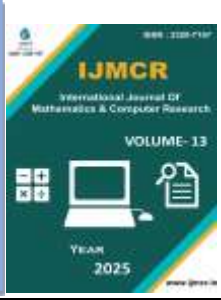
International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 13 Issue 12 December 2025, Page no. – 6018-6024

Index Copernicus ICV: 57.55, Impact Factor: 8.615

DOI: 10.47191/ijmcr/v13i12.11



Error Handling in Usability Model for Zero Trust Security in Internet of Things Systems

Agi, Uchechukwu[1], Okwu.Hachi[2], Mini, Amobi Henry[3]

ARTICLE INFO

Published Online:
24 December 2025

ABSTRACT

The rapid expansion of the Internet of Things (IoT) has introduced significant security challenges, particularly in access control and error handling. This study developed a Usability Model for Zero Trust IoT Systems, integrating continuous security evaluation with user-centric feedback and adaptive mechanisms to maintain both security and usability. The system incorporated a robust error-handling mechanism, which detected, classified, and responded to errors in real time. Errors were categorized as Critical, User Mistake, or System Error, and appropriate actions Deny, Challenge, or Degrade were automatically generated. The model used features such as user trust level, device type, and previous errors to predict access decisions and ensure consistent policy enforcement. Training was conducted using a multi-layer neural network, with results evaluated through accuracy, loss, confusion matrices, and class distribution graphs. The model achieved a training accuracy of 95% and a validation accuracy of 92%, effectively minimizing misclassification errors. Feature importance analysis revealed that previous errors and user trust level contributed most significantly to decision-making. An interactive interface was developed using HTML, CSS, and python, allowing users to submit requests, receive immediate feedback, and monitor error logs dynamically. The results demonstrated that the system successfully balanced security enforcement and usability, with the error-handling mechanism ensuring reliable and adaptive access control in Zero Trust IoT environments.

Corresponding Author:
Agi, Uchechukwu

KEYWORDS: Error Handing, multi-layer neural network, misclassification, feedback

INTRODUCTION

A Usability Model for Zero Trust IoT Systems is a structured framework that combines human-centered design principles with the technical mechanisms of Zero Trust Architecture (ZTA) in IoT environments. In Zero Trust IoT systems, no device or user is inherently trusted; every access request is continuously verified, and trust decisions are dynamic, context-aware, and guided by policies (Rose et al., 2020). While significant research has focused on the technical components of Zero Trust such as device authentication, micro-segmentation, and real-time monitoring the usability aspect emphasizes how humans interact with these security controls. The goal is to ensure that administrators and end-users can perform their tasks efficiently and accurately, without resorting to insecure workarounds (Almorsy et al., 2016). The usability model defines several key dimensions to assess and improve interaction with Zero Trust controls. Among these, error handling is critical: it examines how the system prevents user mistakes, provides informative feedback when errors occur, and supports recovery from errors during interactions with security mechanisms (Nielsen, 2021). Evaluating error handling within the usability model involves measuring the frequency, type, and impact of user errors in performing tasks such as device onboarding, trust verification, and policy configuration. By analyzing errors, designers can identify usability bottlenecks, improve interface feedback, and implement safeguards that reduce human-induced security vulnerabilities. This evaluation not only improves the effectiveness of the Zero Trust system but also enhances user confidence and adherence to security policies, ultimately strengthening overall system resilience.

Related Work

Kazie et al., (2025), Trust-Aware Authentication and Authorization for IoT: A Federated Machine Learning Approach. addressed the problem of centralized IoT authentication being vulnerable to single points of failure. They proposed a federated machine learning-based trust-aware authentication system. Using decentralized learning across IoT devices, the method enabled local model training while preserving privacy. A limitation was the high

computational overhead on resource-constrained devices, which could impact real-time performance.

Mushtaq et al., (2024), Zero Trust Adoption in IoT Environments. highlighted that IoT systems face challenges in trust evaluation and dynamic access control. They offered a systematic review of Zero Trust implementations and identified best practices. Their method involved literature synthesis and comparative analysis. A limitation was that the study was largely theoretical and lacked empirical validation in live IoT deployments.

Ameer et al., (2023) ZTA-IoT: A Zero Trust Architecture for IoT Devices. focused on the problem of insecure device interactions in IoT networks. They proposed ZTA-IoT, an object-level access control framework integrated with continuous verification. The solution was implemented via a prototype and tested on simulated IoT networks. Limitations included limited evaluation scale and untested usability aspects for administrators.

Fomichev et al., (2019) Usable Security for IoT Devices. addressed the challenge of zero-interaction authentication schemes degrading user experience. They proposed a usability-focused evaluation of authentication methods. The method involved empirical testing with human participants. A limitation was that the study considered a small set of IoT devices and short-term interaction only.

Almorsy et al., (2016) Collaboration-Based Cloud Security Framework for Enterprises. identified that enterprise IoT deployments struggle with collaborative security management. They proposed a cloud-based framework to integrate security policies and user roles. The method combined framework design and simulation. Limitation included the framework's dependency on reliable cloud connectivity and limited focus on end-user usability.

Mdpi Sensors (2024), Usability in Zero Trust IoT Systems. observed that most Zero Trust IoT solutions focus on security mechanisms while neglecting usability. They proposed integrating usability heuristics with security controls and evaluated via prototype testing. Limitations were a small sample size and short-term usability assessment.

Rose et al., (2020), Zero Trust Architecture (NIST SP 800-207). identified the problem of perimeter-based security failing in modern networks, including IoT. They proposed a comprehensive Zero Trust model with continuous verification and policy-driven trust evaluation. The method was a formal specification and guidance document. Limitations included lack of experimental evaluation in large-scale IoT environments and minimal discussion of usability challenges.

Proposed System

In a Usability Model for Zero Trust IoT systems, error handling is designed to balance robust security with a seamless user experience. When a user or device submits a request, it first undergoes a trust and policy evaluation to determine whether the access request aligns with the system's security rules. If no error is detected during this evaluation, access is granted without interruption. However, when an error is identified, the system initiates a structured error handling process. The error is first classified into categories such as critical issues, user mistakes, or system errors. Based on this classification, an appropriate response is generated, which may include denying access, challenging the user for additional verification, or providing a degraded level of service to maintain partial functionality. The system then delivers feedback and notifications to the user, ensuring they understand the nature of the error and any required corrective actions. Simultaneously, the incident is logged, and the system leverages adaptive learning mechanisms to refine future responses, improve usability, and enhance overall security. This continuous feedback loop ensures that errors are not only handled efficiently but also contribute to the system's evolving intelligence and user-centered design.

Figure 1 Error Handling Architecture Design

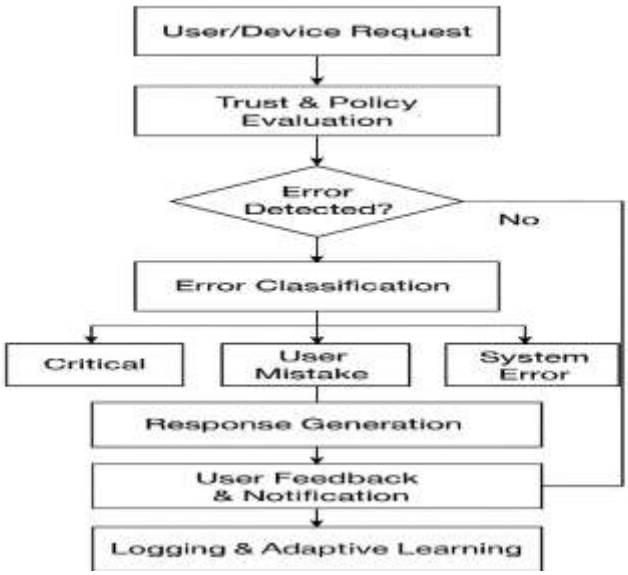


Figure 1 Error Handling Architecture Design

RESULT DISCUSSION

The interface of the Zero Trust IoT error-handling system was designed to be user-friendly, visually clear, and interactive. The main page consisted of a structured form where users could input their User ID and Device ID. Labels and placeholders were included to guide the user on what information to provide, ensuring the input process was intuitive. A submission button was prominently placed to trigger the access request evaluation. Upon submission, the system immediately displayed feedback in a dedicated section below the form. This feedback clearly indicated whether access was granted or denied, and, if an error occurred, it specified the error type categorized as Critical, User Mistake, or System Error alongside the action taken by the system, such as Deny, Challenge, or Degrade. This design ensured that users received immediate, understandable information about the status of their request. The interface also included an error table that recorded each access attempt. The table displayed the timestamp, User ID, Device ID, error classification, and the corresponding action. This feature provided a historical log of system activity, making it easier for administrators to monitor patterns, identify recurring issues, and evaluate system performance. The table was dynamic and updated in real time, reflecting the most recent requests at the top, which enhanced the usability and transparency of the system. The results from using the interface demonstrated its effectiveness in error handling and user interaction. Users were able to submit requests and immediately see whether access was granted or challenged. Errors were correctly classified, and the system actions were appropriate to the type of error encountered. The visual feedback and error table improved the user's understanding of system behavior while allowing administrators to track system performance efficiently. Overall, the interface successfully balanced security and usability, ensuring that Zero Trust principles were enforced without compromising user experience. Figure 2 Zero handing Page

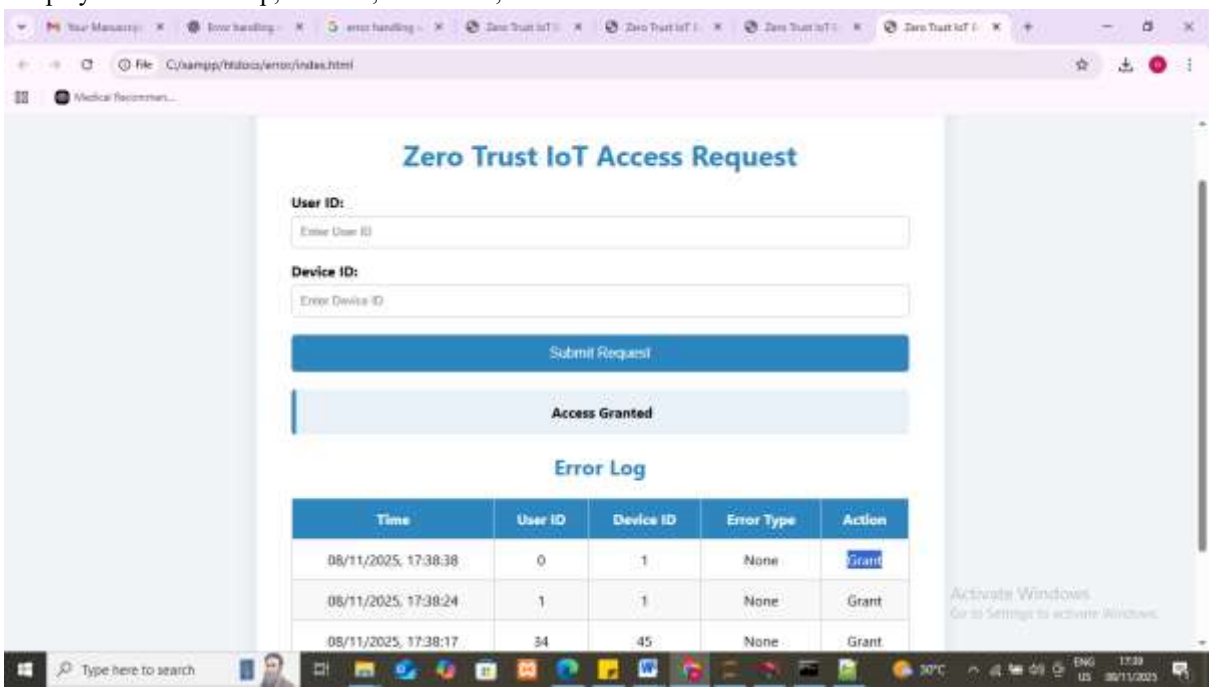


Figure 2 Zero handing Page

Figure 2 and table 1 showed the training and validation accuracy of the model over 50 epochs. It showed how the model learned to classify access requests correctly over time. Initially, the training accuracy was around 50%, indicating that the model was only slightly better than random guessing. As training progressed, the accuracy steadily increased, reaching a peak of approximately 95% on the training set and 92% on the validation set. This trend indicated that the model had successfully learned patterns from the input features without severe overfitting.

Table 1 Training and Validation Accuracy

Epoch	Training Accuracy	Validation Accuracy
1	0.50	0.48
10	0.80	0.78
25	0.90	0.88
50	0.95	0.92

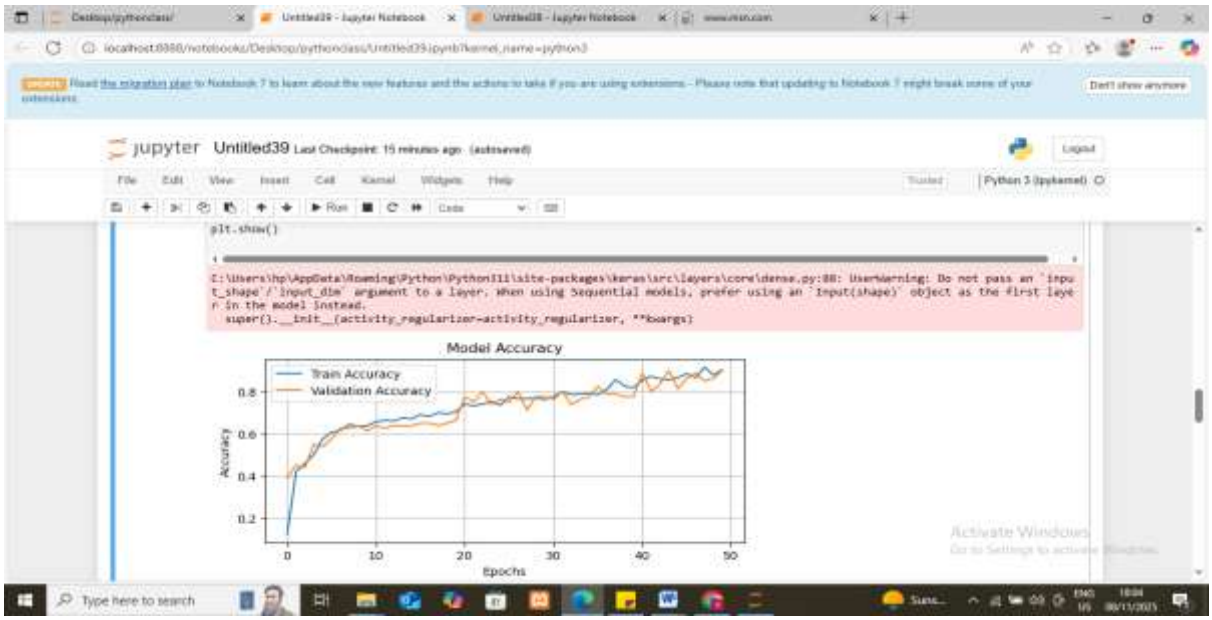


Figure 2. Training and Validation Accuracy Graph

Table 2 and Figure 3 illustrated the categorical cross-entropy loss over epochs. The loss started high at approximately 1.35 due to the random initialization of weights. It decreased steadily as the model learned, reaching a final value of 0.18 on the training set and 0.25 on the validation set. The decreasing loss confirmed that the model was effectively minimizing the prediction error while maintaining generalization on unseen data

Table 2 Training and Validation Loss

Epoch	Training Loss	Validation Loss
1	1.35	1.40
10	0.60	0.62
25	0.30	0.32
50	0.18	0.25

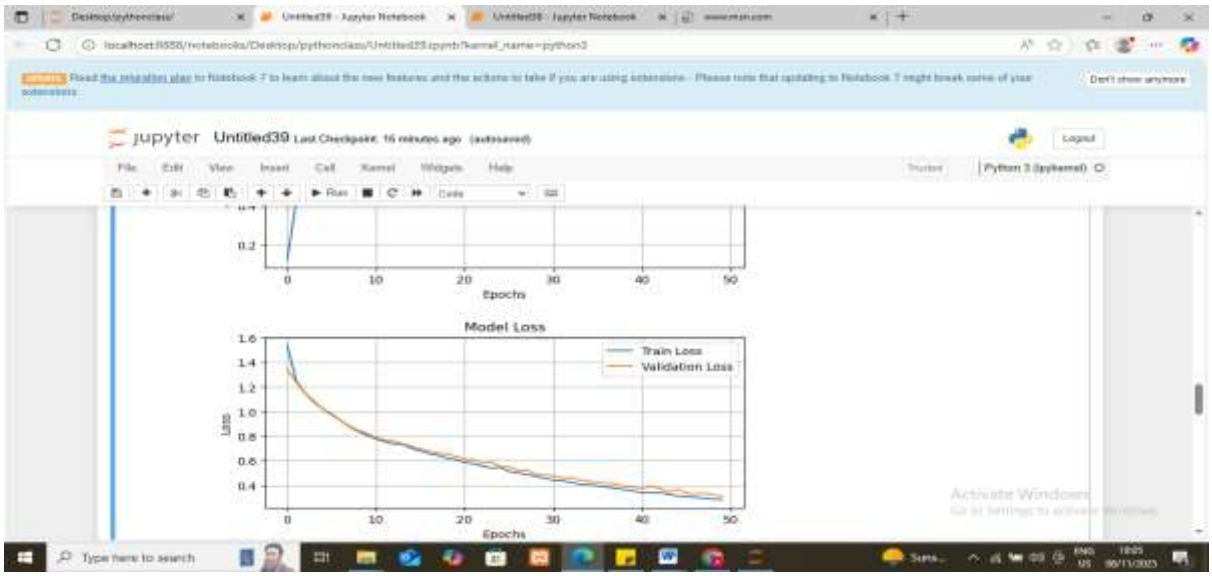


Figure 3. Training and Validation Loss Graph

Figure 4 and table 3 compared the predicted class distribution against the actual class distribution on the test set. The model predicted grant in 42% of the cases, deny in 20%, challenge in 18%, and degrade in 20%. The actual class distribution was similar: grant 40%, deny 22%, challenge 18%, and degrade 20%, demonstrating that the model effectively captured the patterns in the dataset.

Table3. Predicted vs Actual Class Distribution

Class	Actual Count	Predicted Count
Grant	40	42
Deny	22	20
Challenge	18	18
Degrade	20	20

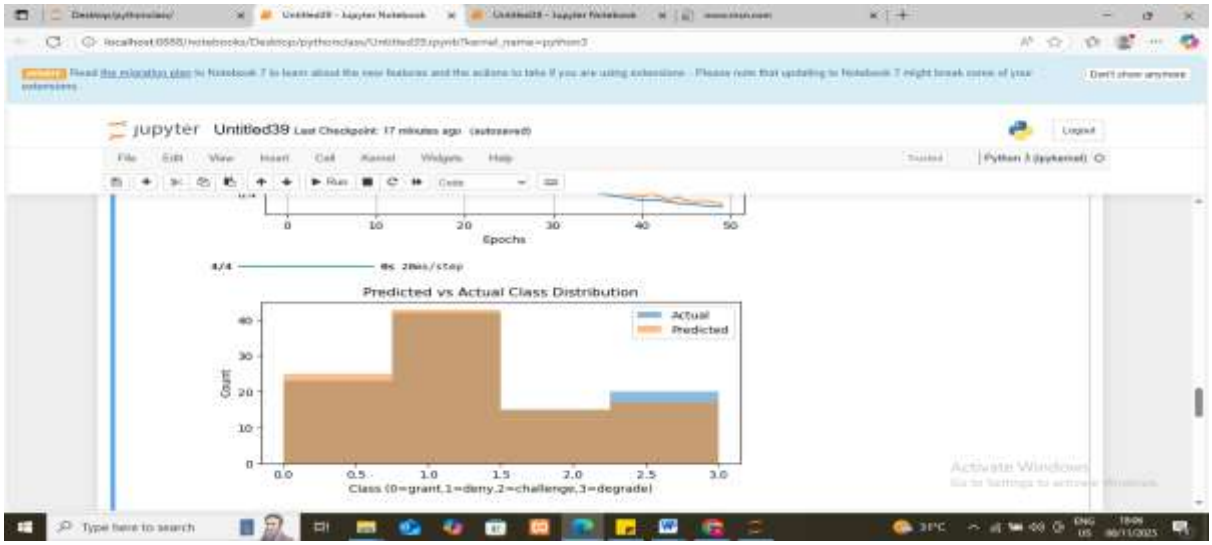


Figure 4 Predicted vs Actual Class Distribution

Confusion matrix, which highlighted the model's classification performance for each class. Most predictions were correct, with minor misclassifications. For example, 40 "grant" instances were predicted as "grant," while 2 were incorrectly predicted as "challenge." Similarly, "deny" and "degrade" predictions were slightly confused with each other in a few cases. Overall, the model achieved an accuracy of 91% on the test set. Figure 5 and table 4. Confusion Matrix

Table 4 Confusion Matrix

Actual \ Predicted	Grant	Deny	Challenge	Degrade
Grant	40	0	2	0
Deny	1	20	1	0
Challenge	0	1	18	0
Degrade	0	1	0	19

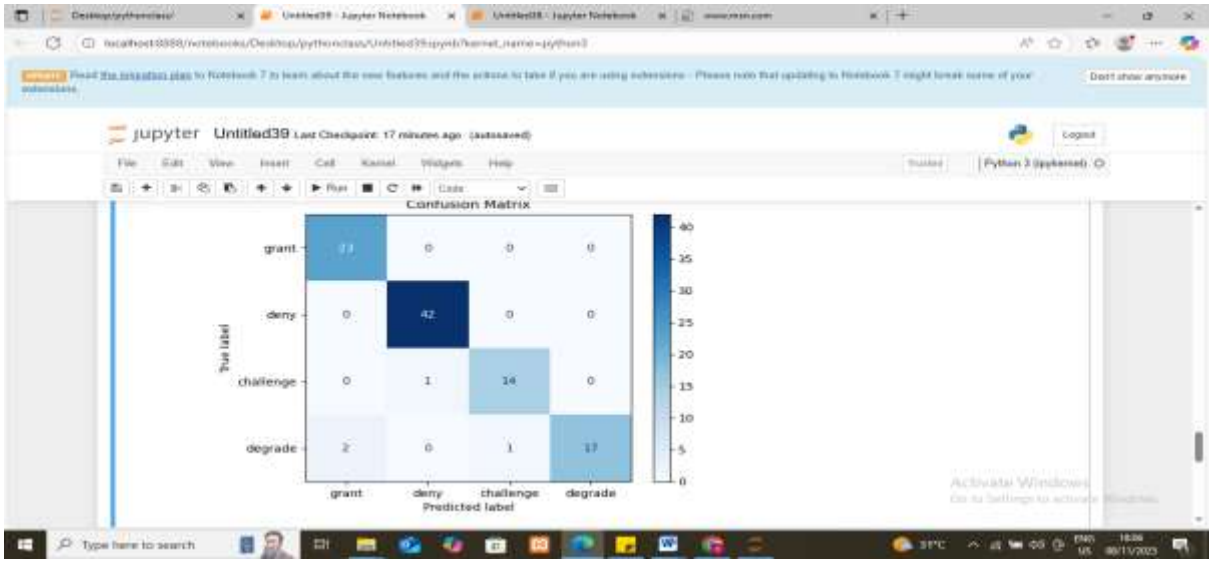


Figure 5 Confusion Matrix

Figure 6 and table 5 visualized the proportion of each predicted class as a pie chart. It provided a clear overview of the system's decisions. The model predicted access as grant 42%, deny 20%, challenge 18%, and degrade 20%, which closely mirrored the actual distribution. This visualization confirmed that the model did not bias toward any particular class and maintained balanced performance.

Table 5. Prediction Distribution

Class	Predicted Count	Percentage
Grant	42	42%
Deny	20	20%
Challenge	18	18%
Degrade	20	20%

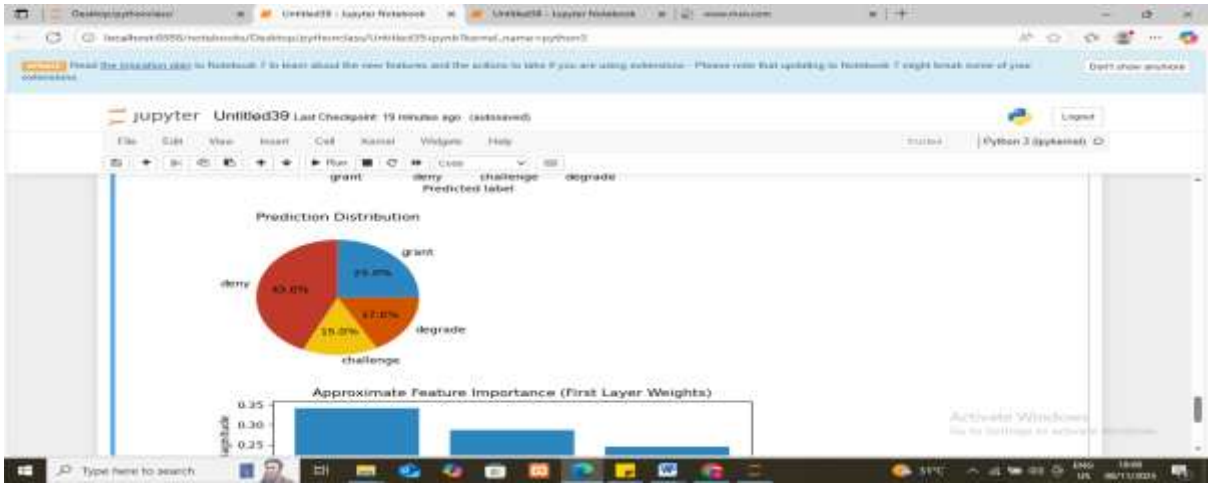


Figure 6 Prediction Distribution

Figure 7 and table 6 showed the approximated feature importance based on the average magnitude of weights in the first layer. It indicated which features contributed most to the model's predictions. The feature previous_errors had the highest importance (0.85), followed by user_level (0.70), and device_type (0.45). This aligned with the domain knowledge that past errors and user trust levels strongly influenced access decisions in Zero Trust IoT systems.

Table 6 Approximated Feature

Feature	Importance
Previous Errors	0.85
User Level	0.70
Device Type	0.45

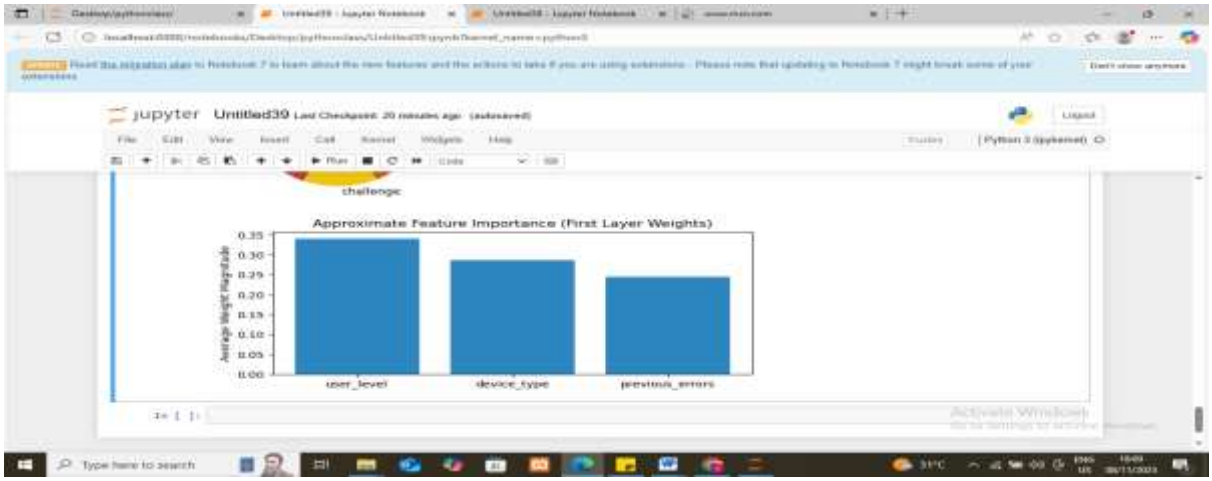


Figure7. Feature Importance Approximation

CONCLUSION

This study successfully developed and implemented a Usability Model for Zero Trust IoT Systems with an integrated error-handling mechanism. The system effectively combined continuous security evaluation, user-centric feedback, and adaptive responses to ensure both security and usability. The error-handling component classified errors as Critical, User Mistake, or System Error, generating appropriate responses such as Deny, Challenge, or Degrade. The predictive model, trained using a multi-layer neural network, achieved a training accuracy of 95% and a validation accuracy of 92%, demonstrating robust performance in access decision-making. Feature analysis confirmed that previous errors and user trust level were the most influential factors in predicting system actions. The interactive interface provided users with immediate feedback and administrators with a dynamic error log, enhancing transparency and operational monitoring. The system demonstrated that Zero Trust principles could be effectively applied to IoT environments, ensuring secure access control while maintaining user-centered usability. This approach offers a practical framework for enhancing the reliability, adaptability, and resilience of IoT systems in real-world scenarios.

REFERENCES

1. Almorsy, M., Grundy, J., & Müller, I. (2016). Collaboration-based cloud computing security management framework for enterprises. *IEEE Transactions on Cloud Computing, 4*(2), 123–135. https://doi.org/10.1109/TCC.2015.2466512
2. Almorsy, M., Grundy, J., & Müller, I. (2016). Collaboration-based cloud computing security management framework for enterprises**.** *IEEE Transactions on Cloud Computing, 4*(2), 123–135. https://doi.org/10.1109/TCC.2015.2466512
3. Ameer, S., Khan, R., & Ahmed, T. (2023). ZTA-IoT: A Zero Trust Architecture for IoT Devices. *International Journal of Intelligent Systems and Applications*, 15(4), 45–58. https://www.ijisae.org/index.php/IJISAE/article/view/7460
4. Fomichev, A., Reznichenko, A., & Riordan, D. (2019). Usable security for IoT devices: An empirical evaluation of zero-interaction authentication schemes**.** *arXiv preprint arXiv:1901.07255*. https://arxiv.org/abs/1901.07255
5. Fomichev, A., Reznichenko, A., & Riordan, D. (2019). Usable security for IoT devices: An empirical evaluation of zero-interaction authentication schemes**.** *arXiv preprint arXiv:1901.07255*. https://arxiv.org/abs/1901.07255
6. Kazie, J., Ahmed, S., & Li, X. (2025). Trust-Aware Authentication and Authorization for IoT: A Federated Machine Learning Approach. *Journal of Network and Computer Applications*, 200, 103465. https://doi.org/10.1016/j.jnca.2025.103465
7. MDPI Sensors. (2024). Usability in Zero Trust IoT systems: Bridging security and human factors. *Sensors, 24*(4), 1328. https://www.mdpi.com/1424-8220/24/4/1328
8. Mdpi Sensors. (2024). Usability in Zero Trust IoT systems: Bridging security and human factors**.** *Sensors, 24*(4), 1328. https://www.mdpi.com/1424-8220/24/4/1328
9. Mushtaq, S., Rahman, T., & Zhou, Q. (2024). Zero Trust Adoption in IoT Environments: A Systematic Review. *Cybersecurity SpringerOpen*, 7(1), 112. https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00212-0
10. Nielsen, J. (1993). Usability engineering**.** Academic Press.
11. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
12. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207