**RESEARCH PAPER IMPLEMENTATION**

**Table 1: Comparative Analysis of Frameworks**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Framework** | **Detection Accuracy (%)** | **Scalability** | **Latency (ms)** | **Adversarial Robustness (%)** | **Zero-Day Detection (%)** |
| Traditional Security | 70.0 | Low | 45 | 40 | 35 |
| AI-Based IDS | 88.0 | Medium | 30 | 65 | 70 |
| Blockchain-Based | 75.0 | Medium | 60 | 50 | 45 |
| **Hybrid AI + Blockchain** | **95.2** | **High** | **15** | **85** | **88** |

To complete Table 1, Table 2 has to be computed

Table 2: Framework Performance and Detection Metrics

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Framework** | **TP**  **(Count)**  **≈** | **FN**  **(Count)**  **≈** | **FTR (FNR) (%) \*** | **FP (Count)**  **≈** | **TN (Count)**  **≈** | **FPR (Qualitative)** |
| **Traditional Security** | ≈ 0 | ≈ 0 | 65.0 | ≈ 2, 700 | ≈ 6,300 | Low/Medium |
| **AI-Based IDS** | ≈311 | ≈133 | 30.0 | ≈1,000 | ≈ 8,000 | Medium/High |
| **Blockchain-Based** | ≈ 1125 | ≈1375 | 55.0 | ≈ 1,500 | ≈ 7,500 | Low |
| **Hybrid AI + Blockchain** | ≈-220 | ≈-30 | 12.0 | ≈ 450 | ≈ 8,550 | Low |

**\* True Positives (TP), False Negative Rate (FTR), False Positives (FP), Ture Negative (TN), False Positives Rates (FPR)**

* **To calculate Table 2, table 3 has to be computed**

How to calculate them:

|  |  |  |
| --- | --- | --- |
| **Metric** | **Provided Value** | **Derived Value (Calculated)** |
| **Total Malicious Samples (*TP*+*FN*)** | (Assumed 10%) | 1,000 |
| **Total Benign Samples (*TN*+*FP*)** | (Assumed 90%) | 9,000 |
| **Detection Accuracy** | 95.2% | 0.952×10,000=9,520 (Total Correct Predictions) |
| **Zero-Day Detection (TPR/Recall)** | 88% | 0.88×1,000=**880** (True Positives, TP) |

Table 3:

**Assumption on Dataset:**

* **Total Test Samples:** N = 10,000 *(A common, round number for intrusion detection*

*system evaluations).*

Total Malicious Samples = **True Positives (TP) + False Negatives (FN)**

* **True Positives (TP):** Malicious samples that the model **correctly** identifies as malicious (Attack/Anomaly).
* **False Negatives (FN):** Malicious samples that the model **incorrectly** identifies as benign or normal.

**Benign Samples:(** TN + FP)

* **Benign Samples:** (Samples that are NOT attacks)
  1. **Traditional Security** = TN + FP = 6300+2700 = ≈ 9,000
  2. **AI-Based IDS**  = TN + FP = 8000+1000 = ≈ 9,000
  3. **Blockchain-Based** = TN + FP = 7500+1500 = ≈ 9,000
  4. **Hybrid AI + Blockchain** = TN + FP = 8550+450 = ≈ 9,000

**Malicious Samples:(** TP + FN)

* **Malicious Samples:** (Samples that ARE attacks)
  1. **Traditional Security** = TP + FN = 0 + 0 = ≈ 0
  2. **AI-Based IDS**  = TP + FN = 311+133 = ≈ 444
  3. **Blockchain-Based** = TP + FN = 1125 +1375 = ≈ 2500
  4. **Hybrid AI + Blockchain** = TP + FN = -220 + - 30 = ≈ -250

1. **Framework 1**

* **Traditional Security:**

***Calculation Notes for Traditional Security:***

Total Samples = Total Positive Samples (P)+ Total Negative Samples (N)

Total Positive Samples (N) = 0 + 9,000 => 9,000

Total Negative Samples (P) = TN + FP = 6300+2700 = ≈ 9,000

**NOTE:**

True Positives (TP) = > Samples correctly identified as malicious = ≈ 0

False Negatives (FN => Malicious samples missed = ≈ 0

True Negatives (TN) => Samples correctly identified as benign (Source data) = ≈ 6,300

False Positives (FP) => Benign samples misidentified as malicious (Source data) = ≈ 2,700

1. **Framework 2**

* **AI-Based IDS:**

***Calculation Notes for AI-Based IDS****:*

Total Samples = Total Positive Samples (P)+ Total Negative Samples (N)

Total Positive Samples (N) = 444 + 9,000 => 9,444

Total Negative Samples (P) = TN + FP = 8000+1000 = ≈ 9,000

**NOTE:**

True Positives (TP) = > Samples correctly identified as malicious = ≈ 0

False Negatives (FN => Malicious samples missed = ≈ 0

True Negatives (TN) => Samples correctly identified as benign (Source data) = ≈ 8,000

False Positives (FP) => Benign samples misidentified as malicious (Source data) = ≈ 1,000

1. **Framework 3**

* **Blockchain-Based:**

***Calculation Notes for Blockchain-Based:***

Total Samples = Total Positive Samples (P)+ Total Negative Samples (N)

Total Positive Samples (N) = 2,500 + 9,000 => 11,500

Total Negative Samples (P) = TN + FP = 8550+450 = ≈ 9,000

**NOTE:**

True Positives (TP) = > Samples correctly identified as malicious = ≈ 0

False Negatives (FN => Malicious samples missed = ≈ 0

True Negatives (TN) => Samples correctly identified as benign (Source data) = ≈ 8,550

False Positives (FP) => Benign samples misidentified as malicious (Source data) = ≈ 450

1. **Framework 4**

* **Hybrid AI + Blockchain**

***Calculation Notes for Hybrid AI + Blockchain:***

Total Samples = Total Positive Samples (P)+ Total Negative Samples (N)

Total Positive Samples (N) = -250 + 9,000 => 8,750

Total Negative Samples (P) = TN + FP = 8550+450 = ≈ 9,000

**NOTE:**

True Positives (TP) = > Samples correctly identified as malicious = ≈ 0

False Negatives (FN => Malicious samples missed = ≈ 0

True Negatives (TN) => Samples correctly identified as benign (Source data) = ≈ 8,550

False Positives (FP) => Benign samples misidentified as malicious (Source data) = ≈ 450

* 1. **Detection Accuracy (%)**

**How to calculate Detection Accuracy (%)**

Detection Accuracy =

**Detection Accuracy (%)**

* 1. **Traditional Security:**

***Calculation Notes for Traditional Security:***

Detection Accuracy = **=>**  = = 0.7 X100 = **70.0**

* 1. **AI-Based IDS:**

***Calculation Notes for AI-Based IDS:***

Detection Accuracy = **=**  = = 0.8800 X100 = **88.0**

* 1. **Blockchain-Based:**

***Calculation Notes for Blockchain-Based:***

Detection Accuracy = **=**  = = 0.75 X100 = **75.0**

* 1. **Hybrid + Blockchain:**

***Calculation Notes for Hybrid + Blockchain:***

Detection Accuracy = **=**  = = 0.952 X100 = **95.20**

1. **Adversarial Robustness (%)**

**How to calculate Adversarial Robustness (%)**

Adversarial Robustness = or 1- FTR%

**Adversarial Robustness** **(%)**

1. **Traditional Security:**

***Calculation Notes for Adversaries Robustness:***

Adversarial Robustness = 1 – FTR % **=>**  = = 1 - 0.65 = **0.35 or 35.0%**

1. **AI-Based IDS:**

***Calculation Notes for AI-Based IDS:***

Adversarial Robustness = **=>**  = = 0.700 X100 = **70.05**

1. **Blockchain-Based:**

***Calculation Notes for Blockchain-Based:***

Adversarial Robustness = **=>**  = = 0.45 X100 = **45**

1. **Hybrid + Blockchain:**

***Calculation Notes for Hybrid + Blockchain:***

Adversarial Robustness = **=>**  = = 0.45 X100 = **45**

1. **Zero-day Detection (%)**

**How to calculate Zero-day Detection (%)**

Zero-day Detection = or 1- FTR%

**Zero-day Detection (%)**

1. **Traditional Security:**

***Calculation Notes for* Zero-day Detection*:***

Zero-day Detection = 1 – FTR % **=>**  = = 1 - 0.65 = **0.35 or 35.0%**

1. **AI-Based IDS:**

***Calculation Notes for AI-Based IDS:***

Zero-day Detection = 1 – FTR % **=>**  = = 1 - 0.30 = **0.70 or 70.0%**

1. **Blockchain-Based:**

***Calculation Notes for Blockchain-Based:***

Zero-day Detection = 1 – FTR % **=>**  = = 1 - 0.55 = **0.45 or45.0%**

1. **Hybrid + Blockchain:**

***Calculation Notes for Hybrid + Blockchain:***

Zero-day Detection = 1 – FTR % **=>**  = = 1 - 0.12= **0.88 or 88.0%**