1, in order to accomplish the stated objectives. Therefore, critiques and flaws of the current methods clearly highlight the problem in the initial stage. During the second phase, our objective is to enhance the existing EPSB model and execute the proposed solution.

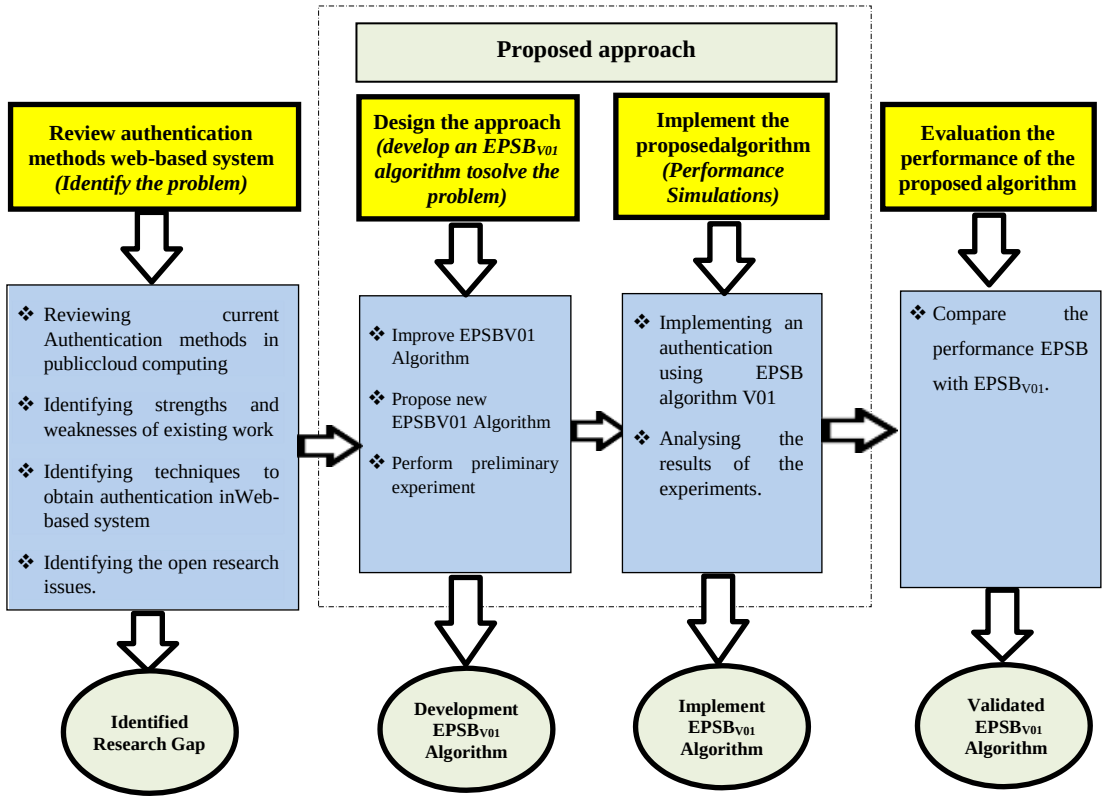

Figure 1. Research Methodology

The $EPSB_{algorithmV01}$ will be implemented on a specific sample of users, comprising 45 persons, for a duration of ten days. During this phase, the sample will employ $EPSB_{algorithmV01}$. Subsequently, tests will be conducted based on several scenarios and hypotheses, assuming the system intruder possesses an effective password. The system's ability to differentiate between legitimate and illegitimate users will be evaluated when the unauthorized user has an effective password, focusing on both users' speed of password entry. In the last stage, we will examine the final results to ensure the validation. This $EPSB_{algorithmv01}$ validation method was computed based on a comparison of the ability of the $EPSB_{algorithm}$ and the $EPSB_{algorithmV01}$ to distinguish between legitimate and unauthorized users during stolen password attacks.

4- Results and Discussion

In this section, the researcher will elaborate on the refined components of the EPSB algorithm, which have undergone improvements based on Shakir's initial EPSB algorithm model [5]. The primary objective of $EPSB_{algorithmv01}$ is to enhance accuracy in differentiating between authorized and unauthorized users. This is achieved by utilizing three key variables: $EPSB_{Style}$, $EPSB_{Time}$, and $EPSB_{Error}$. These improvements are meant to stop attacks using stolen passwords by adding confidence range (CR) outputs as new inputs to the ARIMA time series analysis process. This will create new confidence points for the algorithm to consider, allowing for a more precise identification of unauthorized users. Additionally, the refined components of the EPSB algorithm also incorporate machine learning techniques to adapt and continuously improve its accuracy over time. Combining these advancements, the $EPSB_{algorithmv01}$ aims to provide a robust and reliable solution for detecting and preventing unauthorized access attempts (real users). It is worth mentioning that the EPSBDecision Node has not undergone any updates, as it remains structured in the same format as originally designed in the first version of the EPSB. Below are the details of the updates made to the updated EPSBV01. The $EPSB_{Time}$ monitors the time it takes the user to enter their password, looking for any unusual patterns or suspicious behavior. For this investigation, we exclusively utilized the $EPSB_{Time}$ Node for time series analysis. The rationale for this decision is that this node comprises merely six elements, and research has indicated the necessity for enhancement and additional inquiry [5]. Thus, it has been improved, and if its effectiveness is confirmed, it could be implemented in the remaining components of the algorithm in the future. The utilization of the ARIMA time-series analysis approach was considered appropriate for this investigation owing to its capacity to examine data chronologically and discern patterns or trends. The researchers wanted to comprehensively analyze and improve the effectiveness of the EPSBTime Node, which has a restricted number of points. If the findings are successful, they have the potential to facilitate the implementation of these enhancements throughout all components of the EPSB algorithm in future investigations.

4-1- $EPSB_{Timev1}$

This component involves measuring the duration of password input. Its primary function is to generate an $EPSB_{Time}$ using the Confidence Range (CR) for each legitimate user. The ARIMA equation has been integrated with the CR to create new confidence points based on legitimate user behavior. The CRPd (Confidence Range Password Duration) results are obtained by analyzing keystroke speed from password entry until the login key is activated. The Password Duration (Pd) element primarily identifies unauthorized users based on the time duration within the CRPd range. Each time a legitimate user enters their password into the system, a record of how fast they can type on the keyboard is made. If there are fewer than 30 entries, the algorithm estimates a confidence range based on the available figures. However, the algorithm chooses only the last 30 valid, legitimate user activities if the count exceeds 30 and then generates a confidence score. This confidence score is then compared to the CRPd range, which is a predefined threshold for determining whether a user is authorized. The user is considered authorized and granted access if the confidence score falls within the CRPd range. Otherwise, they are flagged as unauthorized and denied access to the system. The keystroke speed analysis helps identify legitimate users and detect potential security breaches. Moreover, the Confidence Range (CR) outputs will be fundamental inputs into the ARIMA time series analysis equation to generate new confidence points (APd - ARIMA Password Duration) for legitimate users. These points will be combined with the CR points and the effective password. The following algorithm outlines the CRPd and APd for $EPSB_{Time}$ (see Figure 2). Finally, CRPd and APd will provide the conclusive outcomes to the decision (D) component for comparison (Table 1). The algorithm and flow chart details are provided by Figure 3.

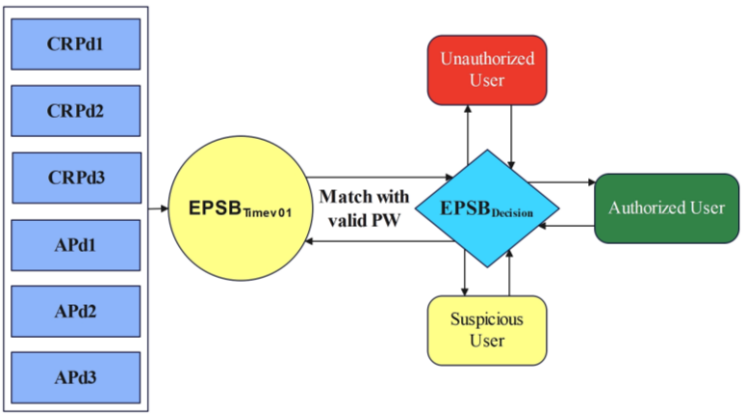

Figure 2. $EPSB_{Timev01}$ Components

Table 1. Electronic Personal Synthesis BehaviorV01 (EPSB)$_{Timev01}$

Algorithm: Electronic Personal Synthesis BehaviorV01 (EPSB)Timev01
Input1: Pd (float) {duration Typed password}, Confidence Range Password duration (CRpd) = CRPd1, CRPd2, CRPd3
Output1, **Input2**: Confidence Range Password Duration (CRPd (1-3))
Output 2: ARIMA Password Duration (APd(1-3))

```
If d start
Do
Count d
While (press enter)
Recorded d
Input 1 : d
Calculate CRPd
d=d+1
if d>30
 ignore old d
Integrated d Value
if d<=30
Output 1: Confidence range (CRPd1, CRPd2, CRPd3)
Input 2: (CRPd1, CRPd2, CRPd3)
Calculate APd1-3
Output 2: ARIMA Password Duration (APd1, APd2, APd3)
Send Output 1,2 to Decision (D)
```

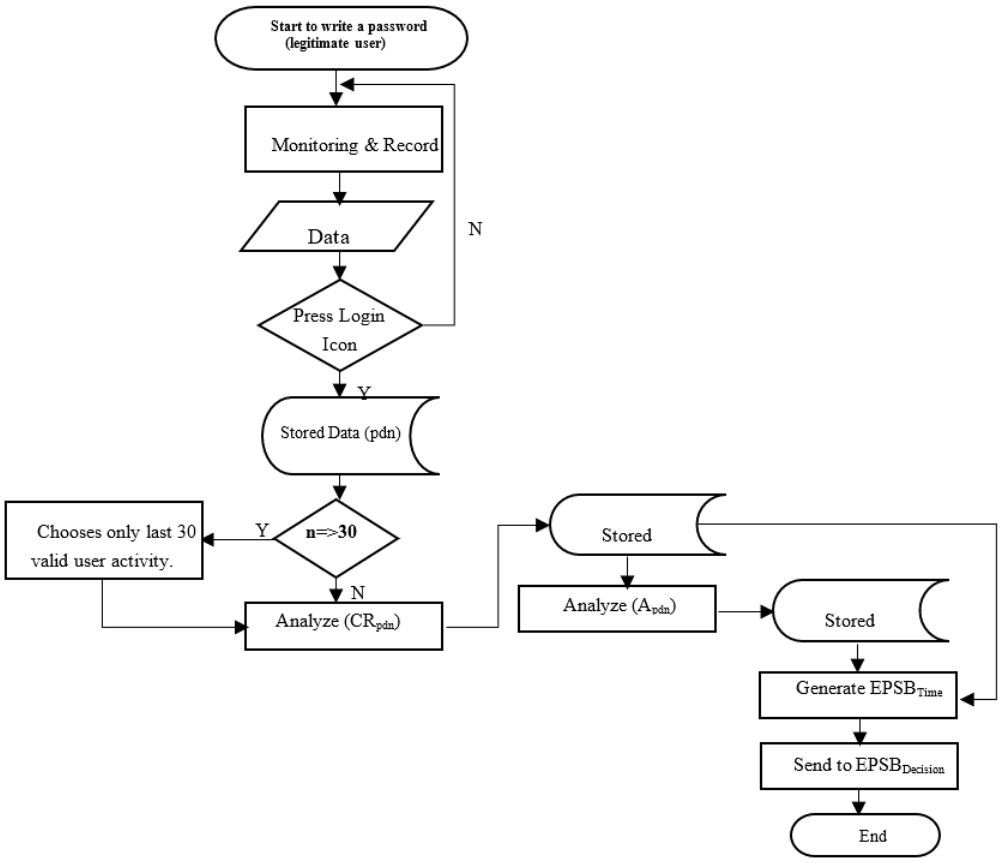

Figure 3. EPSBTimev01 Flowchart

4-2-Implement the EPSB$_{Algorithmv01}$

The execution of this study had three primary phases: establishing authentication with the EPSB algorithm, conducting preliminary experiments, and assessing the outcomes. Initially, the development of authentication utilizing the EPSB$_{algorithmv01}$ was implemented using Python programming. The selection process involved incorporating and verifying these languages for use in the web domain. The algorithm's primary components collaborate to acquire the essential data to construct the confidence range. The technique involved conducting two preliminary experiments for randomly selected consumers. From January 13 to February 1, 2024, 45 users were registered. Ultimately, the final phase governs user conduct, documents all accomplished tasks, conducts statistical analysis on them, and periodically transmits

the statistical analysis findings as inputs to the time series analysis layer incorporated in this research to produce the outcomes forwarded to the decision component. This enables the comparison of the latest outputs with earlier findings in order to ascertain the extent of algorithmic advancement.

The time series analysis layer of this study is essential for producing results for the decision component. Regularly obtaining statistical analysis findings from the previous phase allows for a direct comparison between new outputs and prior results, thus assessing the extent of algorithmic progress made. This iterative method guarantees ongoing enhancement and fine-tuning of the algorithm, taking into account user behavior and completed actions.

4-3- The $EPSB_{Algorithmv01}$ Implementation Scenarios

This research delves into the impact of user behavior on system security within the application, particularly when utilizing the authentication interface. The study presents a scenario to demonstrate the potential application of the $EPSB_{algorithmv01}$ in real-world situations. In this scenario, Alice, a regular user, typically employs her laptop to access the Fin-Tch application through a web-based system. Her efficient login routine involves directly entering her password, which remains consistent daily. However, a security breach unfolds when Alice, momentarily leaving her laptop unattended, becomes susceptible to an unauthorized access attempt by Bob. Bob's exploiting a stolen password (a result of a stolen password attack) underscores the necessity for heightened security measures within the Fin-Tch application. In the aforementioned situations, the nodes are triggered according to the characteristics of the scenario. The effectiveness of the Pd Node is active across all contexts, as it is directly correlated with the user's speed in password entry, which is a consistent action performed by the user in all scenarios (Table 2).

Table 2. Actions between Scenarios and EPSB Components Processes

	EPSB Components Processes			
	Password Time (Pd)	Password Style (PS)	Password Error (Pe)	Decision(D)
Scenarios	Active	Inactive	Inactive	Active

4-4- Implementation of $EPSB_{TimeV01}$ and $EPSB_{Decision}$

The EPSB algorithm is demonstrated through the example of Alice, an employee who uses a password to create a connection with a web-based system. To create $EPSB_{Time}$, careful observation, recording, and analysis of Alice's typical behaviors are necessary. If Alice enters her password correctly and without any changes, the Pd component will function, while the Pe and PS components will not. The Pd component will generate a new $EPSB_{TimeV01}$ based on Alice's actions, as depicted in Table 3. In the following example, we will demonstrate the functionality of $EPSB_{algorithmv01}$ when authorized users use passwords in a web-based system. Suppose that, over some time, data about the authentication behavior of users of web-based services has been gathered. An electronic print has been created for each user as a component called $EPSB_{TimeV01}$, effectively representing the person's usual behavior. In the given scenario, Alice, an employee, usually begins by accessing the web-based system through her user profile page. She uses her password daily. Consequently, she effortlessly inputs her password. The $EPSB_{TimeV01}$ is utilized to observe, document, and analyze the time necessary for Alice to input the password. These procedures aim to create the $EPSB_{TimeV01}$ for Alice, which consists of CRPd1, CRPd2, CRPd3, APd1, APd2, and APd3. Yes. The $EPSB_{TimeV01}$ component is essential for monitoring and analyzing Alice's password-typing behavior. The system can generate an accurate $EPSB_{TimeV01}$ for Alice by measuring the time it takes her to type her password. Subsequently, this data can be utilized to augment the security and usability of the internet-based platform for Alice and other users. The $EPSB_{TimeV01}$ component can provide valuable insights into her typing speed and patterns by analyzing Alice's password-typing behavior. This information can enhance the overall user experience and strengthen the security measures of the internet-based platform for all users. Additionally, the $EPSB_{TimeV01}$ can help identify any potential vulnerabilities or weaknesses in Alice's password input process, allowing for proactive measures to mitigate them.

Table 3. Password Duration (Pd) for Alice

4.332	4.122	4.126	4.225	4.366	4.256	4.111	3.952	3.995	4.023
4.211	4.254	4.126	3.952	4.366	4.261	4.265	3.893	3.858	3.998
4.366	4.352	4.023	4.324	3.896	3.992	3.997	3.899	3.896	4.366

4-5- The $EPSB_{Timev01}$ implementation

The last 30 login attempts for Alice (considered as one user out of 45 users) to access the online application over 18 days are provided in Table 4. Alice's duration to enter the correct password for the system and login is recorded. The algorithm starts recording the duration taken from the beginning of entering the password until pressing the login icon (see Table 3).

The following table and figure illustrate the successive processes that produced the ultimate CR (confidence range) for Alice's endeavors during her engagement with the system. The $EPSB_{algorithmV01}$ measures the duration of Alice's password entry and incorporates this new data into the existing data already recorded by the $EPSB_{algorithmV01}$. This aims to establish a new range of confidence linked to Alice's actions when inputting her password into the web-based system. This range of confidence helps the system determine the likelihood of unauthorized access. By incorporating the duration of Alice's password entry, the algorithm can analyze any variations in her typing speed and patterns, which adds an extra layer of security. This approach allows the system to adapt and update the confidence range password duration (CRPdx) based on Alice's evolving behavior, making it more accurate in detecting potential unauthorized access attempts (Figure 4).

Table 4. Confidence Range (CR) for Alice's

Attempt	Mean	Median	Mode	CRPd1		CRPd2		CRPd3	
				min	max	min	min	max	min
1	4.332	4.332	4.332	4.332	4.332	4.332	4.332	4.332	4.332
2	4.227	4.227	-	4.227	4.332	4.227	4.332	4.332	4.332
3	4.1933	4.126	-	4.1933	4.332	4.126	4.332	4.332	4.332
٤	4.20125	4.1755	-	4.1933	4.332	4.126	4.332	4.332	4.332
5	4.2342	4.225	-	4.1933	4.332	4.126	4.332	4.332	4.332
6	4.23783	4.2405	-	4.1933	4.332	4.126	4.332	4.332	4.332
7	4.22114	4.225	-	4.1933	4.332	4.126	4.332	4.332	4.332
8	4.2075	4.2125	-	4.1933	4.332	4.126	4.332	4.332	4.332
9	4.18722	4.225	-	4.18722	4.332	4.126	4.332	4.332	4.332
10	4.2586	4.2255	-	4.18722	4.332	4.126	4.332	4.332	4.332
11	4.2695	4.225	-	4.18722	4.332	4.126	4.332	4.332	4.332
12	4.2739	4.24825	-	4.18722	4.332	4.126	4.332	4.332	4.332
13	4.2703	4.225	4.126	4.18722	4.332	4.126	4.332	4.126	4.332
14	4.2148	4.20475	4.126, 4.366	4.18722	4.332	4.126	4.332	4.126	4.366
15	4.2302	4.254	4.126, 4.366	4.18722	4.332	4.126	4.332	4.126	4.366
16	4.2693	4.252	4.126, 4.366	4.18722	4.332	4.126	4.332	4.126	4.366
17	4.2634	4.252	4.126, 4.366, 3.952	4.18722	4.332	4.126	4.332	3.952	4.366
18	4.3091	4.255	4.126, 4.366, 3.952	4.18722	4.332	4.126	4.332	3.952	4.366
19	4.3521	4.261	4.126, 4.366, 3.952	4.18722	4.3521	4.126	4.332	3.952	4.366
20	4.3723	4.2405	4.126, 4.366, 3.952	4.18722	4.3723	4.126	4.332	3.952	4.366
21	4.3726	4.2405	4.126, 4.366, 3.952	4.18722	4.3723	4.126	4.332	3.952	4.366
22	4.3588	4.2405	4.126, 4.366, 3.952	4.18722	4.3723	4.126	4.332	3.952	4.366
23	4.013	4.126	4.366	4.013	4.3723	4.126	4.332	3.952	4.366
24	4.151	4.126	4.366	4.013	4.3723	4.126	4.332	3.952	4.366
25	4.0554	4.211	4.366	4.013	4.3723	4.126	4.332	3.952	4.366
26	4.033	4.1685	4.366	4.013	4.3723	4.126	4.332	3.952	4.366
27	4.017	4.211	4.366	4.013	4.3723	4.126	4.332	3.952	4.366
28	4.009	4.1685	4.366	4.009	4.3723	4.126	4.332	3.952	4.366
29	4.003	4.211	4.366	4.003	4.3723	4.126	4.332	3.952	4.366
30	4.0026	4.1685	4.366	4.0026	4.3723	4.126	4.332	3.952	4.366

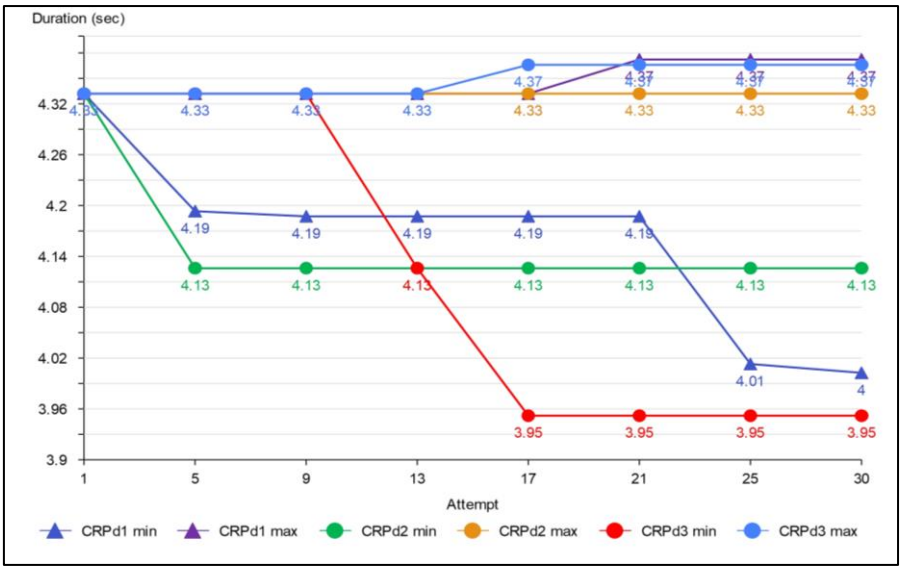

Figure 4. Confidence Range (CR) for Alice's

According to the $EPSB_{algorithmv01}$, the algorithm generates a Confidence Range (CR) based on the input data from the interactions performed by the user with the password, as explained in the Review section. The first range is generated by the Confidence Range Password Duration (CRPdx) for Alice based on the Confidence Range Equation, where the highest value represents the upper limit of the range, and the lowest value represents the lower limit. The values between them represent the green parameters associated with the legitimate user. As shown in Table 5 and Figure 5.

Table 5. Confidence Range Password Duration (CRPdX) for Alice

CRPd1		CRPd2		CRPd3	
min	**max**	**min**	**max**	**min**	**max**
4.0026	4.3723	4.126	4.332	3.952	3.366

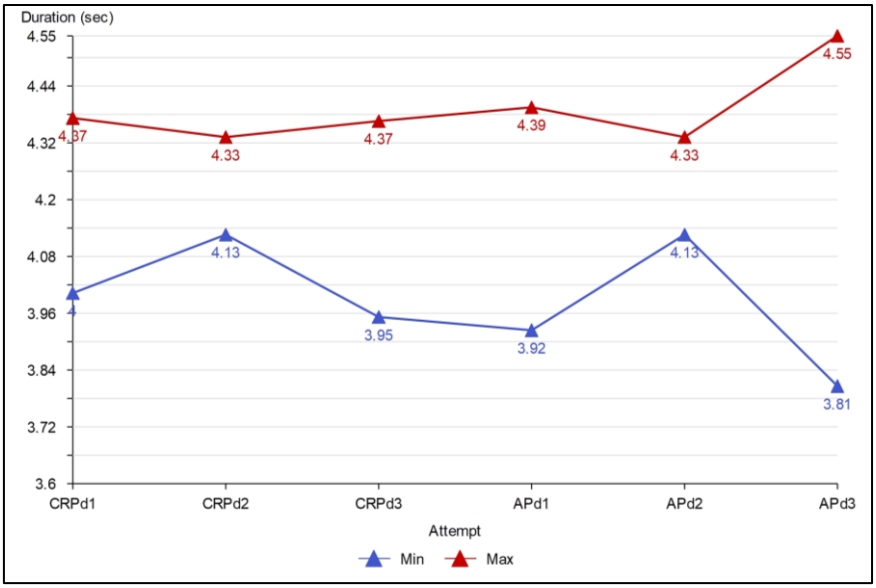

Figure 5. CRPdX & APdX for Alice's

The ARIMA (Auto Regressive Integrated Moving Average) analytical equation was used in this research to generate additional confidence points for the legitimate user, as explained in the study's literature background. The input data for these extra nodes consists of the past thirty confidence ranges generated from a CRPdX at the preceding level of this node. The APdX nodes process the data and produce additional green points (confidence points) linked to Alice's behavior while inputting passwords into the Web-based system. Subsequently, these additional data points are employed to revise the confidence model pertaining to Alice's conduct, enabling more precise authentication determinations. The ARIMA analysis equation incorporates the temporal patterns and trends observed in the previous confidence ranges to produce dependable and pertinent confidence scores for the authorized user As shown in Table 6 and Figure 6.

Table 6. ARIMA Password Duration (APdX) for Alice

APd1		APd2		APd3	
min	**max**	**min**	**max**	**min**	**max**
3.924	4.395	4.126	4.332	3.806	4.546

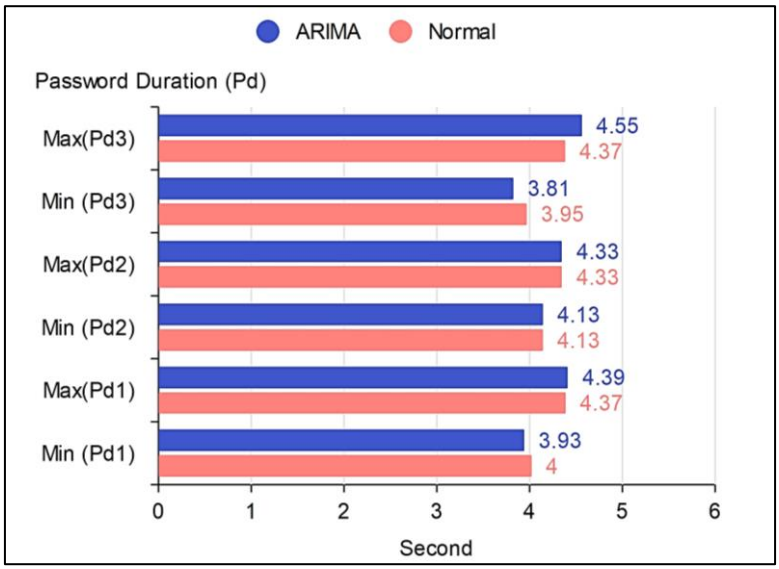

Figure 6. EPSB$_{Timev01}$ Normal vs. ARIMA

4-6- EPSB$_{TimeV01}$ Experimental and Evaluation

In this section, we will compare how well the EPSBV01 determined unauthorized users before and after it started using the adaptation ARIMA method. In a related context, without adopting ARIMA in EPSB$_{Time}$ in the authentication layer, the rate of EPSB algorithm accuracy in determining unauthorized users was 66.66% [5, 57]. Based on the above sections, in this study, we adapted ARIMA in EPSB$_{Timev01}$; thus, we need to examine the accuracy of EPSBV01 in determining unauthorized users after it started using the adaptation ARIMA method. The data collection will be held at the University of Buraimi (UOB) in Oman, where a sample of 22 users will be engaged. It is argued that the purpose of the authentication process is to examine human behavior. The application of behavior recognition techniques will be the approach to mitigating a low impact from stolen password attacks. The secondary metrics are designated to check the security of data with the most target-oriented protection of the web-based systems from unauthorized accessibility by means of passwords. This study lasts for ten days: March 20-30, 2024. The aims of our study are to develop and diagnose all unauthorized users and significantly improve the user authentication process through the adoption of ARMIA in EPSB$_{Time}$.

4.6.1. Experimental Scenario

To evaluate our new algorithm's accuracy, it will be assessed according to the given scenario:

- Alice employs a potent password throughout her system usage. During this interval, the system logs Alice's password entry time to measure her behavior when accessing the system. The program captures and stores all activities associated with each system login. Subsequently, it processes the data about Alice to produce CRPDX and APDX using Node EPSB$_{Timev01}$ for the EPSB$_{algorithmv01}$.
- Bob surveils Alice after acquiring her password via a Stolen Password Attack (SPA). When Alice temporarily leaves her unattended laptop, Bob exploits the opportunity to gain unauthorized access to the system by inputting the correct password. Notably, Alice did not save the password on her personal laptop.
- The algorithm compares Bob's password-related behavior to Alice's Inter-Keystroke EPSBTimingV01 Behavior derived from previous data. It calculates a similarity score that compares the present user behavior with the historical behavior of the authorized user.
- A user is considered legitimate if the match percentage exceeds 60%. The user is categorized as suspicious once the value falls below this level. In such situations, the algorithm initiates security processes by sending a verification notification to the user's email address. If the similarity is above 60%, the decision component (D) will incorporate the EPSB$_{Time}$. Alternatively, if the resemblance falls below 60%, it will activate essential security measures. This technique is utilized to ascertain the most accurate estimated corrected range for generating the EPSB$_{Timev01}$.

4.6.2. Experimental Methodology

The experimental sample size of users tested with the system was 22 users. The above scenario was applied to all of them to compare the results obtained in the current study with the previous study. The purpose of this comparison is to determine the impact of adopting the ARIMA equation on the accuracy of identifying unauthorized users in the experimental sample according to the following stages (see Figure 7).

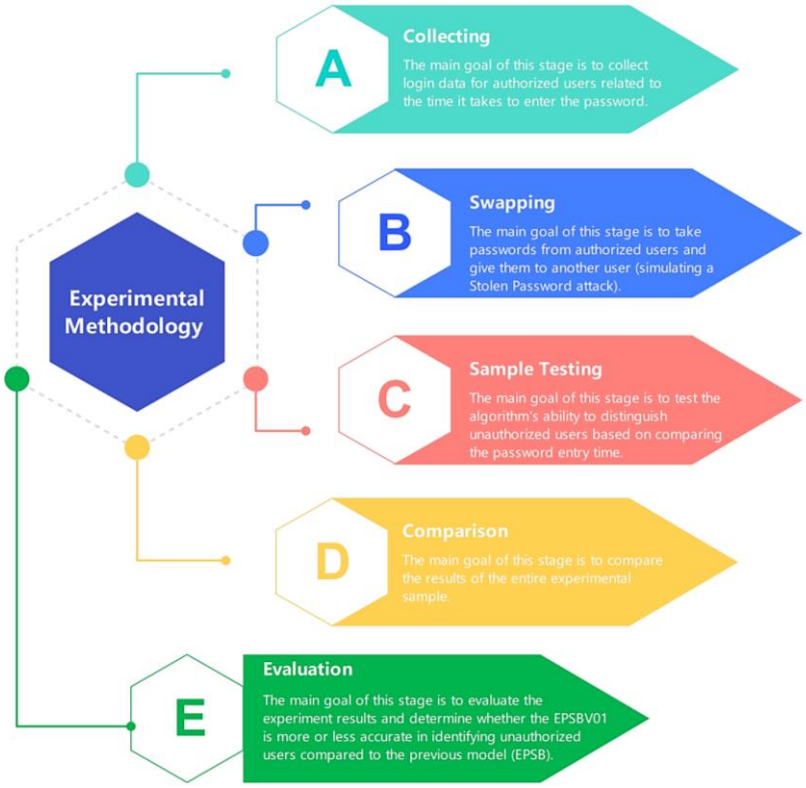

Figure 7. Experimental Methodology

- ***Stage One**: Collecting:*

The main goal of this stage is to collect login data for authorized users related to the time it takes to enter the password. This involves gathering data on the time taken by authorized users to enter the password (from starting to type until pressing the login icon). The algorithm records and documents all activities for each login attempt made by the authorized user throughout the 18-day experiment. The algorithm generates a confidence range (CR) for the time taken and links it as an indicator with the password.

For the study, the experimental setting was based on 22 users who had used the $EPSB_{V01}$ several times or over the course of 18 days by using an effective password. $EPSB_{algorithm}$ the recording and storing of all events and preserved the data, which underwent the automatic procedure of authorization. In each case, the algorithm recorded the time given for password entering and generated a CR, which added an ARIMA model to analyze the inputs made by the users so as to detect parameters related to the user's temporal speed in entering a password. Here, the mean number of login attempts for all participants was 151 login locations during 18 days. The lowest number of user login attempts was 130, and the highest number of user login attempts was 172.

- ***Stage Two**: Swapping:*

Random password swapping in the experimental sample. The main goal of this stage is to take passwords from authorized users and give them to another user (simulating a Stolen Password attack). After the algorithm recorded all events related to authorized users, $EPSB_{Timev01}$ was generated and linked with passwords for 18 days. The experiment supervisor collected all passwords in the sample of authorized users. At this experiment stage, the supervisor simulates a password-stolen attack to test the algorithm's ability to mitigate the effects of this attack. The supervisor gives or changes each user's password to another user based on the assumption that the other user obtained the password through a password-stolen attack.

- ***Stage Three**: Sample Testing:*

In this stage, each user in the experimental sample attempts to log into the system using another user's password (like an unauthorized user when logging in via an active password). The main goal of this stage is to test the algorithm's ability

to distinguish unauthorized users based on comparing the password entry time for the unauthorized user with the password and confidence Range (CR) for the authorized user, which was determined in the first stage.

- ***Stage Four**: Comparison:*

The main goal of this stage is to compare the results of the entire experimental sample, which consists of 22 samples, and determine the number of samples identified by the EPSBV01 as unauthorized users, comparing it with previous studies.

- ***Stage Five**: Evaluation:*

The main goal of this stage is to evaluate the experiment results and determine whether the EPSBV01 is more or less accurate in identifying unauthorized users compared to the previous model (EPSB).

5- Discussion

Regarding stage one (Collecting), the authorized user employed the efficient password for 18 days during the test. The $EPSB_{algorithmV01}$ was implemented to ensure the password's security. The system logged and scrutinized all activities associated with the legitimate user's password. At this stage, the algorithm collected data related to the interactions of (Alice), who represents the legitimate user, with the password (Figure 8). Thus, the algorithm now possesses the necessary data related to Alice to compare it with any login attempts to the system. In 18 days, Alice used the system where she logged in by typing her password at least 10 times a day. Each time, she keyed her genuine password in the space provided for it on the legitimate web link. The algorithm logged the time period for which Alice took to write the password on the interface and press the login button. It then subdivided these into confidence levels generated with regards to Alice. In this way, the higher the frequency of using the password input, the better the algorithm understands the behavior of Alice, thereby promoting the accuracy of differentiation in Tables 5 and 6.

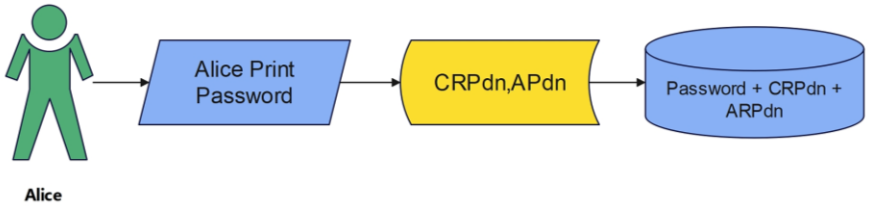

Figure 8. EPSBV01 Dala Collecting

To test the method, we move on to the second stage (swapping). The password was deliberately shared with another user (Bob); at this stage, the Stolen password Attack is simulated by assuming that an unauthorized user (Bob) has obtained the password (provided to him by the experiment administrator). Bob attempts to log into the system using the same device Alice uses with the same password.

In the next stage (Sample Testing), it took Bob 5.62 seconds from the moment he began typing the password in the designated field until he pressed the "Log In" icon. Hence, the current user's password duration (Pd) is 5.62 seconds. The algorithm records this entry and compares it with the recorded data of the authorized user's password-related activities (Stage One). The comparison stage is performed to ascertain the level of consistency between the present input and the preceding data. The duration taken by the current user will be compared with the historical data of the legitimate user to determine the degree of correlation between the two values. Based on Alice's historical data, the $EPSB_{algorithmV1}$ records that Alice's Confidence Ranges(CR) for password duration(Pd) was (CR_{pdn}) between (CR_{Pd1}(min (4.0026) – max (4.3723))), (CR_{Pd2} (min (4.126) – max(4.332))), (CR_{Pd3} (min(3.952) – max(4.366))), (CR_{APd1} (min(3.924) – max(4.395))), CR_{APd2} (min(4.126)– max(4.332)), (CR_{APd3} (min(3.806) – max(4.546.))) as shown in Figure 6.

In the evaluation stage, the percentage similarity between the two values (the current value and the historical data) is calculated. If the user attains a match of 60% or higher, they are deemed legitimate and authorized to view the data. Alternatively, suppose the user fails to meet the system's requirements. In that case, they will be denied access, and an email notification will be issued to the authorized user to confirm the entry procedure at the end of the evaluation stage. The provided table (see Table 7 and Figure 6) demonstrates the process the $EPSB_{algorithmV01}$ uses to authenticate the user by looking at the frequency of password entry. In the stolen password attack simulation mentioned above, Bob, representing the unauthorized user in our experiment, attempted to log into the system. The $EPSB_{algorithmV01}$ recorded his login time, which was CRPd = 5.62 seconds as previously stated. Upon comparison with all the indicators, the result did not match Alice's historical behavior. Therefore, the algorithm flagged Bob as a suspicious user. Bob's CRPd was significantly higher and outside the trusted range. According to the above EPSBV01 experimental test, they considered him an unauthorized user based on $EPSB_{Timev01}$ results, even though he has an active password. The reason for this is that the $EPSB_{algorithmV01}$ was able to record and analyze the legitimate user's activity. It generated new trust points associated with the password, which will be considered during user authentication. Thus, the $EPSB_{algorithmV01}$ was able to

mitigate the effects of a stolen password attack, and it denied Bob access to the system. Expanding on the details of the $EPSB_{algorithmV01}$, it is a robust algorithm that effectively evaluates the similarity percentage between the current value and the historical data. This evaluation plays a crucial role in determining the legitimacy of a user. With a required match of 60% or higher, the $EPSB_{algorithmV01}$ ensures that only authorized users are granted access to view the valuable data. In cases where a user does not meet the system's requirements, a strict denial of access is implemented. Furthermore, an email notification is promptly sent to the authorized user to confirm the entry procedure, ensuring transparency and security in the evaluation stage. To provide clarity on the authentication process, the $EPSB_{algorithmV01}$ relies on a comprehensive table (referenced as Table 7) and a visually detailed Figure 9. These visual representations assist in understanding how the algorithm analyzes the frequency of password entry to authenticate users effectively. One notable scenario that demonstrates the reliability of the $EPSB_{algorithmV01}$ is the stolen password attack simulation. In this simulation, an unauthorized user, represented by Bob, attempts to log into the system.

The $EPSB_{algorithmV01}$ diligently records Bob's login time, which is precisely measured as CRPd = 5.62 seconds, as mentioned earlier. Performing a meticulous comparison with all the indicators, the algorithm determines that Bob's behavior does not align with Alice's historical pattern. This discrepancy raises a red flag, identifying Bob as a suspicious user. Notably, Bob's CRPd significantly surpasses the trusted range, emphasizing the deviation from expected behavior. Based on the thorough $EPSB_{V01}$ experimental test conducted, the algorithm classifies Bob as an unauthorized user, despite having an active password. This decision is primarily driven by the $EPSB_{Timev01}$ results, which reflect the algorithm's ability to meticulously record and analyze the activities of legitimate users. Furthermore, the EPSBalgorithmV01 generates new trust points associated with the password. These trust points play a vital role in future user authentication processes, highlighting the algorithm's continuous adaptation and learning capabilities. By leveraging the trust points and considering the extensive analysis of the legitimate user's activity, the $EPSB_{algorithmV01}$ effectively mitigates the disruptive effects of a stolen password attack. With its comprehensive evaluation and robust procedures, the algorithm successfully denies Bob access to the system, safeguarding the sensitive data within.

Table 7. Process of EPSBTimev01 with $EPSB_D$

<table>
<tr><td colspan="2">Attempt</td><td colspan="8">1</td></tr>
<tr><td colspan="2">Scenario</td><td>1</td><td colspan="7">Bob began entering his password actively until he pressed the login button. The duration required to type the password is 5.62 seconds.</td></tr>
<tr><td colspan="4">$EPSB_{Timev01}$</td><td colspan="3">$EPSB_{Stylev01}$</td><td>$EPSB_{Errorv01}$</td></tr>
<tr><td rowspan="2">Step1</td><td>Data</td><td colspan="2">5.62</td><td colspan="3">Inactive</td><td>Inactive</td></tr>
<tr><td>Record</td><td colspan="2">5.62</td><td colspan="3"></td><td></td></tr>
<tr><td>Step2</td><td colspan="3">Analysis (current user)</td><td colspan="3"></td><td></td></tr>
<tr><td rowspan="2">Step2.1</td><td rowspan="2">Password Duration (Pd)</td><td>Min</td><td>Max</td><td colspan="3" rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>5.62</td><td>5.62</td></tr>
<tr><td>Step3</td><td colspan="7">Generated Pd= 5.62</td></tr>
<tr><td>Step4</td><td colspan="7">Send Pd to Decision (D)</td></tr>
<tr><td colspan="8">$EPSB_D$</td></tr>
<tr><td>Step1</td><td>Input Data</td><td>Pd</td><td colspan="5">5.62</td></tr>
<tr><td>Step2</td><td>Records</td><td>Pd in $EPSB_{Time}$</td><td colspan="5">5.62</td></tr>
<tr><td rowspan="8">Step3</td><td colspan="7">Compare</td></tr>
<tr><td rowspan="7">Current Pd</td><td rowspan="7">5.62</td><td colspan="4">Historical $EPSB_{Timev01}$</td></tr>
<tr><td></td><td>Min</td><td>Max</td><td>Results</td></tr>
<tr><td>Step3.1</td><td>CR_{Pd1}</td><td>4.0026</td><td>4.3723</td><td>Fail</td></tr>
<tr><td>Step3.2</td><td>CR_{Pd2}</td><td>4.126</td><td>4.332</td><td>Fail</td></tr>
<tr><td>Step3.3</td><td>CR_{Pd3}</td><td>3.952</td><td>4.366</td><td>Fail</td></tr>
<tr><td>Step 3.4</td><td>A_{Pd1}</td><td>3.924</td><td>4.395</td><td>Fail</td></tr>
<tr><td>Step 3.5</td><td>A_{Pd2}</td><td>4.126</td><td>4.332</td><td>Fail</td></tr>
<tr><td>Step 3.6</td><td>A_{Pd3}</td><td>3.806</td><td>4.546</td><td>Fail</td></tr>
<tr><td>Step3.7</td><td>$EPSB_D$</td><td colspan="6">0.0%</td></tr>
<tr><td>Step4</td><td colspan="7">0.0% <60%</td></tr>
<tr><td>Step5</td><td colspan="7">Active critical process activities</td></tr>
<tr><td>Step5.1</td><td colspan="7">Verification Process</td></tr>
<tr><td></td><td colspan="7">a) Lock System
b) Send a verified email to Alice</td></tr>
</table>

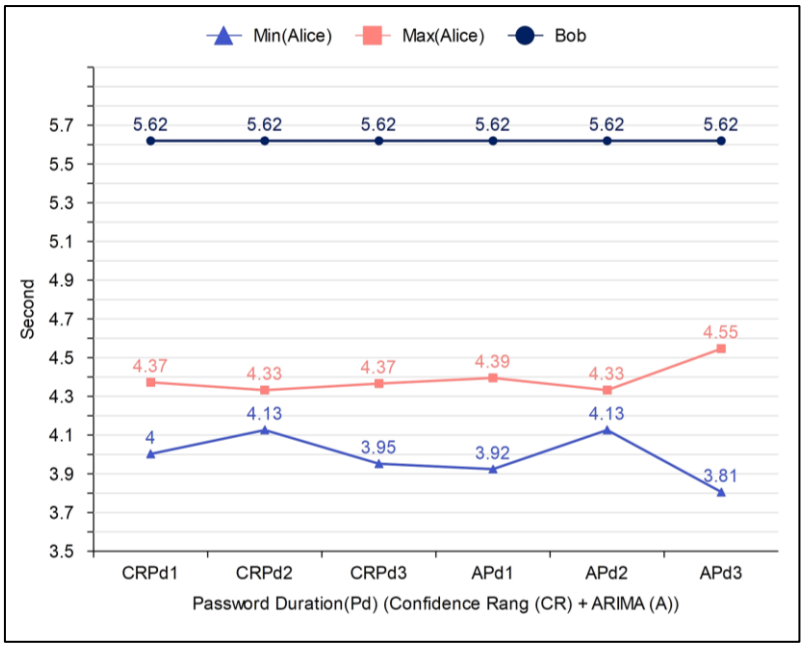

Figure 9. $EPSB_{V01}$ Evaluation Results

The creation of these new data points, associated with the password, improved the function of the system's authentication layer. This enhancement transformed it from a traditional model, which solely relies on password matching, into an intelligent layer capable of learning from user behavior during password interactions. Using intelligent techniques in the authentication layer improved its accuracy in identifying valid users, therefore lowering the risks connected with such assaults, according to the studies of this work, simulating Password Stolen Attacks (PSA). Based on the typing and password submission times, the ARIMA algorithm significantly improved the accuracy of identifying allowed users. The algorithm attained 17 successful identifications from 22 attempts, an increase from 10 successful identifications from 22 attempts before the use of ARIMA. This enhancement highlights the efficacy of intelligent methods in optimizing the authorization layer's ability to identify authentic users. These developments facilitate the creation of intelligent authentication systems that can learn from user interactions across several facets of the system. Furthermore, the intelligent authentication layer can leverage machine learning algorithms to continuously refine its understanding of user behavior.

As more data is collected and analyzed, the system becomes increasingly adept at recognizing patterns and anomalies. This adaptability facilitates the system's ability to adapt to new and emerging threats, providing a robust defense against evolving cyber-attacks. The remarkable advancements in intelligent authentication not only enhance security but also contribute to a more user-friendly experience. With the system's ability to learn and understand user behaviors, the need for complex and cumbersome password requirements can be significantly reduced. Instead, the system can intelligently adapt to each user's unique characteristics, striking a balance between security and convenience. In conclusion, the incorporation of cutting-edge intelligent techniques into the authentication layer revolutionizes the field of authentication systems. The remarkable enhancements in accuracy, efficiency, and adaptability ensure robust protection against unauthorized access attempts. By analyzing user behavior patterns, continuously monitoring sessions, and leveraging machine learning algorithms, the system creates a secure environment that inspires confidence and fosters user satisfaction. These advancements herald a new era of authentication systems, where security, usability, and intelligence converge to provide a level of protection in the ever-changing digital landscape.

6- Conclusion

The algorithm of EPSB uses three key variables—$EPSB_{Style}$, $EPSB_{Time}$, and $EPSB_{Error}$ to make it easier to tell the difference between authorized and unauthorized users and protect against stolen password attacks [8, 22, 48]. The $EPSB_{algorithm}$ suffers from a limited number of parameters associated with the password input duration indicator $EPSB_{Time}$, which has six parameters [5]. Therefore, this research presents a temporal ARIMA model that improves the results produced by the aforementioned functions in $EPSB_{Time}$. The investigation was conducted in three main phases: first, the $EPSB_{algorithmV01}$ was employed to authenticate; second, the experimentation was commenced; and last, the experimentation results were evaluated. To put a practical use of the developed $EPSB_{algorithmv01}$for the purpose of authentication, the Python programming language was utilized for the first implementation. Using a similar context, we compare the results of the test carried out using the $EPSB_{V01}$ in detecting unauthorized users before and after the adaptation through the ARIMA approach.

Based on the above scenario, Bob is an unauthorized user who obtained the password through a password theft attack. In the experiment conducted in this study during the fifth stage outlined in the section above, this stage tests the attempt of an unauthorized user who has obtained a valid password to access the system. The system will check the password as well as the user's behavior with the password by comparing the time Bob took from starting to type the password to pressing the enter button with the time taken by the legitimate user during previous logins. The algorithm EPSB without ARIMA successfully identified 12 unauthorized users out of 22 in the experiment sample during the password theft attack simulation on the system. Thus, we can say that the EPSB without ARIMA was able to identify 54.54% of unauthorized users, while it failed to identify 45.45% of them. When conducting the same experiment in the same environment with the same sample of 22 users, using the algorithm $EPSB_{V01}$ with the adoption of ARMA and the equation for analyzing the historical data of the authorized user and comparing it with the current user, the algorithm was able to identify 17 unauthorized users out of 22 during the Stolen Password Attack (SPA) simulation.

The sample consisted of a carefully chosen set of individuals, with passwords regularly changed among them to mimic a scenario of password theft. Every user tried to log in using a different user's password to evaluate the algorithm's capability to differentiate between authorized and unauthorized users. In a related context, based on the above formulas and using the ARMA algorithm, the system's performance attained up to 77.27%. This also reveals that the EPSBV01 increased by 22.73% in preventing unauthorized users from accessing the system in the case of SPA when we compared it with normal EPSB (see Figure 10). Therefore, enhancing the $EPSB_{algorithmv01}$ by integrating it with the new ARMA and analyzing the CR equation eventually contributed to significantly improving the algorithm's accuracy in detecting unauthorized users. However, the algorithm had a high error rate in detecting the five unauthorized users who gained access to the system data during the Stolen Password Attack (SPA) simulation.

In contrast, an information system that does not incorporate the Electronic Personal Synthesis Behavior (EPSB) algorithm would allow all 22 users with a valid password to access the data housed within the system. This lack of security measures can potentially lead to severe security breaches, jeopardizing the confidentiality and integrity of sensitive information. It is absolutely crucial for organizations, regardless of their size or industry, to prioritize the implementation of robust security measures, such as the highly effective and reliable EPSB algorithm, in order to effectively safeguard their systems and prevent unauthorized access. By continuously evaluating, refining, and enhancing the algorithm's capabilities, organizations are able to remain several steps ahead of potential attackers, ensuring the utmost security and integrity of their valuable data and critical systems. Implementing the EPSB algorithm not only serves as a proactive defense mechanism but also serves as a testament to the organization's unwavering commitment to maintaining the highest level of data protection. The EPSB algorithm's ability to efficiently encrypt passwords, coupled with its exceptional blocking capabilities, significantly mitigates the risk of unauthorized access and potential security breaches. As organizations increasingly harness the power of technology and digital systems, it becomes paramount to prioritize and invest in robust security measures, enabling seamless operations while maintaining the utmost confidentiality, integrity, and availability of sensitive information. By staying vigilant, proactive, and committed to the continuous improvement of security measures, organizations can truly protect their systems against potential threats, fortifying their data and maintaining the trust of their stakeholders.

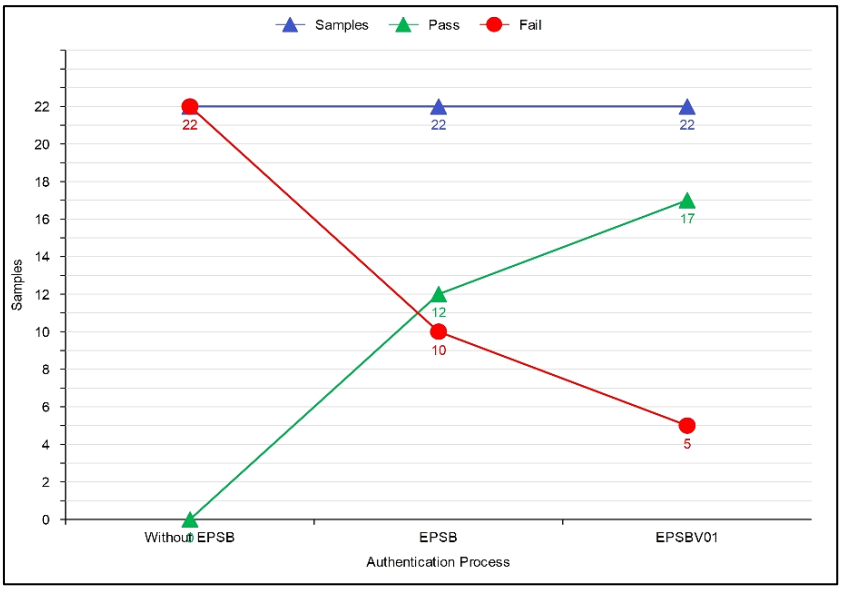

Figure 10. Compare Algorithm (EPSB & EPSBV01)

7- Declarations

7-1- Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7-2- Funding and Acknowledgments

This work is part of a project submitted to the University of Buraimi (UoB) in Al Buraimi, Oman, under Reference No. IRG/UoB/CoB-005/2022-23. I thank UoB for providing us with the necessary facilities to complete this work.

7-3- Institutional Review Board Statement

Not applicable.

7-4- Informed Consent Statement

Not applicable.

7-5- Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the author.

8- References

[1] Golar, P. C. (2023). Intelligent Systems and Applications in Security Analysis of the Graphical Password-Based Authentication Systems with Different Attack Proofs. International Journal of Intelligent Systems and Applications in Engineering, 11(10), 155-165.

[2] Shakir, M. (2022). Applying Human Behaviour Recognition in Cloud Authentication Method—A Review. Proceedings of International Conference on Emerging Technologies and Intelligent Systems. ICETIS 2021. Lecture Notes in Networks and Systems. Springer, Cham, Switzerland. doi:10.1007/978-3-030-85990-9_45.

[3] Basha, P. H., Prathyusha, G., Rao, D. N., Gopikrishna, V., Peddi, P., & Saritha, V. (2024). 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, 12, 361–374.

[4] Golar, P. C., & Sharma, R. (2023). Security Analysis of the Graphical Password-Based Authentication Systems with Different Attack Proofs. International Journal of Intelligent Systems and Applications in Engineering, 11(10), 155–165.

[5] Shakir, M. T. (2020). User authentication in public cloud computing through adoption of electronic personal synthesis behavior. PhD Thesis, Universiti Tenaga Nasional, Kajang, Malaysia.

[6] Shakir, M., Abubakar, A. B., Yousoff, Y., Al-Emran, M., & Hammood, M. (2016). Application of confidence range algorithm in recognizing user behavior through EPSB in cloud computing. Journal of Theoretical and Applied Information Technology, 94(2), 416–427.

[7] Zeng, A., Chen, M., Zhang, L., & Xu, Q. (2023). Are Transformers Effective for Time Series Forecasting? Proceedings of the 37th AAAI Conference on Artificial Intelligence, AAAI 2023, 37, 11121–11128. doi:10.1609/aaai.v37i9.26317.

[8] Jeng, H. A., Singh, R., Diawara, N., Curtis, K., Gonzalez, R., Welch, N., Jackson, C., Jurgens, D., & Adikari, S. (2023). Application of wastewater-based surveillance and copula time-series model for COVID-19 forecasts. Science of the Total Environment, 885, 163655. doi:10.1016/j.scitotenv.2023.163655.

[9] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, Privacy and Risks within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers, 24(2), 393–414. doi:10.1007/s10796-020-10044-1.

[10] Dincelli, E., & Yayla, A. (2022). Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective. The Journal of Strategic Information Systems, 31(2), 101717. doi:10.1016/j.jsis.2022.101717.

[11] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS. Sensors, 22(4), 1448. doi:10.3390/s22041448.

[12] Shakir, M., Abubakar, A., Yousoff, O., Waseem, M., & Al-Emran, M. (2016). Model of security level classification for data in hybrid cloud computing. Journal of Theoretical and Applied Information Technology, 94(1), 133-141.

[13] Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. Applied Sciences (Switzerland), 13(19), 10871. doi:10.3390/app131910871.

[14] Rooney, M. J., Levy, Y., Li, W., & Kumar, A. (2024). Comparing experts' and users' perspectives on the use of password workarounds and the risk of data breaches. Information & Computer Security. doi:10.1108/ics-05-2024-0116.

[15] Hossain, M. A., & Assiri, B. (2022). Facial expression recognition based on active region of interest using deep learning and parallelism. PeerJ Computer Science, 8, 894. doi:10.7717/PEERJ-CS.894.

[16] Srivastava, G., & Bag, S. (2023). Modern-day marketing concepts based on face recognition and neuro-marketing: a review and future research directions. Benchmarking: An International Journal, 31(2), 410–438. doi:10.1108/bij-09-2022-0588.

[17] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics (Switzerland), 12(6), 1333. doi:10.3390/electronics12061333.

[18] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, 55(2), 1029–1053. doi:10.1007/s10462-021-09976-0.

[19] Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., Ofusori, L., & Ome, U. (2023). Password-based authentication and the experiences of end users. Scientific African, 21, 1743. doi:10.1016/j.sciaf.2023.e01743.

[20] Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. Ad Hoc Networks, 146, 103159. doi:10.1016/j.adhoc.2023.103159.

[21] Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2021). Behavioral biometrics & continuous user authentication on mobile devices: A survey. Information Fusion, 66, 76–99. doi:10.1016/j.inffus.2020.08.021.

[22] Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. Computers and Electrical Engineering, 119, 109485. doi:10.1016/j.compeleceng.2024.109485.

[23] Gudala, L., Reddy, A. K., Sadhu, A. K. R., & Venkataramanan, S. (2022). Leveraging Biometric Authentication and Blockchain Technology for Enhanced Security in Identity and Access Management Systems. Journal of Artificial Intelligence Research, 2(2), 21–50.

[24] Tongsubanan, S., & Kasemsarn, K. (2024). Developing a Design Guideline for a User-Friendly Home Energy-Saving Application That Aligns with User-Centered Design (UCD) Principles. International Journal of Human-Computer Interaction, 1–23. doi:10.1080/10447318.2024.2398324.

[25] Walden, A., Garvin, L., Smerek, M., & Johnson, C. (2020). User-centered design principles in the development of clinical research tools. Clinical Trials, 17(6), 703–711. doi:10.1177/1740774520946314.

[26] Li, W., Cheng, H., Wang, P., & Liang, K. (2021). Practical Threshold Multi-Factor Authentication. IEEE Transactions on Information Forensics and Security, 16, 3573–3588. doi:10.1109/TIFS.2021.3081263.

[27] Kim, J., & Kim, N. (2022). Quantifying Emotions in Architectural Environments Using Biometrics. Applied Sciences (Switzerland), 12(19), 9998. doi:10.3390/app12199998.

[28] Li, Y., Yang, G., Su, Z., Li, S., & Wang, Y. (2023). Human activity recognition based on multienvironment sensor data. Information Fusion, 91, 47–63. doi:10.1016/j.inffus.2022.10.015.

[29] Ren, Y., Leng, Y., Qi, J., Sharma, P. K., Wang, J., Almakhadmeh, Z., & Tolba, A. (2021). Multiple cloud storage mechanism based on blockchain in smart homes. Future Generation Computer Systems, 115, 304-313. doi:10.1016/j.future.2020.09.019

[30] Bhuva, D. R., & Kumar, S. (2023). A novel continuous authentication method using biometrics for IoT devices. Internet of Things (Netherlands), 24, 100927. doi:10.1016/j.iot.2023.100927.

[31] Patel, R. V., Bhoi, D., & Pawar, C. S. (2020). Security hazards attacks and its prevention techniques in cloud computing: A detail review. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 6(4), 48-58.

[32] Zhong, Y., Deng, W., Hu, J., Zhao, D., Li, X., & Wen, D. (2021). SFace: Sigmoid-Constrained Hypersphere Loss for Robust Face Recognition. IEEE Transactions on Image Processing, 30, 2587–2598. doi:10.1109/TIP.2020.3048632.

[33] Upadhyay, D., Malhotra, S., Rawat, R. S., Gupta, M., & Mishra, S. (2024). Utilization of MFCC in Conjuction with Elaborated LSTM Architechtures for the Amplification of Lexical Descrimination in Acoustic Milieus Characterized by Pronounced Nocturnal Disturbance. 2024 2nd International Conference on Disruptive Technologies, ICDT 2024, 440–445. doi:10.1109/ICDT61202.2024.10489344.

[34] Gonzalez-Compean, J. L., Sosa-Sosa, V. J., Garcia-Hernandez, J. J., Galeana-Zapien, H., & Reyes-Anastacio, H. G. (2022). A Blockchain and Fingerprinting Traceability Method for Digital Product Lifecycle Management. Sensors, 22(21), 8400. doi:10.3390/s22218400.

[35] Al Alkeem, E., Kim, S. K., Yeun, C. Y., Zemerly, M. J., Poon, K. F., Gianini, G., & Yoo, P. D. (2019). An enhanced electrocardiogram biometric authentication system using machine learning. IEEE Access, 7, 123069–123075. doi:10.1109/ACCESS.2019.2937357.

[36] Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern Authentication Methods: A Comprehensive Survey. AI, Computer Science and Robotics Technology, 2022, 1–24. doi:10.5772/acrt.08.

[37] Progonov, D., Cherniakova, V., Kolesnichenko, P., & Oliynyk, A. (2022). Behavior-based user authentication on mobile devices in various usage contexts. Eurasip Journal on Information Security, 2022(1), 6. doi:10.1186/s13635-022-00132-x.

[38] Zhou, P., Xu, H., Lee, L. H., Fang, P., & Hui, P. (2022). Are You Left Out? Are you left out? An efficient and fair federated learning for personalized profiles onwearable devices of inferior networking conditions. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 6(2), 1–25. doi:10.1145/3534585.

[39] Rehman, A., Hassan, M. F., Hooi, Y. K., Qureshi, M. A., Shukla, S., Susanto, E., Rubab, S., & Abdel-Aty, A. H. (2022). CTMF: Context - Aware Trust Management Framework for Internet of Vehicles. IEEE Access, 10, 73685–73701. doi:10.1109/ACCESS.2022.3189349.

[40] Do, N. Q., Selamat, A., Krejcar, O., Herrera-Viedma, E., & Fujita, H. (2022). Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions. IEEE Access, 10, 36429–36463. doi:10.1109/ACCESS.2022.3151903.

[41] Miller, K. (2021). Ping Identity Announces the Acquisition of Secured Touch to Accelerate Identity Fraud Capabilities. Ping Identity Holding Corp, Denver, United States. Available online: https://www.businesswire.com/news/home/20210621005719/en/Ping-Identity-Announces-the-Acquisition-of-SecuredTouch-to-Accelerate-Identity-Fraud-Capabilities (accessed on January 2025).

[42] Koster, E. (2019). Why Samsung NEXT and HYPR believe the future will be passwordless. Samsung Newsroom USA, Ridgefield Park, United States. Available online: https://news.samsung.com/us/samsung-next-hypr-believe-future-will-passwordless/ (accessed on January 2025)

[43] TwoSense. (2025). AI, Continuous multifactor authentication. Twosense Brooklyn, United States. Available online: https://www.twosense.ai/ (accessed on January 2025).

[44] Noë, B., Turner, L. D., Linden, D. E. J., Allen, S. M., Winkens, B., & Whitaker, R. M. (2019). Identifying Indicators of Smartphone Addiction Through User-App Interaction. Computers in Human Behavior, 99, 56–65. doi:10.1016/j.chb.2019.04.023.

[45] Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3, 1-18. doi:10.1186/s42400-020-00050-w.

[46] Hamdani, T. M., Won, J. M., Alimi, A. M., & Karray, F. (2011). Hierarchical genetic algorithm with new evaluation function and bi-coded representation for the selection of features considering their confidence rate. Applied Soft Computing, 11(2), 2501-2509. doi:10.1016/j.asoc.2010.08.020.

[47] Anderson, T. W. (2011). The statistical analysis of time series. John Wiley & Sons, Hoboken, United States.

[48] Duncan, G.T., Gorr, W.L., Szczypula, J. (2001). Forecasting Analogous Time Series. Principles of Forecasting. International Series in Operations Research & Management Science. Springer, Boston, United States. doi:10.1007/978-0-306-47630-3_10.

[49] Durbin, J. (1959). Efficient Estimation of Parameters in Moving-Average Models. Biometrika, 46(3/4), 306. doi:10.2307/2333528.

[50] Pankratz, A. (2012) Forecasting with Dynamic Regression Models. John Wiley & Sons, Hoboken, United States.

[51] Stein, E. M., & Shakarchi, R. (2011). Fourier analysis: An Introduction. World Book Publishing Company, Chicago, United States.

[52] Silva, A. B. D. S., Araújo, A. C. de M., de Frias, P. G., Vilela, M. B. R., & Do Bonfim, C. V. (2021). Auto-regressive integrated moving average model (Arima): Conceptual and methodological aspects and applicability in infant mortality. Revista Brasileira de Saude Materno Infantil, 21(2), 647–656. doi:10.1590/1806-93042021000200016.

[53] Rao, T., Su, Y., Xu, P., Zheng, Y., Wang, W., Jin, H. (2024). You Reset I Attack! A Master Password Guessing Attack against Honey Password Vaults. Computer Security – ESORICS 2023. ESORICS 2023. Lecture Notes in Computer Science, vol 14346. Springer, Cham, Switzerland. doi:10.1007/978-3-031-51479-1_8.

[54] Goenka, R., Chawla, M., & Tiwari, N. (2024). A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy. International Journal of Information Security, 23(2), 819–848. doi:10.1007/s10207-023-00768-x.

[55] Pallivalappil, A. S., & Jagadeesha, S. N. (2021). Social Engineering Attacks on Facebook–A Case Study. International Journal of Case Studies in Business, IT and Education, 5(2), 299-313. doi:10.47992/ijcsbe.2581.6942.0135.

[56] Kamiljonovna, S. N. (2021). Multi-factor Authentication and Fingerprint based Debit Card System. European Journal of Research Development and Sustainability, 2(5), 43-49.

[57] Shakir, M., Abood, R., Sheker, M., Alnaseri, M., Al-Hashimi, M., & Tawafak, R.M. (2021). Users Acceptance of Electronic Personal Synthesis Behavior (EPSB): An Exploratory Study. Recent Advances in Technology Acceptance Models and Theories. Studies in Systems, Decision and Contro. Springer, Cham, Switzerland. doi:10.1007/978-3-030-64987-6_30.