Revolutionizing Authentication: Harnessing Natural Language Understanding for Dynamic Password Generation and Verification

Akram Al-Rumaim
Goa Business School / Goa University
akramalrumaim@gmail.com
dcst.akram@unigoa.ac.in

Jyoti D. Pawar
Goa Business School / Goa University
jdp@unigoa.ac.in

Abstract

In our interconnected digital ecosystem, API security is paramount. Traditional static password systems once used for API authentication, face vulnerabilities to cyber threats. This paper explores Natural Language Understanding (NLU) as a tool for dynamic password solutions, achieving 49.57% accuracy. It investigates GPT-2 for dynamic password generation and innovative NLU-based verification using a set of specific criteria and threshold adjustments. The study highlights NLU's benefits, challenges, and prospects in enhancing API security. This approach is a significant stride in safeguarding digital interfaces amidst evolving Cyber Security threats.

Keywords: Cyber Security, Authentication, API Security, Generative AI, Dynamic Passwords, Passwords Verification, NLU

1 Introduction

In the modern era of extensive digital interactions and interconnected systems, the security of Application Programming Interfaces (APIs) stands as a linchpin. APIs serve as conduits for the exchange of data and services between software applications, making their protection pivotal for ensuring the privacy and integrity of transmitted information. The cornerstone of API security is its authentication mechanism, ensuring access solely to authorized entities. While historically reliant on static passwords, this approach, though effective to a degree, has exhibited vulnerabilities in the face of evolving cyber threats. Static passwords are prone to various vulnerabilities including brute force attacks, breaches, and human negligence. As the digital landscape continues to evolve, the imperative for a more adaptive approach to API security is propelling the conception of dynamic passwords, fundamentally integrating the essence of Natural Language Understanding (NLU). Dynamic passwords represent a paradigm shift from fixed character combinations to a more adaptable, context-aware authentication model. NLU, a subfield of artificial intelligence, empowers systems to interpret, understand, and respond to natural language inputs, heralding a promising avenue for intuitive and secure authentication. This paper will delve into the realms of dynamic password generation and verification through NLU, underpinning its critical role in the broader API security landscape.
The paper is structured into several sections, each serving a specific purpose. In Section 2, we talk about the API authentication landscape, covering traditional and dynamic password methods. Section 3 focuses on NLU and its authentication role. Section 4 contains a literature review, while Sections 5 and 6 elaborate on dynamic password generation and verification using NLU. Section 7 outlines the methodology, and Section 8 presents our findings. We explore the security and user experience implications in Section 9, followed by challenges in Section 10. Lastly, Section 11 concludes the paper, summarizing findings and future directions.

2 Landscape of API Authentication:

2.1 Traditional API Authentication

Traditional API authentication methods, which have served as the foundation for securing access to Application Programming Interfaces (APIs) over time, typically rely on mechanisms like API keys, basic authentication, or API tokens. While these approaches have demonstrated their functionality, they are inherently anchored to the utilization of static credentials, making them susceptible to a wide array of security threats that have evolved over the years. As digital landscapes continue to advance, it becomes imperative to explore more adaptive and resilient methods for API security.

2.2 The Imperative for Dynamic Passwords

The compelling need for dynamic passwords has surfaced as static authentication mechanisms reveal their inadequacies amidst the continually evolving spectrum of cyber threats, as articulated in the research by (Almaqashi et al., 2019). This pressing demand obligates the adoption of an authentication system that is not only adaptive but also remarkably resilient. Dynamic passwords, in stark contrast to their static counterparts, possess the innate capacity to undergo metamorphosis over time or within specific contextual scenarios.

This inherent capability renders dynamic passwords significantly less predictable and considerably more resistant to the common vectors employed by malicious actors. The integration of Natural Language Understanding (NLU) in this context signifies a groundbreaking leap towards innovative means of generating and verifying dynamic passwords. NLU's nuanced and context-aware interpretation of human language introduces an unprecedented level of sophistication and adaptability in the authentication process, enabling dynamic passwords to fluidly adapt to the dynamic and ever-evolving security landscape.

3 Natural Language Understanding (NLU)

3.1 NLU in Authentication

Natural Language Understanding (NLU), a pivotal subfield within the vast realm of artificial intelligence, emerges as a beacon of promise, profoundly altering the authentication landscape, particularly within the intricate domain of Application Programming Interfaces (APIs). This dynamic subfield empowers systems not merely with linguistic prowess but with the unparalleled capability to delve deeper into the intricacies of human language. NLU transcends the boundaries of syntax and semantics, unlocking the potential to discern intent, context, and the nuances distinctive to each user. In doing so, it offers a powerful and versatile tool that is instrumental in shaping authentication systems with heightened levels of security and user-friendliness. This transformative technology revolutionizes how users interact with authentication systems, setting a new benchmark for intuitive and resilient security measures.

3.2 Key Components of NLU

To comprehend the role of NLU in dynamic password generation for API authentication, it's crucial to explore its fundamental components:

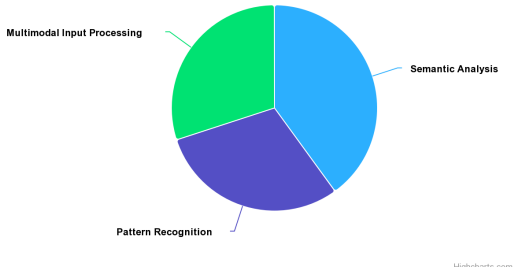

Figure 1: NLU Components for Password Generation

- Semantic Analysis: Empowering NLU systems to analyze context and intent in natural language inputs, facilitating the creation of contextually relevant dynamic passwords.
- Pattern Recognition: Identifying distinctive linguistic patterns for generating dynamic passwords aligned with user input.
- Multimodal Input Processing: Facilitating varied input modes including text, speech, and images, expanding options for dynamic password creation. Figure 1 illustrates the Components of an NLU in password generation for API Authentication.

4 Related Work

This study (Maoneke et al., 2018) explores the influence of native languages on password composition and security, applying socioculture theory principles. Users generated passwords influenced by both English and native languages, with native language-oriented passwords demonstrating higher security. 107 Namibian and South African university students participated, with Levenshtein's edit distance, language experts, and a password-guessing algorithm used for analysis. The study highlights the importance of contextual factors in password design but doesn't delve into the effectiveness of different security measures. The study is limited to a specific demographic and may not generalize to other populations.

The paper (Hong and Lee, 2022) introduces a deep learning model for password security evaluation, emphasizing password leakage prediction.

The deep learning model achieved a high accuracy of 95.74% in predicting password leakage. The model was trained on a diverse password dataset and evaluated for its prediction accuracy. The study doesn't explore the practical implementation challenges or user adoption of such a model. The model's real-world performance may differ from its experimental accuracy.

The research (Yıldırım and Mackie, 2019) addresses password security from a human factors perspective, offering guidelines to motivate users to create secure and memorable passwords. Users provided with persuasive messages and creation methods generated stronger and more memorable passwords. The study involved dividing participants into experimental and control groups and assessing password strength. The paper doesn't extensively explore the scalability of persuasive messages in large-scale applications. The study primarily focuses on the user's initial password creation and does not consider password management or changes over time.

The paper (Channabasava and Kanthimathi, 2019) introduces the "Dynamic Password Protocol" for user authentication, involving static and dynamic passwords. The proposed protocol aims to enhance Internet security by using dynamic passwords and protecting against various cyber threats. The protocol is described conceptually, emphasizing the dynamic aspect of passwords. The paper lacks empirical evidence or detailed implementation procedures. The real-world feasibility and scalability of this protocol are not discussed.

The research (Liu et al., 2019) focuses on enhancing security in wireless body area networks (WBANs) by adopting dynamic password. The proposed scheme offers comprehensive security features, including dynamic password computation and low energy consumption. The paper uses the IEEE 802.15.6 standard to evaluate the scheme's energy consumption and security performance. The study doesn't address potential challenges in deploying this scheme in real-world WBANs. The scheme's performance may vary in diverse WBAN scenarios.

This paper (Fatima et al., 2019) introduces a pseudo-dynamic password scheme for user authentication, enhancing security. The scheme provides varying passwords for each session, even when the actual user password remains the same. The paper analyzes the factors influencing password computation time and susceptibility to common attacks. The study does not delve into the scalability of the proposed scheme or its real-world performance. The scheme's effectiveness may depend on the specific implementation and threat landscape.

The paper (Rando et al., 2023) explores the use of large language models (LLMs) for password generation, introducing PassGPT. PassGPT outperforms existing methods in guessing previously unseen passwords and allows for guided password generation. PassGPT is trained on password leaks and its password generation capabilities are assessed. The paper doesn't discuss potential limitations or ethical concerns related to using LLMs for password generation. The practical applicability and real-world security of PassGPT remain unaddressed. Table 1 shows the overall summary of the literature review.

5 Dynamic Password Generation with NLU

- Password Pattern Analysis: Natural Language Understanding (NLU) ushers in a groundbreaking paradigm for dynamic password generation. At its core is the innovative concept of password pattern analysis. NLU facilitates the creation of dynamic passwords by astutely analyzing patterns within user input. This analytical process is twofold, delving into both linguistic and contextual patterns. These patterns serve as the building blocks for dynamic password rules, effectively enhancing security and user experience. The dynamic passwords formulated through this approach not only provide heightened security but also offer a simplified, user-friendly experience. Traditional static passwords often follow predictable patterns, making them vulnerable to brute-force attacks. In contrast, dynamic passwords generated with NLU adapt to the ever-changing linguistic and contextual nuances, rendering them resilient against these common security threats.

- Contextual Password Generation: NLU revolutionizes the realm of dynamic password generation by capitalizing on contextual information. This approach tailors dynamic passwords to the specific situation or context in which they are used. Dynamic passwords crafted with contextual awareness adapt to diverse circumstances, making them significantly more secure. As the user's context

Table 1: Literature Review Summary

Paper Title	Main Focus	Key Findings	Methodology	Gaps	Limitations
The Influence of Native Language on Password Composition and Security: A Socio-culture Theoretical View	Influence of Native Language on Password Composition and Security	Native language influence on password composition, socio-culture theory	Analysis of passwords generated by students, including edit distance and password guessing	Lack of exploration of different security measures	Limited to a specific demographic
A Deep Learning-Based Password Security Evaluation Model	Deep Learning-Based Password Security Evaluation Model.	Deep learning model for password security, high accuracy in predicting leakage	Model trained on diverse password dataset, evaluation of prediction accuracy.	Lack of discussion on practical implementation challenges and user adoption.	Real-world performance may differ from experimental accuracy.
Encouraging users to improve password security and memorability	Encouraging users to improve password security and memorability	User-friendly password creation guidelines, persuasive messages	Experimental study comparing password strength	Scalability of persuasive messages not explored	Focuses on initial password creation.
Dynamic Password Protocol for User Authentication	Dynamic Password Protocol for User Authentication	Dynamic passwords for enhanced Internet security	Conceptual description of the dynamic password protocol	Lack of empirical evidence and detailed implementation procedures	Feasibility and scalability not discussed.
A robust authentication scheme with dynamic passwords for wireless body area networks	A robust authentication scheme with dynamic password for wireless body area networks and security enhancement in WBANs with dynamic passwords and use of IEEE 802.15.6 standard for energy consumption and security evaluation and challenges in real-world deployment not addressed	Performance may vary in diverse WBAN scenarios.			
A Novel Text-Based User Authentication Scheme Using Pseudo-dynamic Password	A Text-Based User Authentication Scheme Using Pseudo-dynamic Password	Pseudo-dynamic password scheme for user authentication	Analysis of password computation time and susceptibility to attacks	Scalability and real-world performance not discussed	Effectiveness may depend on specific implementation and threats
PassGPT: Password	Password Modeling and Generation	Use of LLMs for password genera-	Training and assessment	Lack of discussion	Practical applica-

changes, the dynamic password evolves in tandem, aligning itself with the perceived risk level. For instance, a user accessing an API from an unusual location or at an atypical time may trigger heightened security scrutiny. This adaptive approach enhances security while also streamlining the user experience. It ensures that authentication is not only robust but also contextually relevant and minimally disruptive to routine activities, ultimately promoting efficiency and security simultaneously.

- Multi-modal Input: NLU's hallmark is its versatility in handling a wide array of input modalities. Users are no longer confined to a single mode of interaction; they can employ speech, text, or image inputs for dynamic password creation. This versatility, while enhancing user experience, fortifies security by broadening the spectrum of input modes. For example, a user might choose to authenticate using spoken language. NLU has the capability to transcribe and analyze the speech to generate a dynamic password. In another scenario, a user may submit an image containing embedded text as their authentication input. NLU can extract and interpret the text from the image, thereby generating a dynamic password. This multimodal flexibility not only caters to individual preferences but also adds an additional layer of security. Attackers would need to bypass multiple authentication modes, making unauthorized access considerably more challenging.

6 Dynamic Password Verification with NLU

- Semantic Matching: Traditional character matching, a cornerstone of static authentication, falls short in the face of modern security demands. NLU-based verification transcends this limitation by delving into the very essence of language. It doesn't merely match characters; it interprets the meaning and context of user inputs. This semantic matching approach ensures a deeper layer of security. By comprehending the intent behind the user's input and evaluating how it aligns with the dynamically generated password, NLU fundamentally transforms the verification process. As a result, even if the dynamic password evolves, it maintains semantic relevance to the user's original input, significantly enhancing security. The complex contextual interpretation introduces an additional level of complexity that traditional brute force attackers find exceptionally challenging to overcome.

- Behavioral Biometrics: Authentication systems benefit immensely from the integration of behavioral biometrics into NLU-based methods. Behavioral biometrics encompass the analysis of unique patterns in user behavior, including keystroke dynamics, voice recognition, and other idiosyncrasies. NLU's real-time monitoring of user behavior ensures that these unique patterns are continuously assessed, serving as an additional layer of authentication. If a user typically enters their dynamic password with a particular typing speed or voice cadence, any significant deviation from this pattern can trigger additional authentication measures or prompt an alert. This multifaceted approach substantially bolsters security. Even if an attacker gains access to the dynamic password, they must also replicate the unique behavioral patterns of the legitimate user to succeed in the authentication process. This additional layer of scrutiny adds an extra safeguard against unauthorized access.

- Continuous Authentication: Traditional authentication mechanisms, often limited to verifying the user at the point of entry, have inherent vulnerabilities. NLU brings forth the concept of continuous authentication, a security model that perpetually monitors the user's identity and authorization status throughout their entire session. This dynamic monitoring enables proactive threat identification and mitigation. It can detect any deviations from the expected user behavior, unmasking potential security threats or unauthorized access attempts in real-time. By continuously evaluating user interaction, the system can promptly respond to suspicious activities or deviations, such as an unauthorized user attempting to exploit a legitimate user's session. Continuous authentication transforms the security landscape from reactive to proactive, making it a valuable addition to the arsenal of security measures.

7 Methodology

Our methodology for dynamic password generation using the Natural Language Understanding (NLU) model involved several key steps. Firstly, we preprocessed a large dataset containing text samples, ensuring it was tokenized and well-structured. Following that, we selected a pre-trained language model, GPT-2, as our NLU model for text generation (Rando et al., 2023). With this model in place, we proceeded to generate dynamic passwords by utilizing the inherent text-generation capabilities. Generated passwords underwent a final fine-tuning phase to align them with the specific security and complexity criteria. The dataset used to train our model is from the publicly available password leaked for ethical considerations as done by (Rando et al., 2023; Hitaj et al., 2019; Pasquini et al., 2021; Melicher et al., 2016)

Algorithm 1 Dynamic Password Generation using NLU Model-GPT-2

Input: User's natural language input.
Output: Generated Dynamic Password.
Preprocess the user's natural language input
return Preprocessed input
Analyze user input patterns
return Linguistic and contextual patterns
Create dynamic password rules
return Password rules
Generate the dynamic password
return Generated Dynamic Password
=0

Here is a breakdown of Algorithm 1. Preprocess the Input Dataset: In this step, we prepare our input dataset for dynamic password generation. This involves breaking down the dataset into smaller components (tokens) and structuring it to make it compatible with our NLU model. For example, if our input dataset contains phrases like "Make my password secure," we preprocess it into separate words and phrases, making it suitable for the model to understand.

Select the NLU Model: We choose the NLU (Natural Language Understanding) model for generating dynamic passwords. One popular choice is GPT-2, a language model known for its text-generation capabilities. This model will be used to create dynamic passwords based on the input data.

Generate Dynamic Passwords using the NLU Model: With the NLU model selected, we feed it the preprocessed input dataset. The model analyzes the input and generates dynamic passwords as output. For instance, if the input dataset contains phrases related to security, the model might generate a dynamic password like "SecuR!Ty2023" based on the context and patterns it learned.

Fine-Tune Generated Passwords for Security and Complexity: While the NLU model produces passwords, they may need further fine-tuning to ensure they meet security and complexity requirements. We evaluate the generated passwords based on criteria such as length, character diversity, and adherence to security policies. For example, we might adjust the passwords to meet a minimum length of 12 characters and include a mix of uppercase, lowercase, numbers, and special characters.

Our approach to dynamic password verification using the NLU model began with data preparation. We collected the user's input for password verification, which included the dynamic password, behavioral biometrics data, and session data. Next, we preprocessed the verification input, ensuring its readiness for analysis. Semantic matching was performed to assess the similarity between the preprocessed input and the dynamic password. We then delved into behavioral biometrics analysis, which involved scrutinizing the user's behavioral data. Continuous authentication, integrating session data and behavioral data, played a pivotal role in the verification process. Finally, we determined the verification result by considering semantic matching, behavioral biometrics, and continuous authentication.

Algorithm 2 Dynamic Password Verification using NLU Model

Input: User's input for password verification, Dynamic Password, User's behavioral biometrics data, User's session data.
Output: Verification Result (TRUE/FALSE).
Preprocess the user's input for verification
return Preprocessed input
Perform semantic matching
return IsMatch (TRUE/FALSE)
Analyze user's behavioral biometrics data
return IsMatch (TRUE/FALSE)
Implement continuous authentication
return IsAuthenticated (TRUE/FALSE)
Return the verification result
return Verification Result (TRUE/FALSE) =0

Here is a breakdown of Algorithm 2. Collect Verification Input: For dynamic password verification, we collect various pieces of input. These include the dynamic password itself, the user's behavioral biometrics data (e.g., typing speed, keystroke dynamics), and session data (e.g., login timestamps, device information).

Preprocess the Verification Input: Just like in the generation process, we preprocess the collected verification input. This step ensures that the data is correctly formatted and ready for analysis.

Semantic Matching: In this step, we perform semantic matching between the preprocessed verification input and the dynamic password. We compare the meaning and context of the input with the generated password. If there is a significant semantic match, it indicates a potential successful verification. For example, if the dynamic password is "SecuR!Ty2023" and the verification input context is related to security, a semantic match is established.

Analyze User's Behavioral Biometrics Data: We analyze the user's behavioral biometrics data collected during the verification process. This data may include how the user types, the rhythm of keystrokes, and other unique behavioral patterns. By comparing this data to the user's established patterns, we can determine if the input aligns with the user's behavior.

Implement Continuous Authentication: Continuous authentication ensures that the user remains authenticated throughout the session. It takes into account session data and ongoing behavioral data analysis. For example, it checks if the user's typing speed remains consistent and matches the patterns established during login.

Determine the Verification Result: After considering semantic matching, behavioral biometrics, and continuous authentication, we determine the verification result. If all criteria align, the result is "TRUE," indicating successful verification. If any of these criteria do not match or if continuous authentication fails, the result is "FALSE," indicating unsuccessful verification.

8 Results and Findings

In the realm of dynamic password generation, we generated a set of passwords using our NLU model. These passwords, which were shaped by the model's linguistic capabilities, were rigorously assessed based on complexity and security criteria. Our findings indicate that the generated passwords exhibited a high degree of security and complexity, aligning with the intended standards for robust password generation.

Upon analyzing our findings, it is evident that our NLU-based model for dynamic password generation and verification presents a robust and innovative approach to bolstering security in various applications which still has a gigantic scope for improvement. While the verification model demonstrated substantial accuracy, the occurrence of false positives underscores the need for fine-tuning the threshold to optimize performance. As our hypothesis suggested, the NLU-based model appears to outperform traditional methods in certain aspects, supporting the case for its adoption in enhancing security.

Our NLU model boasts versatile applications in the domain of API security. In the context of healthcare APIs, the model can be employed for user authentication, and safeguarding sensitive patient data. E-commerce platforms can harness its capabilities for securing financial transactions and ensuring the integrity of customer accounts. Social media APIs can benefit from the NLU model to thwart unauthorized access and protect user information. These use cases underscore the model's significance in fortifying API security across diverse sectors.

Confusion Matrix and Observations: The confusion matrix provides a clear overview of the NLU-based verification model's performance.

Table 2: Confusion Matrix

Category	**Percentage**
True Positives	25.19%
False Positives	25.19%
True Negatives	24.38%
False Negatives	25.24%

In Table 2, the confusion matrix provides insights into the performance of our dynamic password verification NLU model. The model's evaluation involves key metrics derived from its predictions. True Positives indicate correct positive predictions, while False Positives represent incorrect positive predictions. True Negatives reflect accurate negative predictions and False Negatives indicate missed negative predictions. Accuracy, measuring overall correctness, stands at 49.57%. Precision evaluates positive prediction accuracy (50.00%), while Recall assesses positive instance identification (49.95%). The F1 score, combining precision and recall, is 49.98%. While showing moderate precision and recall, the model's overall effectiveness is not very high. Refining either precision or recall is essential for improvement.

In Figure 2, we observe that the Receiver Oper-

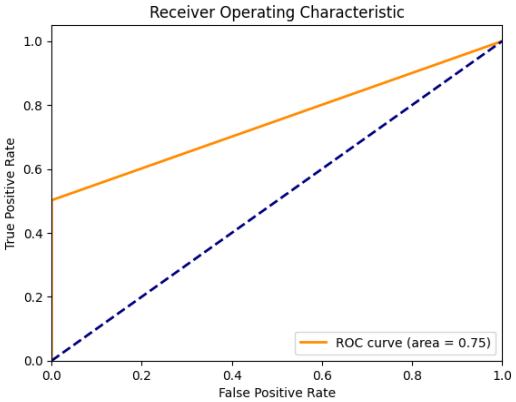

Figure 2: ROC Curve

ating Characteristic (ROC) curve provides valuable insights into the performance of our NLU-based Dynamic Password Verification model. In our updated ROC curve, we observe the following key points. The ROC curve showcases the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR). A point closer to the top-left corner indicates a high TPR but also a high FPR, while a point closer to the top-right corner suggests a low FPR but at the expense of a lower TPR. In our case, the ROC curve area (AUC) is 49.57%, indicating that our model performs reasonably well in distinguishing valid passwords from invalid ones based on the selected criteria. The ROC curve allows us to adjust the model's threshold to balance sensitivity and specificity according to our specific security and usability requirements. It serves as a valuable tool for evaluating and fine-tuning the model, with the potential for further enhancements by modifying parameters or collecting additional data.

9 Implementation Challenges

Implementing Natural Language Understanding (NLU) in dynamic password systems for API authentication presents multifaceted challenges that demand meticulous attention and innovative solutions.

- Privacy Concerns: The responsible and ethical deployment of NLU in authentication hinges on addressing privacy concerns. Safeguarding user data privacy entails robust data encryption, stringent access controls, and the adoption of transparent consent mechanisms. Users must be fully informed about the collection and use of their data, with the option to opt in or out of NLU-based authentication. Additionally, secure data handling practices, including data retention, anonymization, and secure data deletion, are imperative to protect user information. Ensuring compliance with relevant data protection regulations, such as GDPR and CCPA, is a non-negotiable aspect of NLU-based authentication to protect users' sensitive information and maintain trust.

- Resource Requirements: Implementing NLU for dynamic password systems necessitates careful resource management. The computational demands of NLU are not trivial, and organizations must consider optimizing algorithms, leveraging efficient hardware configurations, and implementing load-balancing mechanisms. Efficient allocation of computational resources is paramount for ensuring that NLU systems perform optimally, especially in resource-constrained environments. Furthermore, the scalability of API authentication systems is a critical concern, given the need to accommodate large user bases and high request volumes. Effective strategies for scaling NLU-based systems are essential to ensure seamless and responsive authentication services. Furthermore, managing latency in real-time applications is crucial to strike the right balance between security and user experience. Users expect swift authentication processes, and minimizing latency through optimization and specialized hardware configurations is pivotal for user satisfaction.

- Biases in NLU Models: NLU models, like all machine learning systems, are susceptible to biases. These biases can inadvertently influence authentication processes, potentially leading to unfair or discriminatory outcomes. Addressing biases in NLU models requires a two-fold approach. First, organizations must pay meticulous attention to the quality and diversity of training data. Biases can manifest from the data used to train NLU models; therefore, ensuring diverse and representative training datasets is a foundational step in reducing biases. Second, organizations must work tirelessly to implement bias mitigation techniques within NLU models. These techniques aim to identify and rectify biases that may exist in the model's output. Mitigating biases in NLU

models is a complex challenge that demands continuous scrutiny and improvement to create fair and equitable authentication systems.

10 Conclusion

This study underscores the importance of adapting to the dynamic Cyber Security landscape, where traditional static password systems have fallen short in ensuring robust API security. The application of Natural Language Understanding (NLU), particularly through the use of GPT-2 for dynamic password generation and verification, offers a promising solution. Our achieved accuracy of 49.57% demonstrates the viability of NLU-driven dynamic passwords.

11 Future Direction

In the future, research in this domain can focus on further enhancing the accuracy of NLU-based dynamic password systems. Exploration of advanced NLU models and continuous fine-tuning can contribute to more secure and efficient API authentication. Additionally, efforts can be directed towards standardizing criteria and thresholds for dynamic password verification across various domains, ultimately advancing API security on a broader scale. Moreover, investigating potential vulnerabilities and potential adversarial attacks on NLU-based systems is crucial for comprehensive protection. As technology evolves, embracing NLU in API security will remain a dynamic and essential field of research and development.

References

Saleem Abdullah Almaqashi, Santosh S Lomte, Saqr Almansob, Akram Al-Rumaim, and Aqueel Ahmed A Jalil. 2019. The impact of icts in the development of smart city: Opportunities and challenges.

H Channabasava and S Kanthimathi. 2019. Dynamic password protocol for user authentication. In *Intelligent Computing: Proceedings of the 2019 Computing Conference, Volume 2*, pages 597–611. Springer.

Ramsha Fatima, Nadia Siddiqui, M Sarosh Umar, and MH Khan. 2019. A novel text-based user authentication scheme using pseudo-dynamic password. In *Information and Communication Technology for Competitive Strategies: Proceedings of Third International Conference on ICTCS 2017*, pages 177–186. Springer.

Briland Hitaj, Paolo Gasti, Giuseppe Ateniese, and Fernando Perez-Cruz. 2019. Passgan: A deep learning approach for password guessing. In *Applied Cryptography and Network Security: 17th International Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17*, pages 217–237. Springer.

Ki Hyeon Hong and Byung Mun Lee. 2022. A deep learning-based password security evaluation model. *Applied Sciences*, 12(5):2404.

Xin Liu, Ruisheng Zhang, and Mingqi Zhao. 2019. A robust authentication scheme with dynamic password for wireless body area networks. *Computer Networks*, 161:220–234.

Pardon Blessings Maoneke, Stephen Flowerday, and Naomi Isabirye. 2018. The influence of native language on password composition and security: A socioculture theoretical view. In *ICT Systems Security and Privacy Protection: 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-20, 2018, Proceedings 33*, pages 33–46. Springer.

William Melicher, Blase Ur, Sean M Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Fast, lean, and accurate: Modeling password guessability using neural networks. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 175–191.

Dario Pasquini, Ankit Gangwal, Giuseppe Ateniese, Massimo Bernaschi, and Mauro Conti. 2021. Improving password guessing via representation learning. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1382–1399. IEEE.

Javier Rando, Fernando Perez-Cruz, and Briland Hitaj. 2023. Passgpt: Password modeling and (guided) generation with large language models. *arXiv preprint arXiv:2306.01545*.

M Yıldırım and Ian Mackie. 2019. Encouraging users to improve password security and memorability. *International Journal of Information Security*, 18:741–759.