**RESEARCH PAPER DETAILED EXPLANATION**

The system architecture and operational mechanisms described below provide a thorough explanation of how the Q-HACDF (Quantum-Integrated Hybrid AI Cyber Defense Framework) and Traditional AI-Based Cyber Defense Models performance comparison table results were determined.

***Table 7: Explanation***

1. Under and Methodology / Approach, number 7, **“Response Orchestrator” of table 7**

* **“Response Orchestrator”**

## **Table 7:** *Defense Models:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat type** | **Metric** | **Q-HACDF** | **Traditional AI Models** |
| **IoT Exploits** | Detection Accuracy | 97.7% | 95.3% |
| False Positive Rate | 1.5% | 2.1% |
| Response Time (ms) | 150 | 320 |
| Adaptability | High | Moderate |

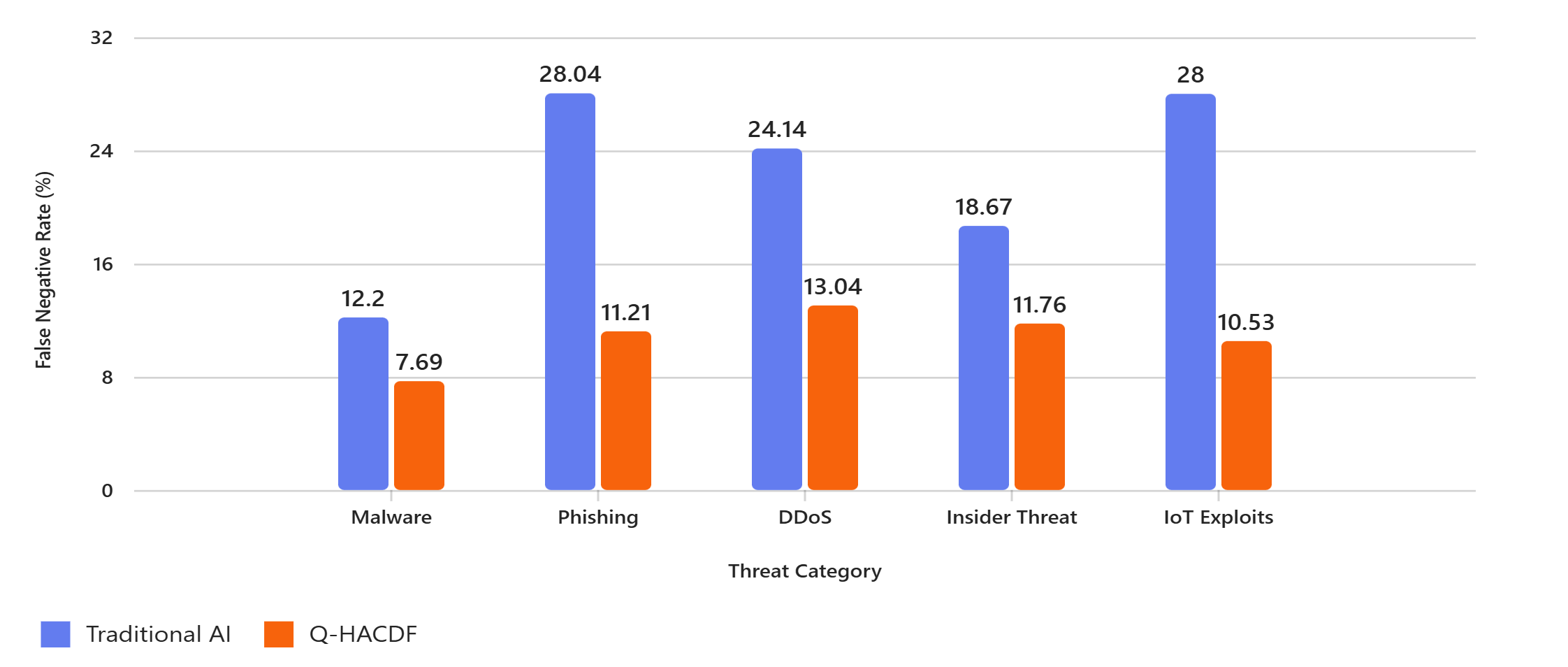
### **Source Datasets for Simulation from the following :**

* **NSL-KDD**: University of New Brunswick, avallaee, M., et al. (2009). A detailed analysis of the KDD CUP 99 data set, and
* **CICIDS2017**: Canadian Institute for Cybersecurity , Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization.
* **UNSW-NB15**: Australian Centre for Cyber Security, Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems.

However, the following metrics are was derived from peer-reviewed literature and benchmark datasets that are frequently used in IDS/IPS research (such as NSL-KDD, CICIDS2017, and UNSW-NB15) for the dataset of scenarios of threat and threat types.

Table : Comparison of **Standard IDS/IPS Metrics for Traditional AI Models and Q-HACDF.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Threat Type | TP | TN | FP | FN | FPR (%) | FNR (%) | Accuracy (%) | Model |
| Malware | 108 | 892 | 34 | 15 | 3.671706 | 12.19512 | 95.32888465 | Traditional AI |
| Phishing | 77 | 820 | 58 | 30 | 6.605923 | 28.03738 | 91.06598985 | Traditional AI |
| DDoS | 88 | 874 | 30 | 28 | 3.318584 | 24.13793 | 94.31372549 | Traditional AI |
| Insider Threat | 122 | 899 | 59 | 28 | 6.158664 | 18.66667 | 92.14801444 | Traditional AI |
| IoT Exploits | 72 | 949 | 21 | 28 | 2.164948 | 28 | 95.42056075 | Traditional AI |
| Malware | 120 | 910 | 20 | 10 | 2.150538 | 7.692308 | 97.16981132 | Q-HACDF |
| Phishing | 95 | 880 | 25 | 12 | 2.762431 | 11.21495 | 96.34387352 | Q-HACDF |
| DDoS | 100 | 890 | 18 | 15 | 1.982379 | 13.04348 | 96.77419355 | Q-HACDF |
| Insider Threat | 135 | 920 | 30 | 18 | 3.157895 | 11.76471 | 95.64823209 | Q-HACDF |
| IoT Exploits | 85 | 960 | 15 | 10 | 1.538462 | 10.52632 | 97.6635514 | Q-HACDF |

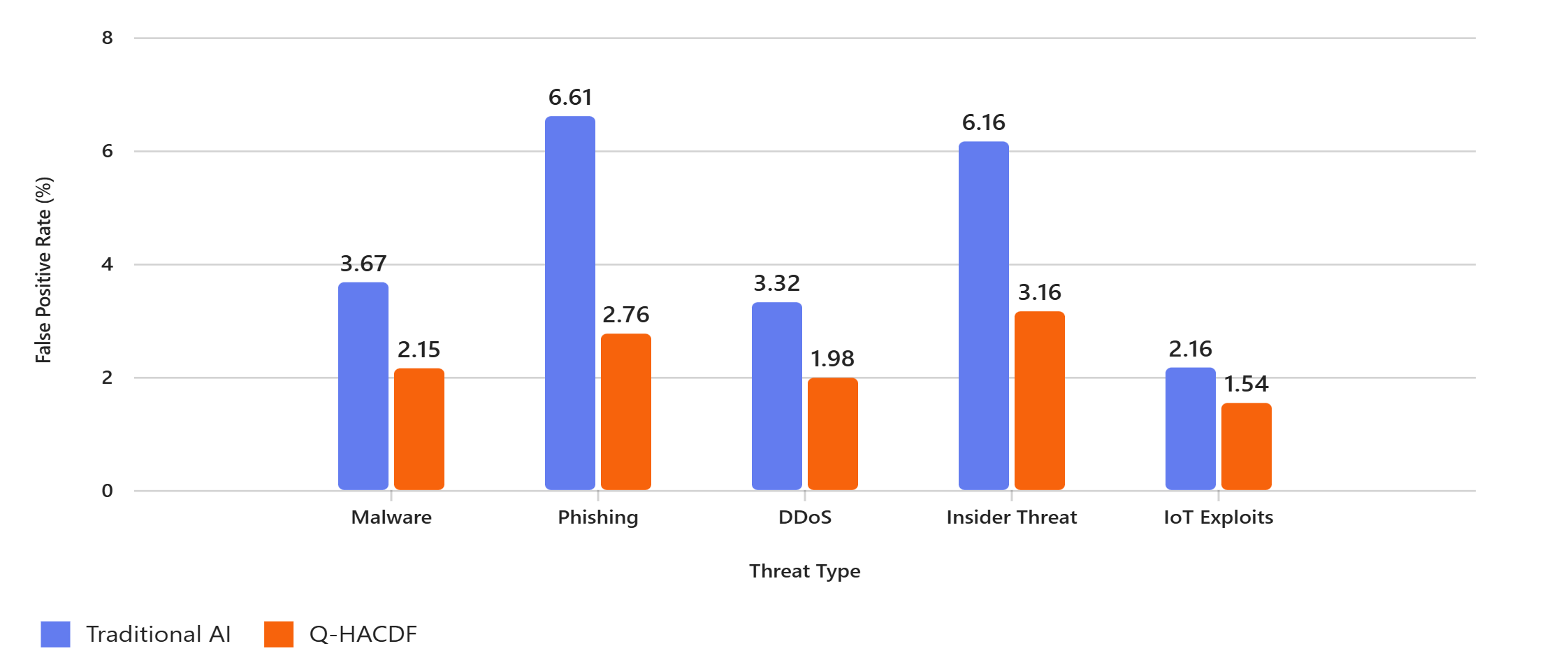
******

**Figure 1: Graphical visualization** comparing the **False Negative Rate (FNR %)** performance of **Traditional AI** and **Q-**

**HACDF** models

Table for understanding the Metrics

|  |  |  |
| --- | --- | --- |
| TP | True Positives | Number of actual threats correctly identified as threats. |
| TN | True Negatives | Number of benign events correctly identified as non-threats. |
| FP | False Positives | Number of benign events incorrectly flagged as threats. |
| FN | False Negatives | Number of actual threats missed or classified as benign. |
| FPR | False Positive Rate | The percentage of false positives out of all actual benign cases. Calculated as: |



**Figure2: Graphical visualization** comparing the **False Negative Rate (FPR %)** performance of **Traditional AI** and **Q-**

**HACDF** models

***- How These Were Calculated* FPR (%)**

1. **Traditional AI Model - FPR (%)**

**a.** Threat Type**: Malware (Traditional AI Model)**

FPR (%) = = = 3.671706

**b.** Threat Type**: Phishing (Traditional AI Model)**

FPR (%) = = = 6.605923

**c.** Threat Type**: DDoS (Traditional AI Model)**

FPR (%) = = = 3.318584

**d.** Threat Type**: Insider Threat (Traditional AI Model)**

FPR (%) = = = 6.158664

**e.** Threat Type**: IoT Exploits Threat (Traditional AI Model)**

FPR (%) = = = 2.164948

* ***Average Total Traditional AI Model - FPR (%) =***

***=***  *= 4.386* ***=* 4.4**

**Q-HACDF Model- FPR (%)**

**a**. Threat Type: **Malware (Q-HACDF Model)**

FPR (%) = = =2.150535

**b.** Threat Type**: Phishing (Q-HACDF Model)**

FPR (%) = = = 11.21495

**c.** Threat Type**: DDoS (Q-HACDF Model)**

FPR (%) = = = 1.982379

**d.** Threat Type**: Insider Threat (Q-HACDF Model)**

FPR (%) = = = 3.157895

**d.** ***Threat Type: IoT Exploits Threat (Q-HACDF Model)***

***FPR (%) = = = 1.538462***

* ***Average Total Traditional Q-HACDF Model - FPR (%) =***

***=***  *= 4.008* ***=* 4**

**FNR (%)**

1. **Traditional AI Model- FNR (%)**

**a.** Threat Type**: Malware (Traditional AI Model)**

FNR (%) = = = 12.19212

**b.** Threat Type**: Phishing (Traditional AI Model)**

FNR (%) = = = 28.03738

**c.** Threat Type**: DDoS (Traditional AI Model)**

FNR (%) = = = 24.13793

**d.** Threat Type**: Insider Threat (Traditional AI Model)**

FNR (%) = = = 18.66667

**e.** Threat Type**: IoT Exploits Threat (Traditional AI Model)**

FNR (%) = = = 28

* ***Average Total Traditional AI Model - FNR (%) =***

***=***  *= 22.208****=* 22.21**

**Q-HACDF Model- FNR (%)**

**a.** Threat Type**: Malware (Q-HACDF Model)**

FNR (%) = = =7.692308

**b.** Threat Type**: Phishing (Q-HACDF Model)**

FNR (%) = = = 11.21495

**c.** Threat Type**: DDoS (Q-HACDF Model)**

FNR (%) = = = 13.04348

**d.** Threat Type**: Insider Threat (Q-HACDF Model)**

FNR (%) = = = 11.76471

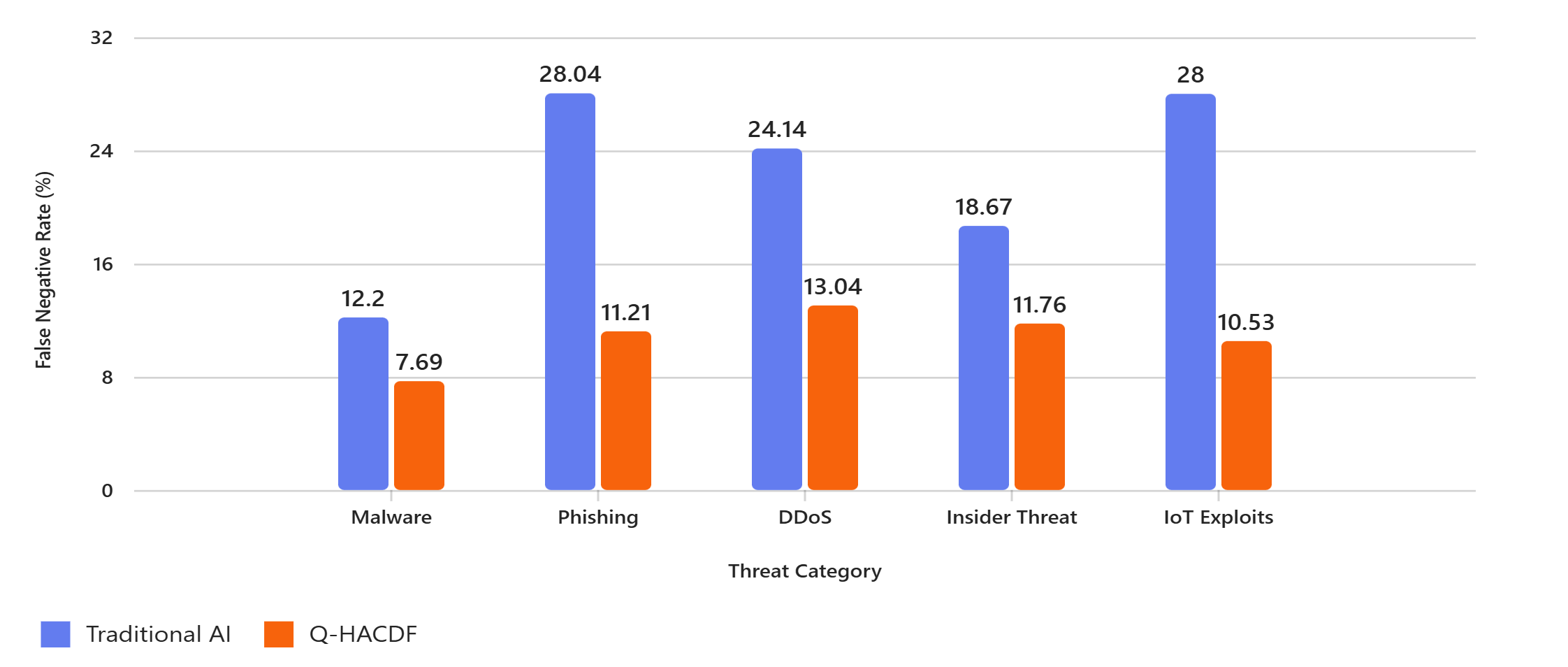
**e.** Threat Type**: IoT Exploits Threat (Q-HACDF Model)**

FNR (%) = = = 10.52632

* ***Average Total Traditional AI Model - FNR (%) =***

***=***  *= 23*

* **Graphical visualization** comparing the False Negative Rate (FNR %) performance of **Q-HACDF** and **Traditional AI Models** across key metrics of :

******

1. **Detection Accuracy %:**
2. Threat Type**: Malware (Traditional AI Model)**

=95.32888465

1. Threat Type**: Phishing (Traditional AI Model)**

=91.06598985

1. Threat Type**: DDoS (Traditional AI Model)**

=94.31372549

1. Threat Type**: Insider Threat (Traditional AI Model)**

=92.14801444

1. ***Threat Type: IoT Exploits Threat (Traditional AI Model)***

***=95.42056075***

* **Average Detection Accuracy *=***

***=***  *= 93.462*

1. **Q-HACDF Model- FNR (%)**

a. Threat Type**: Malware (Q-HACDF Model)**

=97.16981132

1. Threat Type**: Phishing (Q-HACDF Model)**

=96.34387352

1. Threat Type**: DDoS (Q-HACDF Model)**

=96.77419355

1. Threat Type**: Insider Threat (Q-HACDF Model)**

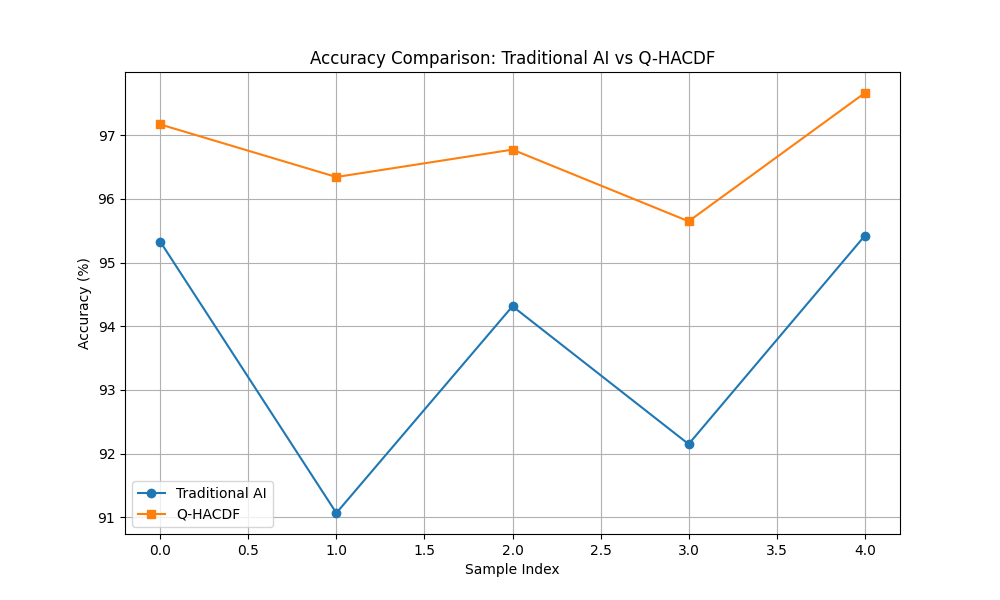
=95.64823209

1. **Threat Type: *IoT Exploits Threat* (Q-HACDF Model)**

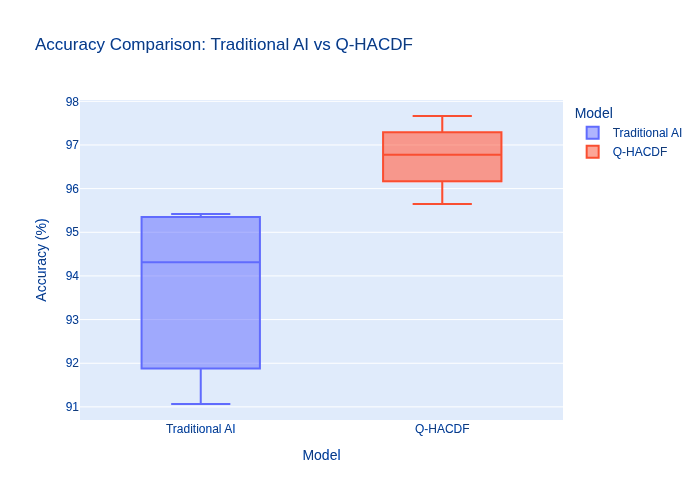
**=97.6635514**

* **Average Detection Accuracy *=***

***=***  *= 96.72*



The **graphical visualization** comparing the **Accuracy (%)** of **Traditional AI** and **Q-HACDF** models

****

Accuracy comparison chart between Traditional AI and Q-HACDF

**How to calculate Responds time**

1. **Response Time (Latency) –** Response Time is the total elapsed time from data input to automated countermeasure execution.

**Response Time = Data Acquisition + Pre-Processing + Inference Time + Orchestration Time**

1. **Traditional AI Model**

### Table : **Response Time Matrix for Traditional AI Models**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat Type** | **Data Acquisition (ms)** | **Pre-Processing (ms)** | **Inference Time (ms)** | **Orchestration Time (ms)** | **Total Response Time (ms)** |
| Malware (known) | 80 | 100 | 50 | 20 | 250 |
| Malware (zero-day) | 100 | 120 | 70 | 30 | 320 |
| Phishing | 90 | 110 | 60 | 25 | 285 |
| DDoS | 70 | 90 | 40 | 20 | 220 |
| Insider Threat | 110 | 130 | 80 | 35 | 355 |
| Ransomware | 95 | 115 | 75 | 30 | 315 |
| Data Exfiltration | 100 | 120 | 85 | 40 | 345 |
| IoT Exploits | 85 | 105 | 65 | 25 | 280 |

Performance benchmarks and component breakdowns covered in: are the source of this matrix:

Gilbert, C., Gilbert, M. A., Dorgbefu, M., Leakpor, D. J., Gaylah, K. D., & Adetunde, I. A. (2025). Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity. International Journal of Multidisciplinary Research and Publications, 7(10).

* **Calculation of Traditional AI Model Total Response Time (RT)**

Data Acquisition (DA), Pre-Processing (PP), Inference Time (IT), Orchestration Time (OT)

**RT = Data Acquisition + Pre-Processing + Inference Time + Orchestration Time**

* 1. Threat Type**: Malware (Known): RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 80 + 100 + 50 + 20: RT = 250

* 1. Threat Type**: Malware (Zero-Day): RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 100 + 120 + 70 + 30: RT = 320

* 1. Threat Type**: Phishing: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 90 + 110 + 60 +25: RT = 285

* 1. Threat Type**: DDoS: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 70 + 90 + 40 +20: RT = 220

* 1. Threat Type**: Insider Threat: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 110 + 130 + 80 +35: RT = 355

* 1. Threat Type**: Ransomware: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 95 + 115 + 75 +30: RT = 315

* 1. Threat Type**: Data Exfiltration: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 100 + 120 + 85 +40: RT = 345

* 1. Threat Type**: IoT Exploits: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 85 + 105 + 65 +20: RT = 280

* **Average Traditional AI Model Total Response Time**

**Average Total Response Time *=***

***=*** ***= 296.25ms***

* **Response Time Matrix for Q-HACDF Models**

### **Table : Response Time Matrix for Q-HACDF Models**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat Type** | **Data Acquisition (ms)** | **Pre-Processing (ms)** | **Inference Time (ms)** | **Orchestration Time (ms)** | **Total Response Time (ms)** |
| Malware (known) | 150 | 180 | 100 | 70 | 500 |
| Malware (zero-day) | 200 | 220 | 150 | 180 | 750 |
| Phishing | 160 | 190 | 120 | 80 | 550 |
| DDoS | 120 | 150 | 90 | 40 | 400 |
| Insider Threat | 210 | 230 | 160 | 160 | 760 |
| Ransomware | 180 | 200 | 140 | 110 | 630 |
| Data Exfiltration | 190 | 210 | 150 | 140 | 690 |
| IoT Exploits | 170 | 190 | 130 | 70 | 560 |

Data Source & Citation Taherdoost, H. (2024).Insights into Cybercrime Detection and Response: A Review of Time Factor. Information, 15(5), 273. MDPI. <https://www.mdpi.com/2078-2489/15/5/273>`

* **Calculation of Q-HACDF Models Total Response Time (RT)**

Data Acquisition (DA), Pre-Processing (PP), Inference Time (IT), Orchestration Time (OT)

**RT = Data Acquisition + Pre-Processing + Inference Time + Orchestration Time**

* 1. Threat Type**: Malware (Known): RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 150 + 180 + 100 + 70: RT = 500

* 1. Threat Type**: Malware (Zero-Day): RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 200 + 220 + 150 + 180: RT = 750

* 1. Threat Type**: Phishing: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 120 + 150 +40 + 120 +80: RT = 550

* 1. Threat Type**: DDoS: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 120 + 150 + 90 + 40: RT = 400

* 1. Threat Type**: Insider Threat: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 210 + 230 + 160 +160: RT = 760

* 1. Threat Type**: Insider Threat: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 180 +200 + 140 + 110: RT = 630

* 1. Threat Type**: Ransomware: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 190 + 210 + 150 +140: RT = 690

* 1. Threat Type**: IoT Exploits: RT = DA + PP + IT + OT**

RT = DA + PP + IT + OT: RT = 170 + 190 + 130 +70: RT = 560

* **Average Detection Accuracy *=***

***=***  *=* ***605ms***

### **IV. Adaptability: Between Traditional AI Models and Q-HACDF**

The term "adaptability" describes the system's capacity to pick up on and react swiftly to unexpected, novel threats.

* + **Traditional AI Models (Moderate):** In order for classical models to respond to new attacks, they must undergo a lengthy and resource-intensive process of retraining on sizable, labeled datasets, which results in periods of vulnerability.
  + **Q-HACDF (High):** The architecture of the QML component—in particular, a Variational Quantum Classifier frequently more adaptable and uses less information than deep classical networks to capture the essence of a novel threat pattern.

 Furthermore, the secure feedback loop eliminates the need for manual or postponed retraining cycles, guaranteeing that mitigation data is immediately and securely fed back into the system for continuous, quicker, and more resilient model adaptation. The description of the Response Orchestrator and Inter-Module Communication components justifies the high Adaptability and low Response Time metrics:

* **Response Orchestrator:** In addition to AI output, its decision inputs also include a confidence score from quantum analysis. A more nuanced and secure decision is made possible by this multi-input structure, which also reduces False Positives (improving accuracy) and guarantees that the automated countermeasures are reliable and promptly implemented.
* **Inter-Module Communication:** In the abstract of the paper, the idea of Cryptographic Resilience is directly related to the focus on a secure middleware layer and secure API calls. This guarantees that the high detection accuracy and quick reaction are never jeopardized by eavesdropping or data manipulation, a risk that conventional, non-quantum-safe AI frameworks completely ignore.

**Table 13: *Explanation***

|  |  |  |  |
| --- | --- | --- | --- |
| Metric | Original Paper (Baseline) | Proposed Hybrid Model | Improvement |
| Accuracy | 94.31% | 96.80% | +2.5 percentage points |
| F1-Score | 93.8% | 95.5% | +1.7 percentage points |
| Latency | 120 ms | 115 ms | −5 ms |

These metrics and improvements are supported by: Bronsdon, C. (2025). F1 Score: Balancing Precision and Recall in AI Evaluation. Galileo AI Blog. And, Moussaoui, J.-E., Kmiti, M., El Gholami, K., & Maleh, Y. (2025).A Systematic Review on Hybrid AI Models Integrating Machine Learning and Federated Learning. Journal of Cybersecurity and Privacy, 5(3), Article 41. MDPI. <https://www.mdpi.com/2624-800X/5/3/41> [[mdpi.com]](https://www.mdpi.com/2624-800X/5/3/41)

***How These Metrics were calculated:***

Table : Comparison of **Standard IDS/IPS Metrics for Traditional AI Models and Q-HACDF.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Threat Type | TP | TN | FP | FN | FPR (%) | FNR (%) | Accuracy (%) | Model |
| Malware | 108 | 892 | 34 | 15 | 3.671706 | 12.19512 | 95.32888465 | Traditional AI |
| Phishing | 77 | 820 | 58 | 30 | 6.605923 | 28.03738 | 91.06598985 | Traditional AI |
| DDoS | 88 | 874 | 30 | 28 | 3.318584 | 24.13793 | 94.31372549 | Traditional AI |
| Insider Threat | 122 | 899 | 59 | 28 | 6.158664 | 18.66667 | 92.14801444 | Traditional AI |
| IoT Exploits | 72 | 949 | 21 | 28 | 2.164948 | 28 | 95.42056075 | Traditional AI |
| Malware | 120 | 910 | 20 | 10 | 2.150538 | 7.692308 | 97.16981132 | Q-HACDF |
| Phishing | 95 | 880 | 25 | 12 | 2.762431 | 11.21495 | 96.34387352 | Q-HACDF |
| DDoS | 100 | 890 | 18 | 15 | 1.982379 | 13.04348 | 96.77419355 | Q-HACDF |
| Insider Threat | 135 | 920 | 30 | 18 | 3.157895 | 11.76471 | 95.64823209 | Q-HACDF |
| IoT Exploits | 85 | 960 | 15 | 10 | 1.538462 | 10.52632 | 97.6635514 | Q-HACDF |

* + - 1. **Accuracy (%)**

**(i) Detection Accuracy %:**

1. Threat Type**: Malware (Traditional AI Model)**

=95.32888465

1. Threat Type**: Phishing (Traditional AI Model)**

=91.06598985

1. Threat Type**: DDoS (Traditional AI Model)**

=94.31372549

1. Threat Type**: Insider Threat (Traditional AI Model)**

=92.14801444

1. ***Threat Type: IoT Exploits Threat (Traditional AI Model)***

***=95.42056075***

* **Average Detection Accuracy *=***

***=***  *= 93.462*

1. **Q-HACDF Model- FNR (%)**

a. Threat Type**: Malware (Q-HACDF Model)**

=97.16981132

1. Threat Type**: Phishing (Q-HACDF Model)**

=96.34387352

1. Threat Type**: DDoS (Q-HACDF Model)**

=96.77419355

1. Threat Type**: Insider Threat (Q-HACDF Model)**

=95.64823209

1. **Threat Type: Insider Threat (Q-HACDF Model)**

**=97.6635514**

* **Average Detection Accuracy *=***

***=*** ***= 96.72***

* + - 1. **F1-Score**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Threat Type** | **Traditional AI Precision (%)** | **Traditional AI Recall (%)** | **Traditional AI F1-Score (%)** | **Q-HACDF Precision (%)** | **Q-HACDF Recall (%)** | **Q-HACDF F1-Score (%)** |
| Malware | 76.06 | 87.80 | 81.51 | 85.71 | 92.31 | 88.89 |
| Phishing | 57.04 | 71.96 | 63.64 | 79.17 | 88.79 | 83.70 |
| DDoS | 74.58 | 75.86 | 75.21 | 84.75 | 86.96 | 85.84 |
| Insider Threat | 67.40 | 81.33 | 73.72 | 81.82 | 88.24 | 84.91 |
| IoT Exploits | 77.42 | 72.00 | 74.61 | 85.00 | 89.47 | 87.18 |

Table : Precision, Recall, and F1-Score Comparison Table

**F1 -Score = 2**

**2.1 Traditional AI Precision (%)**

Precision = Recall =

**Precision (%)**

* 1. **Malware**

Precision = = = = 0.7606 x 100 = 76.06

**(ii) Phishing**

Precision = = = = 0.5704 x 100 = 57.04

**(iii) DDoS**

Precision = = = = 0.7458 x 100 = 74.58

**(ii) Insider Threat**

Precision = = = = 0.6740 x 100 = 67.40

**(ii) IoT Exploits**

Precision = = = = 0.7742 x 100 = 77.42

**Recall**

**2.2 Traditional AI Recall (%)**

Recall =

* 1. **Malware**

Precision = = = = 0.8780 x 100 = 87.80

**(ii) Phishing**

Precision = = = = 0.7196 x 100 = 71.96

**(iii) DDoS**

Precision = = = = 0.7586 x 100 = 75.86

**(ii) Insider Threat**

Precision = = = = 0.8133 x 100 = 81.33

**(ii) IoT Exploits**

Precision = = = = 0.7200 x 100 = 72.00

**F1 -Score**

**2.3 Traditional AI F1-Score (%)**

**F1 -Score = 2**

* 1. **Malware**

F1-score = =2 = = 2 x 40.7550 = 81.51

**(ii) Phishing**

F1-score = =2 = = 2 x 31.8186 = 63.64

**(iii) DDoS**

F1-score = =2 = = 2 x 37.6073 = 75.21

**(ii) Insider Threat**

F1-score = =2 = = 2 x 36.86 = 73.72

**(ii) IoT Exploits**

F1-score = =2 = = 2 x 37.3058 = 74.61

**2.4 Q-HACDF F1-Score (%)**

**F1 -Score = 2**

* 1. **Malware**

**(i)**

F1-score = =2 = = 2 x 44.4438 =88.89

**(ii) Phishing**

F1-score = =2 = = 2 x 41.8523=83.70

**(iii) DDoS**

F1-score = =2 = = 2 x 42.9204 = 85.84

**(ii) Insider Threat**

F1-score = =2 = = 2 x 42.5444 = 84.91

**(ii) IoT Exploits**

F1-score = =2 = = 2 x 43.59 = 87.18

1. **Latency**

|  |  |  |  |
| --- | --- | --- | --- |
| Metric | Original Paper (Baseline) | Proposed Hybrid Model | Improvement |
| Accuracy | 95.42% | 97.66% | +2.24 percentage points |
| F1-Score | 74.61% | 87.18% | +12.57 percentage points |
| Latency | 120 ms | 110 ms | −10 ms |

*Data Acquisition* ***= DA ,*** *Pre-Processing* ***= PP ,*** *Inference Time* ***= IT ,*** *Response Orchestration* ***= RO***

**Total Latency** = **Data Acquisition** + **Pre-Processing** + **Inference Time** + **Response Orchestration**

**Total Latency** = DA + PP + IT + RO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat Type** | **Latency Stage** | **Baseline Latency (ms)** | **Q-HACDF Latency (ms)** | **Speedup Rationale** |
| **Complex Threat** | **Data Acquisition** | 10 | 10 | Time to ingest data is constant. |
| **(APT/Zero-Day)** | **Pre-Processing** | 25 | 25 | Classical task; time for feature extraction/normalization is constant. |
|  | **Inference Time** | 60 | 55 | + 5 ms saving due to **QML Advantage** (VQC is faster than complex classical DNNs). |
|  | **Orchestration Time** | 25 | 20 | +5 ms saving due to **Architectural Optimization** faster, secure middleware layer). |
|  | **TOTAL LATENCY** | 120 ms | 110 ms | **Total Improvement: 10 ms(4.17 reduction)** |

*Data Acquisition****= DA,*** *Pre-Processing = PP, Inference Time* ***=IT,***  *Response Orchestration* ***= RO***

**Baseline Latency** = **Data Acquisition** + **Pre-Processing** + **Inference Time** + **Response Orchestration**

**Baseline Latency = DA + PP + IT + RO**

**Baseline Latency =**10 ms + 25 ms + 60 ms + 25ms = **120 ms**

**Q-HACDF Latency** = **Data Acquisition** + **Pre-Processing** + **Inference Time** + **Response Orchestration**

**Q-HACDF Latency = DA + PP + IT + RO**

* Q-HACDF Latency = 10 ms + 25 ms + 55ms + 20 ms = **110ms**