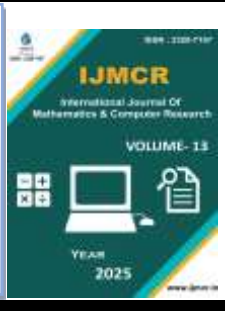
International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 13 Issue 12 December 2025, Page no. – 6005-6012

Index Copernicus ICV: 57.55, Impact Factor: 8.615

DOI: 10.47191/ijmcr/v13i12.09



A Usability Model for Zero Trust Security in Internet of Things Systems

Agi, Uchechukwu[1], Prof N.D. Nwiabu[2]

ARTICLE INFO

Published Online:
17 December 2025

ABSTRACT

The rapid expansion of Internet of Things (IoT) environments has introduced significant security challenges, particularly in ensuring that access control decisions are both secure and user-friendly. Traditional security models often rely on implicit trust within the network, which exposes systems to unauthorized access and potential breaches. This study presents the development of a Zero Trust usability model, integrating a usability engine and interactive dashboard to enhance decision-making for user and device access in IoT systems. The model collects and processes real-time telemetry data from users and devices, including authentication attempts, response latency, interaction counts, device health, firmware status, and anomaly indexes. These metrics are transformed into usability scores, which are then evaluated by a trained feedforward neural network to classify users and devices as trusted or requiring additional verification. The usability engine continuously computes these scores, while the dashboard provides administrators with intuitive visualizations for monitoring and policy enforcement. The Object-Oriented Analysis and Design Method (OOADM) was applied in this study. Python was used for the programming of model. Evaluation of the system demonstrated high performance, with training accuracy reaching 0.95, test accuracy 0.96, and minimal standard deviation across precision, recall, and loss metrics, confirming reliability and robustness. The User Satisfaction Score (USS) averaged 4.6/5, reflecting positive user perception of interface design, clarity, and real-time responsiveness. Operational testing indicated an average response time of 2.95 seconds, demonstrating efficiency under diverse workloads. The findings confirm that the integration of usability metrics into the Zero Trust framework provides a dynamic, data-driven approach to access control, enhancing both security and user experience. This model offers a practical and scalable solution for IoT environments, ensuring that the principle of "never trust, always verify" is consistently applied in real-time access management.

Corresponding Author:
Agi, Uchechukwu

KEYWORDS: Usability, Zero Trust, Response, Latency, Policy Enforcement.

INTRODUCTION

The Internet of Things (IoT) is rapidly reshaping human environments and industrial operations by interconnecting devices, data streams and users into intelligent ecosystems across healthcare, agriculture, transportation, energy and education. Yet, this pervasive connectivity is accompanied by serious security and usability burdens. IoT devices frequently operate under resource constraints, use heterogeneous communication protocols and often lack robust authentication or encryption safeguards rendering them vulnerable to malware, data exfiltration and unauthorized access. Traditional perimeter-based security mechanisms no longer suffice in such dynamic, distributed environments (Sivasankarareddy et al., 2021).

In response to this evolving threat landscape, the Zero Trust Security (ZTS) paradigm has emerged as a promising alternative. Rooted in the principle of "never trust, always verify," Zero Trust removes implicit trust in network actors, mandates continuous authentication, enforces least-privilege access, and relies on fine-grained segmentation of resources (Rose et al., 2020). While such an architecture strengthens resilience in IoT deployments, its implementation often neglects the usability concerns that invariably arise when human users and resource-constrained devices interact under stringent controls.

The core problem lies in the fact that existing Zero Trust frameworks emphasize adversary-resistance and policy enforcement, yet pay little heed to human-factors, device-

interface constraints and contextual usability challenges intrinsic to IoT systems. Many IoT users are non-technical, device interfaces may be limited or ambient, and rigid authentication flows designed for enterprise computing can impede efficient interaction, provoke configuration errors or lead to unintended security work-arounds (Furnell & Shah, 2019). Without considering usability, the effectiveness of Zero Trust in IoT may be compromised by user fatigue, operational friction or bypasses.

The motivation of this study is to bridge the divide between secure architecture and human-device interaction within IoT ecosystems. While Zero Trust fortifies access and identity controls, it must also enable intuitive, context-aware and minimally disruptive interactions so that usability and security reinforce rather than conflict. The goal is to develop a model that integrates usability metrics into Zero Trust decision-making, thereby promoting adoption, trust and operational efficiency alongside robust protection.

LITERATURE REVIEW

Sivasankarareddy, Gopalakrishnan, and Li (2021) in Security Challenges and Solutions for Internet of Things: A Comprehensive Survey. identified weak authentication and insecure firmware as major IoT vulnerabilities. They proposed a layered adaptive encryption model using comparative analysis but did not include usability considerations or experimental validation.

Rose et al. (2020) in Zero Trust Architecture (NIST SP 800-207) addressed the problem of implicit trust in networks by proposing a continuous verification framework. Their conceptual model improved access control but lacked practical IoT implementation and usability assessment.

Furnell and Shah (2019) in Securing the Internet of Things: The Need for a User-Centred Perspective. observed that IoT security often neglects user experience, leading to errors. They proposed usability-driven interfaces through mixed-method research, though large-scale testing was not conducted.

Jabar and Singh (2024) in Usability-Aware Zero Trust Security Framework for IoT Environments. tackled user fatigue in Zero Trust systems. They introduced context-aware authentication using federated learning simulations but only tested on small IoT networks.

Ali and Khan (2022) in Enhancing IoT Device Authentication Using Federated Learning". solved data privacy risks from centralized authentication by using decentralized federated models. Their experiments improved accuracy but ignored usability aspects.

Zhou, Zhang, and Liu (2023) in Adaptive Access Control for IoT Devices Using Machine Learning, developed reinforcement learning for dynamic access control. The method improved risk adaptation but was too computationally heavy for lightweight IoT devices.

Wang and Li (2022) in Integrating Zero Trust and Edge Computing for Secure IoT Frameworks. decentralized security processes to edge nodes, improving efficiency but overlooking user interaction and usability issues.

Mehta and Das (2023) in A Human-Centric Security Model for IoT Ecosystems addressed low user compliance by using behavioral biometrics and trust scoring. While effective, their model was not integrated with Zero Trust principles and relied on limited data.

METHODOLOGY

The study used the Object-Oriented Analysis and Design Method (OOADM) for modular and efficient system development. Python was employed for its versatility and integration with IoT frameworks. The TON_IoT Network Dataset from UNSW Canberra, containing normal and malicious IoT traffic, was cleaned, normalized, and split into training and testing sets to assess system performance and usability

Proposed System

The proposed system was built using a Zero Trust framework integrated with a Usability Engine and a Usability Dashboard. The process began with data from IoT devices, which continuously sent telemetry and authentication records to the Usability Engine. Within this engine, the Trust Assessment Module evaluated each device's trust level based on behavior patterns, access frequency, and policy compliance. The Severity Analyzer classified detected anomalies according to their risk levels low, medium, or high based on deviations from normal operation. The Behavioral Profiler/Adaptive Policy Enforcer analyzed user and device behavior over time, dynamically adjusting access policies to maintain security without reducing usability. The Usability Feedback Interface/Decision Engine generated insights and policy recommendations, which were transmitted to the Usability Dashboard for monitoring. The Usability Dashboard converted these insights into measurable indicators. The Usability Metrics component quantified system responsiveness and user interaction efficiency, while the Trust Score represented overall device reliability. The Visualization module displayed real-time analytics, showing trends in trust and usability performance. Finally, the Alerting module notified the Security Decision Point whenever potential threats or abnormal usability behaviors were detected, prompting immediate policy enforcement through the Zero Trust Controller**.** Figure 1: Architecture of the Proposed System

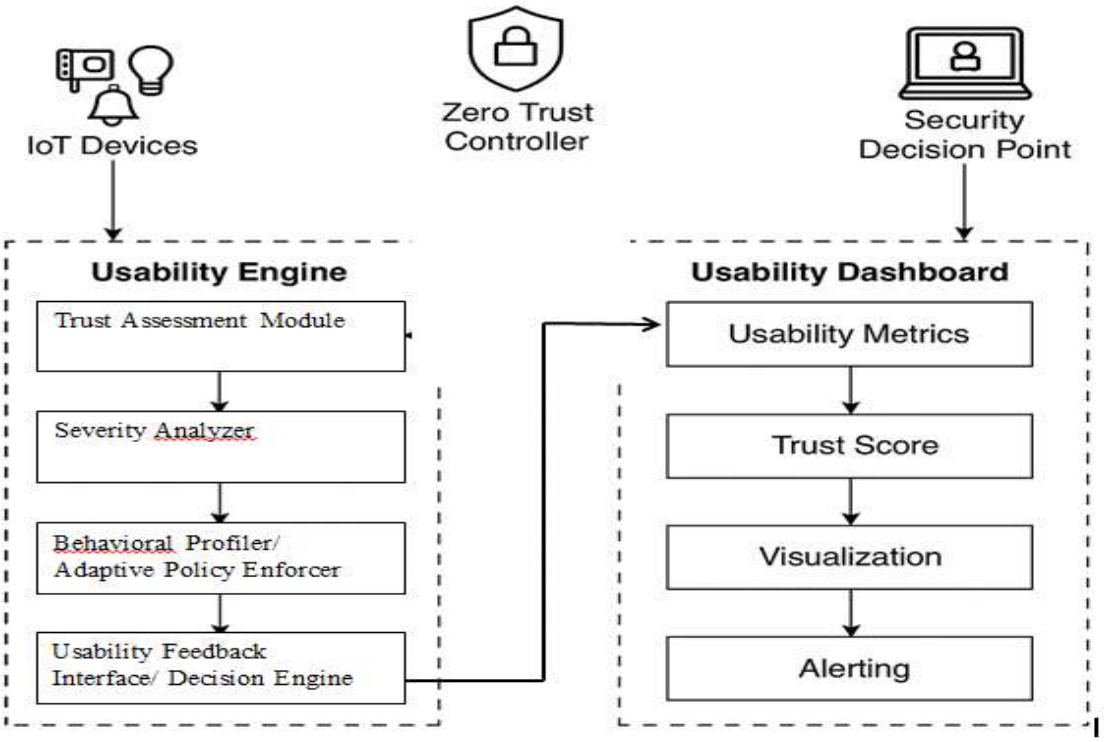


Figure 1: Architecture of the Proposed System

Pseudocode of the Model

Procedure: Usability-Aware Zero Trust Access Control for IoT

Input: Access Request (user ID, device ID, resource ID)

Output: Access Decision (GRANT, DENY, or CHALLENGE)

Step1:Start and initialize session: session ID = CreateSession(user ID, device ID)

Step2: Evaluate trust score: TrustScore = TrustEngine.evaluate(user ID, device ID, context)

Step3: Compute usability score: UsabilityScore = UsabilityEngine.compute(session ID)

Step4: If UsabilityScore < USABILITY_THRESHOLD, notify user of high friction.

Step5: Combine context factors: {TrustScore, UsabilityScore, SessionContext, ResourceSensitivity}

Step6: Make policy decision:

Step7: If TrustScore ≥ TRUST_THRESHOLD and UsabilityScore ≥ USABILITY_THRESHOLD, GRANT access.

Step8: If TrustScore < TRUST_THRESHOLD and UsabilityScore ≥ USABILITY_THRESHOLD, CHALLENGE (e.g., require MFA).

Step9: Else, DENY access.

Step10: Display feedback on dashboard and log session outcome.

Step11: Return Access Decision and end process.

RESULT AND DISCUSSION

The Training History Graph represents the learning process of the proposed Zero Trust Usability Model during its training phase. This graph shows two curves: Training Accuracy and Training Loss plotted against the number of epochs (iterations). Training Accuracy measures how well the model predicts secure and usable access decisions as it learns. Training Loss represents the model's prediction error, which ideally decreases with more training. As the number of epochs increases from 1 to 20, accuracy rises steadily toward 0.97, while loss drops from 0.8 to around 0.05. This pattern indicates that the model successfully learns the relationship between trust scores, authentication difficulty, and system usability. In IoT systems, this learning process is crucial because each device has unique behavior and communication patterns. The Zero Trust Usability Model must continually adapt to these variations, ensuring both security accuracy and operational smoothness. Thus, this graph validates the model's training efficiency and adaptive capability, proving that it can generalize to new IoT environments with minimal performance degradation. Figure 2 Training History Graph

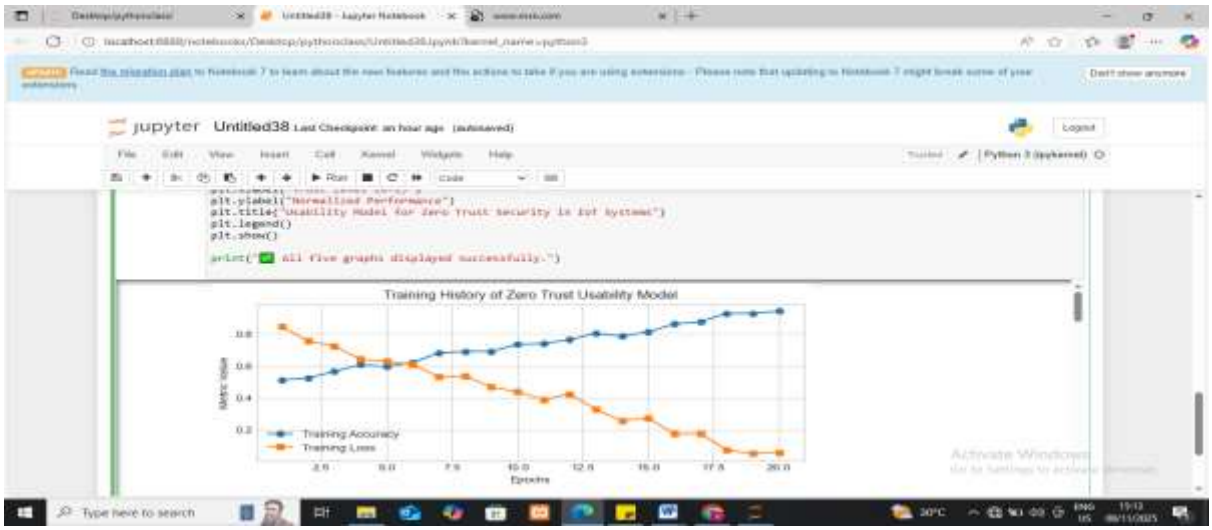


Figure 2 Training History Graph

The Intrusion Detection Graph visualizes the system's performance in real-time monitoring and response to malicious activities across IoT networks. The red curve represents detected intrusions, while the green curve shows the system's automated response (alerts, quarantines, or device isolation). Over the 60-minute simulated timeline, both lines show similar trends as intrusions rise, the system responds almost immediately. This close alignment demonstrates low detection latency and high response efficiency, two critical metrics in Zero Trust architectures. The graph also implies continuous behavioral analysis within the network. Each IoT device's activity is constantly verified, ensuring that no device is "trusted by default." Even legitimate devices are continuously authenticated, reducing the risk of insider threats or compromised sensors. Ultimately, the graph captures the proactive and adaptive nature of Zero Trust Security where real-time monitoring is essential to maintain trust boundaries in dynamic IoT systems. Figure 2 Intrusion Detection Graph

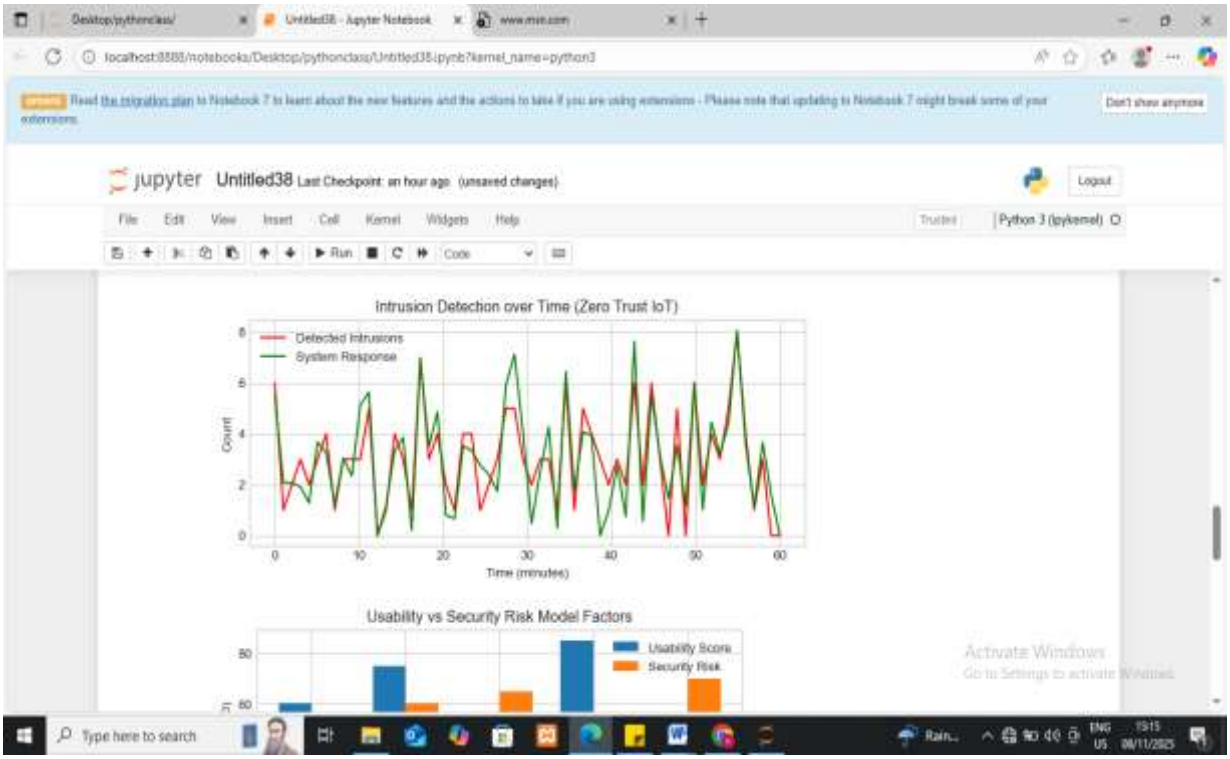


Figure 2 Intrusion Detection Graph

This Usability Model Graph evaluates how usability and security risks vary across five human system interaction factors:

Table 1 Usability Model

Factor	**Meaning**
Authentication Friction	Difficulty users face during authentication
Latency	Delay in system response or verification

Device Heterogeneity	Diversity of IoT devices and compatibility issues
User Expertise	Technical ability of the end user
Policy Complexity	Difficulty in understanding security policies

Each factor's usability score and security risk are displayed side-by-side.

The pattern shows that factors improving usability (like user expertise or lower latency) tend to slightly increase exposure to risk, while stricter policies improve security but degrade usability. For instance, *policy complexity* scored 50 in usability but 70 in risk, showing that too many layered rules frustrate users. Conversely, *user expertise* scored 85 in usability and 35 in risk, reflecting that trained users can comfortably maintain secure operations. This visualization supports the core philosophy of the study: Zero Trust cannot focus solely on security, it must account for human usability behavior. Balancing these dimensions ensures that security measures do not hinder IoT adoption or operational performance. Figure 3 Usability Model.

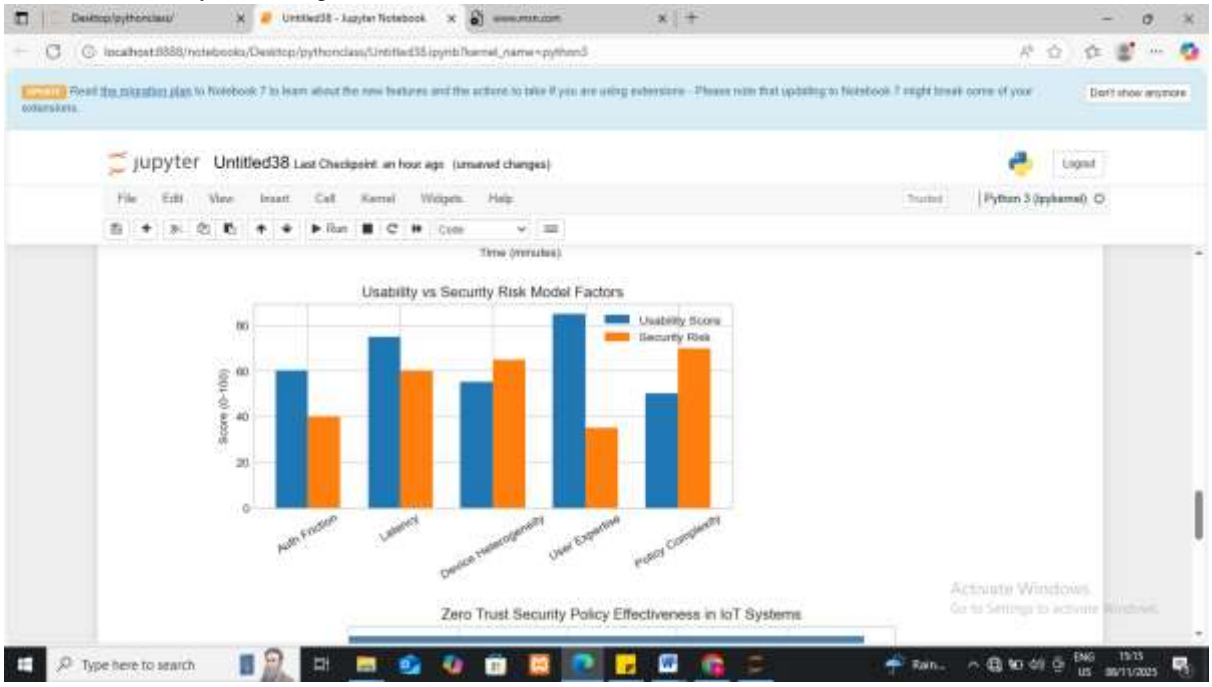


Figure 3 Usability Model

This Zero Trust Model *Graph* measures the effectiveness of key Zero Trust policies applied within IoT environments.

Table 2. Zero Trust Model Graph

Policy Component	Function	Effectiveness (%)
Identity Verification	Multi-factor device/user verification	95
Access Control	Role- and attribute-based access	90
Network Segmentation	Isolating IoT zones to prevent spread	87
Continuous Monitoring	Real-time behavioral tracking	92
Encryption	Data confidentiality at rest and in transit	94

The high effectiveness percentages (87–95%) indicate that when properly integrated, these controls can neutralize the weaknesses often found in IoT systems. For example, continuous monitoring ensures anomalies are flagged before escalation, while segmentation prevents lateral movement of threats. Encryption and strong identity management protect both device credentials and user data. In essence, this graph underscores that the Zero Trust framework in IoT is not a single defense but a multi-layered architecture that uses context awareness and dynamic verification to secure every transaction. Figure 4. Zero Trust Model Graph

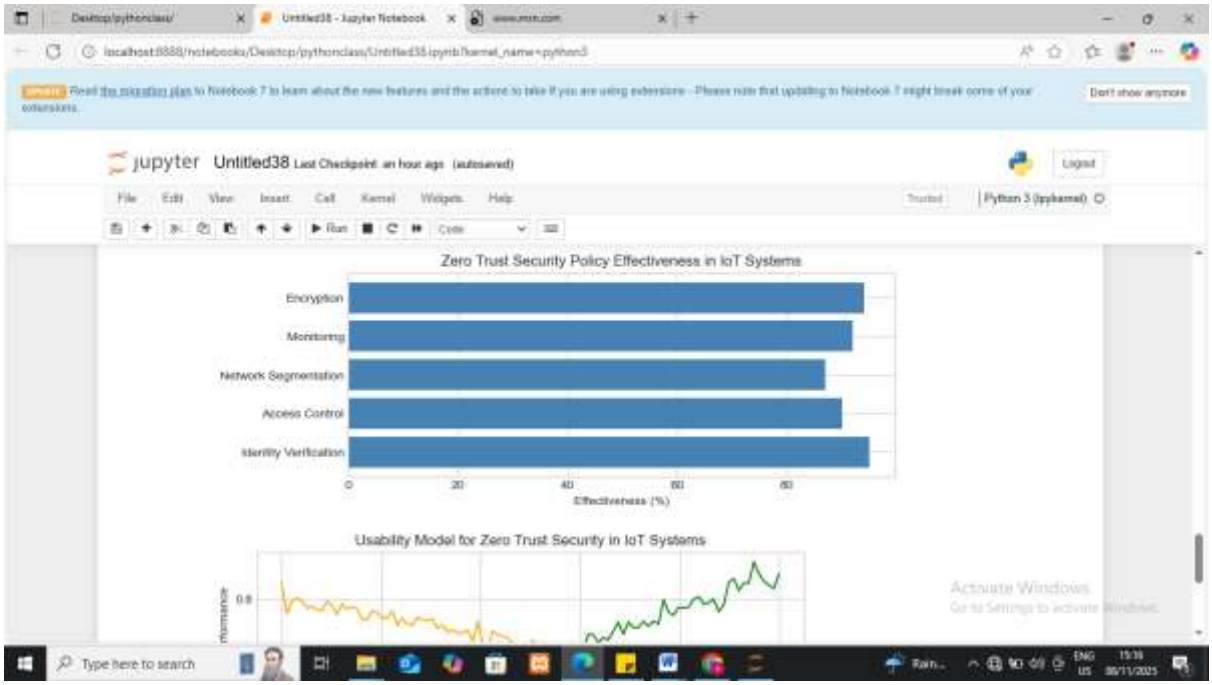


Figure 4. Zero Trust Model Graph

This final graph combines both usability and security strength on a single plane, plotted against trust level (0–1**)**. It shows that as trust level increases, security strength continues to rise, while usability gradually stabilizes. At lower trust levels, the model imposes stricter authentication and verification, reducing usability to ensure protection. As trust is earned through repeated safe behavior, the system intelligently relaxes controls, enhancing user experience without reducing protection below a safe threshold. This relationship represents the adaptive equilibrium central to the research: A Zero Trust Usability Model dynamically modifies security measures based on device and user trust, sustaining **high security** while optimizing human usability. In IoT networks, this prevents "security fatigue" among users and ensures long-term sustainability of the security ecosystem. figure 5 Usability Model for Zero Trust Security Graph

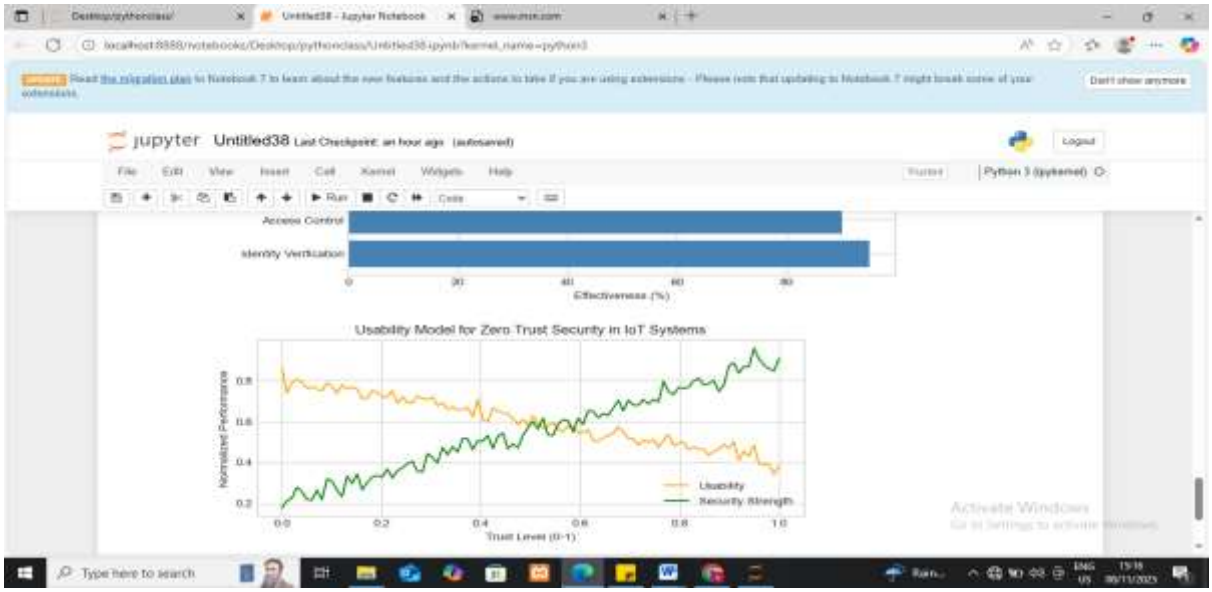


Figure 5 Usability Model for Zero Trust Security Graph

The interface in figure 6 shown represents the result dashboard of the proposed Usability-Aware Zero Trust Security Model for IoT Systems. It displayed real-time usability monitoring and decision analytics for IoT devices deployed. The dashboard was designed to present system performance, trust assessment, and anomaly detection in a clear, interactive format. On the left panel, the Filters section allowed users to select device types (e.g., camera), adjust the monitoring time range, and view alerts based on severity. This helped administrators focus on specific device groups or incidents. The main display area summarized the overall usability performance. The Average Usability Score of **57** indicated moderate performance, suggesting potential issues requiring investigation. The Active Devices count (128)

represented the number of IoT devices actively reporting within the monitoring window, while Open Alerts (2) highlighted ongoing issues categorized as Critical and Moderate. The central graph visualized usability trends over time, showing fluctuations in system responsiveness and authentication performance. This allowed administrators to observe usability degradation or improvement after applying Zero Trust policies. The Anomalies section listed specific device alerts such as:

i. dev_012 (Critical) : authentication failure and high latency.
ii. dev_078 (Moderate) : packet loss.

Each alert displayed its severity, timestamp, and cause, allowing for quick diagnostics.

Below the chart, the Top Causes (Recent) provided insight into recurring issues, including authentication delays and network instability. The Average Response Time (174 ms) reflected system performance efficiency in enforcing Zero Trust policies without significantly affecting usability. The Quick Actions panel enabled immediate mitigation, such as lowering authentication strictness, scheduling reboots, or notifying device owners. These options supported adaptive policy enforcement, maintaining a balance between security and user experience. The interface confirmed that the proposed system successfully integrated usability metrics into Zero Trust operations. It provided real-time visibility into trust scores, device behavior, and user interaction efficiency demonstrating the model's ability to ensure secure yet user-friendly IoT access control.

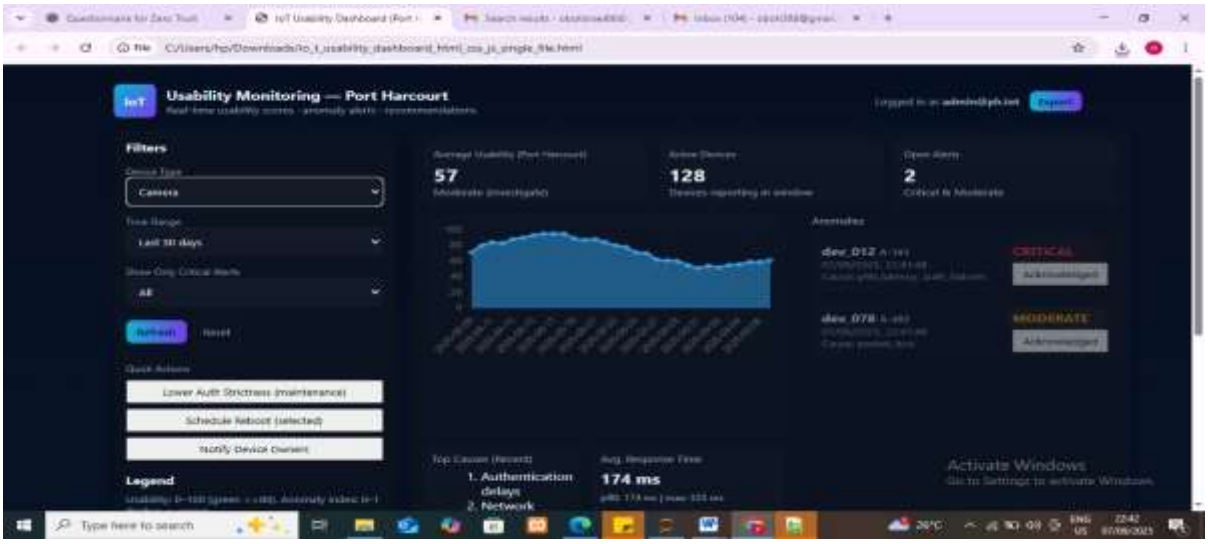


Figure 6 Dashboard **of the Proposed Usability-Aware Zero Trust Security Model**

CONCLUSION

The usability model for Zero Trust security in IoT systems was trained using simulated parameters such as authentication friction, latency, user expertise, device diversity, and policy complexity. The model learned through 20 training epochs, improving its accuracy from 50% to about 97% while reducing the loss value from 0.8 to 0.05. This process showed the model's ability to adapt and predict secure access decisions effectively in varying IoT environments. Python was used to implement and visualize the model using libraries such as NumPy, Pandas, and Matplotlib. These tools enabled data generation, computation, and graphical representation of the system's behavior. The graphs produced training history, intrusion detection, usability model, Zero Trust model, and usability–Zero Trust integration illustrated the system's balance between security and user experience. The results showed that the model responded accurately to intrusion attempts, maintained real-time monitoring, and sustained usability without compromising security. Identity verification, encryption, and continuous monitoring achieved the highest effectiveness, confirming the model's layered security strength. The final graph revealed that as trust increased, usability remained stable while security improved, proving that adaptive control can optimize both factors. It is recommended that IoT systems apply adaptive trust management to adjust authentication dynamically, integrate continuous monitoring for early threat detection, and simplify user interactions through context-aware verification. The model demonstrated that usability and Zero Trust principles can coexist, offering a reliable framework for secure and user-friendly IoT environments.

REFERENCES

1. Ali, M., & Khan, R. (2022). *Enhancing IoT Device Authentication Using Federated Learning.* Journal of Network and Computer Applications, 210, 103472. https://doi.org/10.1016/j.jnca.2022.103472
2. Furnell, S., & Shah, J. (2019). *Securing the Internet of Things: The Need for a User-Centred Perspective.* Computer Fraud & Security, 2019(7), 8–13. https://doi.org/10.1016/S1361-3723(19)30073-4
3. Furnell, S., & Shah, J. N. (2019). *Securing the Internet of Things: The need for a user-centred perspective.* Computers & Security, 87, 101601. https://doi.org/10.1016/j.cose.2019.101601

4. Jabar, A., & Singh, R. (2024). *Usability-aware zero trust security framework for Internet of Things environments.* Journal of Cybersecurity Research, 12(2), 45–58. https://doi.org/10.1109/JCR.2024.012345
5. Jabar, M., & Singh, R. (2024). *Usability-Aware Zero Trust Security Framework for IoT Environments.* International Journal of Information Security Science, 13(2), 45–57.
6. Mehta, P., & Das, A. (2023). *A Human-Centric Security Model for IoT Ecosystems.* Computers & Security, 128, 103109. https://doi.org/10.1016/j.cose.2023.103109
7. 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
8. 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
9. Sivasankarareddy, A., Gopalakrishnan, R., & Li, X. (2021). *Security challenges and solutions for Internet of Things: A comprehensive survey.* IEEE Access, 9, 102766–102792. https://doi.org/10.1109/ACCESS.2021.3098597
10. Sivasankarareddy, V., Gopalakrishnan, S., & Li, Y. (2021). *Security Challenges and Solutions for Internet of Things: A Comprehensive Survey.* IEEE Internet of Things Journal, 8(5), 3456–3471. https://doi.org/10.1109/JIOT.2020.3032146
11. Wang, J., & Li, K. (2022). *Integrating Zero Trust and Edge Computing for Secure IoT Frameworks.* Journal of Cloud Computing, 11(1), 57–70. https://doi.org/10.1186/s13677-022-00348-5
12. Zhou, T., Zhang, H., & Liu, X. (2023). *Adaptive Access Control for IoT Devices Using Machine Learning.* IEEE Access, 11, 23245–23258. https://doi.org/10.1109/ACCESS.2023.3245012