Intelligent Authentication Gateway: Bridging the Gap between Traditional and FIDO2 Security through AI/ML Enhancement

Dasari Nishith[1], Ikshit Samanta[2], and Dr. Rajarajan G[3]

Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India
nishithdasari100@gmail.com, ikshitsamanta@gmail.com

Abstract. The prevalence of password-based authentication remains a significant security risk, susceptible to attacks like phishing and credential stuffing. FIDO2 presents a promising alternative, offering robust public-key cryptography and various authenticators for a more secure and user-friendly experience. However, transitioning from traditional systems to FIDO2 faces challenges, including integrating with existing infrastructure and ensuring a seamless user experience. We propose an Intelligent Authentication Gateway (IAG) that bridges this gap, leveraging the strengths of both traditional and FIDO2 authentication. The IAG employs an ML model, called Gator, trained on various parameters to dynamically assess risk and direct users to the appropriate authentication method. For high-risk scenarios, FIDO2 provides enhanced security, while low-risk situations utilize traditional methods for efficiency and convenience. This hybrid approach optimizes security based on context while minimizing disruption to user experience, enabling organizations to smoothly transition to FIDO2 and addressing user acceptance and integration complexities.

Keywords: Intelligent Authentication Gateway, AI/ML, FIDO2, dynamic risk assessment, transition, authentication, security, user experience, passwordless, Gator model, classification

1 Introduction

In the ever-evolving digital era, the security of online systems is paramount. Traditional password-based authentication methods, while ubiquitous, have become a glaring vulnerability in the fabric of cybersecurity. These methods are fraught with risks, as weak or reused passwords can be easily compromised, leading to unauthorized access and data breaches. The advent of Fast Identity Online (FIDO2) standards heralds a new age of authentication, offering a beacon of hope with its robust public-key cryptography and a variety of authenticators, including security keys and biometrics. This innovative approach promises to bolster security defenses and streamline the user experience, marking a significant departure from the password paradigm.

However, the transition from entrenched password systems to the avant-garde FIDO2 framework is not without its challenges. The integration of FIDO2 into the diverse and complex infrastructures of contemporary enterprise systems poses a formidable task. Organizations grapple with the intricacies of adopting this new standard while maintaining operational continuity and ensuring a seamless user experience. It is within this context that we propose the Intelligent Authentication Gateway (IAG), a solution designed to bridge the chasm between the old and the new, marrying the familiarity of traditional methods with the security enhancements of FIDO2.

The IAG is not merely a conduit for authentication methods; it is a sophisticated platform that leverages machine learning to discern and mitigate risks. At the heart of the IAG lies the Gator model, an intelligent system trained on a myriad of parameters such as IP location, device type, historical traffic patterns, and threat intelligence feeds. This model serves as the gatekeeper, dynamically evaluating the risk level of each access attempt and directing users to the most appropriate authentication method. In scenarios deemed high-risk, the IAG enforces the use of FIDO2 authentication, providing a fortified barrier against potential threats. In contrast, in low-risk situations, it allows the efficiency and convenience of traditional methods, thus optimizing the balance between security and user experience.

The IAG's strategic implementation of FIDO2 for high-risk access attempts is a game changer, significantly reducing dependence on vulnerable passwords and limiting the avenues for cyberattacks. In addition, it acknowledges and addresses concerns surrounding the acceptance of passwordless authentication. By fostering user familiarity and trust, the IAG paves the way for a smoother adoption of these advanced methods.

The Intelligent Authentication Gateway stands as a testament to the potential of harmonizing security and convenience. It acts as a pivotal bridge, enabling organizations to transition to FIDO2 with minimal disruption, gradually integrating it into their existing systems and authentication workflows. This phased approach is key to overcoming the hurdles of user acceptance and the complexities of integration, ensuring a methodical and user-centric deployment.

The IAG's dynamic risk assessment, powered by the Gator model, embodies the principle of continuous learning and adaptation. It is designed to evolve, responding to the ever-changing threat landscape and the unique behaviors of individual users. This adaptability is crucial for the real-world application of the IAG, allowing it to provide a resilient and flexible security solution that will stand the test of time.

In summary, the Intelligent Authentication Gateway offers a compelling proposition for organizations seeking to elevate their security measures. By seamlessly integrating FIDO2 into existing systems and adapting authentication protocols based on AI-driven risk assessments, the IAG delivers a robust and user-friendly authentication experience. It is a beacon of innovation in the quest for a more secure digital world.

1.1 Motivation

The motivation behind this project stems from the urgent need to address the vulnerabilities associated with password-based authentication and improve overall security posture. With data breaches becoming increasingly common and costly, organizations are seeking innovative solutions to mitigate these risks. FIDO2 presents a promising opportunity to enhance security while also improving user experience. However, widespread adoption of FIDO2 has been hindered by various challenges, including compatibility concerns and user acceptance issues. By developing an Intelligent Authentication Gateway that seamlessly integrates traditional and FIDO2 authentication methods, we aim to overcome these obstacles and provide organizations with a practical solution to enhance security and user experience.

1.2 Objectives

1. To implement a dynamic risk assessment system using machine learning algorithms, such as the Gator model, to classify access attempts as high or low risk.
2. To dynamically adjust authentication methods based on the assessed risk, with high-risk scenarios triggering FIDO2 authentication and low-risk scenarios utilizing traditional methods.
3. Facilitate a smooth transition to FIDO2 by enabling gradual integration into existing infrastructure and authentication flows.
4. Enhance security by reducing reliance on vulnerable passwords, especially in high-risk situations, and leveraging FIDO2's robust authentication mechanisms.
5. To improve user and enterprise system experience by enabling passwordless authentication through FIDO2 and offering a streamlined login process.

2 Literature Survey

2.1 Survey on Existing Systems

Existing authentication systems predominantly rely on password-based methods, which pose significant security vulnerabilities due to the susceptibility to various attacks such as phishing, credential stuffing, and brute-force attempts. Multi-factor authentication (MFA) offers some security improvement, but secondary factors like SMS codes can also be compromised. Moreover, the accumulation of technical debt in software development further exacerbates security risks and system stability.

– Research on Integrated Authentication Using Passwordless Authentication Method [1]: Implemented a prototype integrating FIDO with Shibboleth for passwordless authentication, addressing registration phase vulnerabilities and session hijacking risks. Future work includes improving registration phase security and expanding browser support.

- A Comprehensive Study on Passwordless Authentication [2]: Conducted an extensive review of passwordless authentication technologies, analyzing their advantages and disadvantages. Future work involves focused analysis on specific passwordless methods and evaluating security, privacy, and acceptance aspects.
- Moving forward passwordless authentication: challenges and implementations for the private cloud [3]: Introduced FIDO2 passwordless authentication implementation in an OpenStack cloud, focusing on fingerprint-based authentication. Future work includes evaluating other biometric authenticators and their performance compared to passwords.
- Bypassing Push-based Second Factor and Passwordless Authentication with Human-Indistinguishable Notifications [4]: Identified vulnerabilities in push-based 2FA and passwordless authentication, proposing the HIENA attack. Future work involves testing the attack against broader user populations and exploring secure notification binding methods.
- FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones [5]: Conducted a lab study comparing platform and roaming FIDO2 authentication on smartphones. Future work includes improving user education about FIDO2 and developing solutions compatible with various devices.
- Multi-Factor Authentication in Cyber-Physical System: A State of Art Survey [6]: Reviewed the evolution of authentication from single factor to multi-factor, comparing different authentication schemes. Future work involves investigating security, privacy implications, and developing new, more secure MFA methods.
- Multifactor Authentication using Android Mobile [7]: Proposed a multifactor authentication scheme using GPS location, timestamp, and preshared number. Future work includes exploring alternatives to GPS for location verification and addressing user privacy concerns.
- A Framework for Security and Risk Analysis of Enrollment Procedures: Application to Fully-remote Solutions based on eDocuments [8]: Introduced a framework for the security and risk analysis of enrollment procedures, focusing on formalizing enrollment protocols and analyzing attackers. Future work involves enriching the framework to support more procedures and automating the analysis process.
- A Security and Usability Analysis of Local Attacks Against FIDO2 [9]: Analyzed potential attacks against FIDO2 from malicious browser extensions and physical access to security keys. Future work involves exploring more effective ways to alert users when attacks occur.
- SDD: A trusted display of FIDO2 transaction confirmation without trusted execution environment [10]: Proposed modifications to FIDO2 protocol for ensuring transaction integrity and introduced the Secure Display Daemon (SDD) process. Future work involves analyzing vulnerabilities in current FIDO2 implementations.
- Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study [11]: Conducted an online questionnaire with IT professionals on the

usability and challenges of FIDO2. Future work includes providing recommendations for the FIDO2 community based on identified priority areas.

- Evaluating the Security Posture of Real-World FIDO2 Deployments [12]: Conducted manual analysis of real-world FIDO2 deployments and analyzed landing sites of the top domains. Future work involves leveraging automated crawlers for improved detection of FIDO2 usage
- FIDOnuous: A FIDO2/WebAuthn Extension to Support Continuous Web Authentication [13]: Proposed an extension of FIDO2/WebAuthn for continuous web authentication. Future work includes evaluating negotiable aspects of the authentication mechanism type and annotating real-world web services.
- Is FIDO2 Passwordless Authentication a Hype or for Real?: A Position Paper [14]: Conducted a literature review of passwordless authentication and FIDO2. Future work includes standardized setup processes, persuasive user interface design, and usability studies on account recovery options.
- Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication [15]: Conducted a lab study comparing FIDO2 with passwords. Future work involves long-term field studies and investigating additional authentication modalities like wearables.
- Passwordless VPN using FIDO2 Security Keys: Modern authentication security for legacy VPN systems [16]: Proposed using FIDO2 authentication for legacy VPN protocols and reviewed existing 2FA methods for VPN. Future work involves implementing and testing the proposed solution and improving VPN clients for FIDO2 authentication.
- Should We Rush to Implement Password-less Single Factor FIDO2-based Authentication? [17]: Compared password-based vs. FIDO2 single-factor authentication threat models and analyzed factors that inhibit the adoption of FIDO2. Future work includes addressing account recovery, delegation, and usability in FIDO certification.
- simFIDO - FIDO2 User Authentication with SimTPM [18]: Implemented a FIDO2 authentication stack using a SIM card-based TPM and introduced new Android services. Future work involves conducting security analysis, performance evaluation, and user studies on usability and perception.
- FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation [19]: Conducted a formal security analysis of FIDO2 with CTAP 2.1 and WebAuthn 2 and suggested post-quantum instantiations. Future work involves analyzing additional modes and features.
- FeIDo: Recoverable FIDO2 Tokens Using Electronic IDs [20]: Proposed the FeIDo system to derive FIDO2 credentials from eID attributes and evaluated the authentication efficiency. Future work involves extending system applicability, handling attribute changes during eID renewal/migration, and analyzing limitations for additional authentication scenarios.
- Twin eye Authentication Gateway Architecture Resilient to DDoS attacks in 6LoWPAN IoT Network Using ML Techniques [21] Proposes a gateway architecture to combat DDoS attacks in IoT networks, achieving high accu-

racy in attack detection. However, lacks real-world deployment evaluation and scalability considerations.
- Managing Authentication and Authorization in Distributed Science Gateway Middleware [22] Integrates Keycloak with Apache Airavata for authentication, offering abstraction and automation. Yet, it overlooks security beyond authentication and lacks scalability discussion.
- Using Keycloak for Gateway Authentication and Authorization [23] Presents Keycloak integration for Gateway Authentication, emphasizing automation. However, it lacks comprehensive security coverage and a discussion of scalability.
- Secure and Efficient User Authentication Scheme for Multi-gateway WSNs [24] Proposes a secure authentication scheme for WSNs, demonstrating resilience against security attacks. However, assumes gateway node trust and overlooks anonymity requirements.
- AI Techniques for Information Security Risk Assessment [25] Develops an AI-based risk assessment model for DBMS, showing promising results but requiring further scalability evaluation.
- Cyber Security Risk Assessment on Industry 4.0 using ICS Testbed with AI and Cloud [26] Proposes a cyber security risk assessment approach for Industry 4.0, providing insight into emerging technology challenges. However, concerns are noted regarding the complexity of the testbed and the validation of countermeasures.
- Systematic Mapping Study on AI-Supported Security Risk Assessment [27] Analyzes AI-supported security risk assessment approaches, highlighting a growing interest. However, limitations in sample size and focus on supervised learning approaches are noted.
- Authentication at Scale [28] Proposes USB tokens and SSL certificates for enhanced authentication, addressing portability and security. However, challenges in consumer adoption and complexity of integration are mentioned.
- Employee Perceptions Towards BYOD Second-Factor Authentication [29] Investigates employee perceptions of a BYOD-based authentication system, providing insights into usability and adoption dynamics. However, limitations in sample representativeness and technical aspects are acknowledged.

2.2 Research Gaps

The research gaps identified in the literature are as follows:

- **Security Vulnerabilities**: Password-based authentication methods are vulnerable to various attacks, compromising both individual users and organizational data.
- **Technical Debt**: The accumulation of technical debt in software development restricts organizations from optimizing their code base, leading to increased maintenance costs and decreased system stability.
- **Compatibility Challenges**: Integrating FIDO2 with existing infrastructure can require modifications or upgrades, which can cause disruptions and delays for organizations.

- **User Experience Disruption**: Introducing FIDO2 authentication may initially frustrate users accustomed to passwords, impacting user adoption and satisfaction.
- **Lack of Awareness**: Limited understanding and awareness of the benefits of FIDO2 among users and organizations hinder widespread adoption.

2.3 Problem Statement

The main problem addressed by the Intelligent Authentication Gateway (IAG) is the inadequacy of traditional password-based authentication methods to ensure security and user experience. This includes:

- **Security Vulnerabilities**: Pervasive reliance on password-based authentication creates security vulnerabilities susceptible to various attacks.
- **Technical Debt**: Accumulated technical debt in software development impedes the optimization of code base, leading to increased maintenance costs and decreased system stability.
- **Compatibility Challenges**: Integrating FIDO2 with existing infrastructure poses challenges, including potential disruptions and delays for organizations.
- **User Experience Disruption**: Introduction of FIDO2 authentication may initially frustrate users accustomed to passwords, impacting user adoption and satisfaction.
- **Lack of Awareness**: Limited understanding and awareness of FIDO2 benefits among users and organizations hinder widespread adoption.

The solution aims to bridge the gap between legacy password-based systems and FIDO2 by providing a seamless and secure authentication gateway that prioritizes user convenience while minimizing disruption. This involves dynamically assessing the risks associated with each login attempt, using AI-driven risk assessment, and intelligently switching between traditional and FIDO2 authentication methods to achieve optimal security without sacrificing user experience. Additionally, the solution facilitates a smooth transition to FIDO2 for organizations, ensuring compatibility and minimizing adoption hurdles.

3 Design Approach and Details

3.1 System Architecture

This diagram outlines a typical cloud-based system architecture for running the Flask server with an ML model:

Flask Server: Contains the root endpoint (/) which checks the request using the ML Model. Depending on the model's prediction, it either returns a JSON response for benign requests or redirects to the /malicious endpoint for malicious requests.

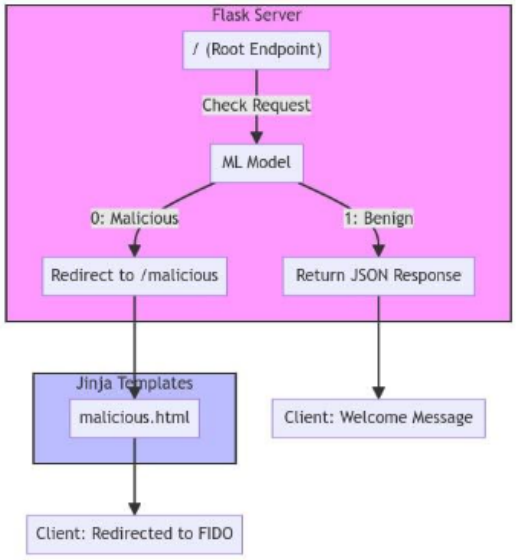


Fig. 1. System Architecture Diagram

Jinja Templates: Contains the malicious.html template used to display the "Redirected to FIDO" message for malicious requests.

Client: Shows the different responses the client receives based on the request's nature, either a welcome message or a redirection notice.

3.2 Design

The system design outlined here is a robust and secure architecture for handling client requests and managing user data:

Internet: This is the starting point where the client, typically using a web browser, begins interaction with the system.

Cloud Environment: This is the main hosting platform for the system's core components, providing scalability and flexibility.

Load Balancer: This component efficiently distributes incoming client requests across the web server, ensuring optimal resource utilization and response times.

Web Server (Flask): This server handles client requests. It interacts with the Machine Learning model (Gator) for request validation, manages sessions using Redis for quick access, and retrieves user data from the database.

ML Model: This server handles client requests. It interacts with the Machine Learning model (Gator) for request validation, manages sessions using Redis for quick access, and retrieves user data from the database.

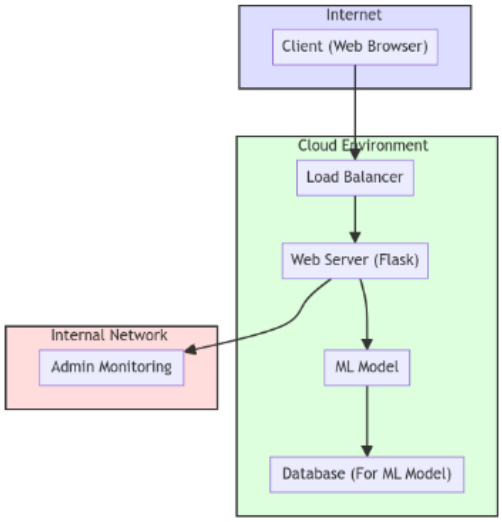


Fig. 2. System Design Diagram

Redis (Session Store): This server handles client requests. It interacts with the Machine Learning model (Gator) for request validation, manages sessions using Redis for quick access, and retrieves user data from the database.

Internal Network: This server handles client requests. It interacts with the Machine Learning model (Gator) for request validation, manages sessions using Redis for quick access, and retrieves user data from the database.

4 Module Description

4.1 Module - 1: Gator Model

- The Gator Model, an integral component of the Intelligent Authentication Gateway (IAG), is a cutting-edge machine learning-based module meticulously designed to conduct dynamic risk assessments for every login attempt, serving as a formidable line of defense against potential security threats.
- Leveraging advanced algorithms and sophisticated techniques, Gator comprehensively analyzes a multitude of parameters, encompassing user behavior patterns, device attributes, and contextual data, to evaluate the security risk associated with each log-in request, ensuring a holistic and robust assessment.
- One of its key functions is the highly accurate classification of incoming IP addresses or requests into categories of benign or malicious, based on a rigorous analysis of historical data and real-time intelligence. Our model has achieved an accuracy of 97%
- Through continuous learning from a vast repository of past authentication patterns and integrated threat intelligence feeds, Gator continuously refines

and enhances its risk assessment capabilities, ensuring an ever-increasing accuracy in identifying potential anomalies, suspicious activities, and emerging security threats.
- By providing real-time, actionable insights into the security posture of incoming login attempts, Gator significantly bolsters the overall security framework of the IAG, serving as an indispensable component in ensuring robust protection against unauthorized access, malicious activities, and other nefarious attempts to compromise the system's integrity.

4.2 Module - 2: FIDO2 Authentication

- The FIDO2 Authentication module, an integral part of the Intelligent Authentication Gateway (IAG), is a pioneering solution that facilitates passwordless authentication by implementing the FIDO2 standard. This innovative approach enables users to authenticate securely without the need for traditional passwords, which are often the weakest link in security chains and a common target for cybercriminals.
- By eliminating the reliance on passwords, the FIDO2 authentication module mitigates a host of security vulnerabilities typically associated with password-based authentication methods. These include, but are not limited to, brute force attacks, dictionary attacks, and keylogger attacks.
- By supporting the FIDO2 standard, the module not only aims to enhance security but also improve the user experience. Passwordless authentication mechanisms are not only more secure, but also more convenient. Users no longer need to remember complex passwords or worry about their passwords being stolen.
- The module incorporates various FIDO2 authenticators, including security keys, biometrics, and platform authenticators, providing users with diverse and secure authentication options customized to their preferences and requirements.
- Furthermore, the FIDO2 authentication module promotes the widespread adoption of passwordless authentication mechanisms. As more and more organizations recognize the benefits of passwordless authentication, it is hoped that this will lead to a paradigm shift in how user authentication is handled.

5 Results

In the next section, we share the results of our research and development work, including a detailed explanation of methods, tests, and important findings that confirm our ideas and open new areas for future research. Our Gator model has achieved an impressive 97% accuracy in classifying requests as benign or malicious. Although it occasionally mislabels FTP-BruteForce attacks as DoS attacks, this minor issue does not cause problems as all non-benign requests are redirected to the FIDO2 authentication gateway, keeping enterprise systems secure.

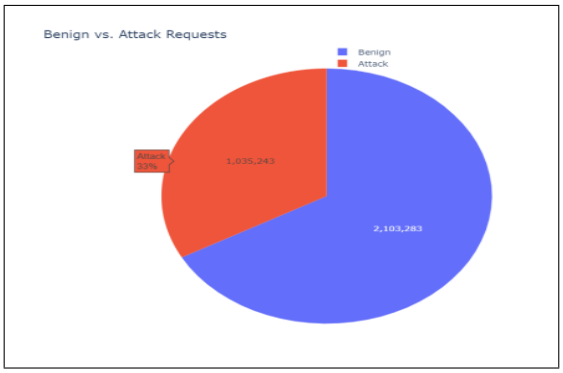


Fig. 3. Pie chart displaying Benign vs Attack requests

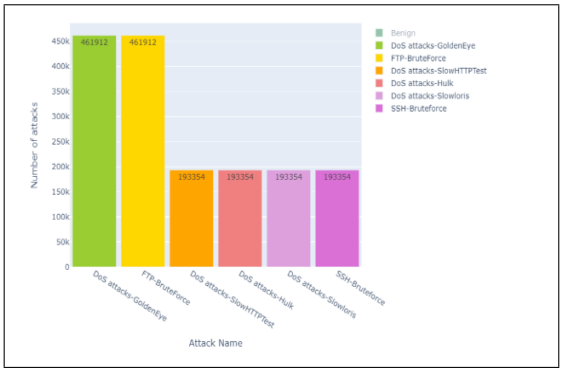


Fig. 4. The bar chart that shows the distribution of different attack classes

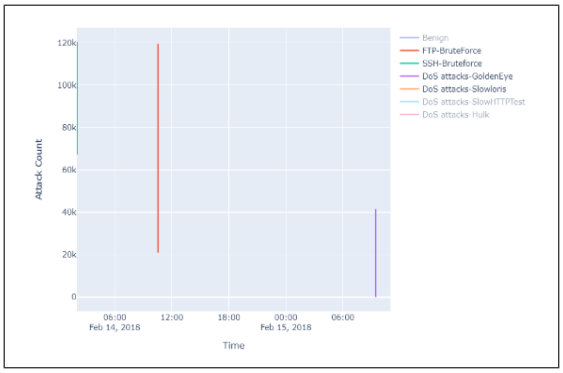


Fig. 5. Frequency of Attack types over time

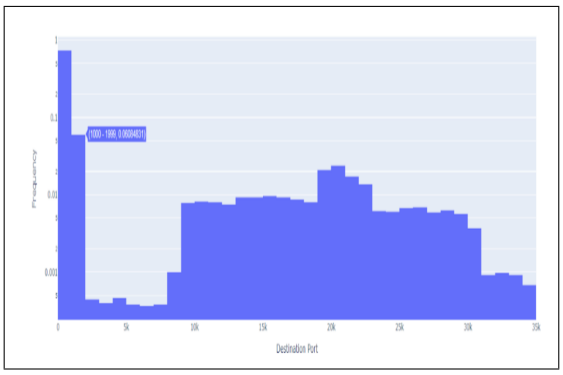


Fig. 6. The histogram illustrates destination port distribution in the dataset, with a logarithmic scale for frequency. A prominent peak around ports 1000–1999 suggests heavy traffic targeting well-known ports like 1025 for Microsoft RPC services. Smaller peaks at various ranges indicate traffic for different services, while the long tail of less frequent ports is typical. Correlating this distribution with other dataset features and domain knowledge is crucial for precise analysis and anomaly detection.

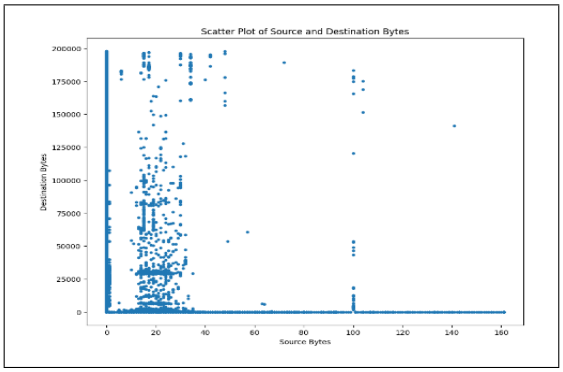


Fig. 7. The scatter plot depicts the relationship between source bytes and destination bytes in network traffic data. Concentration near the origin signifies instances with minimal data transmission. Increasing source bytes show varied destination bytes, suggesting inconsistent correlation. . Vertical and horizontal lines indicate instances of data reception without transmission and vice versa, possibly indicative of network attacks or behaviors. Sparse areas suggest rare instances of high data transmission. Further analysis and correlation are needed to interpret specific network activities accurately.

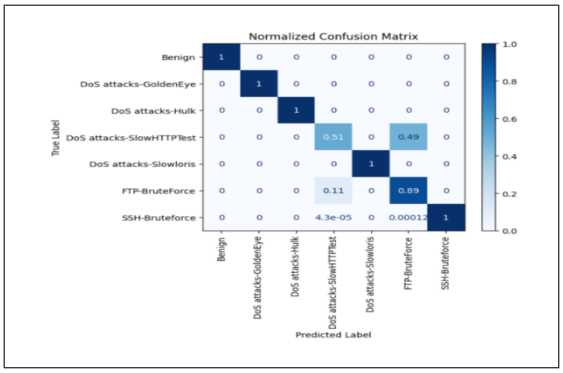


Fig. 8. The model demonstrates strong performance in classifying benign attacks, DoS attacks, and SSH-Bruteforce, though it faces challenges with FTP-BruteForce, occasionally mislabeling them as DoS attacks. This analysis provides valuable information for refining and improving the accuracy of the model in these specific areas.

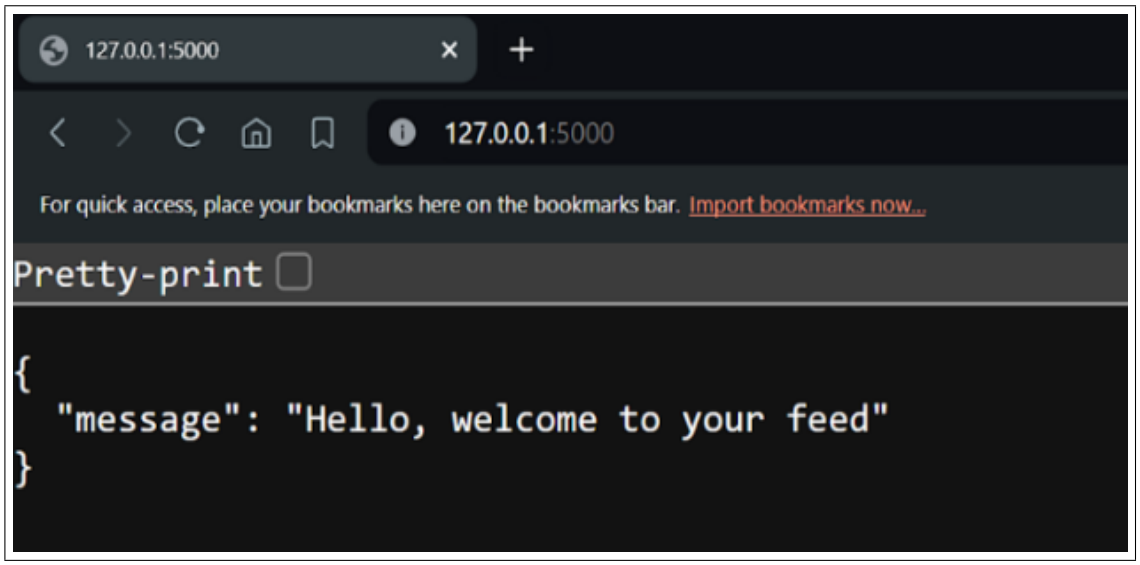


Fig. 9. The model detects a benign request and redirects the user to his/her home feed

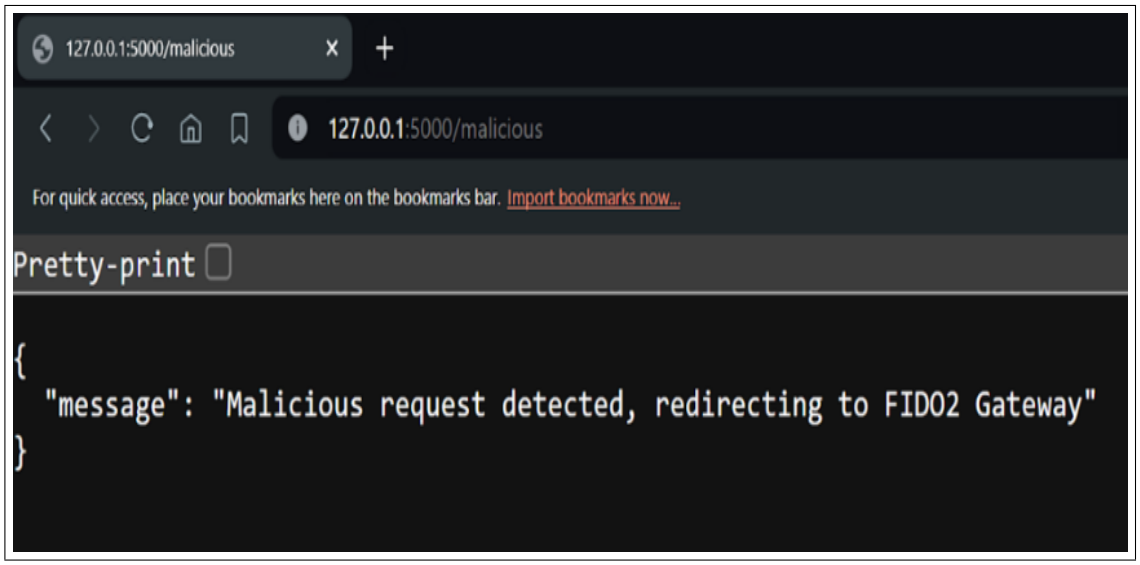
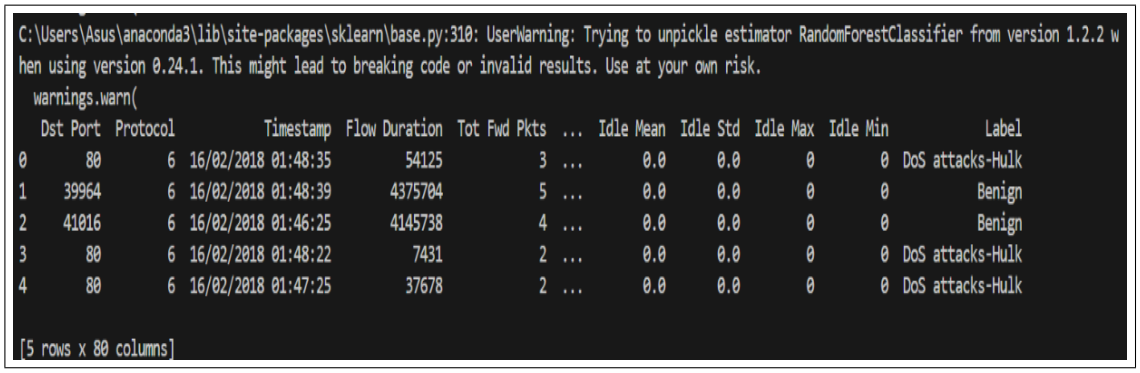


Fig. 10. The model detects a malicious request and redirects the user to FIDO2 gateway



```
C:\Users\Asus\anaconda3\lib\site-packages\sklearn\base.py:310: UserWarning: Trying to unpickle estimator RandomForestClassifier from version 1.2.2 w
hen using version 0.24.1. This might lead to breaking code or invalid results. Use at your own risk.
  warnings.warn(
   Dst Port  Protocol          Timestamp  Flow Duration  Tot Fwd Pkts  ...  Idle Mean  Idle Std  Idle Max  Idle Min           Label
0        80         6  16/02/2018 01:48:35          54125             3  ...        0.0       0.0         0         0  DoS attacks-Hulk
1     39964         6  16/02/2018 01:48:39        4375704             5  ...        0.0       0.0         0         0          Benign
2     41016         6  16/02/2018 01:46:25        4145738             4  ...        0.0       0.0         0         0          Benign
3        80         6  16/02/2018 01:48:22           7431             2  ...        0.0       0.0         0         0  DoS attacks-Hulk
4        80         6  16/02/2018 01:47:25          37678             2  ...        0.0       0.0         0         0  DoS attacks-Hulk

[5 rows x 80 columns]
```

Fig. 11. Example Destination ports and its label.

6 Summary

This research journey reached its zenith with the creation and assessment of the Intelligent Authentication Gateway (IAG). This innovative solution serves as a bridge between traditional password-based authentication and the more secure Fast Identity Online (FIDO2) standard. The IAG, powered by an AI-driven risk assessment system, dynamically alternates between FIDO2 and conventional methods based on the risk level assessed. This approach prioritizes not only the security of the user but also the user experience and the enterprise system experience.

As the adoption of FIDO2 continues to grow, the IAG is poised to play a crucial role. It can serve as a vital bridge, ensuring a seamless and secure transition for both users and enterprises. This is particularly important in our increasingly digital world, where the need for robust online security measures is paramount.

By facilitating this transition, the IAG is not just a tool but a catalyst for change, helping to shape a more trustworthy and protected online ecosystem. This, in turn, can lead to greater confidence in online transactions and interactions, fostering a safer and more secure digital environment for all. Ultimately, the IAG stands as a testament to the power of innovative thinking and technological advancement in addressing contemporary security challenges.

Acknowledgement

Our heartfelt gratitude goes to Dr. Rajarajan G, whose insightful feedback and recommendations have significantly improved the quality of our paper. We, the authors, also extend our appreciation to the School of Computer Science and Engineering at VIT Vellore. Their consistent assistance in reviewing our work and their unwavering support throughout the research and development process have been invaluable.

References

1. M. Morii et al., "Research on Integrated Authentication Using Passwordless Authentication Method," 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 2017, pp. 682-685, doi: 10.1109/COMPSAC.2017.198.
2. V. Parmar, H. A. Sanghvi, R. H. Patel and A. S. Pandya, "A Comprehensive Study on Passwordless Authentication," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2022, pp. 1266-1275, doi: 10.1109/ICSCDS53736.2022.9760934.
3. I. Gordin, A. Graur, S. Vlad and C. I. Adomniței, "Moving forward passwordless authentication: challenges and implementations for the private cloud," 2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet), Iasi, Romania, 2021, pp. 1-5, doi: 10.1109/RoEduNet54112.2021.9638271.

4. Jubur, M., Shrestha, P., Saxena, N. and Prakash, J., 2021, May. Bypassing push-based second factor and passwordless authentication with human-indistinguishable notifications. In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (pp. 447-461).
5. Würsching, Leon, et al. "FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones." Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. 2023.
6. S. Ibrokhimov, K. L. Hui, A. Abdulhakim Al-Absi, h. j. lee and M. Sain, "Multi-Factor Authentication in Cyber Physical System: A State of Art Survey," 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South), 2019, pp. 279-284, doi: 10.23919/ICACT.2019.8701960.
7. Kamble, K., Mishra, M., Shirdhankar, T. and Bora, R., Multifactor Authentication using Android Mobile. International Journal of Computer Applications, 975, p.8887.
8. Pernpruner, M., Sciarretta, G. and Ranise, S., 2021. A Framework for Security and Risk Analysis of Enrollment Procedures: Application to Fully-remote Solutions based on eDocuments. In SECRYPT (pp. 222-233).
9. Yadav, T., & Seamons, K. (n.d.). A Security and Usability Analysis of Local Attacks Against FIDO2. Retrieved February 9, 2024, from https://arxiv.org/pdf/2308.02973.pdf
10. Guan, J., Li, H., Ye, H., & Zhao, Z. (2022). A formal analysis of the FIDO2 protocols. In Lecture Notes in Computer Science (pp. 3–21). https://doi.org/10.1007/978-3-031-17143-7_1
11. Barbosa, M., Boldyreva, A., Chen, S., & Warinschi, B. (2021). Provable security analysis of FIDO2. In Lecture Notes in Computer Science (pp. 125–156). https://doi.org/10.1007/978-3-030-84252-9_5
12. Is FIDO2 the kingslayer of user authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. (2020, May 1). IEEE Conference Publication — IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9152694
13. Farke, F. M. (2020). "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. https://www.usenix.org/conference/soups2020/presentation/farke
14. Chakraborty, D., & Sven Bugiel. (2019). simFIDO. https://doi.org/10.1145/3319535.3363258
15. Kunke, J. (2021, May 26). Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication. arXiv.org. https://arxiv.org/abs/2105.12477
16. Schwarz, F., Do, K., Heide, G., Hanzlik, L., & Rossow, C. (2022). FEIDO. Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3548606.3560584
17. Lassak, L. (2021). "It's stored, hopefully, on an encrypted server": mitigating users' misconceptions about FIDO2 biometric WebAuthn. https://www.usenix.org/conference/usenixsecurity21/presentation/lassak
18. FIDONuous: a FIDO2/WebAuthN extension to support continuous web authentication. (2020, December 1). IEEE Conference Publication — IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9343231
19. Breit, Z. (2022). Exploration of the security and usability of the FIDO2 Authentication Protocol. Digital Repository at the University of Maryland (DRUM). https://drum.lib.umd.edu/items/483cb1ea-8af6-4425-a249-0a9ab611f540

20. Kuchha, D., Oest, A., & Saad, M. (2023, November 21). Evaluating the Security Posture of Real-World FIDO2 Deployments (F. Li, Ed.) [Review of Evaluating the Security Posture of Real-World FIDO2 Deployments]. Acm Digital Library; acm. https://dl.acm.org/doi/10.1145/3576915.3623063
21. L, M.; RAJU, G. T. Twin eye Authentication Gateway Architecture Resilient to DDoS attacks in 6LoWPAN IoT Network Using Machine Learning Techniques. 2023 International Conference on Network, Multimedia and Information Technology (NMITCON), Network, Multimedia and Information Technology (NMITCON), 2023 International Conference on, [s. l.], p. 1–7, 2023. DOI 10.1109/NMITCON58196.2023.10276264.
22. Srinivas, J., Mukhopadhyay, S., & Mishra, D. (2017). Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Networks, 54, 147–169. doi:10.1016/j.adhoc.2016.11.002
23. Christie, M. A., Bhandar, A., Nakandala, S., Marru, S., Abeysinghe, E., Pamidighantam, S., & Pierce, M. E. (2019). Managing authentication and authorization in distributed science gateway middleware. Future Generation Computer Systems. doi:10.1016/j.future.2019.07.018
24. Bhandar, A. (2023). Using KeyCloak for gateway authentication and authorization. https://www.academia.edu/99521567/
25. Basallo, Y.A., Senti, V.E. and Sanchez, N.M., 2018. Artificial intelligence techniques for information security risk assessment. IEEE Latin America Transactions, 16(3), pp.897-901.
26. Matsuda, W., Fujimoto, M., Aoyama, T. and Mitsunaga, T., 2019, November. Cyber security risk assessment on industry 4.0 using ics testbed with ai and cloud. In 2019 IEEE conference on application, information and network security (AINS) (pp. 54-59). IEEE.
27. Erdogan, G., Garcia-Ceja, E., Hugo, Å., Nguyen, P.H. and Sen, S., 2021, July. A systematic mapping study on approaches for Al-supported security risk assessment. In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 755-760). IEEE.
28. Grosse, E. and Upadhyay, M., 2012. Authentication at scale. IEEE Security & Privacy, 11(1), pp.15-22.
29. Weidman, J. and Grossklags, J., 2017, December. I like it, but i hate it: Employee perceptions towards an institutional transition to byod second-factor authentication. In Proceedings of the 33rd Annual Computer Security Applications Conference (pp. 212-224).