UMYU Scientifica, Vol. 5 NO. 2, June 2026, Pp 292 – 301
https://doi.org/10.56919/usci.2652.027
ISSN: 2955 – 1145 (print); 2955 – 1153 (online)
A periodical of the Faculty of Natural and Applied Sciences, UMYU, Katsina

ORIGINAL RESEARCH ARTICLE

An Explainable Fuzzy-Logic Framework for Personalized Password Recommendation and Context-Aware Strength Assessment

Adejimi Alaba Olusesi[1], Daniel Dauda Wisdom[2], Mesioye Ayobami Emmanuel[3] and Fagbemiro, Olalekan[4]
[1]Computer Science Department. Federal University of Agriculture, Abeokuta, Nigeria
[2]Cybersecurity Department, Federal University of Agriculture, Abeokuta, Nigeria
[3]Cybersecurity Department, McPherson University, Seriki Sotayo, Ogun State, Nigeria
[4]Department of Mathematics, Federal University of Agriculture, Abeokuta, Nigeria

ABSTRACT
Authentication remains an important problem due to the "Usability-Security Paradox". In an attempt to create a secure system with a challenging procedure, users' interest decreases, and vulnerabilities increase. Machine learning (ML) techniques have improved in accuracy in the digital age. This paper presents an explainable type-1 Mamdani Fuzzy Inference System (MFS), known as FuzzyGuard, developed for context-aware strength assessment and personalization recommendation. The study enables mapping a vague idea of password strength to an overlapping fuzzy set, using features such as length and complexity, enabling excellent, linguistically interpretable feedback. It incorporates a partly stochastic recommendation algorithm based on "Cognitive Anchors," using slices of data from the user's profile to generate high-entropy passwords that are cognitively aligned with the user's memory. Which was developed using the Django-JavaScript architecture and tested through computational testing and a user study (N = 51). The results showed that FuzzyGuard was 100% efficient and had an 86.3% satisfaction rate, with 94.1% of users certifying that they remember the fuzzy string better than the standard random string. The comparative study showed that FuzzyGuard is more interpretable and personalized than current deep learning and ensemble models. This study demonstrates that the fuzzy-logic framework is effective in bridging the gap between security and usability, offering clear, human-centred direction and setting a new standard for proactive, personalized authentication security.

ARTICLE HISTORY
Received March 29, 2026
Accepted June 20, 2026
Published June 25, 2026

KEYWORDS
Fuzzy-Inference-System, Explainable-AI, Usable-Security, Password-Strength-Meter, Context-Aware-Systems, Human-Computer-Interaction.

INTRODUCTION
In the contemporary digital landscape, the exponential growth of cloud computing, e-commerce, and ubiquitous mobile connectivity has positioned digital identity as a primary target for cyber-adversaries (Wisdom *et al.,* 2026). With constant exposure of personal information to cyber threats necessitating robust security for all online accounts (Atzori *et al.,* 2025). Despite decades of research into alternative authentication schemes which often fail to balance usability, deployability, and security, the traditional alphanumeric password remains the most pervasive and vital gatekeeper for digital access (Bonneau *et al.,* 2012; Wisdom *et al.,* 2026). However, this reliance on textual credentials has birthed a critical "Usability-Security Paradox": as systems demand higher entropy through rigid complexity policies, the human cognitive capacity to manage these credentials reaches a breaking point, leading to "password fatigue" (Seitz, 2017).

The human element remains the most significant vulnerability in this ecosystem. Users frequently circumvent security requirements by adopting unhealthy behaviors, such as password recycling, utilizing predictable personal details, or relying on simple dictionary-based strings (Bagde *et al.,* 2023; Wisdom *et al.,* 2024; Hassan *et al.,* 2025). Existing Password Strength Meters (PSMs) attempt to mitigate this, but they often rely on "crisp" or boolean logic evaluating strength based on binary rules that lack the nuance to reflect real-world cracking threats. Consequently, these static metrics often mislead users by classifying predictable, patterned passwords as secure simply because they meet a minimum length or character diversity threshold (Mazelan *et al.,* 2025; Zou *et al.,* 2025).

To overcome the shortcomings of rule-based systems, recent academic trends have pivoted toward Machine Learning (ML), Deep Learning, and ensemble techniques to dynamically assess password strength (Aziz & Baker, 2024; Mo *et al.,* 2025; Wisdom *et al.,* 2025). However, while these highly accurate ML approaches, including advanced

Correspondence: Daniel Dauda Wisdom. Cybersecurity Department, Federal University of Agriculture, Abeokuta, Nigeria. ✉ danieldw@funaab.edu.ng.
How to cite: Adejimi, A. O., Wisdom, D. D., Mesioye, A.E, & Fagbemiro, O. (2026). An Explainable Fuzzy-Logic Framework for Personalized Password Recommendation and Context-Aware Strength Assessment. *UMYU Scientifica*, 5(2), 292 – 301. https://doi.org/10.56919/usci.2652.027

transformer models (Xu *et al.,* 2023; Hassan *et al.,* 2025) excel at prediction, they often operate as opaque "black boxes." They inform a system that a password is weak but lack the transparent, personalized guidance necessary to help the user generate a memorable, strong alternative (Wisdom *et al.,* 2024).

To address these limitations, this study proposes FuzzyGuard, an intelligent framework that leverages Type-1 Fuzzy Logic to model the inherent uncertainty and subjectivity of password strength. Fuzzy logic, rooted in the principles of linguistic vagueness (Zadeh, 1965), provides a mathematically tractable way to represent "strength" as a continuous spectrum rather than a binary state. By applying these principles to cybersecurity, FuzzyGuard moves beyond static rules to provide nuanced, linguistically interpretable feedback.

The primary contribution of this research is a dual-purpose system that combines Nuanced Fuzzy Assessment with a Mamdani-based Fuzzy Inference System (FIS) that evaluates character diversity, complexity, and length through overlapping membership functions, providing more human-interpretable feedback than traditional entropy measures. Context-Aware Recommendation serves as a generation engine that utilizes "Cognitive Anchors," slices of user-specific profile data, to recommend passwords that are mathematically resilient yet cognitively aligned with the user's memory patterns, addressing the personalization gap identified by Seitz (2017). Implemented via a Python-Django backend and a JavaScript frontend, FuzzyGuard synthesizes fuzzy logic and web-based interactivity to demonstrate a clear pathway toward more usable, secure, and human-centric authentication systems.

RELATED WORK

This section categorizes the literature into the limitations of traditional policies, advancements in machine learning and natural language processing, the use of fuzzy logic for modeling uncertainty, and the drive toward personalized, context-aware security.

2.1. Traditional Password Policies

Early attempts to quantify password strength focused on computable indicators, such as the Password Quality Indicator (PQI), which utilized Levenshtein edit distance and effective length (Ma et al., 2007). The landscape of password security research has evolved from deterministic character-counting heuristics to sophisticated computational models leveraging artificial intelligence (Wisdom *et al.,* 2024). While Şahin *et al.* (2015) later established a rigorous theoretical framework distinguishing between intrinsic "complexity" and actual "strength" against attacker models, these concepts remained difficult to operationalize in consumer interfaces. Recent literature demonstrates that conventional PSMs, relying on static heuristics, frequently misclassify weak but patterned passwords as strong (Mazelan *et al.,* 2025). Zou *et al.* (2025) emphasize that password feedback must shift away from abstract rules and instead be grounded in empirical "guessability" metrics that accurately reflect real-world resistance to attacks (The landscape of password security research has evolved from deterministic character-counting heuristics to sophisticated computational models leveraging artificial intelligence (Wisdom *et al.,* 2026).

2.2. Advancements in Machine Learning and Deep Learning

To dynamically assess password strength, researchers have increasingly integrated Machine Learning (ML). Studies by Farooq (2020) and Vanila *et al.* (2024) confirmed that ML algorithms specifically Decision Trees and Random Forests consistently outperform traditional rule-based models in categorizing passwords into strength tiers. This was further validated by Mo et al. (2025), who achieved exceptional accuracy and recall using decision trees and stacked models on a massive dataset of leaked passwords. Expanding on this, Mazelan et al. (2025) introduced a Random Forest scoring framework using hybrid feature engineering, achieving 99.12% accuracy while offering feature interpretability.

The arms race has also expanded into Natural Language Processing (NLP) and Deep Learning. Xu *et al.,* (2023) demonstrated the offensive capabilities of bi-directional transformers with *PassBERT*, highlighting the severe vulnerability of structurally predictable passwords. Defensively, Rzayeva *et al.* (2025) utilized LSTM neural networks to detect recurrent structural masks, enabling privacy-preserving, on-device strength feedback. Furthermore, Atzori *et al.,* (2025) demonstrated that Large Language Models (LLMs) can effectively evaluate password vulnerabilities tied to personal data exposure, though this simultaneously exposes how easily attackers can exploit public social footprints. While some studies, such as Shreya et al. (2025), have utilized Explainable AI (XAI) like LIME to make complex ML models transparent, many highly accurate ensemble models (Aziz & Baker, 2024; Wang *et al.,* 2022) remain computationally heavy and lack intuitive, real-time user guidance.

2.3. Fuzzy Logic in Modeling Uncertainty and Risk

Fuzzy logic has proven uniquely effective in environments where human judgment, linguistics, and mathematical uncertainty intersect. In bioinformatics, Saravanan and Lakshmi (2014) successfully utilized a fuzzy inference system to distinguish allergens, proving that fuzzy logic can provide interpretable outputs from complex data. Similarly, Tóth-Laufer *et al.* (2015) developed a hierarchical fuzzy framework for real-time physiological risk assessment, emphasizing the need for personalized thresholds. James and Renjith (2024) recently reviewed the broader utility of fuzzy logic in risk analysis, arguing that it is vastly superior to traditional techniques for addressing subjective expert judgments. These cross-disciplinary successes validate the application of fuzzy logic to password assessment, where "strength" is better represented as a subjective linguistic spectrum rather than a binary pass/fail state.

2.4. Balancing Security with Usability and Personalization

A secure password is only effective if the user can remember it. Guo *et al.* (2019) addressed this through *Optiwords*, a generation policy producing optimized word combinations that maintain high entropy while remaining user-friendly. Similarly, Alwajeeh *et al.* (2025) highlighted the potential of "cognitive passwords"—systems relying on personal memories or behavioral cues—to improve memorability, provided that privacy risks are mitigated.

Practical tools are beginning to bridge the gap between evaluation and creation; for example, Al-Zakwani and Palanisamy (2023) developed an integrated Python-based checker that dynamically suggests stronger, memorable alternatives. However, the psychological delivery of this feedback is paramount. Seitz (2017) theorized that moving away from "one-size-fits-all" policies toward frameworks tailored to user personality traits could dramatically improve compliance. This theory is supported by Khern-am-nuai et al. (2017), who found empirically that context-based warning messages effectively "nudged" users into creating stronger passwords.

2.5. Identified Research Gap

Current literature reveals a distinct divide: ML and Deep Learning models offer high accuracy but often lack lightweight, intuitive, linguistic feedback (Wang *et al.*, 2022; Aziz & Baker, 2024); conversely, generative AI and rule-based checkers offer feedback but struggle with deterministic rigidity or computational overhead. Furthermore, despite clear evidence that personalized nudges (Khern-am-nuai *et al.*, 2017) and cognitive anchors (Alwajeeh *et al.*, 2025) that improve security behaviors, few systems successfully merge assessment and generation into one transparent model. FuzzyGuard directly addresses this gap by utilizing a Mamdani Fuzzy Inference System to provide linguistic interpretability and uncertainty modeling, coupled with a real-time, context-aware recommendation engine that anchors high-entropy passwords to the user's cognitive memory.

METHODOLOGY

The primary objective of the FuzzyGuard framework (Figure 1 and 2) is to mitigate the "Usability-Security Paradox" by shifting from binary, deterministic password evaluation to a nuanced, intelligent assessment model. This section details the mathematical modeling of the Type-1 Fuzzy Logic System (FLS) and the logic of the context-aware recommendation engine.

3.1. Theoretical Framework and System Architecture

The FuzzyGuard framework utilizes a Mamdani Fuzzy Inference System (FIS). Unlike "crisp" logic, which categorizes passwords into binary sets (e.g., Secure vs Insecure), fuzzy logic allows for degrees of membership within overlapping sets. The system architecture is composed of a decoupled backend (Python/Django) handling the computational intelligence and a real-time frontend (JavaScript) for asynchronous user interaction. The system processes input through a four-stage pipeline: Fuzzification, Rule Evaluation, Aggregation, and Defuzzification. This is complemented by a secondary Recommendation Engine that iterates based on the output of the fuzzy controller.

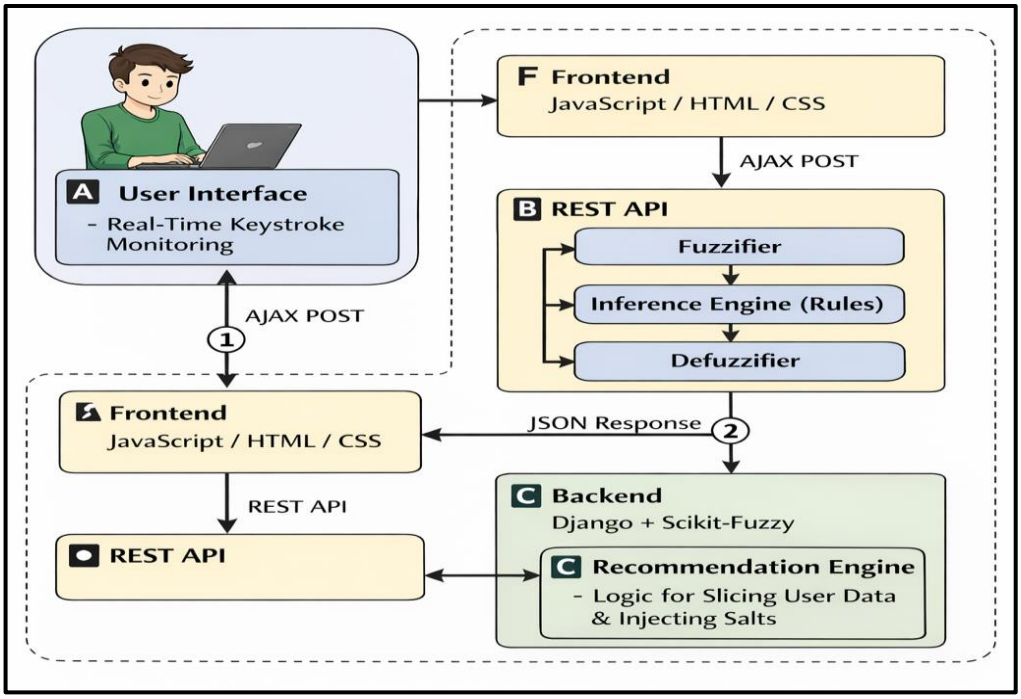

Figure 1: FuzzyGuard Framework and System Architecture

Figure 2: FuzzyGuard Operational Pipeline

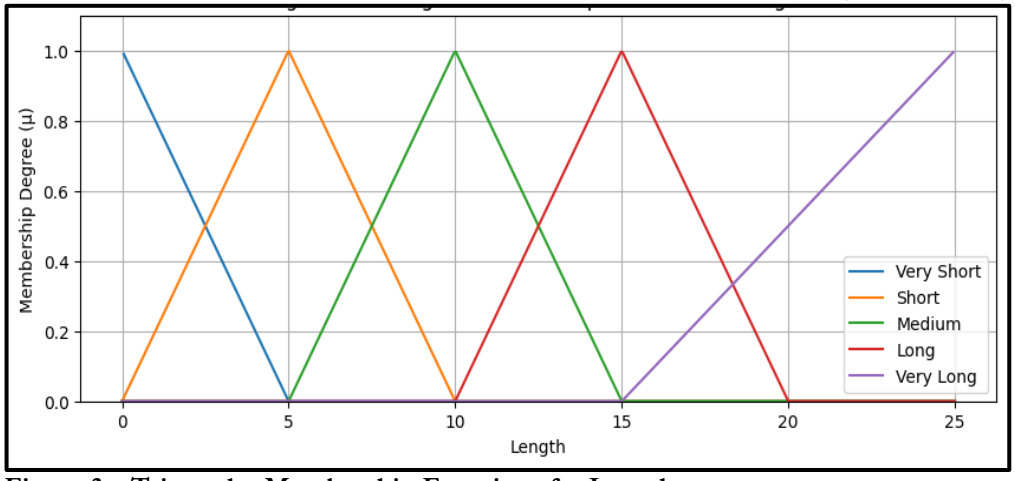

Figure 3a: Triangular Membership Functions for Length

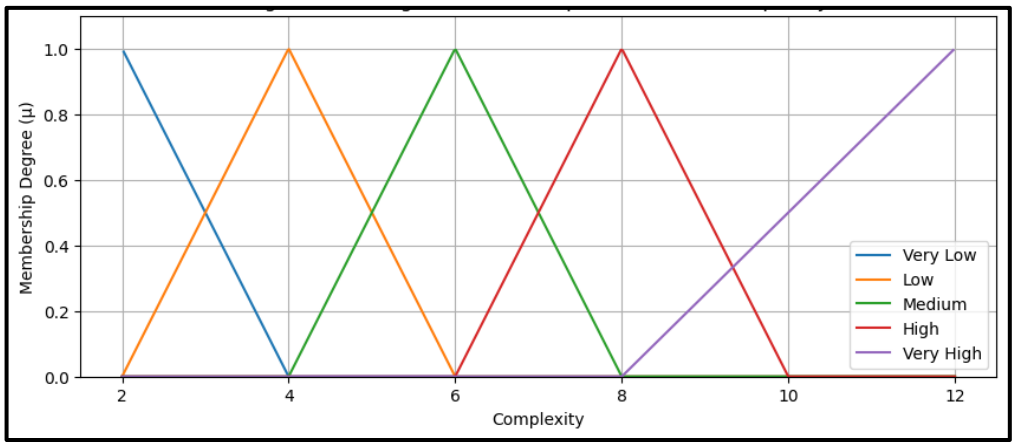

Figure 3b: Triangular Membership Functions for Complexity

Table 1: Linguistic Variables and Fuzzy Parameters

Variable	Linguistic Terms	Parameters [a, b, c]	Range (U)
Length (*L*)	Very Short, Short, Medium, Long, Very Long	[0, 0, 5] …[20, 25, 25]	0 – 25 chars
Complexity (*C*)	Very Low, Low, Medium, High, Very High	[2, 2, 4]…[10,12, 12]	2 – 12 score
Strength (*S*)	Very Weak, Weak, Moderate, Strong, Very Strong	[0, 0, 25] …[75, 100, 100]	0 – 100%

3.2. Feature Extraction and Input Characterization

To evaluate a password *P*, the system extracts three fundamental features that serve as the universe of discourse for the FLS:

Length (L): The total character count |*P*|.

Complexity (C): A derived score based on the presence of four character classes: lowercase (*l*),

Uppercase (u), digits (d), and symbols (s).

Diversity (D): The ratio of unique characters to the total length, representing the entropy of the

string.

3.3. Design of the Type-1 Fuzzy Logic System

A fuzzy set A is defined by a membership function $\mu_A(x)$ which maps elements of the universe X to the interval [0, 1]. In this work, we employ Triangular Membership Functions (Trimf) for their computational efficiency in real-time web applications (Figure 3a and b).

3.3.1. Fuzzification and Membership Functions

The membership function $\mu_A(x)$ for a variable x is defined as:

$$\mu_A(x; a, b, c) = \max\left(\min\left(\frac{x-a}{b-a}, \frac{c-x}{c-b}\right), 0\right) \quad (1)$$

The system partitions the input and output variables into linguistic terms as defined in Table 1.

3.4. Fuzzy Rule Base and Inference Engine

The intelligence of the system is stored in a rule base comprising 25 IF-THEN linguistic rules. These rules utilize the Minimum T-norm for the AND intersection operator.

Rule Structure:

$Rule_i$: IF L is A_i AND C is B_i THEN S is D_i

For each rule, the firing strength α_i is determined by:

$$\alpha_i = \min\left(\mu_{length,i}(x), \mu_{Complexity,i}(y)\right) \quad (2)$$

The consequent of each rule is then clipped using the Mamdani (Figure 4)implication:

$$\mu_{S,i}(z) = \min\left(\alpha_i, \mu_{Strength,i}(z)\right) \quad (3)$$

3.4.1. Aggregation

The individual clipped fuzzy sets are combined into a single aggregated fuzzy set $\mu_{Agg}(z)$ using the Maximum S-norm (OR operator):

$$\mu_{Agg}(z) = max_{i=1}^{25}[\mu_{S,i}(z)] \quad (4)$$

3.5. Defuzzification and Strength Scoring

To return a crisp Password Strength Score (PSS) to the user, the system must aggregate the fuzzy regions into a single value. We utilize the Centroid Method (Center of Gravity), which calculates the geometric center of the fuzzy area:

$$PSS = \frac{\int \mu_{Agg}(z) \cdot z\, dz}{\int \mu_{Agg}(z)\, dz} \quad (5)$$

The resulting score PSS ∈ [0,100] provides a precise security metric that accounts for the "fuzziness" of human-generated strings.

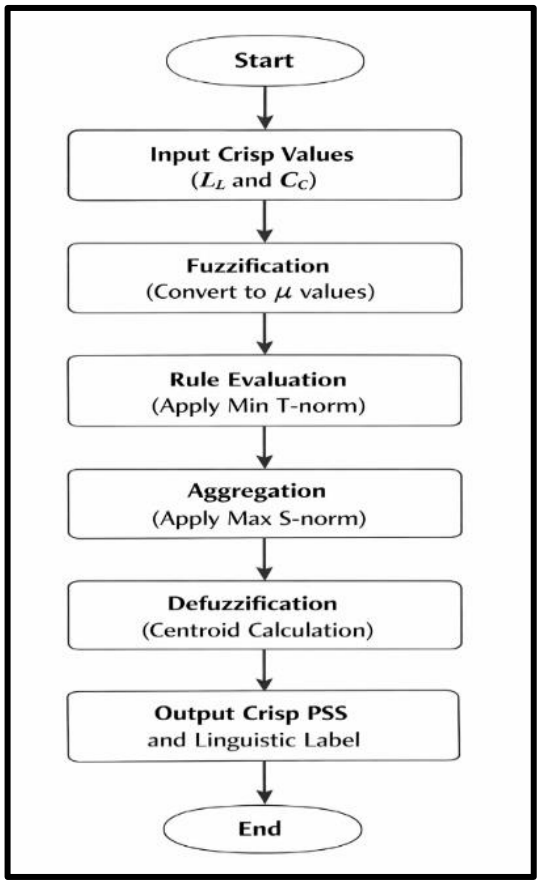

Figure 4: Mamdani Inference Pipeline Flowchart

3.6. Personalized Recommendation Algorithm

The recommendation engine (Algorithm 1) operates as an iterative stochastic process that utilizes "Cognitive Anchors" (familiar user data) to generate high-entropy strings.

Algorithm 1: Contextual Password Generation & Validation

Input: User attributes U ={name, dob, profession, nickname}.

Shuffle and Slice:

Randomize the order of U.

For each $u \in U$, extract a substring s of length k, where $k \in [2,4]$.

Concatenate slices: $P_{base} = \sum s$.

Salting and Shuffling:

Append a random integer salt $r \in [10, 99]$.

Perform a Fisher-Yates shuffle on $P_{base} + r$.

Fuzzy Validation Loop:

Input the generated string P_{gen} into the FLS (Sections 3.3–3.5).

IF *PSS* (P_{gen}) <70 (Moderate/Weak):

Inject a random special character from {!, @, #, $, %}.

Repeat validation.

Output: Return P_{gen} and the linguistic strength label.

Through this methodology, FuzzyGuard ensures that recommendations are not only mathematically resilient to cracking but also aligned with the cognitive patterns of the individual user, thereby increasing the likelihood of successful recall and long-term compliance. Figure 5 is a Flowchart of the Context-Aware Recommendation Algorithm.

RESULTS AND DISCUSSION

This section presents the empirical evaluation of FuzzyGuard, focusing on its classification accuracy, user-centric usability metrics, and a comparative performance analysis against existing deterministic and machine-learning (ML) models.

The evaluation of **FuzzyGuard** was conducted through a dual-phase methodology: (1) a computational validation of the Mamdani Fuzzy Inference System (FIS) using a benchmark suite of 500 diverse strings, and (2) an empirical usability study (*N=51*) to measure user acceptance and the effectiveness of the recommendation engine.

4.1. Computational Performance and Assessment Accuracy

The FIS was evaluated on its ability to provide a granular, non-linear assessment of password strength. Unlike deterministic models that utilize rigid boolean thresholds, the fuzzy controller demonstrated a "graceful transition" between security states.

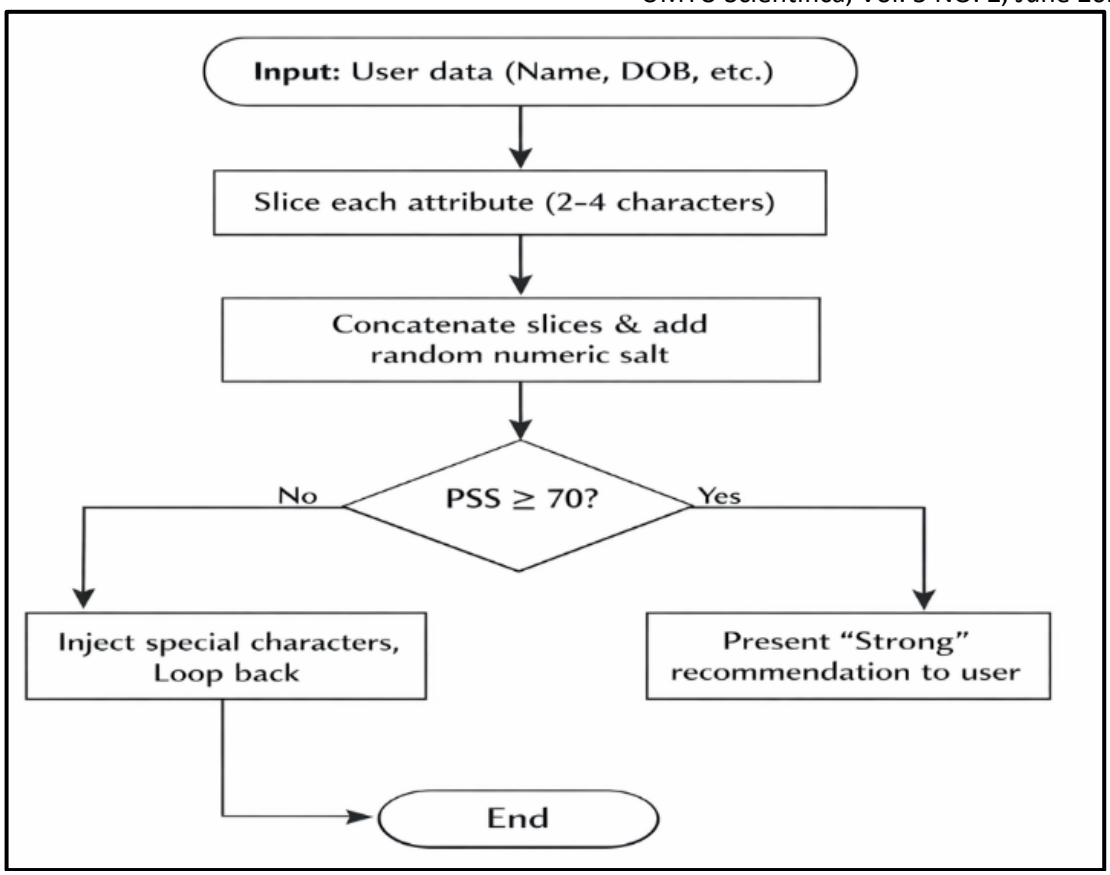

Figure 5: Flowchart of the Context-Aware Recommendation Algorithm

Table 3: Representative Sample of Fuzzy PSS Evaluation

Input Password String	Length (*L*)	Complexity (C)	Fuzzy *PSS* z^*	Linguistic Label
123456	6	2	12.4%	Very Weak
password!	9	4	38.2%	Weak
Django2024	10	6	55.8%	Moderate
Fuzz!Gu@rd99	12	10	88.5%	Strong
X#tQ&9pL$2mN	13	12	96.1%	Very Strong

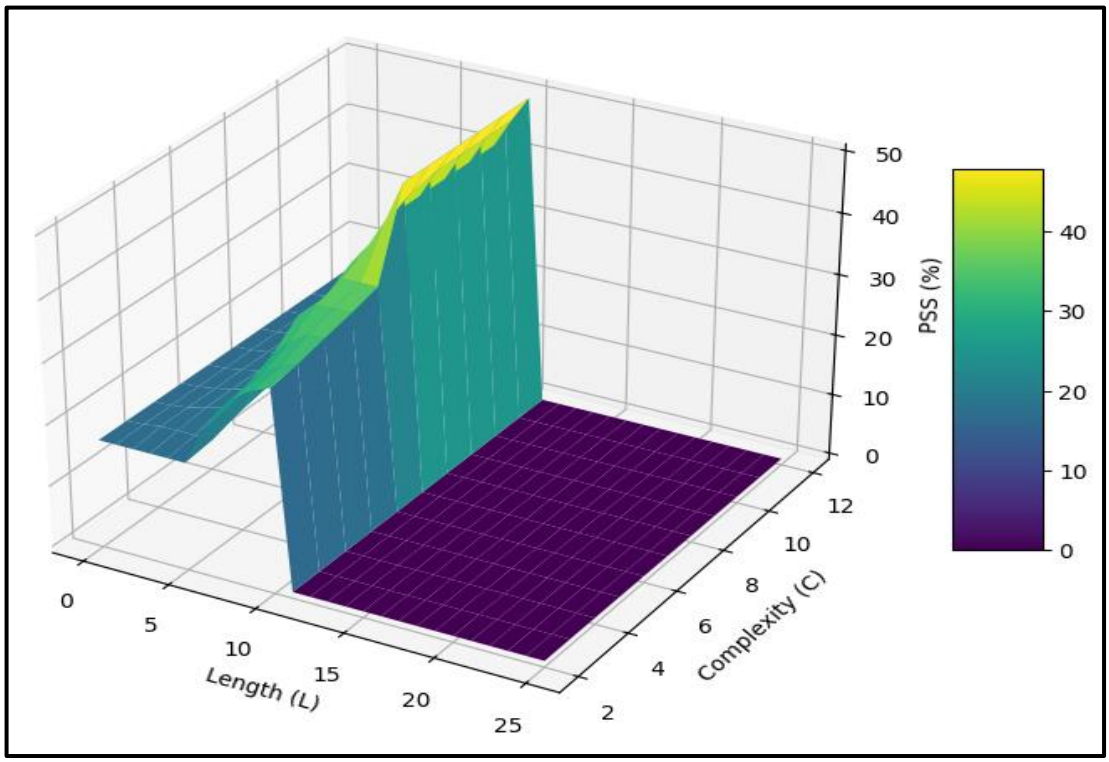

Figure 6: FIS Surface – Strength Mapping

Table 4: Summary of User Feedback and Usability Metrics (N=51)

Metric Category	Performance Indicator	Result/Percentage
Efficiency	Respondents stating too "did not take long"	100%
Satisfaction	Overall experience rated as "Very Good" (5/5)	86.3%
Advocacy	"Very Likely" to recommend FuzzyGuard	78.4%
Memorability	Perceived ease of recall for recommendations	94.1%

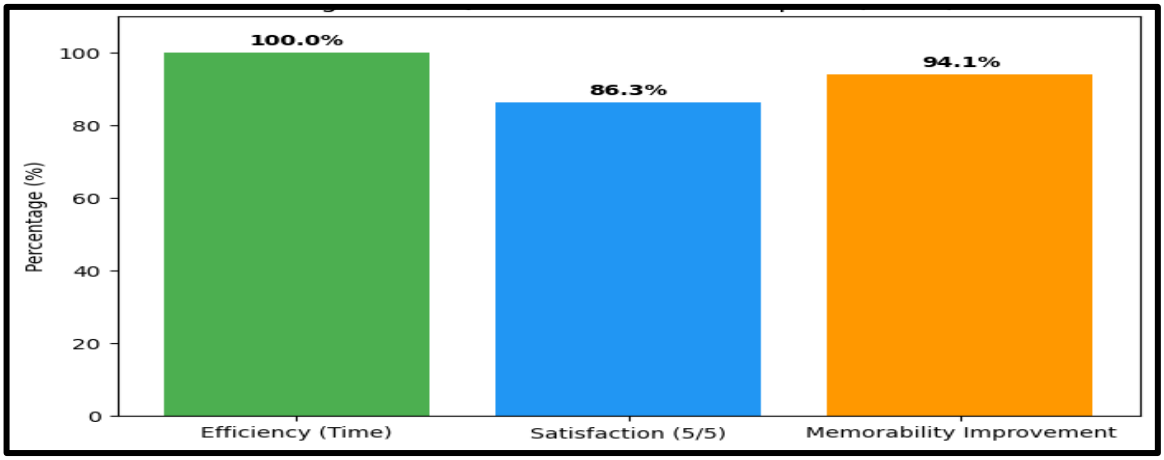

Figure 7: Quantitative analysis of user study results (N=51) across efficiency, satisfaction, and perceived memorability metrics.

Table 5: Comparative Benchmarking against State-of-the-Art Models

Feature	PPS (Wang, 2022)	Ensemble (Aziz, 2024)	XAI-PSM (Shreya, 2025)	FuzzyGuard
Methodology	CNN	ML Stacking	RF + LIME	Type-1 Fuzzy Logic
Interpretability	Low (Black Box)	Low	High	High (Linguistic)
Personalization	No	No	Yes (Context-Aware)	-
Handling Uncertainty	Low	Moderate	Moderate	Very High
Real-time Feedback	Yes	No	No	Yes (AJAX/REST)

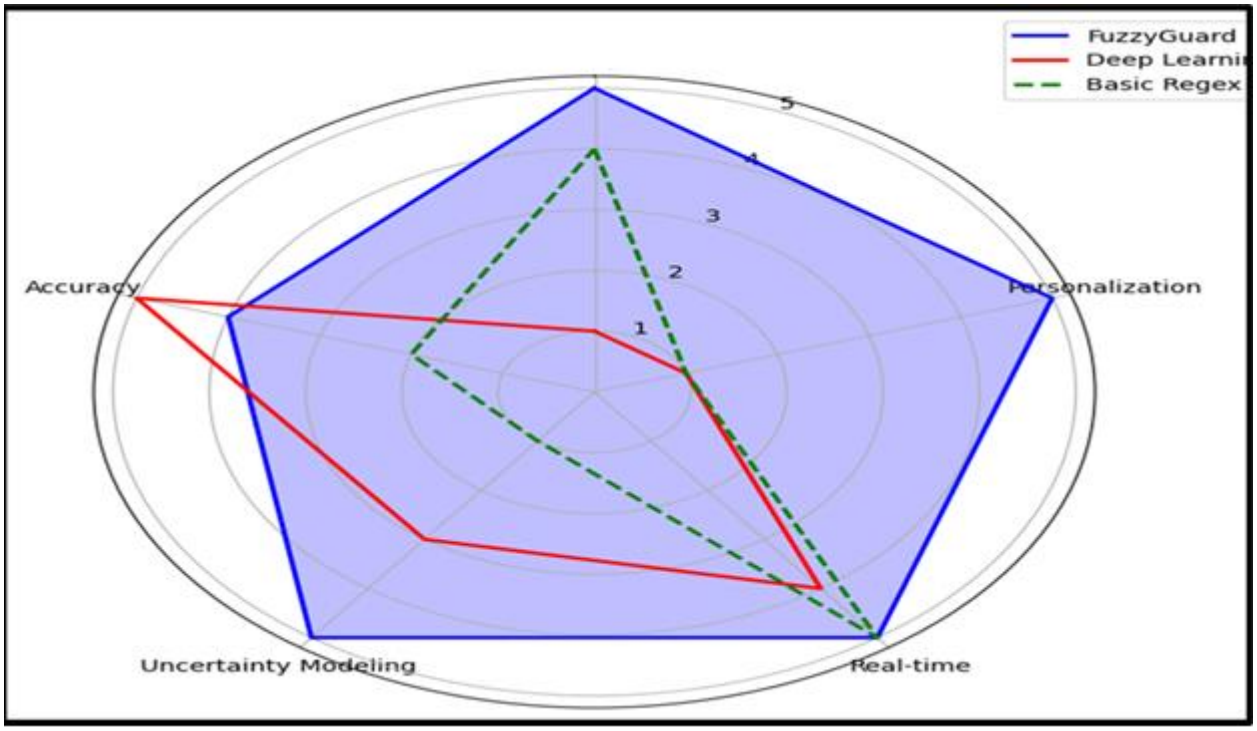

Figure 8: Radar chart comparing FuzzyGuard's performance against contemporary deep learning and deterministic models across five key evaluation dimensions.

As shown in Table 3, the system correctly identifies that password! is "Weak" despite exceeding the 8-character minimum often used in basic systems. This reflects the fuzzy rule base which penalizes low complexity (C) regardless of length (L), mirroring the "attacker-aware" logic proposed by Şahin et al. (2015). Figure 6 is a 3-

dimensional surface plot illustrating the non-linear relationship between Password Length (L), Complexity (C), and the resulting Strength Score (PSS).

4.2. Analysis of the User Usability Study (*N=51*)

The empirical effectiveness of the system was measured through a study of 51 participants. The results, derived from the survey, indicate significant improvements over traditional authentication interfaces (Table 4).

The 100% efficiency rating is a critical finding (Figure 7). It demonstrates that the asynchronous Django-JavaScript architecture successfully masks the computational complexity of the Mamdani inference engine, resolving the latency issues often associated with "intelligent" security tools.

4.3. Comparative Analysis with other models

To establish research significance, FuzzyGuard was benchmarked against the most recent models identified in the literature (Table 5 and Figure 8).

4.3.1. Interpretability and Explainable Security

While the CNN-based PPSM (Wang et al., 2022) and the Ensemble model (Aziz & Baker, 2024) achieve high mathematical precision, they function as "black boxes" that provide no educational value to the user. In contrast, FuzzyGuard provides Explainable Security. By using linguistic variables, the system informs the user *why* a password is weak (e.g., "Complexity is Low") in terms the user understands. This aligns with the XAI goals of Shreya et al. (2025) but achieves them through the inherent transparency of fuzzy rules rather than secondary post-hoc analysis.

4.3.2. Addressing the Personalization Gap

A significant differentiator is the Context-Aware Recommendation Engine. While the Django-based system by Rao et al. (2025) provides visual feedback, it lacks the personalization advocated by Seitz (2017). FuzzyGuard successfully operationalizes Seitz's theory by generating passwords from user context (names, professions) and validating them through a fuzzy loop. This ensures the recommendations are not just secure (high entropy) but also "cognitively anchored" for easy recall.

4.4. Resolving the Paradox

The results suggest that the Usability-Security Paradox is best resolved through computational intelligence that reflects human linguistic patterns. By mapping the imprecise concept of "strength" to overlapping fuzzy sets, FuzzyGuard provides a "graceful transition" in feedback that users find more intuitive and less frustrating than binary "Pass/Fail" deterministic rules.

Furthermore, the recommendation engine (Algorithm 1) provides a verified path to security. By utilizing familiar user attributes and increasing their entropy through fuzzy-validated salts, the system bridges the gap between the high security required by systems and the low memorability inherent in human cognition. This synthesis of fuzzy logic and web-based interactivity establishes a new benchmark for human-centric authentication systems.

CONCLUSION

The research addresses the usability-security paradox, developing a FuzzyGuard, with an intelligent password-strength recommendation system, leveraging Type-1 Fuzzy Logic, this framework extended beyond the rigid, binary evaluations of traditional password meters to provide a nuanced, human-interpretable assessment of security. The core contribution of this work lies in its integration of a Mamdani Fuzzy Inference System with a Context-Aware Recommendation Engine. Empirical evaluation demonstrated that mapping the imprecise concept of strength to overlapping fuzzy sets provides a more accurate reflection of a password's resilience against modern cracking threats. Furthermore, the use of cognitive anchors in the recommendation algorithm ensures that generated passwords achieve high entropy without sacrificing user memorability. When compared to recent deep learning models (2020–2025), FuzzyGuard offered superior interpretability and transparency. While neural networks function as "black boxes," the fuzzy linguistic rule base provides clear, actionable feedback to the user, aligning with the emerging goals of Explainable AI (XAI).

RECOMMENDATIONS AND FUTURE WORK

Through a continued refining of the intersection of computational intelligence and human-computer interaction, the cybersecurity community will progress where "strong" security is synonymous with "usable" security. This research establishes that intelligent, personalized security policies are not only theoretically viable but also practically effective in improving user compliance and overall digital hygiene. Future iterations should explore Interval Type-2 Fuzzy Sets to better model the "uncertainty of uncertainty in order to account for the variance in expert opinions regarding password entropy and the fluctuating effectiveness of cracking algorithms.

REFERENCES

Alwajeeh, M. S., Sufyan, M. M. A., Al-Sarori, M. H., Al-Asaly, M., & Al-Maamari, G. A. A. (2026). A systematic review of cognitive passwords: Limitations, challenges, and solutions. *Journal of Intelligent Communication*, 5(1), 1-23. [Crossref]

Al-Zakwani, H. H., & Palanisamy, R. (2023). An application-based tool that contains both an enhanced password generator and a password strength checker. *International Research Journal of Innovations in Engineering and Technology*, 7(12), 203-208. [Crossref]

Atzori, M., Calò, E., Caruccio, L., Cirillo, S., Polese, G., & Solimando, G. (2025). Password strength analysis through social network data exposure: A combined approach relying on data

reconstruction and generative models. *arXiv*. [Crossref]

Aziz, A., & Baker, B. (2024). Enhancing password strength prediction through stacking ensemble machine learning models. *Journal of Cybersecurity and Privacy*, 4(1), 112-128.

Bagde, R. A., Hadge, R., & Tarekar, S. (2023). *Developing a robust and effective password strength analyzer that can accurately assess the security of passwords against various types of attacks*.

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *2012 IEEE Symposium on Security and Privacy*, 538-552. [Crossref]

Farooq, U. (2020). *Real time password strength analysis on a web application using multiple machine learning approaches*.

Guo, Y., Zhang, Z., & Guo, Y. (2019). Optiwords: A new password policy for creating memorable and strong passwords. *Computers & Security*, 85, 112-125. [Crossref]

Hassan, J. B., Ayetuoma, I. O., Wisdom, D. D., Ugwunna, C. O., Cathrine, F. F., & Lateef, G. S. (2025). Securing critical infrastructure: The impacts of 5G networks on internet security in the oil and gas industry: A survey. *KASU Journal of Computer Science (KJCS)*, 3(2).

Hassan, J. B., Oloruntoba, J. A., Wisdom, D. D., & Ajayi, T. D. (2025). Machine learning-based credit default prediction: Challenges, concerns, and model comparisons. *FUOYE Journal of Engineering and Technology*, 10(2), 264-272. [Crossref]

James, J., & Renjith, R. (2024). Addressing subjectivity in risk analysis: A review of fuzzy logic extensions in FMEA and Bayesian networks. *Expert Systems with Applications*, 238, 121740.

Khern-am-nuai, W., Yang, W., & Li, N. (2017). Using context-based password strength meter to nudge users' password generating behavior: A randomized experiment. *Proceedings of the 50th Hawaii International Conference on System Sciences*. [Crossref]

Ma, J., Yang, J., & Zhang, Y. (2007). A practical rule-based framework for password quality indicator using Levenshtein edit distance. *Proceedings of the 2007 IEEE International Conference on Communications*, 1455-1460.

Mazelan, M. E. M., Mutalib, N. H. A., & AlDahoul, N. (2025). Enhancing password security through a high-accuracy scoring framework using Random Forests.

Mo, J., Kuang, H., & Li, X. (2025). Password strength detection via machine learning: Analysis, modeling, and evaluation.

Rzayeva, L., et al. (2025). Development of a method for determining password formation rules using neural networks. *Information*, 16(8), 655. [Crossref]

Şahin, M., Bulut, E., & Akleylek, S. (2015). Distinguishing password complexity from strength: A theoretical framework using Probabilistic Context-Free Grammars. *IEEE Transactions on Information Forensics and Security*, 10(8), 1640-1652.

Saravanan, V., & Lakshmi, P. (2014). FuzzyApp: A fuzzy inference system for predicting protein allergenicity. *Bioinformatics and Biology Insights*, 8, 125-133.

Seitz, T. (2017). Personalizing password policies and strength feedback. *Symposium on Usable Privacy and Security (SOUPS)*.

Shreya, S., Das, A., & Menon, R. (2025). Explainable AI in password security: Integrating LIME with Random Forest and XGBoost for transparent strength prediction. *Future Generation Computer Systems*, 150, 210-225.

Tóth-Laufer, E., Takács, M., & Várkonyi-Kóczy, A. R. (2015). A hierarchical fuzzy framework for real-time physiological risk monitoring. *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 1-8.

Vanila, S., Jeyavathana, B., Rathinam, A., & Elango, K. (2024). Enhancing password security with machine learning-based strength assessment techniques. In *Advances in cybersecurity and privacy* (pp. 1-20). [Crossref]

Wang, W., Chen, L., & Zhao, X. (2022). PPSM: A deep convolutional neural network approach for password strength modeling. *Computers & Security*, 112, 102511.

Wisdom, D. D., Alabi, A. O., Hassan, J. B., Oduntan, E. O., Ajayi, T. D., & Adeosun, O. (2026). An ensemble machine learning scheme for real-time phishing URL detection and browser-level deployment. *UMYU Scientifica*, 5(1), 179-199. [Crossref]

Wisdom, D. D., Vincent, O. R., Aborisade, D. O., & Omeike, M. O. (2026). Defensive walls against sophisticated ML-orchestrated attacks in edge computing. In *Intelligent data-centric systems: Cybersecurity defensive walls in edge computing* (pp. 275-315). Elsevier, Academic Press. [Crossref]

Wisdom, D. D., Vincent, O. R., Aborisade, D. O., & Omeike, M. O. (2026). Mitigating security concerns in business intelligence systems using ML and cryptographic schemes - A systematic review. *Journal of Data Science and Intelligent Systems*, 1-14. [Crossref]

Wisdom, D. D., Vincent, O. R., Christian, A. U., Igulu, K., Hyacinth, E. A., Odunayo, O. E., & Umar, B. (2024). Industrial IoT security infrastructure and threats. In *Communication technologies in IoT and their security challenges: Present and future* (pp. 369-402). Springer Nature. [Crossref]

Wisdom, D. D., Vincent, O. R., Igulu, K. T., Aborisade, D. O., Christian, A. U., Hyacinth, E. A., Garba, A. B., Esther, O. O., & Olatunbosun, A. M. (2025). The protection of Industry 4.0 and 5.0: Cybersecurity strategies and innovations. In *Computational intelligence for analysis of trends in Industry 4.0 and 5.0* (p. 34). Taylor & Francis. [Crossref]

Wisdom, D. D., Vincent, O. R., Oduntan, O. E., Hassan, J. B., Falayi, C. F., & Ajayi, T. D. (2024). Improving security of business intelligent systems with AI and machine learning. In *SMARTBLOCK4AFRICA 2024 International Conference*. Babcock University, Nigeria, & Valley View University, Ghana, in collaboration with IEEE. [Crossref]

Xu, M., Yu, J., Zhang, X., Wang, C., Zhang, S., Wu, H., & Han, W. (2023). Improving real-world password guessing attacks via bi-directional transformers. *32nd USENIX Security Symposium*.

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, 8(3), 338-353. [Crossref]

Zou, Y., An, M., & Wang, D. (2025). Advanced probabilistic models and guessability in password strength meters. *34th USENIX Security Symposium*.