CLOUD COMPUTING

Intrusion Detection Systems

PROF. SHAMIK SURAL

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

IIT KHARAGPUR

Intrusion Detection Systems

- Misuse Detection
  - Less False Positive
  - Cannot handle zero-day attacks
- Anomaly Detection
  - Learning based approach
  - Can detect new attacks
  - Impacted by Base Rate Fallacy

Base Rate Fallacy

I – Intrusion, A – Alarm, I’ – No Intrusion, A’ – No Alarm

$P(I/A) = (P(A/I)*P(I))/P(A)$

By B.T.,

$$P(I/A) = (P(A/I)*P(I))/(P(A/I)*P(I)+P(A/I')*P(I'))$$

P(A/I) – True Positive (TP), P(A’/I’) – True Negative (TN)

P(A/I’) – False Positive (FP), (A’/I) – False Negative (FN)

Find $P(I/A)$ for $P(I)=10^{-7}$, TP=95%, TN=95%

Thank You!