Journal of Infrastructure, Policy and Development 2024, 8(15), 9441.
https://doi.org/10.24294/jipd9441

Article

Enhancing secure access through time-stamped password analysis: Implications for infrastructure and policy development

Mohanaad Shakir[1], Boumedyen Shannaq[1,*], Oualid Ali[2], Basel Bani-Ismail[3]

[1] University of Buraimi, Al Buraimi, Sultanate of Oman
[2] College of Arts & Science, Computer Sciences Department, Applied Science University, Manama, Kingdom of Bahrain
[3] Faculty of Information Technology, Majan University College, Muscat, Sultanate of Oman
*** Corresponding author:** Boumedyen Shannaq, boumedyen@uob.edu.om

CITATION

Shakir M, Shannaq B, Ali O, Bani-Ismail B. (2024). Enhancing secure access through time-stamped password analysis: Implications for infrastructure and policy development. Journal of Infrastructure, Policy and Development. 8(15): 9441. https://doi.org/10.24294/jipd9441

ARTICLE INFO

Received: 2 October 2024
Accepted: 11 November 2024
Available online: 13 December 2024

Abstract: The proposed research work encompasses implications for infrastructure particularly the cybersecurity as an essential in soft infrastructure, and policy making particularly on secure access management of infrastructure governance. In this study, we introduce a novel parameter focusing on the timestamp duration of password entry, enhancing the algorithm titled EPSBalgorithmv01 with seven parameters. The proposed parameter incorporates an analysis of the historical time spent by users entering their passwords, employing ARIMA for processing. To assess the efficacy of the updated algorithm, we developed a simulator and employed a multi-experimental approach. The evaluation utilized a test dataset comprising 617 authentic records from 111 individuals within a selected company spanning from 2017 to 2022. Our findings reveal significant advancements in EPSBalgorithmv01 compared to its predecessor namely EPSBalgorithmv00. While EPSBalgorithmv00 struggled with a recognition rate of 28.00% and a precision of 71.171, EPSBalgorithmv01 exhibited a recognition rate of 17% with a precision of 82.882%. Despite a decrease in recognition rate, EPSBalgorithmv01 demonstrates a notable improvement of approximately 14% over EPSBalgorithmv00.

Keywords: cybersecurity; time-stamped password analysis; infrastructure governance; EPSBalgorithmv01; ARIMA

1. Introduction

The Today's modern technological environment necessitates the daily use of information systems (Szymkowiak et al., 2021). The rapid advancement in this field has highlighted the critical importance of maintaining information security and privacy (AL-HASHIMI et al., 2017; Ismagilova et al., 2022). Moreover, Large Language Models (LLMs) and Generative AI (GenAI) have recently emerged as powerful tools in cybersecurity, enabling automated generation of both defensive and offensive tactics. Leveraging their vast training on diverse datasets, LLMs can simulate potential cyber-attacks, allowing cybersecurity professionals to identify system vulnerabilities proactively and understand how malicious actors might exploit them (Adebiaye, et al., 2024; Chaudhary et al., 2023; Shannaq, 2024a; Shannaq, 2024b; Shannaq and Shakir, 2024).

Consequently, developing efficient mechanisms for data and information access has become essential (Al-Shamsi et al., 2024; Alshamsi et al., 2024; Tsang et al., 2019). Intelligent authorization techniques, which combine passwords with individual user behavior, are prime examples of such mechanisms (Papaspirou et al., 2021). Intelligent authorization methods are tools and techniques designed to provide safer access

channels for information system users. These techniques rely on understanding and analyzing user behavior to determine appropriate access levels (Hazratifard et al., 2022). The main goal is to mitigate risks associated with unauthorized information access and prevent security breaches (James and Rabbi, 2023; M et al., 2016). Key methods include:

a. Two-Factor Authentication: Requires users to provide two forms of identification (Papaspirou et al., 2021).
b. Multifactor Authentication: Allows users to provide more than just a password (Das et al., 2019).
c. User Behavior Analysis: Uses typical patterns of user behavior, such as typing or color choices (Stylios et al., 2021).

Intelligent authorization, combining user behavior analysis with password authentication, represents a significant advancement in security and convenience for information access.

Additionally, experts have extensively studied time series prediction methods (Guarracino et al., 2010). Temporal data methodologies involve analyzing time series to derive statistics and other attributes (Ahmed et al., 2023). Time series prediction uses past data to forecast future values (Zeng et al., 2023). While regression analysis is practical for determining relationships between time series, it is not typically classified as "time series" analysis (Jeng et al., 2023). Discrete-time series analysis identifies trends and allows for interventions affecting the underlying variable (Shakir et al., 2016). EPSB uses a duration index to differentiate between legal and illegal users based on password typing duration and method selection, enhancing security. The primary aim of developing the EPSB algorithm is to enhance the differentiation between authorized and unauthorized users. This is achieved by storing and classifying authorized user behavior data, alongside the password, across various aspects such as password input duration and the user's password selection style. The EPSB algorithm is introduced to strengthen the authorization layer during instances of password theft by analyzing the user's historical behavior with the password.

In the EPSB algorithm, analyzing historical user data is pivotal, achieved through the Confidence Range (CR) function, which integrates median, mean, and mode equations to establish crucial reference points for distinguishing authorized users from unauthorized ones.

However, the EPSB algorithm is limited by the number of parameters associated with the password input duration indicator, EPSBTime, which includes only six parameters.

This study introduces a novel dimension to the analysis process concerning EPSBTime, considering it as the seventh parameter. We propose a time series analysis equation, designed to enhance the outcomes produced by the aforementioned functions within EPSBTime. This enhancement results in the generation of fresh data points that serve as distinct markers for authorized users. The improvements made to the EPSB algorithm significantly enhance its discriminatory capabilities and bolster its security features. Our focus will be on understanding the implementation of these enhancements and evaluating their effectiveness in safeguarding sensitive data within modern information systems, particularly in 'Fin-Tech' applications. Hence, the study aims to address the following research questions:

- RQ1: What limitations are associated with the authentication accuracy of the EPSB algorithm?
- RQ2: How can the EPSB algorithm be refined to enhance authentication accuracy?
- RQ3: How can the validity of the proposed enhanced EPSB algorithm be assessed?

Furthermore, within the same context, the research objectives of this study are outlined as follows:

- To assess the current EPSB algorithm and identify its strengths and weaknesses regarding authentication accuracy.
- To enhance authentication accuracy and differentiate between authorized and unauthorized users by refining the EPSB algorithm (Version 1).
- To implement and validate the proposed enhancements to the EPSB algorithm (Version 1).

It is important to mention that this work aligns with the NIST Cybersecurity Framework by emphasizing the framework's core (NIST, 2018).

2. Literature review

2.1. Intelligent authentication methods

Advanced authentication methods, incorporating biometrics, machine learning, and artificial intelligence, aim to fortify authentication systems (Al Alkeem et al., 2019; Shannaq et al., 2024). Traditional methods like passwords and PINs have become vulnerable due to technological progress (Papathanasaki et al., 2022). Scientists focus on developing precise algorithms to record and interpret biometric data, ensuring high authentication accuracy (Progonov et al., 2022). With significant advancements in artificial intelligence, integrating authentication techniques with AI becomes imperative to enhance accuracy (M et al., 2016). Machine learning emerges as a pivotal technique (Roopashree et al., 2022). Machine learning dominates intelligent authentication, employing innovative algorithms for thorough data analysis and accurate predictions (Basha et al., 2024; Shams et al., 2022; Shannaq et al., 2019). Researchers utilize support vector machines, neural networks, and decision trees to create sophisticated authentication models, adept at assessing user behavior, device attributes, and contextual cues for authenticity (Ashtari and Alizadeh, 2022). These models adapt to complex threats, bolstering defenses against authentication attacks. Behavior-based authentication (BBA) focuses on analyzing individual behavioral patterns, such as typing rhythm and mouse movements, to validate identities. Continuous monitoring and analysis of user behavior enable intelligent authentication systems to detect anomalies and ensure user authenticity. Researchers explore various machine learning and statistical methodologies to model user actions effectively, paving the way for unobtrusive authentication solutions (Golar and Sharma, 2023). While intelligent authentication methods hold promise, several challenges persist (Golar and Sharma, 2023). Addressing privacy concerns, data security, interoperability, and user-friendliness is crucial for widespread adoption (Jaime et al., 2023). Robust algorithms capable of thwarting adversarial attacks and impersonation attempts are paramount for research (Alqahtani and Kumar, 2024). Future studies should prioritize enhancing accuracy, efficiency, and user experience by integrating emerging technologies like blockchain, advanced computing, and deep learning

(Shastry and Shastry, 2023). These methods significantly bolster authentication system security offering superior accuracy and security compared to traditional methods (Thomas and Preetha Mathew, 2023). Integration of intelligent algorithms can revolutionize authentication across domains like finance, healthcare, and e-commerce (Jebamikyous et al., 2023; Vyas and Hurry, 2023). Continuous multi-factor authentication, utilizing various verification factors persistently, further enhances security (Yang et al., 2024). Modern continuous multi-factor authentication solutions like 'One Span' and Zighra rely on detecting unusual usage patterns (Progonov et al., 2022). However, they struggle to track changes in behavioral records due to shifts in user habits, necessitating frequent profile updates, which can inconvenience users (Zhou et al., 2022). Enhancing access control system (ACS) accuracy involves analyzing contextual information from user interactions and physical activities. This makes it difficult for intruders to manipulate contextual data, reducing spoofing effectiveness (Do et al., 2022). Examples of context-based ACS solutions include Secured Touch (now part of Ping Identity), Samsung HYPR, NuData Security, and TwoSense (Continuous Multi-Factor Authentication, 2024; Progonov et al., 2022; U.S, 2024). These systems continuously track behavior-related features and contextual information, like user location in banking applications. Despite their precision and anti-spoofing measures, some users may prefer solutions addressing privacy, resource consumption, and battery usage concerns. The EPSB algorithm, which records user behavior during authentication without additional hardware, offering cost-effectiveness and easy implementation (Das et al., 2019).

2.2. Electronic Personal Synthesis Behavior (EPSB)

The EPSB algorithm aims to improve the precision of differentiating between authorized and unauthorized users by incorporating three primary variables:

- EPSBStyle, which has been implemented and tested by Shakir et al. (2016) and Szymkowiak et al. (2021).
- EPSBTime and EPSBError are proposed for future implementation to mitigate stolen password attacks, as suggested by Das et al. (2019) and Shakir et al. (2024).

Key considerations include the user's password selection behavior, the time taken to input a password, and legitimate user errors during password entry. These factors are analyzed, as described in **Figure 1**, and the outcomes are forwarded to EPSB Decision to determine whether system access should be granted or denied.

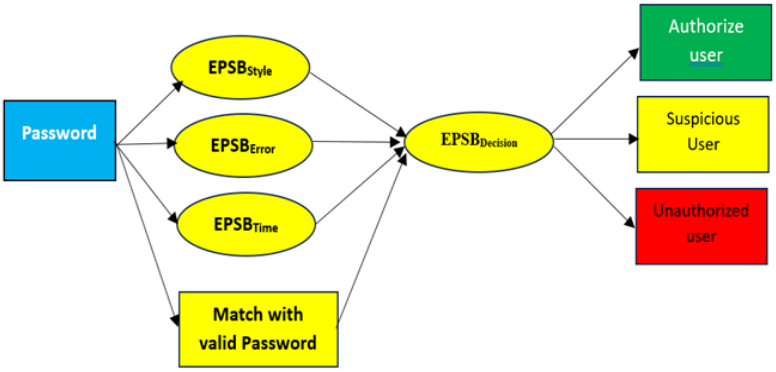

Figure 1. EPSB algorithm structure.

This algorithm captures legitimate users' activities across various variables, constructing a confidence range during user verification at system entry. Confidence Range (CR) comprises points reflecting actual user behavior, including password selection habits, common mistakes, and typing speed. EPSBStyle records all user passwords, storing old ones as historical data. New passwords are used to assess user patterns, generating confidence intervals based on specific parameters like uppercase letters, password length, and special characters. By analyzing these, the algorithm gains insight into password-related behaviors, improving behavior assessment.

EPSBTime captures and analyzes the historical duration taken by legitimate users to input a password, producing a confidence range. This range signifies the shortest and longest timeframes required by legitimate users to manage password entry for system access. Conversely, EPSBError documents instances of legitimate users inputting incorrect passwords. In such cases, users might overlook language settings, incorrectly select uppercase or lowercase letters, make single or double-character errors, or reuse old passwords. Analysis and confidence range generation for erroneous passwords in EPSBError are guided by several indicators:

- Frequency of uppercase letters;
- Frequency of lowercase letters;
- Length of the incorrect password;
- Number of characters;
- Number of digits;
- Number of special symbols;
- Inclusion in the list of old passwords.

When assessing historical data for legitimate users, the EPSB algorithm computes a Confidence Range (CR) for the password using the equation below.

$$\text{Confidence Range (CR)}=\mathrm{L}+\mathrm{h}\frac{\mathrm{fm}-\mathrm{f1}}{(2\mathrm{fm}-\mathrm{f1}-\mathrm{f2})}, \sum_i \frac{xi}{n}, L+\frac{h1}{f}((\mathrm{n}/2)\text{-C} \quad (1)$$

The confidence level for each indicator is determined by generating six key points: the lowest and highest mean, median, and mode. Thus, the algorithm produces: 36 confidence points for EPSBStyle (18 minimum and maximum ranges).

A 60% match ratio in EPSBDecision grants access. Increasing confidence points enhances EPSBTime performance. This study explores time series analysis to generate new points based on historical and current data, predicting future values. This method aims to improve user determination accuracy, comparing results with previous tests.

2.3. Time series analysis

Time Series Analysis is a statistical method used to analyze data collected over time, revealing patterns, trends, and potential forecasts within a dataset (Anderson, 2011). It employs various statistical techniques like regressions and variance analyses to understand temporal connections and predict future values based on past patterns (Anderson, 2011; Lim et al., 2021). Widely used in economics, meteorology, finance, medicine, and data science, it uncovers evolving patterns and trends, aiding in long-term trend recognition, understanding temporal relationships, and forecasting future trends (Ariens et al., 2020; Hewamalage et al., 2021; Liu et al., 2020; Mills, 2019; Zeng et al., 2023; Zhu et al., 2020).

In cyber security field Time Series Analysis (TSA) has become an essential tool for monitoring and predicting patterns in network traffic and user behavior, enabling rapid identification of potential threats. By analyzing data collected over time, TSA can help detect anomalies, such as unusual login patterns or spikes in network activity, which often signal security breaches or insider threats (Ghorbani and Lu, 2021). TSA algorithms, such as autoregressive integrated moving average (ARIMA) and Long Short-Term Memory (LSTM) models, can learn typical behavior patterns and flag deviations, thus enhancing anomaly detection and reducing false positives (Ahmad et al., 2022).

2.3.1. Common equations and models in time series analysis

Several equations and models are employed to analyze time series data and predict future trends:

- Moving Average Model: Calculates the average over a specific period, updating it with each new data point (Durbin, 1959).
- Dynamic Regression Model: Analyzes relationships between variables over time, showing how each variable influences others as time progresses (Durbin, 1959).
- 'Autoregressive Conditional Heteroskedasticity' Model (ARCH): Identifies fluctuations in financial data, predicting risks and market changes(Degiannakis and Xekalaki, 2004).
- Fourier Analysis: Examines periodic time series, breaking them down into different frequency components (Stein and Shakarchi, 2011).
- Autoregressive Integrated Moving Average Model (ARIMA): Forecasts future time series data by considering periodic variables, regression, and moving averages (SciELO, 2024).

ARIMA is widely used in economics, weather forecasting, and finance due to its effectiveness (Murat et al., 2018). It aids in understanding past data patterns and predicting future trends (Emmanuel, 2024; Gunawan and Astika, 2022). The basic equation for ARIMA is (Hằng and Dũng, 2022):

$$Y_t = c + \emptyset_1 Y_{t-1} + \emptyset_2 Y_{t-2} + \cdots + \emptyset_p Y_{t-p} + \theta_1 e_{t-1} + \theta_2 e_{t-2} + \cdots + +\theta_q e_{t-q} + \varepsilon_t \quad (2)$$

where:

- $CapY_t$ Represents the value at time "t". Is a constant term. $Empty\emptyset_1 + \emptyset_2 + \cdots + \emptyset_p$ Are autoregressive parameters;
- $\theta_1 + \theta_2 + \cdots + \theta_q$ Are moving average parameters;
- $e_{t-1} + e_{t-2} + \cdots + e_{t-q}$ Are the error terms;
- ε_t Represents the white noise error term at time "t".

The ARIMA model comprises three key components: Autoregressive (AR), Integrated (I), and Moving Average (MA). In this study, we applied the ARIMA model to meet our research objectives. This involved integrating Confidence Range (CR) outputs as new inputs into the ARIMA time series analysis. These inputs produced new points, acting as confidence points for legitimate users alongside initial points from the CR. Thus, our hypothesis tests whether adopting the ARIMA model in the EPSBAlgorithmv01 enhances its ability to detect unauthorized users in stolen password attacks.

3. Materials and methods

The research methodology aligns with the study objectives, involving gathering and analyzing cutting-edge findings to evaluate existing authentication methods in web-based systems. The project comprises multiple stages, illustrated in **Figure 2**, to achieve these objectives. Critiques of current methods highlight initial issues, while the second phase aims to enhance the EPSB model and implement the proposed solution. EPSB algorithmV01 will be applied to a sample of 111 users from historical data spanning 2017 to 2022. Tests will assess the system's ability to differentiate between legitimate and illegitimate users, focusing on password entry speed. Final results will undergo validation, comparing EPSBalgorithmV00 (6 Parameters) and EPSBalgorithmV01 (With: ARIMA = Seven Parameters) in distinguishing between users during stolen password attacks.

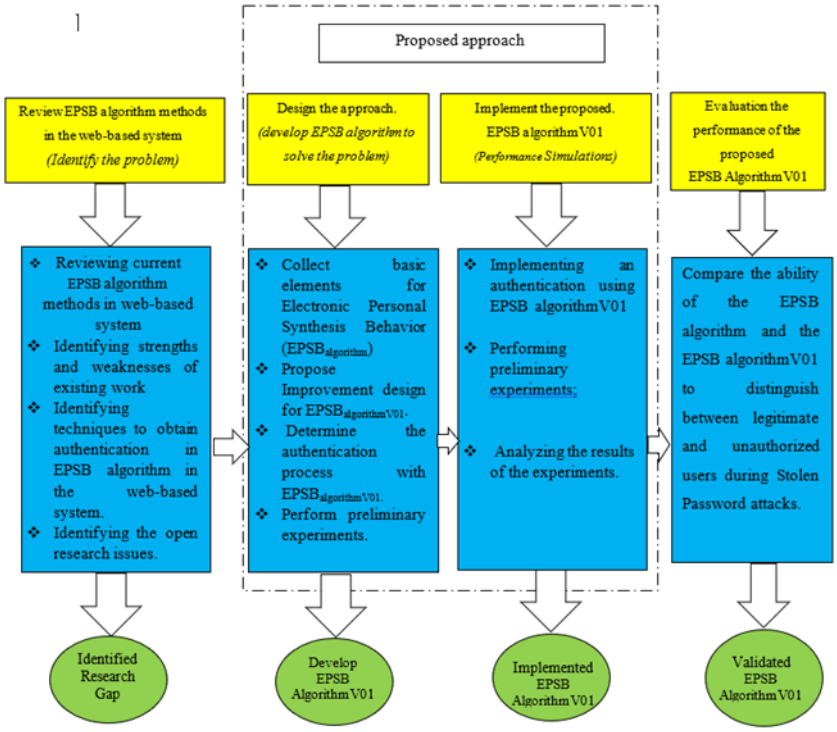

Figure 2. Research methodology.

3.1. Algorithms of the epsbalgorithmv01 components

In this section, the researcher will outline the refined components of the EPSB algorithm, building upon (Shakir et al., 2016) initial model. The primary aim of EPSBalgorithmV01 (six parameters + ARIMA) is to improve accuracy in distinguishing between authorized and unauthorized users, focusing on EPSBStyle (Six Parameters). These enhancements aim to counter stolen password attacks by integrating confidence range (CR) outputs into the ARIMA time series analysis process (EPSBTime), generating new confidence points for precise identification of unauthorized users. By amalgamating these advancements, EPSBalgorithmV01 aims to provide a robust solution for detecting and preventing unauthorized access attempts.

Notably, the EPSBDecision Node remains unchanged. EPSBTime, monitoring users' password entry times, is exclusively utilized for time series analysis, with plans for potential extension to other components based on validation of its effectiveness. The adoption of ARIMA analysis is apt for its chronological data examination capabilities. Researchers strive to comprehensively analyze and enhance EPSBTime's effectiveness, potentially extending improvements to all EPSBalgorithm components in future studies.

3.1.1. EPSBTimev01

This component, depicted in **Figure 3**, measures password input duration to generate EPSBtime using Confidence Range (CR) for each legitimate user. The ARIMA equation integrates with CR to create new confidence points based on user behavior. CRPd (Confidence Range Password Duration) results stem from keystroke speed analysis during password entry until login activation. Password Duration (Pd) identifies unauthorized users within the CRPd range. The algorithm records keyboard typing speed for each legitimate user password entry. If entries are under 30, the algorithm estimates a confidence range based on available data. If over 30, it selects the last 30 valid entries to generate a confidence score, compared to CRPd. Authorized access is granted if the score falls within CRPd; otherwise, access is denied. Keystroke speed analysis aids in user identification and security breach detection. CR outputs serve as inputs for ARIMA, generating new confidence points (APd - ARIMA Password Duration) combined with CR and effective passwords. The algorithm outlines CRPd and APd for EPSBTime, yielding conclusive results for decision-making (D) component comparison. Details are provided in **Figures 4** and **5**.

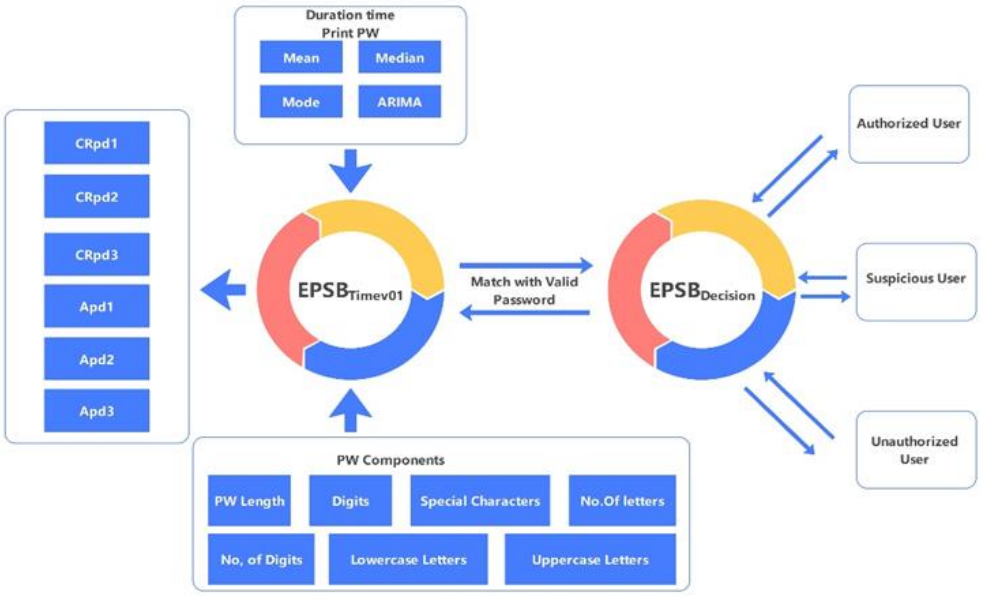

Figure 3. EPSBTimev01.

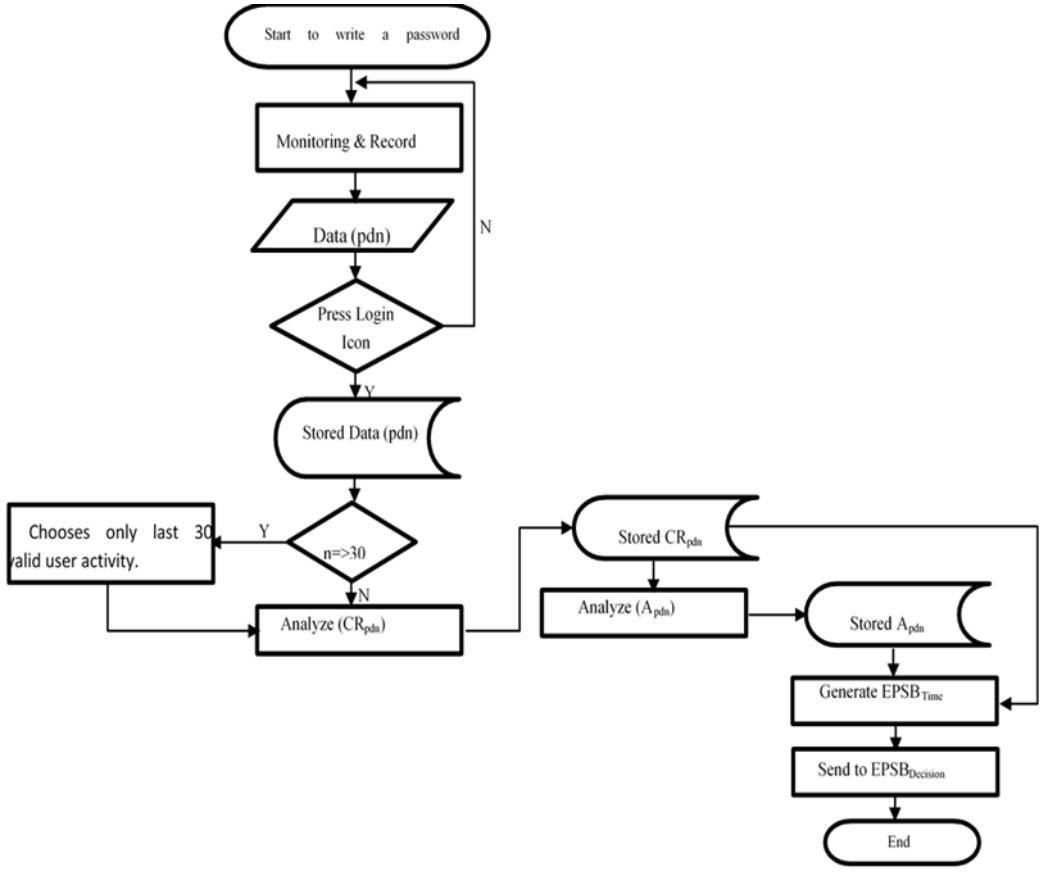

Figure 4. EPSBTimev01 components.

Algorithm: Electronic Personal Synthesis BehaviorV01 (EPSB)$_{Timev01}$
Input1: Pd (float) {duration Typed password}, Confidence Range Password duration (CR_{pd}) = CR_{Pd1}, CR_{Pd2}, CR_{I}
Output1, Input2: Confidence Range Password Duration ($CR_{Pd\,(1\text{-}3)}$)
Output 2: ARIMA Password Duration ($A_{Pd(1\text{-}3)}$)

If *d start*
Do
Count *d*
While (press enter)
Recorded *d*
Input 1 : d
Calculate CR_{Pd}
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 5. Part of the EPSBTimev01 algorithm.

4. Experiment process and evaluation

4.1. Test collection

To evaluate the algorithm, we examined a test dataset comprising 617 authentic records from 111 individuals at a selected company between 2017 and 2022. This five-year span allowed us to scrutinize user actions during password modifications. Upon reviewing the historical login password database, it was evident that 111 users changed their passwords multiple times within the Five-year period, specifically:

- 13 users changed their passwords 4times;
- 43 users did so 5times;
- 41 users made 6 modifications;
- 8 users adjusted theirs 7 times;
- 28 users updated theirs 3 times;
- 6 users changed 8 times.

The user count was 111, and the database contained 617 records. We excluded the last password from each user to create a test collection. Hence, the test collection comprises 111 records, with each record representing the last correct password excluded from the CR-Database for all users.

The selection of users for this study was based on available log data used by the IT department for various tests and experiments. The dataset was created by utilizing each user's most recently updated password.

4.2. Evaluation measure

To assess the effectiveness of the CR algorithm EPSBalgorithmv01, and the. EPSBalgorithmv01, we used the precision metric, which is defined as follows:

Precision (P) measures the proportion of correctly identified passwords that are considered successful.

Precision (P) = #(Relevant Passwords Matched [Pass])/#(Total Test Items). **Table 1** explains the precision calculation concept.

Table 1. Precision (*P*) in terms of *TP*, *FP*.

Matched Password	**Not Matched Password**
Pass	True Positives (*TP*)
Fail	False Negatives (*FN*)

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

4.3. Experiment

For the experiment, the test dataset containing 111 users was uploaded to the developed smart security application. This allowed us to compute the EPSBalgorithmv00 proposed by Shakir et al. (2016) and the EPSBalgorithmv01 proposed in this work, for all 111 users with 111 records. The experimental results are summarized in **Table 2**.

Table 2. Results after the experiment.

Algorithm (*R−DB* = 111)	***TP***	***FP***	***TP + FP***	***TP/(TP + FP)***	**%**
EPSBalgorithmv00	79	32	79 + 32	0.711	71.171
EPSBalgorithmv01	92	19	92 + 19	0.828	82.882

The updated algorithm EPSBalgorithmv01 has demonstrated promising results compared to EPSBalgorithmv00. However, the test collection results highlight the weaknesses of EPSBalgorithmv00 in distinguishing genuine users from false ones, achieving a recognition rate of only 28.00% and with precession of 71.171. In contrast, EPSBalgorithmv01 failed to recognize genuine users from false ones achieving a recognition rate of 17%, and achieved a precision of 82.882%.

The recognition rate of EPSBalgorithmv00 is 71.00%, while the recognition rate of EPSBalgorithmv01 is 82.00%.

The improvement percentage can be calculated using the Equation:

$$\frac{\mathrm{P(EPSBalgorithmv01)-P(EPSBalgorithmv00)}}{\mathrm{P(EPSBalgorithmv00)}} * 100 = \frac{82-71}{71} * 100 = 14\% \quad (3)$$

Therefore, EPSBalgorithmv01 shows an improvement in recognition rate of approximately 14% compared to EPSBalgorithmv00.

5. Results and discussion

The study proceeded through three primary phases: establishing authentication with the EPSB algorithm, conducting preliminary experiments, and assessing outcomes. Initially, authentication development using the EPSBalgorithmv01 was implemented by a developed simulator, after careful consideration and verification for web domain suitability. The algorithm's core components collaborated to gather necessary data for constructing the confidence range. Two preliminary experiments were conducted with 111 users registered from 2017 to 2022, who updated their passwords multiple times. The final phase oversees user conduct, task documentation, statistical analysis, and periodic transmission of findings to the time series analysis layer. This layer, integrated into the research, produces outcomes forwarded to the decision component, facilitating comparison between current and previous outputs to gauge algorithmic advancements.

The study's time series analysis layer is pivotal for decision-making. Regular statistical analysis findings comparison ensures ongoing algorithmic enhancement, considering user behavior and completed actions. The EPSBAlgorithmv01 now includes seven parameters, enhancing the previous six, as depicted in **Table 3**. **Figure 6** illustrates the updated application interface with the new parameter (EPSB)Timev01 by ARIMA.

Table 3. Seven parameters integrated with the EPSBalgorithmV01.

Parameter1	**Parameter2**	**Parameter3**	**Parameter4**	**Parameter5**	**Parameter6**	**Parameter7**
Small letters	Capital Letters	Sum of Small letters + Capital Letters	Numerals	Symbols	Length of the password	ARIMA(EPSBTimev01

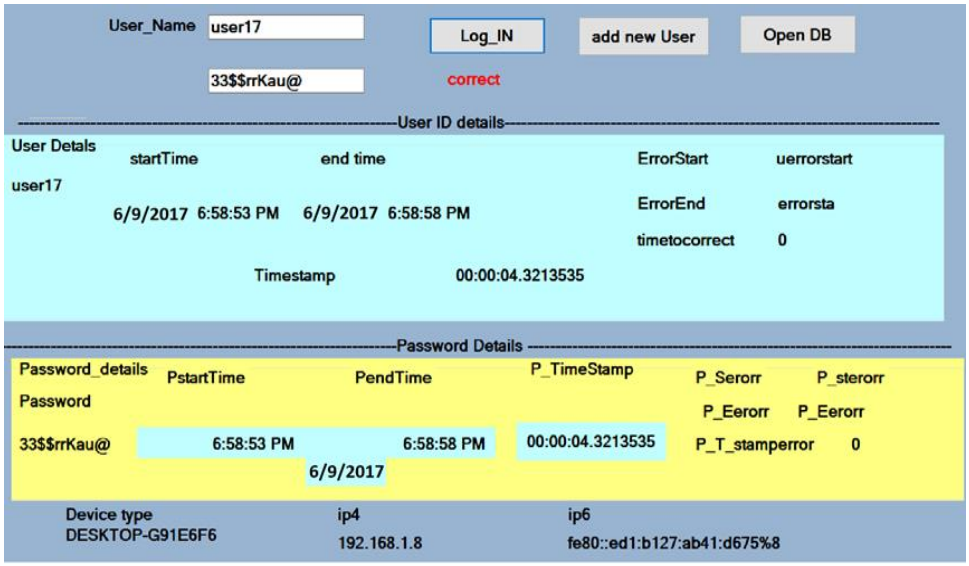

Figure 6. EPSBTimev01 record history interface.

Figures 6–10 extracted from the developed application interfaces to illustrate the application process of the monitoring security system used since 2017 to record user behaviors. This system logs the date and time of each login and measures the duration taken to enter the correct password. **Figure 6** demonstrates this process for user17, who logged in on 09/06/2017. The timer-record procedures were enabled to capture user17's login behavior. For instance, as shown in **Figure 6**, user17 took approximately 4.32 seconds to type the correct password on 09/06/2017. This application continuously monitors all company users and records their activities.

In **Figure 7**, user2 took approximately 5.60 seconds to enter their password. Consequently, all password entry records were continuously recorded and analyzed by the ARIMA algorithm, adding this data as parameter 7 to the security application. **Figure 8** shows how user2's data was analyzed based on the ARIMA algorithm and Confidence Range (CR) from each history record. For user2, the minimum mean time to enter the password was 3.71 seconds, and the maximum was 5.87 seconds. This information is demonstrated in the last two fields of the grid in parallel with the MEAN-CR label on the left side of the application interface. The minimum median time was 3.71 seconds, the maximum median was 6.0 seconds, and the minimum and maximum mode were both 3.71 seconds. For example, when user2 attempted to log in again, it took about 4.78 seconds, as shown in **Figure 8** at the bottom left. The system compares this activity, displaying successful results in green and failed results in red. **Table 4** explains the comparison process executed in **Figure 8**, illustrating how ARIMA with CR was developed and adapted in the CR algorithm application.

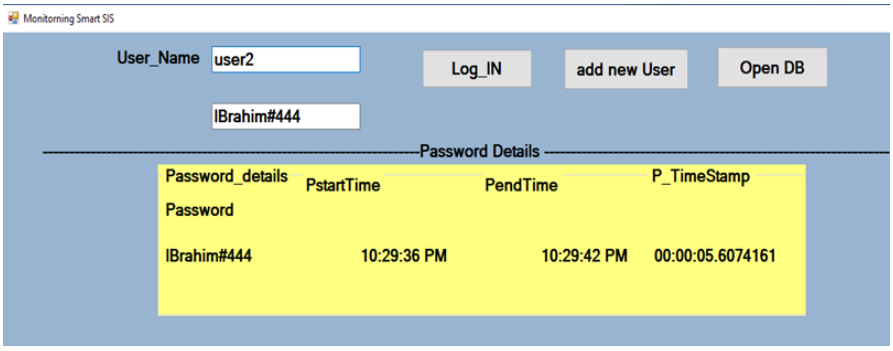

Figure 7. User2 record: EPSBTimev01 record history interface.

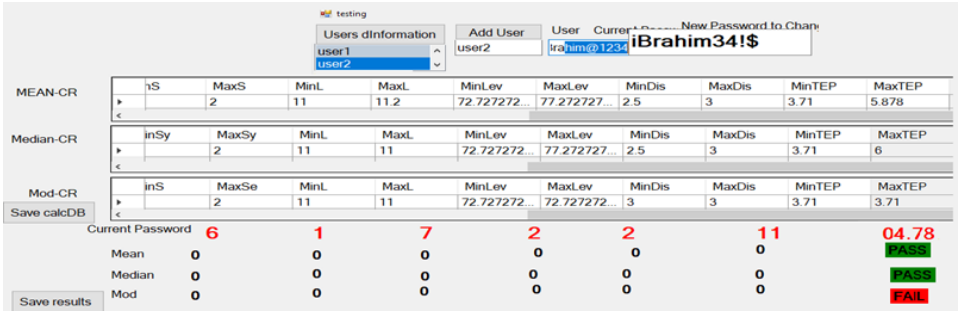

Figure 8. Comparison results for password update of user2 using EPSBTimev01.

Table 4. Comparison process by CR and ARIMA for user2.

	User	**password**		**user**	**Updated password**
	User2	Ibrahim#444		User2	iBrahim34!$
	Min	Max		Min	MAX
Mean-CR	3.71	5.87	PASS	04.78	04.78
Median_CR	3.71	6.0	PASS	04.78	04.78
Mod-CR	3.71	3.71	FAIL	04.78	04.78

As shown in **Table 4** for user2, the time of 4.78 seconds falls within the ranges of 3.71 to 5.87 and 3.71 to 6.0. Therefore, the comparison results for Mean-CR and Median-CR were "Pass." However, since 4.78 seconds is not within the range of 3.71 to 3.71, the result for Mod-CR was "Fail".

In the following scenario, the extracted figures from the security application demonstrate how EPSBTimev01 (ARIMA) (**Figure 9**) was used to improve the results of EPSBalgorithmv00. Figure **10** shows the regular comparison using the six parameters previously explained in **Table 3**. The application matched 10 correct items, resulting in a calculation of (10/18) * 100 = 55.555, which did not meet the configured threshold of ≥ 60. The challenge in this example is that user 17, who plans to update his password, was mistakenly identified by EPSBalgorithmv00 as an unauthorized user (F-User). Such errors could undermine the reliability of the application, especially in sensitive contexts where any mistake could be disastrous. To address this issue, PSBTimev01 (ARIMA) was introduced as a seventh parameter to EPSBalgorithmv00. As indicated by EPSBTimev01 (ARIMA) added 3 pass items to the results, updating the calculation to (13/21) × 100 = 61.904. This result meets the threshold of ≥ 60, allowing the system to correctly identify authorized users.

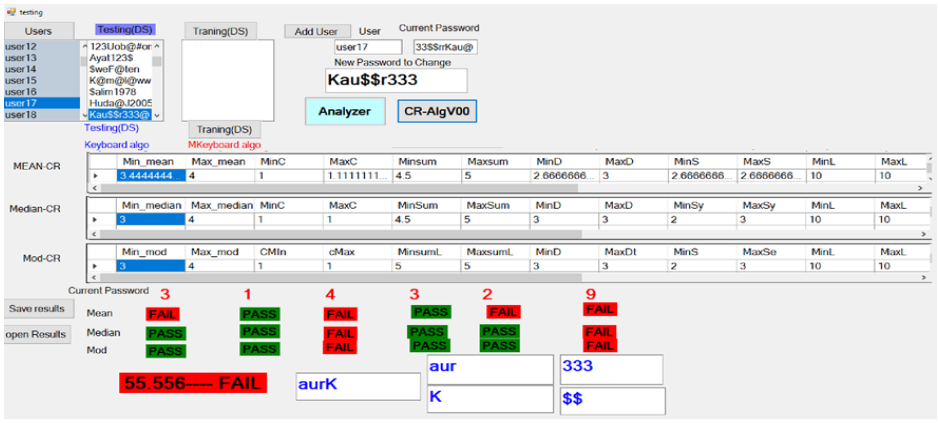

Figure 9. EPSBalgorithmv00 testing user 17.

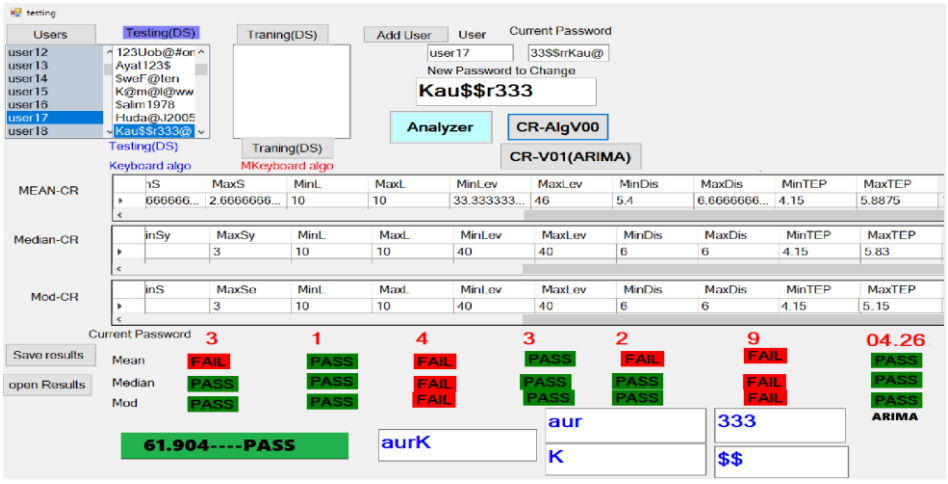

Figure 10. EPSBalgorithmv01 testing user 17.

The evaluation section demonstrates the number of improved cases based on the test collection used in this work.

The updated EPSBalgorithmv01 shows promising outcomes in contrast to EPSBalgorithmv00. However, the test results underscore EPSBalgorithmv00's weaknesses in distinguishing real users from impostors, with a recognition rate of only 28.00% and a precision of 71.171. Conversely, EPSBalgorithmv01 struggles to differentiate genuine users from false ones, achieving a recognition rate of 17% but with a higher precision of 82.882%. EPSBalgorithmv00 attains a recognition rate of 71.00%, whereas EPSBalgorithmv01 achieves an improved recognition rate of 82.00%. The EPSB algorithm utilizes three key variables: EPSBStyle executed by EPSBalgorithmv00 and EPSBTime executed by EPSBalgorithmv01. These variables aid in distinguishing between authorized and unauthorized users and serve as a defense against stolen password attacks. However, EPSBalgorithmv00 is hindered by a limited number of parameters associated with the EPSBTime, which only has six parameters. To address this limitation, this research introduces a temporal ARIMA model aimed at enhancing the functionality of EPSBTime. The investigation unfolds in three main phases: first, the EPSB algorithm is utilized for authentication; second, experimentation commences; and finally, the experimental results are evaluated. The initial implementation of the developed EPSBalgorithmv01 for authentication purposes involves the use of a simulator. Subsequently, the results of tests conducted

using EPSBV01 in detecting unauthorized users are compared before and after adaptation through the ARIMA approach. In a simulated scenario, an unauthorized user, denoted as "X user," gains access through a password theft attack. Throughout the stages presented in this study, tests are conducted to assess the response to such an attempt. The system scrutinizes both the entered password and the user's interaction with it, comparing X user's input time with that of legitimate users during previous logins. In a simulated password theft attack, the EPSB algorithm without ARIMA successfully identified 92 authorized users out of 111. Consequently, it failed to recognize 32 of them. Conducting the same experiment with EPSBalgorithmv01 integrated with ARIMA, the system identified 92 authorized users out of 111 during the Stolen Password Attack (SPA) simulation. The sample comprised carefully selected individuals, with passwords regularly changed to mimic real-world scenarios of password theft. Utilizing the ARIMA algorithm, the system achieved a performance level of up to 82.88%. This demonstrates that EPSBalgorithmv01, with its ARIMA integration, enhances the prevention of unauthorized users from logging in by 14% compared to the standard EPSB algorithm. Thus, the integration of EPSBalgorithmv01 with ARIMA, alongside the analysis of the CR equation, significantly improves the algorithm's accuracy in detecting unauthorized users.

5.1. Limitations

While the proposed EPSBalgorithmv01 demonstrates improved precision in preventing unauthorized access, several limitations were observed that may impact its broader applicability and effectiveness:

Reduced Recognition Rate: Nevertheless, improvements introduced resulted in the decay of the EPSBalgorithmv01 recognition rate to 17%, down from 28% provided by the EPSBalgorithmv00. This decline raises the possibility of a trade-off between the recognition rate and the precision. While, precision increases the security the recognition rate might decrease that affects the usability of the system in special high security environments where: number of users and the precise identification of these users is an essential factor. This can be resolved by perhaps finding the maximum attainable level of accuracy-integral recognition rate trade-off, which could be done by further adjusting the parameters of the model and/or its fine-tuning.

Data Set Constraints: The validation data included 617 records of 111 employee in one organization. This data was informative and helped in development of the algorithm, yet, a more complex data set would confirm the versatility of the algorithm in the presence of different demographic and behavioural parameters. In future work, it is suggested that the dataset should be broadened with more diverse users and organizations for greater generalization.

Reliance on Historical Data and ARIMA: Though ARIMA retains the temporal characteristics of the password entries in the appropriate way, it may not be supersessions because it is based entirely on the past events. Emergent or infrequent behavioral patterns (e.g., anytime of the day the login's were made) may also not be easily identified. This might be solved by incorporating a more adaptive set of machine learning models for more rapid responses to such behavior.

Single-Factor Focus: The current implementation of EPSBalgorithmv01 is anchored in the use of password analysis within a specified time frame as a single factor of authentication. While this enhances the security measure it lacks sufficient measure to block access by unauthorized personnel. The adoption of multiple factors' authentication might be another way to strengthen protection, which is beyond the capabilities of using the time-stamp analysis.

5.2. Future work

Building on the findings and limitations of EPSBalgorithmv01, future research could explore several enhancements and expansions to improve secure access management:

Integration with Multi-Factor Authentication (MFA): TSPA can be extended precisely within the context of multi-factor authentication and its integration into the framework would increase its effectiveness by adding multiple factors, including TSPA, biometrics or OTP. This would afford even better protection particularly to sectors that call for defense including infrastructure industries that can only be secured by enhanced security cover.

Exploring Machine Learning Models for Anomaly Detection: Thus, enhancing flexibility and efficiency of the algorithms, the further studies could explore the models that are designed for identifying anomalous login patterns. Information of the users' login pattern be stored could be dynamically adjusted to make use of a recurrent neural network (RNN) or, in the case of ensemble, identify potential breaches with higher accuracy than statistical methods.

Real-Time Behavioral Analysis: Storing information about login times, geographic locations of the user, as well as the examination of characteristics of the device, TSPA could further be improved to contain the ability to flag any or all access patterns that seemed different from the norm in real-time. Adding behavioral analytics and environmental condition such as geolocation restrictions would make it possible to have a rich model for identifying the out of norm conditions, this would improve the security level.

Industry-Specific Customization: Since the performance of developed algorithm is proven in the field of fintech, the further work can be focused on adaptation of EPSBalgorithmv01 for the other fields including the healthcare or the government technology in which the user activities and security concerns may differ. That is why its modification to take into account sectoral threats/vulnerabilities and data distribution can positively affect both the ease of use and the effectiveness of security measures.

Scalability and Real-Time Application: In future implementations, there is the scaling of the EPSBalgorithmv01 program which will ensure the program's efficiency on larger and highly used systems. Therefore, if TSPA comes up with a real time low latency version of the algorithm, it would fit well with login systems with high frequency without being exposed to security threats.

With these improvements in mind, future investigations of EPSBalgorithmv01 can advance on the work that has been done, identifying the absences and weaknesses

of this architectural solution while exploring further ways to advance the integrated and secure experience of access to different applications and companies.

6. Conclusion

The present research offers important information on the development of the Electronic Personal Synthesis Behavior (EPSB) algorithm, highlighting its weaknesses and recommended alterations that would improve the chances of authenticating a person correctly. The results clearly show there are significant gains when using EPSBalgorithmv01 over the prior EPSBalgorithmv00. Thus, the study propels authentication accuracy, or corresponding augmentation, by methodically mitigating the limitations noted in the prior version of the study, underscoring the necessity of iterative improvement. The incorporation of the ARIMA model into EPSBalgorithmv01 improves its capacity to counteract stolen password attacks by using common login simulations. With this integration it improves the accuracy of the algorithm also on unauthorized user identification that make the security in information systems stronger. To validate the EPSBalgorithmv01 various real-time data and multiple experimental measurements were used. This study added another parameter based on the timestamp duration of the password entry with a future forecast by ARIMA helping to develop more complex algorithm with seven parameters. This study should help emphasize the need to fine-tune cybersecurity algorithms more as fundamental frameworks and policies are being enacted. These enhancements of EPSBalgorithmv01 have given real-world benefits for secure access management as well as practical implications considering the management of infrastructure in the field of information security; it has provided direction for subsequent research and application in the information security arena.

Author contributions: Conceptualization, MS; methodology, BS and OA; software, BS; validation, MS, BS and OA; formal analysis, BS, OA and BB; investigation, MS and BS; resources, BS and OA; data curation, MS, BS and BB; writing—original draft preparation, MS; writing—review and editing, OA, MS, OA and BB; visualization, BS, OA and BB; supervision, BS; project administration, MS; funding acquisition, BS, MS, OA and BB. All authors have read and agreed to the published version of the manuscript.

Acknowledgments: The authors extend their heartfelt gratitude to their Universities for their invaluable support in facilitating this research. This study is part of the ongoing work stemming from the university's internal project, "No. IRG/UoB/CoB-005/2022-23."

Conflict of interest: The authors declare no conflict of interest.

References

Ahmad, M., Azam, M. M., & Khokhar, F. (2022). Leveraging time series analysis for anomaly detection in cybersecurity. Journal of Cybersecurity Research, 8(3), 156-170.

Ahmed, S., Nielsen, I. E., Tripathi, A., Siddiqui, S., Ramachandran, R. P., & Rasool, G. (2023). Transformers in time-series analysis: A tutorial. Circuits, Systems, and Signal Processing, 42(12), 7433–7466.

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. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2937357

Al-Hashimi, M., Shakir M. Hammood, M., and Eldow, A. (2007). Address the Challenges of implementing electronic document system in Iraq e-government-Tikrit City as a Case study. Journal of Theoretical & Applied Information Technology, 95(15).

Al-Shamsi, I. R., Shannaq, B., Adebiaye, R., & Owusu, T. (2024). Exploring biometric attendance technology in the Arab academic environment: Insights into faculty loyalty and educational performance in policy initiatives. Journal of Infrastructure, Policy and Development, 8(9), 6991. https://doi.org/10.24294/jipd.v8i9.6991

Alshamsi, I., Sadriwala, K. F., Ibrahim Alazzawi, F. J., & Shannaq, B. (2024). Exploring the impact of generative AI technologies on education: Academic expert perspectives, trends, and implications for sustainable development goals. Journal of Infrastructure, Policy and Development, 8(11), 8532. https://doi.org/10.24294/jipd.v8i11.8532Alqahtani, H., & Kumar, G. (2024). Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems. Engineering Applications of Artificial Intelligence, 129, 107667. https://doi.org/10.1016/j.engappai.2023.107667

Anderson, T. W. (2011). The Statistical Analysis of Time Series. John Wiley & Sons.

Ariens, S., Ceulemans, E., & Adolf, J. K. (2020). Time series analysis of intensive longitudinal data in psychosomatic research: A methodological overview. Journal of Psychosomatic Research, 137, 110191. https://doi.org/10.1016/j.jpsychores.2020.110191

Ashtari, A., & Alizadeh, B. (2022). A comparative study of machine learning classifiers for secure RF-PUF-based authentication in internet of things. Microprocessors and Microsystems, 93, 104600.

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(1s), Article 1s.

Chaudhary, A., Singh, P., & Kaur, M. (2023). Enhancing cyber defense mechanisms using AI-driven language models. Journal of Cybersecurity and Privacy, 5(2), 134-156.

Continuous Multi-Factor Authentication: The Future of MFA. (2024). Retrieved June 21, 2024, from https://www.twosense.ai/blog/continuous-multi-factor-authentication-the-future-of-mfa

Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019). Evaluating User Perception of Multi-Factor Authentication: A Systematic Review (arXiv:1908.05901). arXiv. https://doi.org/10.48550/arXiv.1908.05901

Degiannakis, S., & Xekalaki, E. (2004). Autoregressive Conditional Heteroscedasticity (ARCH) Models: A Review. Quality Technology & Quantitative Management, 1(2), 271–324. https://doi.org/10.1080/16843703.2004.11673078

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. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3151903

Durbin, J. (1959). Efficient Estimation of Parameters in Moving-Average Models. Biometrika, 46(3/4), 306–316. https://doi.org/10.2307/2333528

Elgar, F. J., Stefaniak, A., & Wohl, M. J. A. (2020). The trouble with trust: Time-series analysis of social capital, income inequality, and COVID-19 deaths in 84 countries. Social Science & Medicine, 263, 113365. https://doi.org/10.1016/j.socscimed.2020.113365

Emmanuel, O. (2024). Estimation of future population status using global birth rate analysis. Retrieved June 21, 2024, from https://www.researchgate.net/profile/Emmanuel-Osho-2/publication/375765213_ESTIMATION_OF_FUTURE_POPULATION_STATUS_USING_GLOBAL_BIRTH_RATE_ANALYSIS/links/655b59c53fa26f66f4182105/ESTIMATION-OF-FUTURE-POPULATION-STATUS-USING-GLOBAL-BIRTH-RATE-ANALYSIS.pdf

Ghorbani, A. A., & Lu, W. (2021). Anomaly detection using time series analysis in cyber defense. IEEE Transactions on Network Security, 30(5), 340-358.

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(10s), Article 10s.

Guarracino, F., Cabrini, L., Baldassarri, R., Petronio, S., De Carlo, M., Covello, R. D., Landoni, G., Gabbrielli, L., & Ambrosino, N. (2010). Noninvasive Ventilation for Awake Percutaneous Aortic Valve Implantation in High-Risk Respiratory Patients: A

Case Series. Journal of Cardiothoracic and Vascular Anesthesia, 294(24), 3124–3130. https://doi.org/10.1053/j.jvca.2010.06.032

Gunawan, D., & Astika, W. (2022). The Autoregressive Integrated Moving Average (ARIMA) Model for Predicting Jakarta Composite Index. Jurnal Informatika Ekonomi Bisnis, 1–6. https://doi.org/10.37034/infeb.v4i1.114

Hằng, L. T. T., & Dũng, N. X. (2022). ARIMA Model – Vietnam's GDP Forecasting. In N. Ngoc Thach, D. T. Ha, N. D. Trung, & V. Kreinovich (Eds.), Prediction and Causality in Econometrics and Related Topics (pp. 145–151). Springer International Publishing. https://doi.org/10.1007/978-3-030-77094-5_14

Hazratifard, M., Gebali, F., & Mamun, M. (2022). Using Machine Learning for Dynamic Authentication in Telehealth: A Tutorial. Sensors, 22(19), Article 19. https://doi.org/10.3390/s22197655

Hewamalage, H., Bergmeir, C., & Bandara, K. (2021). Recurrent Neural Networks for Time Series Forecasting: Current status and future directions. International Journal of Forecasting, 37(1), 388–427. https://doi.org/10.1016/j.ijforecast.2020.06.008

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. https://doi.org/10.1007/s10796-020-10044-1

Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. Sensors, 23(21), Article 21. https://doi.org/10.3390/s23218944

James, E., & Rabbi, F. (2023). Fortifying the IoT Landscape: Strategies to Counter Security Risks in Connected Systems. Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries, 6(1), Article 1.

Jebamikyous, H., Li, M., Suhas, Y., & Kashef, R. (2023). Leveraging machine learning and blockchain in E-commerce and beyond: Benefits, models, and application. Discover Artificial Intelligence, 3(1), 3. https://doi.org/10.1007/s44163-022-00046-0

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.

Khan, H., Khan, U., & Khan, M. A. (2020). Causal Nexus between Economic Complexity and FDI: Empirical Evidence from Time Series Analysis. The Chinese Economy, 53(5), 374–394. https://doi.org/10.1080/10971475.2020.1730554

Lim, B., Arık, S. Ö., Loeff, N., & Pfister, T. (2021). Temporal Fusion Transformers for interpretable multi-horizon time series forecasting. International Journal of Forecasting, 37(4), 1748–1764. https://doi.org/10.1016/j.ijforecast.2021.03.012

Liu, Y., Gong, C., Yang, L., & Chen, Y. (2020). DSTP-RNN: A dual-stage two-phase attention-based recurrent neural network for long-term and multivariate time series prediction. Expert Systems with Applications, 143, 113082. https://doi.org/10.1016/j.eswa.2019.113082

M, S., A, A., O, Y., M, W., & M, A.-E. (2016). Model of security level classification for data in hybrid cloud computing. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85006374982&partnerID=40&md5=a786299f0ff4ea8b573c509cc110952d

McDowall, D., McCleary, R., & Bartos, B. J. (2019). Interrupted time series analysis. Oxford University Press. https://books.google.com/books?hl=ar&lr=&id=bACvDwAAQBAJ&oi=fnd&pg=PP1&dq=Interrupted+Time+Series+Analysis.+Oxford+University+Press,+2019.&ots=BJTnJPghQm&sig=tlv-ku1Fw8eG3N1mPOFgaseuudQ

Mills, T. C. (2019). Applied Time Series Analysis: A Practical Guide to Modeling and Forecasting. Elsevier.

Murat, M., Malinowska, I., Gos, M., & Krzyszczak, J. (2018). Forecasting daily meteorological time series using ARIMA and regression models. International Agrophysics, 32(2), 253–264. https://doi.org/10.1515/intag-2017-0007

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). NIST. https://doi.org/10.6028/NIST.CSWP.04162018

Nguyen, C. H. (2021). Labor force and foreign direct investment: Empirical evidence from Vietnam. The Journal of Asian Finance, Economics and Business, 8(1), 103–112.

Papaspirou, V., Maglaras, L., Ferrag, M. A., Kantzavelou, I., Janicke, H., & Douligeris, C. (2021). A novel Two-Factor HoneyToken Authentication Mechanism. 2021 International Conference on Computer Communications and Networks (ICCCN), 1–7. https://doi.org/10.1109/ICCCN52240.2021.9522319

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

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. https://doi.org/10.1186/s13635-022-00132-x

Roopashree, S., Anitha, J., Mahesh, T. R., Vinoth Kumar, V., Viriyasitavat, W., & Kaur, A. (2022). An IoT based authentication system for therapeutic herbs measured by local descriptors using machine learning approach. Measurement, 200, 111484. https://doi.org/10.1016/j.measurement.2022.111484

Rosnawintang, R., Tajuddin, T., Adam, P., Pasrun, Y. P., & Saidi, L. O. (2020). EFFECTS OF CRUDE OIL PRICES VOLATILITY, THE INTERNET AND INFLATION ON ECONOMIC GROWTH IN ASEAN-5 COUNTRIES: A PANEL AUTOREGRESSIVE DISTRIBUTED LAG APPROACH. International Journal of Energy Economics and Policy, 11(1), 15–21. https://doi.org/10.32479/ijeep.10395

SciELO - Brazil—Auto-Regressive Integrated Moving Average Model (ARIMA): Conceptual and methodological aspects and applicability in infant mortality Auto-Regressive Integrated Moving Average Model (ARIMA): Conceptual and methodological aspects and applicability in infant mortality. . Retrieved June 21, 2024, from https://www.scielo.br/j/rbsmi/a/QyYHhYbYK9wRnKmV3cP5v9n/?lang=en

Shakir M, Abood R, Sheker M, et al. (2024). Users Acceptance of Electronic Personal Synthesis Behavior (EPSB): An Exploratory Study | SpringerLink. (2024). Retrieved June 17, 2024, from https://link.springer.com/chapter/10.1007/978-3-030-64987-6_30

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.

Shams, T. B., Hossain, M. S., Mahmud, M. F., Tehjib, M. S., Hossain, Z., & Pramanik, M. I. (2022). EEG-based biometric authentication using machine learning: A comprehensive survey. ECTI Transactions on Electrical Engineering, Electronics, and Communications, 20(2), 225–241.

Shannaq, B. (2024a). Improving security in intelligent systems: how effective are machine learning models with tf- idf vectorization for password-based user classification. 102(22).

Shannaq, B. (2024b). Unveiling the Nexus: Exploring TAM Components Influencing Professors' Satisfaction With Smartphone Integration in Lectures: A Case Study From Oman. TEM Journal, 2365–2375. https://doi.org/10.18421/TEM133-63

Shannaq, B., & Shakir, M. (2024). Enhancing Security with Multi-Factor User Behavior Identification Via Longest Common Subsequence Analysis. Informatica 48 (2024) 73–82 73, 48(16), 73–82. https://doi.org/10.31449/inf.v48i19.6529.

Shannaq, B., Muniyanayaka, D. K., Ali, O., Bani-Ismail, B., & Al Maqbali, S. (2024). Exploring the role of machine learning models in risk assessment models for developed organizations' management decision policies. Journal of Infrastructure, Policy and Development, 8(13), 9364. https://doi.org/10.24294/jipd9364

Shannaq, B., Shamsi, I. A., & Majeed, S. N. A. (2019). Management Information System for Predicting Quantity Martials. 8(4).

Shastry, K. A., & Shastry, A. (2023). An integrated deep learning and natural language processing approach for continuous remote monitoring in digital health. Decision Analytics Journal, 8, 100301. https://doi.org/10.1016/j.dajour.2023.100301

Srinivasan, M., & C, S. N. (2024). Machine Learning-Based Security Enhancement in Heterogeneous Networks Using an Effective Pattern Mining Framework. International Journal of Intelligent Systems and Applications in Engineering, 12(1s), Article 1s.

Stein, E. M., & Shakarchi, R. (2011). Fourier Analysis: An Introduction. Princeton University Press.

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

Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., & Kundi, G. S. (2021). Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. Technology in Society, 65, 101565. https://doi.org/10.1016/j.techsoc.2021.101565

Thomas, P. A., & Preetha Mathew, K. (2023). A broad review on non-intrusive active user authentication in biometrics. Journal of Ambient Intelligence and Humanized Computing, 14(1), 339–360. https://doi.org/10.1007/s12652-021-03301-x

Tsang, Y. P., Choy, K. L., Wu, C. H., Ho, G. T. S., & Lam, H. Y. (2019). Blockchain-Driven IoT for Food Traceability With an Integrated Consensus Mechanism. IEEE Access, 7, 129000–129017. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2940227

U.S, S. N. (2024). Why Samsung NEXT and HYPR Believe the Future Will Be Passwordless. Retrieved June 21, 2024, from https://news.samsung.com/us/samsung-next-hypr-believe-future-will-passwordless

Vyas, B., & Hurry, R. (2023). Java in Action: AI for Fraud Detection and Prevention. https://doi.org/10.13140/RG.2.2.20929.33125

Yang, B., Liu, S., Xu, T., Li, C., Zhu, Y., Li, Z., & Zhao, Z. (2024). AI-Oriented Two-Phase Multifactor Authentication in SAGINs: Prospects and Challenges. IEEE Consumer Electronics Magazine, 13(1), 79–90. IEEE Consumer Electronics Magazine. https://doi.org/10.1109/MCE.2023.3262904

Zeng, A., Chen, M., Zhang, L., & Xu, Q. (2023). Are transformers effective for time series forecasting? Proceedings of the AAAI Conference on Artificial Intelligence, 37(9), 11121–11128.

Zhou, P., Xu, H., Lee, L. H., Fang, P., & Hui, P. (2022). Are You Left Out? An Efficient and Fair Federated Learning for Personalized Profiles on Wearable Devices of Inferior Networking Conditions. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 6(2), 91:1-91:25. https://doi.org/10.1145/3534585

Zhu, H., Wang, X., Chen, X., & Zhang, L. (2020). Similarity search and performance prediction of shield tunnels in operation through time series data mining. Automation in Construction, 114, 103178. https://doi.org/10.1016/j.autcon.2020.103178