# Effectiveness of Moving Target Defense Techniques to Disrupt Attacks in the Cloud

Salman Manzoor, Antonios Gouglidis, Matthew Bradbury and Neeraj Suri
Lancaster University, UK
{s.manzoor1, a.gouglidis, m.s.bradbury, neeraj.suri}@lancaster.ac.uk

## Cloud

- Offers access to resources (services, data, storage, etc.) over the Internet as utilities.
- Is a complex environment entailing both physical and virtual resources.
- Has a multitude of attack surfaces and dynamic threat propagation pathways.

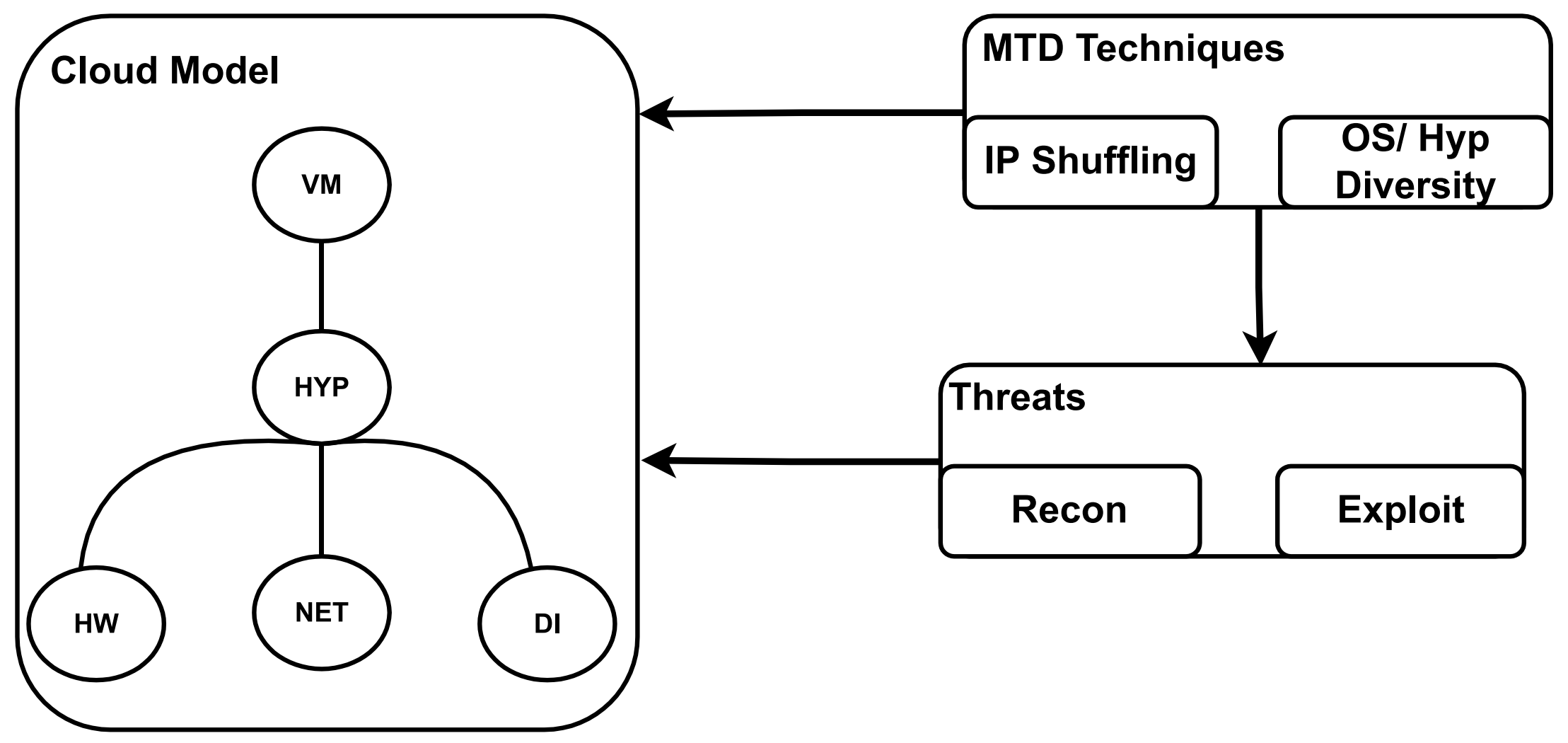
### State of the Art

- Moving Target defences (MTDs) can proactively mitigate threats by dynamically changing attack surfaces (e.g., shuffling IP addresses to increases complexity during the reconnaissance step).
- MTDs deployment is limited to individual components instead of system-wide deployment.

### Our Contributions

- We proposed deployment of MTDs across different layers of the Cloud to evaluate the overall security gains at the system level.
- A novel approach to explore the optimal placement for deploying MTDs across the Cloud operational stack.
- Proposed a quantification method to determine the effectiveness in disrupting single- and multi-stage attacks.

### MTD Framework



Multi layer MTD framework

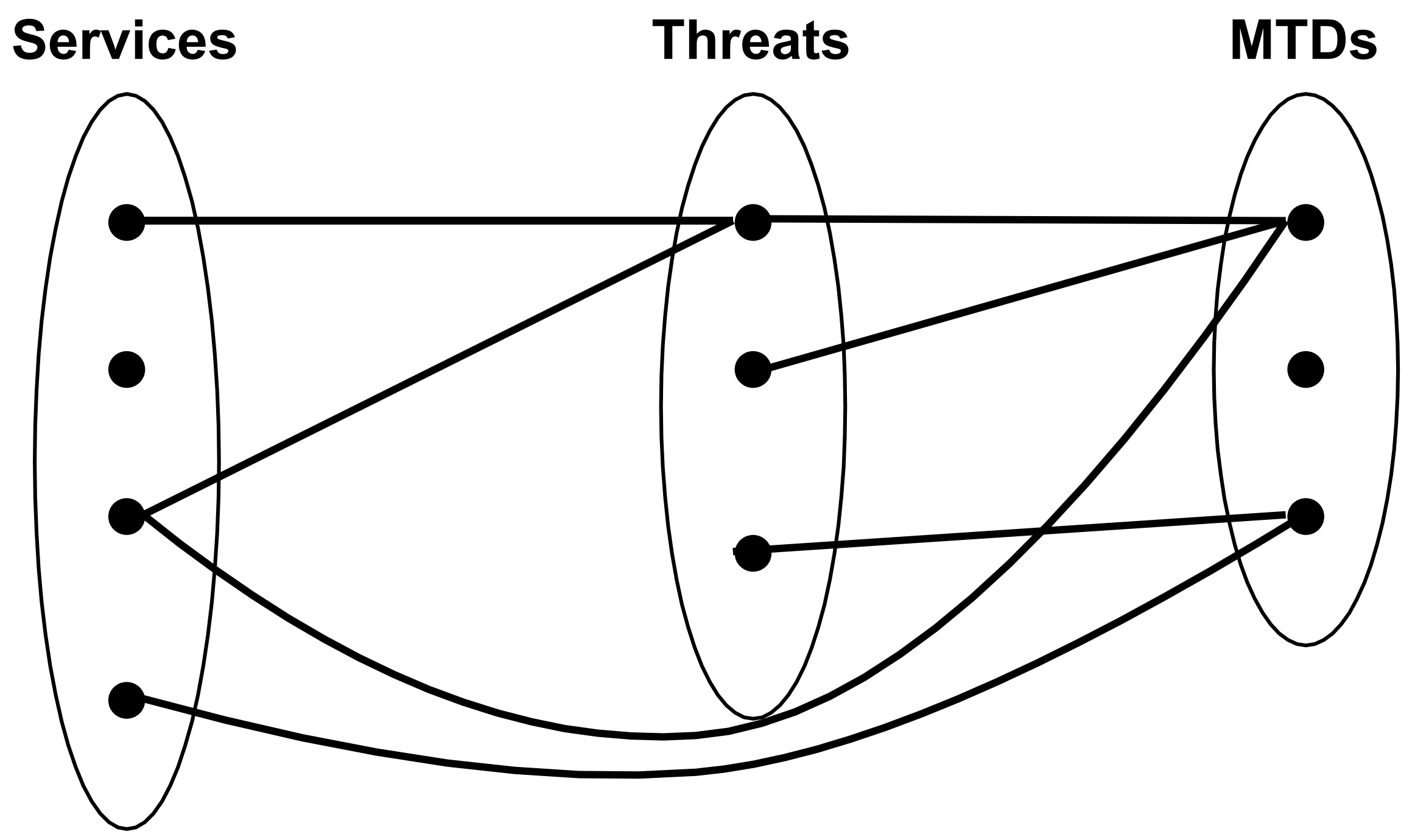
## Multi-layer Framework

**Cloud Model:** Modelling the interaction and information flow among the services to demonstrate the functional behaviour of the Cloud.
**Threats:** Contains threats that can target services in the Cloud. The threats are taken from the national vulnerability database.
**MTD Techniques:** A list of deployable MTDs techniques, e.g., IP Shuffling, OS diversity, etc.

### Relationship Among Layers

The layers and their relationships can be modelled as a 6 tuple (M, T, S, $R_{mt}$, $R_{ms}$, $R_{ts}$) where

- M is a finite set of MTDs
- T is a finite set of threats.
- S is a finite set of services in the Cloud.
- $R_{mt} \subseteq M \times T$ : Impact of MTDs on threats.
- $R_{ms} \subseteq M \times S$ : Applicability of an MTDs on services.
- $R_{ts} \subseteq T \times S$ : Identifies the threats targeting services.



Relationship among the layers

- A threat can impact a single service or multiple services.
- An MTD can impact a single threat or multiple threats.
- An MTD can be deployed or a single or multiple services.
- Therefore the relationship among the layers is many-to-many and finding the most effective solution can be formulated as an optimization problem.

## The Optimization Problem

- Maximize E($M_m$, $T_t$, $S_s$) ; Effectiveness of MTD against a threat targeting a service.
- Minimize C($M_m$, $S_s$) ; Deployment cost MTD on a service.
- Subject to constraints C1, C2, and C3.

where

- The effectiveness can be defined as:

$E(M_m, T_t, S_s) = (T_t, S_s) \in R_{ts} \wedge (M_m, T_t) \in R_{mt} \wedge (M_m, S_s) \in R_{ms}$

- The cost can be calculated as:

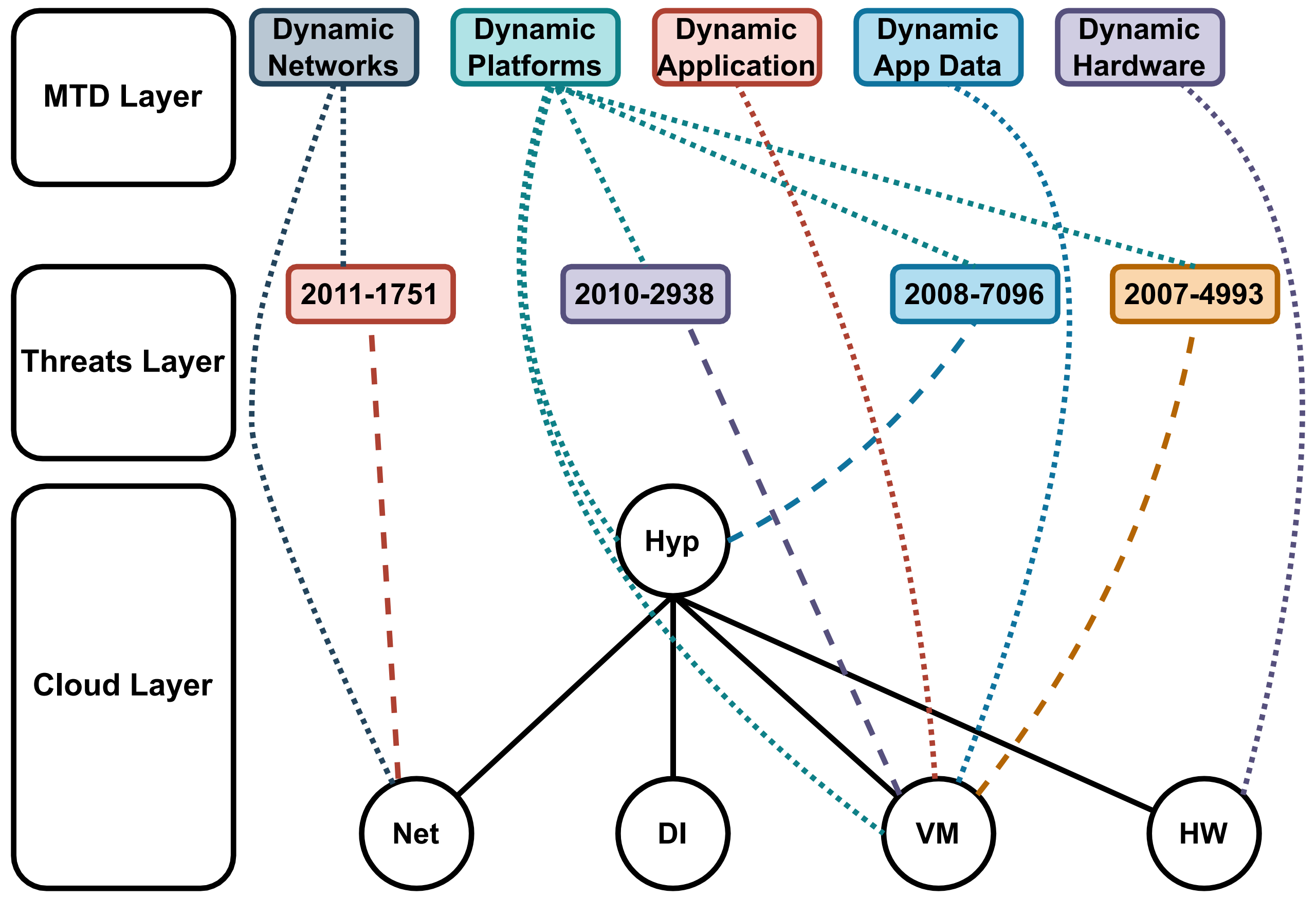
$C(M_m, S_s) = \mathit{Deployment}(M_m, S_s) + \mathit{Overhead}\,(M_m, S_s)$

- The constraints are:

C1 (System's Constraint): Proper termination of the system.
C2 (Attacker's Constraint): A threat with maximum likelihood is used by an attacker at any given time.
C3 (Defender's Constraint): An MTD can only be used if it can target a threat and is deployable on the targeted service.

### Security Analysis

- Solving the optimization problem to identify optimal MTDs placement for single-stage attacks.
- Extending the problem statement to cover multi-stage attacks by using dynamic programming.



Single-stage attack

## Acknowledgments

This work is conducted, in part, under the auspices of the EU Horizon 2020 Research and Innovation program under Grant Agreement No. 830927 (CONCORDIA) and by Security Lancaster under the EPSRC grant EP/V026763/1.