UNIVERSITY OF INSUBRIA – COMO
DEPARTMENT OF THEORETICAL AND APPLIED SCIENCES

Bachelor's Degree in Computer Science

H-SPHERE^3 (Hybrid Semantic Pipeline for Holistic Entropy-based Risk Evaluation in DT ecosystem): Implementation and Synchronization of Hybrid Strategies for the Mitigation of NTP Amplification Attacks and Zero-Day Attacks in Digital Twin Systems

Thesis by:

Davide Facheris

Student ID 752961

Supervisor: Prof. Davide Tosi; Co-Supervisor: Prof. Roberto Pazzi

Academic Year 2024-2025

Contents

Chapter 1

Introduction

Context and Importance: Discussion on the crucial role of Digital Twins in modern connected systems and the unique security challenges they face, emphasizing the need for integrated solutions like H-DIR^2.
Thesis Objectives: Demonstrate how H-SPHERE^3 optimizes Digital Twin security by synergistically combining H-DIR^2 and DIR Hybrid architectures against NTP amplification and Zero-Day attacks.
Thesis Organization: Outline of the thesis structure detailing the integration of Digital Twin security concerns in each chapter.

Title Note H-SPHERE^3 Hybrid Semantic Pipeline for Holistic Entropy-based Risk Evaluation in DT ecosystem evokes an "orbital architecture" that surrounds and protects the Digital Twin like a semantic sphere.

Chapter 2

Digital Twin Security Problems

2.1 DT Security Threats: Analysis of Specific Threats to Digital Twins

Digital Twin technology is particularly sensitive and presents specific security challenges that can significantly impact their functionality and effectiveness. Protecting data confidentiality, integrity, and accessibility is crucial. Security threats can directly or indirectly influence the operational requirements of Digital Twins, raising the question of whether they represent a solution or a challenge for cybersecurity.

2.1.1 Threat Types

Physical Threats: Includes sabotage or spoofing of DT sensors that can disrupt services or system operation. This type of attack is prevalent in sectors such as smart grids, medicine, and transportation.
Privacy Threats: Stem from interception of DT system communications. Private information can be exposed and compromised, particularly in critical sectors like healthcare and smart grids.
Criminal Threats: Attackers can gain remote control of DT systems, disrupting operations and manipulating data and commands. This risk is high in sectors such as smart grids, transportation, and aerospace.
Political and Financial Threats: Cyber warfare between hostile states can lead to attacks on enemy infrastructure DTs, with sabotage of nuclear plants or gas pipelines.

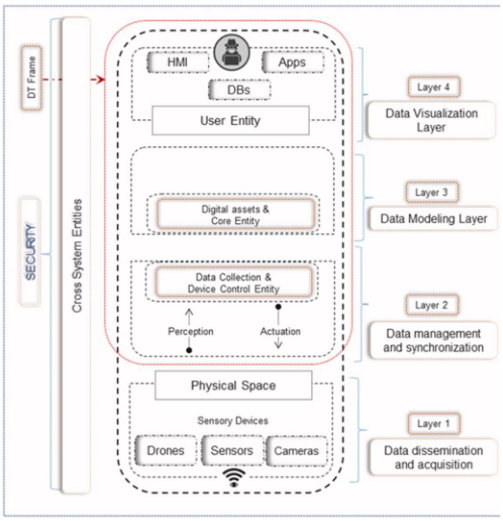
2.1.2 Threats Implications

Threats to Digital Twins can lead to tangible damages, such as injuries to people or the environment, and intangible losses, such as compromised data security. It is essential to understand what or whom DTs need protection from and which vulnerabilities need defense. Understanding threat sources, their motives, and potential targets is fundamental for forming an effective security strategy. Therefore, Digital Twin security requires a complex approach that considers the various threat dimensions and the specific security needs of the application sector. While DTs offer new opportunities, they also present new security challenges that require dedicated and updated solutions to ensure they are both safe and effective in their operation.

[1] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, others, Challenges for securing cyber physical systems. Workshop On Future Directions in Cyber- Physical Systems Security, 2009.

2.2 DT Security Vulnerabilities: Discussion on Digital Twin-Specific Vulnerabilities

This section identifies the main causes of current vulnerabilities in Digital Twins (DT) and analyzes the specific vulnerabilities of each layer, indicating their root causes. For example, vulnerabilities in the first layer might not be present in other DT layers and vice versa. To develop adequate solutions, it is necessary to distinguish between generic and layer-specific vulnerabilities. It is also important to note that different layers can present similar vulnerabilities.
Figure 2.1 illustrates the specific technologies and tools for each Digital Twin layer, providing an overview that facilitates understanding of the overall architecture.
Table 2.2 lists the vulnerabilities discussed in this section, illustrating how recurring vulnerability causes in DTs reflect the complexity and interconnectedness of DT systems. The repetition of certain causes across different layers emphasizes the multifaceted nature of security challenges in these systems, highlighting that although specific vulnerabilities may be unique to certain layers, their root causes often have broader implications, affecting multiple aspects of DT architecture. This understanding is crucial for developing more holistic and effective security strategies, which are layer-specific and address fundamental vulnerabilities common to all layers of the Digital Twin architecture.



Simplified DT Architecture

Table
DT Enabling Technologies and Tools.

Tools	Technologies
Layer 04 – Data Visualization and Access Layer	
· HMI (Visualization Software)	· VR/AR Technologies
· Dashboarding Tools	· Web Portals
· Reporting Tools	· Mobile Apps
Layer 03 - Data Modeling Layer (Modeling, Representation)	
· Agent-Based Simulation	· IronCAD, Anylogic, FlexSim, Simio, Arena
· Discrete System Dynamics	· Enterprise SolidWorks
· Event Simulation	· AutoCAD, Dynamics
· Petri-Nets, CAD	· FreeCAD, AutoMod
Data Analytics	
· AI Models (K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN)	· Artificial Intelligence · Machine Learning · Deep Learning
· TensorFlow, Keras	
Layer 02 – Data Synchronization and Management Layer	
· Databases (e.g., SQL, NoSQL)	· Cloud Services (e.g., AWS, Azure)
· Data Warehouses	· Data Lakes
· ETL Tools	· Middleware
Layer 01 - Data Acquisition and Dissemination Layer	
· Arduino	· Modbus
· Eclipse IoT Project	· MQTT
· NodeRED, Kinoma	· Smart sensors
· Modbus Examiner	· TCP-IP
· IoT Sensors	· OPC-UA
· Smart Meters	· SAGIN Networking (Space-Air-Ground Integrated Network)
· Wearable Devices	

Figure 2.1: DT Technologies and Tools

Table 4
DT Vulnerabilities Summary.

Layers	Vulnerability	Causes
Layer 1. Data Acquisition Layer	1. Power blackouts 2. Equipment physical sabotage 3. Physical unprotected components 4. Jamming and noise 5. Insecure protocols 6. Exposed interconnected field devices. 7. Insecure Access Points (APs) 8. Insecure operating systems and software	1. Heterogeneity, connectivity, and isolation assumption 2. Isolation assumption 3. Isolation assumption 4. Real-time connectivity 5. Realtime connectivity and isolation assumption 6. Realtime connectivity and isolation assumption 7. Realtime connectivity and isolation assumption 8. Realtime connectivity and isolation assumption
Layer 2–3. Data Synchronization and Modeling Layers	1. Wired and wireless communications 2. Insecure communication protocols 3. Web-based attacks 4. Open communication protocols 5. Insecure secondary access points (APs) 6. Insecure operating systems and software	1. Real-time connectivity 2. Realtime connectivity and isolation assumption 3. Realtime connectivity and isolation assumption 4. Openness, real-time connectivity, and isolation assumption 5. Realtime connectivity and isolation assumption 6. Heterogeneity, connectivity, and isolation assumption
Layer 4 Data Visualization Layer	1. Web-based attacks 2. Software attacks 3. Rogues' human-machine interfaces 4. Visualization tempering 5. Media players exploitations 6. Communication software flaws 7. Replay attacks. 8. Location traceability, e.g., Transport DTs 9. Insecure software	1. Heterogeneity and connectivity 2. Heterogeneity and connectivity 3. Isolation assumption and heterogeneity 4. Realtime connectivity and heterogeneity 5. Heterogeneity 6. Real-time connectivity 7. Realtime connectivity and isolation assumption 8. Heterogeneity 9. Heterogeneity, connectivity, and isolation assumption

Figure 2.2: DT Vulnerabilities Schema

2.2.1 Causes of Vulnerabilities in Digital Twins

Increased Connectivity (Real-Time Connectivity): Digital Twins and their physical counterparts maintain continuous real-time communication, introducing new vulnerabilities. For example, a smart city Digital Twin connected to various sensors can be manipulated by attackers if not properly protected, leading to real-world consequences. Real-time connectivity exposes DTs to new attack surfaces, such as the internet or other networks not originally anticipated, increasing the risk of unauthorized access and data manipulation.
Assumption of DT Isolation: It is often assumed that Digital Twins operate in isolation from other systems, which can create significant vulnerabilities. For instance, a manufacturing plant DT supposedly independent from other systems, such as ERP, can compromise the entire production process if breached. This assumption of isolation can also generate a false sense of security, as organizations may consider their DTs secure even if not directly connected to the Internet or other systems. Attackers, however, can access DTs through various means such as physical access, social engineering, or compromised third-party systems.
Heterogeneity: Digital Twins often incorporate a variety of technologies and components, each with different software and hardware, which can introduce new vulnerabilities. For example, a smart building DT may include various sensors, HVAC systems, and security cameras, making uniform protection of all components complex. This heterogeneity requires a holistic approach to DT security, assessing all aspects of the system, from protecting individual components to the entire network architecture. Implementing rigorous access controls, conducting regular security assessments, and ensuring all components are properly updated and protected are essential steps to mitigate these vulnerabilities.

[2] T.Y. Melesse, V. Di Pasquale, S. Riemma, Digital Twin Models in Industrial Operations: a Systematic Literature Review, Procedia Manuf. 42 (2020) 267–272, https://doi.org/10.1016/j.promfg.2020.02.084.

2.3 Existing Security Challenges Solved by DT: Exploration of Existing Security Challenges that Digital Twins Can Mitigate

2.3.1 Existing Security Challenges Addressed by DTs

Digital Twins, and particularly cyber digital twins (CDT), play a crucial role in protecting physical systems from cyber attacks thanks to their modeling, prediction, and physical asset visibility enhancement capabilities. They enable security analyses and monitoring that would be impractical physically without causing interruptions.
Patch Management Improvement: Patch management in Operational Technology (OT) systems presents significant challenges related to inventory management and regular maintenance. DTs offer strategic solutions to these problems, allowing simulation of software updates and testing of effects without direct impacts on operational infrastructure.
Security Testing and Validation: CDTs facilitate threat detection and response

to cyber threats, enabling organizations to analyze vulnerabilities and potential attack vectors before they manifest. This use of DTs allows more effective system and security testing, increasing stakeholder confidence and improving continuous security validation.
Risk Management: DTs provide a virtual representation that can simulate and analyze system behaviour in various scenarios, helping organizations identify and mitigate risks before they become real-world problems. This process enhances overall system resilience and enables more proactive risk management.
Active Cyber Defense: CDTs can enhance incident preparedness by simulating attacks in controlled scenarios to develop skills and improve response strategies. These simulation environments help prevent attacks by providing advanced training and testing reactivity facing potential threats.
Virtual Commissioning: Using DTs in virtual commissioning improves industrial process efficiency, reducing commissioning time and costs. This enables failure prediction, maintenance planning, and system performance testing before actual implementation, reducing the need for costly interventions and improving final product quality.
Autonomy and Predictive Analysis: DT autonomy enables rapid response to changes and anomalies without human intervention, supporting predictive analytics based on real-time data and simulations. This aspect of DTs improves overall system performance, reducing downtime and maintenance costs, and allows more agile adaptation to new conditions or emerging threats.

[3] Z. Liu, A. Li, Z. Sun, G. Shi, X. Meng, Digital Twin-Based Risk Control during Prefabricated Building Hoisting Operations, Sensors 22 (2022), https://doi.org/10.3390/s22072522.
[4] L. Hou, S. Wu, G.(Kevin) Zhang, Y. Tan, X. Wang, Literature Review of Digital Twins Applications in Construction Workforce Safety, Appl. Sci. 11 (2021), https://doi.org/10.3390/app11010339.

2.4 DT Challenges: Technical, Operational, and Security Challenges in DT Implementation and Management

This section explores the technical, operational, and security challenges related to Digital Twin (DT) implementation and management, also addressing general issues, limitations, potential disadvantages, and research opportunities to improve DT performance and security. It concludes by providing indications for future research directions and potential solutions to overcome these obstacles.

2.4.1 Security Challenges for DTs

DTs store and share critical data, heavily relying on digital resources such as algorithms, models, and networks, which can become targets for cyber attacks. It is essential to understand all security challenges that DTs face and implement appropriate defense measures, ensuring adherence to cybersecurity best practices. Commercial pressures can sometimes accelerate product launches, compromising security procedures for quick gains.

Confidentiality: Ensuring authorized data access is essential for maintaining personal and corporate information confidentiality. DTs can facilitate competitors learning trade secrets if not properly protected. An attacker could exploit vulnerabilities to obtain confidential information by manipulating security settings of DT components.
Integrity: Preventing unauthorized data modifications or damage is crucial for DT security. Secure communications between the DT and its physical counterpart are necessary but difficult to achieve in real time. Any malicious alteration in the DT can reflect in the physical system, compromising its integrity.
Availability: Ensuring timely and reliable data access is vital for maintaining DT system functionality and efficiency. Interruptions can cause operational delays, data loss, and other critical impacts on functionality and organizational reputation.
Cybersecurity: The CDT, although useful in simulating attacks to assess vulnerabilities, presents risks if compromised. Attackers can exploit CDT access to test and refine their attacks, increasing the risk of success in the real system.
Intellectual Property: DTs can facilitate intellectual property theft or loss, as input data can be easily replicated and exploited. Interoperability challenges and API standardization can further expose to security risks and legal violations.
While DTs offer significant advantages, their implementations require robust security strategies to mitigate associated risks and ensure effective protection of data and systems they manage.

[5] S. Suhail, R. Jurdak, S. Member, Towards Trusted and Intelligent Cyber-Physical Systems: A Security-By-Design Approach, 2021. `https://arxiv.org/abs/2105.08886v3`.
[6] S. Suhail, R. Jurdak, R. Hussain, D. Svetinovic, Security Attacks and Solutions for Digital Twins, 2022.

2.5 DT Security Challenges Countermeasures

This thesis analyzes established security frameworks for Digital Twins to establish a foundational understanding of the defense mechanisms required in critical sectors such as healthcare, manufacturing, and aerospace. By building upon and synthesizing these existing approaches, including taxonomies of threats and documented countermeasures, the analysis identifies a crucial gap: the need for a holistic, adaptive, and semantically aware security architecture. This investigation directly motivates and paves the way for the introduction of H-SPHERE^3(Hybrid Semantic Pipeline for Holistic Entropy-based Risk Evaluation) which is designed to address these limitations by unifying entropy-based detection, neural risk assessment, and semantic reasoning into an integrated defense stack for Digital Twins.

2.6 DT Open Challenges

High Development Costs: Creating a Digital Twin requires significant reconfiguration of software platforms, production machine hardware, and physical/cloud interfaces, involving considerable expenses. This can limit DT development to large corporations with sufficient financial and human resources. However, the growing availability of experimental and open-source DTs offers opportunities for small businesses

and researchers, facilitating innovation and collaboration through common open-source cloud-based platforms.

Real-Time Interaction Challenges: DTs require high-speed Internet connections for effective bidirectional real-time communication, essential for their optimal functioning. However, the dynamic nature of networks and variability of wireless connections can compromise data transmission, affecting service quality and overall DT functionality.

Complexity and Technical Limitations: As DTs become more complex, difficulties in protecting them from attacks and violations increase. Implementation differences and technical limitations can negatively impact, especially when DTs are connected to humans or other physical objects, presenting unique challenges related to their interoperability and security of transferred data.

Lack of Standardization in Government Policies and Regulations: The absence of standardization in government policies and regulations can make ensuring DT security more difficult. The government needs to establish clear guidelines for DT model validation and approval, especially for those concerning critical sectors like medicine, biology, and aerospace.

HCI and Design Problems: It is essential that DTs are designed so that even non-computer experts can interact with them effectively. A well-designed interface is crucial to enable effective use of DTs by professionals from different disciplines.

Internal Threats: The highly collaborative nature of DTs makes them vulnerable to internal threats, such as data theft or abuse by employees or collaborators with legitimate access. It is essential to implement rigorous access controls and monitoring systems to mitigate these risks and ensure DT security.

[7] E.A. Patterson, M.P. Whelan, A framework to establish credibility of computational models in biology, Prog. Biophys. Mol. Biol. 129 (2017) 13–19, https://doi.org/10.1016/j.pbiomolbio.2016.08.007.

[8] E. Karaarslan, M. Babiker, Digital Twin Security Threats and Countermeasures: an Introduction, in: 2021 International Conference on Information Security and Cryptology (ISCTURKEY), 2021, pp. 7–11, https://doi.org/10.1109/ISCTURKEY53027.2021.9654360.

[13] S. R. Jeremiah, A. El Azzaoui, N. N. Xiong, and J. H. Park, "A comprehensive survey of Digital Twins applications, technologies," Journal of Systems Architecture, vol. 151, p. 103120, 2024.

Conclusions

The analysis conducted in this chapter highlights how Digital Twins represent unique terrain for cybersecurity challenges. Their hybrid nature, combining cyber and physical components, creates specific vulnerabilities that require innovative defensive approaches. Traditional security solutions prove inadequate for protecting such dynamic and interconnected environments, where cyber threats can directly translate into physical consequences. This awareness motivates the introduction of specialized frameworks like H-SPHERE^3, designed to address Digital Twin security with an integrated and intelligent architecture.

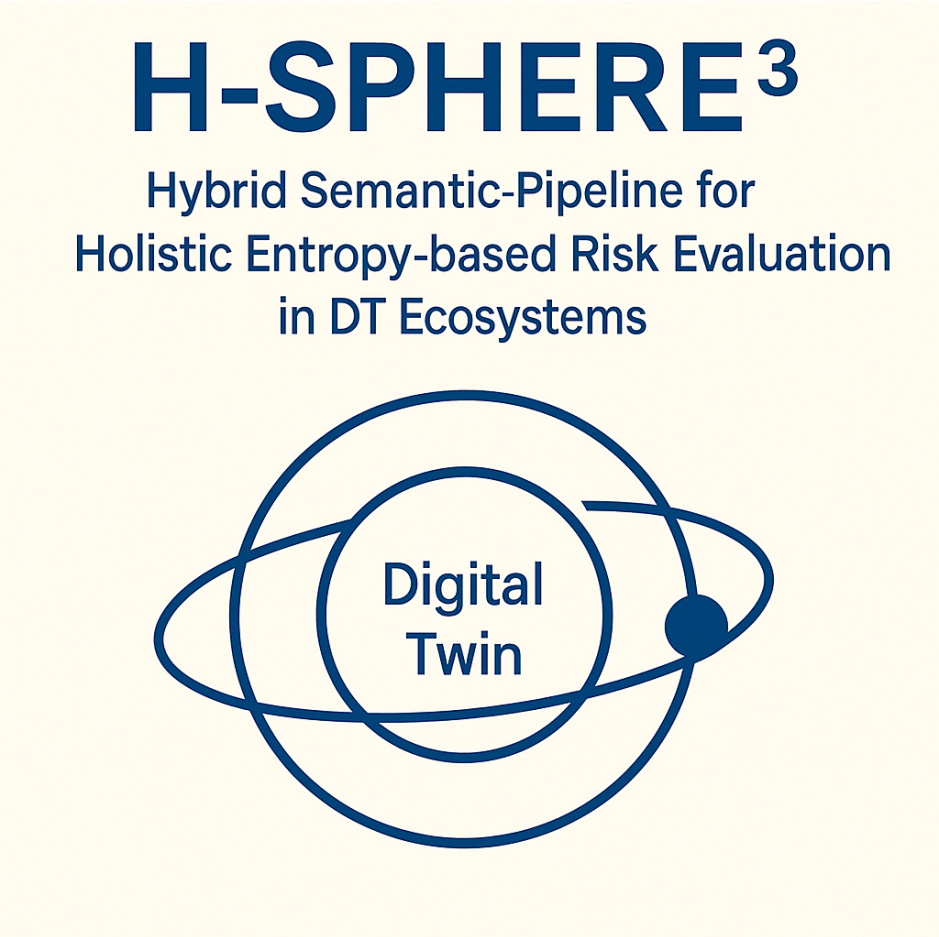


Figure 2.3: H-SPHERE³

Chapter 3

Theoretical Foundations and Hybrid Architectures for Information Retrieval

3.1 Hybrid Architectures and Digital Twins

Hybrid architectures represent a strategic approach for managing data complexity in Digital Twin (DT) systems. These architectures combine sub-symbolic approaches (machine learning) with symbolic methods (semantic rules and descriptive logic). This synergy enables the unification of the predictive power of adaptive models with the transparency and queryability of semantic models. The objective is to enable systems capable of:

- processing heterogeneous data from multiple sensor sources;
- enabling hybrid queries on structured and unstructured data;
- ensuring semantic interoperability between different platforms.

3.2 H-DIR (Hybrid Distributed Information Retrieval)

The H-DIR (Hybrid Distributed Information Retrieval) framework was specifically designed to address the challenges of information retrieval in Cloud-IoT contexts dominated by heterogeneous sensor data. Its strength lies in the fusion of three fundamental pillars:

- **Distributed Big Data Processing**: Using Apache Spark, H-DIR is capable of processing enormous volumes of data in near real-time, a fundamental capability for managing multi-source data streams in complex IoT environments.
- **Semantic Reasoning**: The integration of Apache Jena and the SPARQL query engine allows enriching data with context and meaning. This enables complex queries that correlate seemingly unrelated information through domain ontologies.

- **Hybrid Interoperability**: The translation layer that converts SPARQL to Spark SQL is the enabling element of hybridization. It allows querying both structured data (e.g., system logs in a relational database) and semantically enriched data (RDF descriptions of assets) simultaneously, overcoming the limitation of data silos.

The five-layer architecture of H-DIR, from peripheral monitoring (Layer 1) to semantic integration and reasoning (Layer 5), provides a clear path for transforming raw data into actionable knowledge.

3.3 H-DIR: Layered Structure and Technologies

The H-DIR architecture is organized into five logical layers, each with a specific function in the process of transforming data from raw signals to semantically enriched knowledge.

Layer 1: Monitoring System

This layer constitutes the physical-cyber boundary of the system. It relies on microcontrollers like NodeMCU ESP8266/ESP32 integrated with sensors and cameras for real-time monitoring. Its main function is the collection of raw data (e.g., temperature, humidity, device status) and basic pre-processing at the source.

Layer 2: RDF Mapping

In this layer, heterogeneous data from Layer 1 is converted into a standardized and interoperable format. Using ontologies such as Semantic Sensor Network (SSN) or IoT-Lite and the RDF format, sensor data is mapped into subject-predicate-object triples. This transformation is crucial for preparing data for semantic reasoning.

Layer 3: Ontology Reasoning

The semantic core of the system. This layer uses Description Logic (DL), OWL, and SWRL to formally represent domain knowledge and infer new information. By integrating specific domain ontologies (e.g., OntoSensor, SensorML) with the RDF-mapped data, this layer enables advanced semantic queries and contextual reasoning.

Layer 4: Apache Spark Integration

This layer handles the computational power needed to manage big data. Apache Spark is used for high-performance distributed processing of both structured and semantic data. Integration with Spark allows accessing and querying relational databases as if they were RDF graphs.

Layer 5: Apache Jena Bridge

The orchestration layer that realizes hybridization. Apache Jena is used to manage the RDF knowledge graph. The key innovation here is the translation layer that converts SPARQL (semantic) queries into Spark SQL (relational) queries and vice versa. This

enables hybrid queries that combine Spark's analytical power with SPARQL's semantic richness.

3.4 Validation in Agritech: Smart Greenhouse Case Study

The H-DIR framework was experimentally validated in a precision agriculture context through the monitoring of smart greenhouses. The implementation involved monitoring Blueberry Ash plants (Fraxinus Quadrangulata) in a controlled environment.

3.4.1 Experimental Setup

The architecture was deployed in three greenhouses equipped with:

- 10 IoT sensors for environmental monitoring;
- 3 camera units for visual acquisition;
- Distributed system for managing heterogeneous data streams.

3.4.2 H-DIR Layers Implementation

Layer 1: Data Acquisition

The monitoring system integrated environmental sensors for collecting critical parameters including temperature, relative humidity, light intensity, and plant height measurements through computerized imaging.

Layer 2: Semantic Mapping

Raw sensor data was transformed into RDF triples using specialized ontologies. A specific ontology was developed for the agronomic domain including entities such as greenhouses, sensors, plants, and measurements.

Layer 3: Reasoning and Analysis

An inference system was implemented combining LSTM/GRU models for time series analysis and Natural Language Processing techniques for processing agronomic documents. Preprocessing included tokenization, stop words removal, and word embeddings generation using Word2Vec.

Layer 4: Distributed Processing

Apache Spark was employed for distributed processing of data streams. Integration with SPARQL enabled hybrid queries on structured and semantic data.

Layer 5: Semantic Integration

Apache Jena enabled the execution of SPARQL queries for contextual data interrogation. Example of implemented query:

```
PREFIX ash: <http://example.org/raspberryash#>
PREFIX sd: <http://www.w3.org/2001/XMLSchema#>
SELECT ?plant ?leafWidth ?leafHeight ?waterQualityMetric
WHERE {
    ?plant rdf:type ash:BlueberryAsh.
    ?plant ash:hasLeafMeasurement ?leafMeasurement.
    ?leafMeasurement ash:width ?leafWidth.
    ?leafMeasurement ash:height ?leafHeight.
    ?plant ash:hasWaterQuality ?waterQuality.
    ?waterQuality ash:metric ?waterQualityMetric.
} ORDER BY ?plant
```

3.4.3 Integration with External Data

The system was correlated with external datasets available through the portal `https://data.nsw.gov.au/`, enabling contextual enrichment of collected information.

3.4.4 Observed Results

The implementation demonstrated the H-DIR framework's capability to manage heterogeneous data streams in complex agricultural environments. Semantic integration enabled:

- Unified querying of sensory data and agronomic documentation;
- Advanced correlation between environmental parameters and crop status;
- Contextual reasoning based on domain ontologies.

The validation in agritech confirms the adaptability of the H-DIR architecture to specific application domains, demonstrating its effectiveness in managing complex and interconnected data typical of Digital Twin environments.

Conclusions

In conclusion, the H-DIR architecture provides not only a framework for information retrieval, but also a complete ecosystem for hybrid data analysis. Its layered structure, progressing from physical to logical and from raw data to knowledge, constitutes the solid and proven foundation upon which it was possible to build the evolution towards HDIR^2.

[9] D. Tosi, R. Pazzi, H-DIR Design and Experimentation of a Distributed Information Retrieval-Hybrid Architecture in Cloud IoT Data Centers, IFIP International Internet of Things Conference, 2024.

Chapter 4

H-DIR^2 - Architecture and Implementation in Digital Twins

4.1 Architecture of the H-DIR^2 Framework

H-DIR^2(Hybrid–Dynamic Information Risk) combines the principles of distributed information retrieval with a defense cycle based on entropy, neural networks, and semantic reasoning. H-DIR^2 was designed to counter complex attacks such as NTP Amplification, DAO-DIO, SYN Flood through a pipeline that combines:

- semantic data representation (RDF + SPARQL);
- entropy analysis;
- machine learning with adaptive neural networks (ARNN);
- automated mitigation strategies;
- adaptability and explainability of decisions.

4.2 Operational Pipeline of H-DIR^2 (O1–O6)

The H-DIR^2 framework processes network traffic through six sequential operators that transform raw packets into actionable security intelligence. Each operator has a specific, deterministic function ensuring reproducible and explainable threat detection.

O1 – RDF Serialization

Converts raw network packets into semantic RDF triples using W3C standards. Each packet becomes a set of subject-predicate-object statements describing source/destination IPs, protocols, ports, and timestamps. This enables formal reasoning and semantic querying.

O2 – Spark SQL Windowing

Applies 500ms sliding windows to the telemetry stream using Apache Spark SQL. This stage performs real-time aggregation and filtering of multi-terabyte data flows, enabling statistical analysis with sub-second latency.

O3 – Feature Vectorization

Transforms structured network data into numerical feature vectors using one-hot encoding. Critical attributes like TCP flags, port numbers, and packet sizes are converted into a format suitable for neural network processing.

O4 – ARNN Risk Scoring

The Adaptive Random Neural Network evaluates each packet and assigns a risk score $R_i \in [0, 1]$. The model dynamically updates its understanding of network behaviour, learning normal patterns and identifying anomalies through a composite loss function that balances classification accuracy and topological consistency.

O5 – Semantic Graph Injection

Converts neural risk scores back into semantic knowledge by injecting RDF triples into the graph. For example, high-risk packets are marked with properties like `:hasRiskScore "0.87"` and `:underMitigation true`, enabling policy-driven security enforcement.

O6 – Dynamic Update Loop

Closes the observation-prediction-action cycle by continuously updating the system state. This structure allows querying the DT knowledge base with SPARQL to extract suspicious packets and generate real-time reports.

4.3 Core Technologies of the H-DIR² Framework

The H-DIR² architecture is based on a hybrid technology stack that integrates distributed processing, semantic reasoning, and machine learning, as outlined in the original paper.

Apache Spark and Spark SQL

Core of distributed processing. Apache Spark provides the processing engine for micro-batch analytics on multi-terabyte data streams. Spark SQL enables large-scale relational queries, with sliding time windows (Δtt = 500 ms) for near real-time analysis. The management of RDDs (Resilient Distributed Datasets) guarantees fault-tolerance for iterative workloads.

Apache Jena and Fuseki

Management of the RDF knowledge graph. Apache Jena provides the framework for manipulating RDF graphs, while Fuseki operates as a SPARQL server for semantic queries and updates. This layer enables the serialization of network packets into RDF triples and the execution of reasoning based on domain ontologies.

Adaptive Random Neural Network (ARNN)

Machine learning model for attack graphs. The ARNN implements the dynamic update of weights in the network attack graph, combining classification loss (L_{cls}) and graph loss (L_{graph}) for real-time risk estimation. Training minimizes the composite function $L_{total} = \alpha L_{classification} + \beta L_{graph}$.

SPARQL 1.1

Semantic query language. SPARQL 1.1 enables complex pattern matching on the knowledge graph, supporting the contextual enrichment of alerts and the definition of security rules based on ontologies (e.g., isolation of high-risk flows).

This technological combination enables the fundamental properties of H-DIR²: vertical scalability (millions of endpoints) and horizontal scalability (multi-terabyte), while maintaining semantic explainability through the RDF/SPARQL layer.

4.4 Mitigation Strategy

The H-DIR² framework implements differentiated mitigation strategies per attack type, with dynamic thresholds based on neural evaluation and semantic context.

4.4.1 Protocol-Specific Intervention Thresholds

The mitigation activation thresholds are specific to each attack class:

- **NTP Amplification**: $R_i > 0.55$ for mitigation activation;
- **DAO–DIO**: $R_i > 0.6$ for identification of compromised nodes;
- **SYN Flood**: $\Delta H_{flags} > \theta_H$ for entropy detection.

4.4.2 Specific Countermeasures

For flows classified as high risk, the system applies protocol-specific countermeasures:

TCP/SYN Flood

Adaptive Rate Limiter based on entropy analysis of TCP flags (ΔH_{flags}), with SYN cookie mechanisms to prevent resource exhaustion.

RPL/DAO–DIO

Route Sanitiser that recalculates and purifies RPL routing tables based on entropy analysis of paths (ΔH_{path}), with dynamic reconfiguration of the DAG topology.

UDP/NTP Amplification

Amplification Throttler that applies filters based on entropy of packet sizes (ΔH_{size}), combined with edge caching and anycast load distribution.

4.4.3 Semantic Orchestration

Mitigation decisions are guided by SPARQL queries that correlate multiple evidence sources in the RDF graph. The risk scores generated by the ARNN are reified as semantic triples (e.g., `:host_A :hasRiskScore "0.87"`), enabling contextual querying and isolation of suspicious flows. This integration between neural evaluation and semantic reasoning guarantees a timely and contextually informed mitigation response, while maintaining full traceability and explainability of decisions through the RDF/SPARQL layer.

Conclusions

This chapter presented the practical implementation of H-DIR², from RDF serialization to SPARQL mitigation queries. The O1–O6 pipeline, integrated with distributed technologies, demonstrates the feasibility of a hybrid approach combining adaptive machine learning and semantic reasoning. These formal properties and mitigation mechanisms form the basis for extending H-DIR² to H-SPHERE³, discussed in the next chapters.

[10] D. Tosi, R. Pazzi, *H-DIR2: A Scalable Entropy-Based Framework for Anomaly Detection and Cybersecurity in Cloud-IoT Data Centers*, Technical Report, University of Insubria, 2024.

Chapter 5

The Challenge of Zero-Day and NTP Amplification Attacks in Digital Twin Systems

5.1 NTP Amplification Attacks in Digital Twin Systems

NTP (Network Time Protocol) amplification attacks represent a significant threat to Digital Twin systems, especially those connected to public internet networks or dependent on external time synchronization services. This type of attack exploits the intrinsic characteristics of the NTP protocol to generate high-volume DDoS (Distributed Denial of Service) traffic, potentially compromising the availability of DT services.

5.1.1 Impact on Digital Twins

In Digital Twin contexts, NTP amplification attacks present specific risks:

Synchronization Disruption: DTs require precise temporal synchronization between digital twin and physical entity. An attack can:

- Compromise critical temporal alignment for monitoring;
- Cause discrepancies in sensor data timestamps;
- Slow down or interrupt digital twin update cycles.

Network Resource Consumption: Amplified traffic saturates available bandwidth:

- Impacts real-time communications between DT and sensors/actuators;
- Increases latency in critical cyber-physical operations;
- Can mask other more sophisticated attacks.

Characteristic Entropy Anomalies: These attacks produce identifiable signatures:

- Peaks in packet size entropy (ΔH_{size});
- Abnormal concentration of traffic on UDP port 123;
- Asymmetric request/response patterns in network traffic.

5.1.2 Considerations on DT Resilience

Protection against NTP amplification attacks is particularly critical for Digital Twins due to their cyber-physical dual nature. A prolonged interruption can indeed:

- Compromise simulation data integrity;
- Cause desynchronization between digital twin and physical entity;
- Lead to operational decisions based on inconsistent temporal data.

The hybrid approach of H-SPHERE^3 ensures not only timely detection, but also the ability to maintain limited operability even during ongoing attacks, through graceful degradation mechanisms and semantic failover.

5.2 Introduction to the Zero-Day Concept

Cybersecurity is a continuous race between defenders and attackers. In this context, zero-day attacks represent the most elusive and potentially most damaging threat. By definition, a zero-day is an unknown software vulnerability or an attack vector for which there is no patch.
However, this traditional definition, while correct, is insufficient to describe the operational reality of such attacks in complex and dynamic environments like Digital Twins (DT). DTs, with their intrinsic interconnection between cyber and physical worlds, multiply the attack surface and potential consequences of an unknown exploit. Therefore, it's necessary to adopt a more operational and functional definition that guides the design of adequate defense mechanisms.
This section analyzes the zero-day threat through two complementary perspectives, represented by the CIL-NIDS (Class Incremental Learning) and H-DIR^2 (Hybrid–Dynamic Information Risk) approaches, then synthesizes them into a holistic vision suitable for the Digital Twin ecosystem.

5.2.1 The CIL-NIDS Perspective: Incremental Learning of New Classes

The CIL-NIDS (Class Incremental Learning for Network Intrusion Detection) approach addresses the zero-day problem by formalizing it as an incremental machine learning problem.

CIL-NIDS Operational Definition

A zero-day attack is an unknown attack class at the time of initial training of a Network Intrusion Detection System (NIDS). It manifests as anomalous behaviour in network traffic that:

- Does not fit into any known class (C^{old});
- Is not labeled in the base training dataset;
- Is incrementally inserted into the operational flow (C^{new}), often with a very limited number of observable examples (few-shot condition).

Main Challenges for CIL-NIDS

- **Catastrophic Forgetting:** The model must learn the new class (C^{new}) without forgetting or degrading its performance in recognizing already known classes (C^{old}).
- **Limited Memory:** Detection must often occur with very few examples available (e.g., 5-25 network flows), requiring efficient learning techniques.
- **Critical Explainability:** It's essential not only to detect the anomaly, but also to explain why it was classified as a new class, distinguishing it from noise or legitimate traffic variations. Techniques like SHAP (SHapley Additive exPlanations) or Integrated Gradients (IG) are essential for this purpose.
- **Feature Sensitivity:** Detection success depends on the choice of informative network features, such as Inter-Arrival Time (IAT), flow direction (DIR), payload length (PL), and TCP window size (WIN).

This approach is powerful but depends on a supervised or semi-supervised labeling and update mechanism, which can introduce delays and operational complexity.

5.2.2 The H-DIR² Perspective: Hybrid Detection

The H-DIR² framework adopts a fundamentally different philosophy, hybridizing sub-symbolic (neural networks) and symbolic (semantic reasoning) methods.

H-DIR² Operational Definition

A zero-day attack is a previously unobserved network event that causes a significant statistical deviation in the system's entropy distribution. This deviation, measured by the entropy variation (ΔH) calculated on dynamic time windows, exceeds an adaptive threshold (θ_H) established during a baseline phase, triggering an autonomous cycle of neural interpretation and mitigation response.

Pillars of the H-DIR² Approach

- **Dual Risk Assessment:**
  1. **Entropy Layer (O2):** Calculates entropy variation (ΔH). A sudden and sustained peak is a strong indicator of an anomalous event, potentially a zero-day, as it alters the "normal" traffic distribution.
  2. **Neural Layer (O4):** The Adaptive Risk Neural Network (ARNN) evaluates the packet. Having learned the representation of normal traffic, it assigns a high-risk score to packets that appear "out-of-distribution", such as those from an unknown attack.
- **Closed Adaptive Cycle:** Observation leads to a decision (risk score) that translates into an action (mitigation) and an update of the knowledge graph (O5, O6), all without initial human intervention.

In summary, while CIL-NIDS seeks to name the new threat, H-DIR² focuses on detecting its anomalous presence and activating an immediate response.

5.2.3 Synthesis: A Holistic Vision for Digital Twin Security

The two perspectives are not antagonistic, but represent complementary phases of a complete defense cycle against zero-days in DT environments.

H-DIR²

The entropy module and ARNN of H-DIR² serve as a high-speed early-warning system. They are the first line of defense, designed to immediately detect and mitigate any significant statistical deviation, before it is even classified. This is crucial for DTs, where response time can have physical implications.

Analysis and Classification (CIL-NIDS)

Once the alarm is triggered and suspicious traffic has been isolated and semantically marked in the RDF graph, a CIL-NIDS type system can come into play. A security analyst or automated process can use the packets labeled as "high-risk" by H-DIR² as a pre-filtered dataset to incrementally train a classifier, thus naming the zero-day and permanently enriching the system's knowledge.

Architectural Synergy

This synergy is key to a resilient security architecture:

- H-DIR² provides the speed and flexibility needed for real-time response.
- A CIL-NIDS module (potential future extension) would provide the precision and long-term evolution of system knowledge.

For the H-DIR² framework presented in this thesis, the reference operational definition is that of H-DIR². The simulation described in Chapter 7 demonstrates precisely this capability: the ΔH peak and the high ARNN score during the attack phase simulate the detection of an unknown event (zero-day), while the SPARQL queries enable the explainability that is the first step toward its subsequent classification. This hybrid, layered vision provides effective protection for Digital Twins against the most elusive threats.

[14] Cerasuolo F., Bovenzi G., Ciuonzo D., Pescape A. (2025). Attack-adaptive network intrusion detection systems for IoT networks through class incremental learning. Computer Networks, 263, 111228.

Chapter 6

H-SPHERE³: Semantic Orbital Architecture

The H-DIR² framework provides the methodological foundations for hybrid cyber-physical threat detection. However, effective protection of Digital Twin environments requires an evolution towards H-SPHERE³ (Hybrid Semantic Pipeline for Holistic Entropy-based Risk Evaluation in DT ecosystem), which extends and specializes the original framework for the specificities of digital twins. Its name intentionally evokes an "orbital architecture" that surrounds and protects the Digital Twin like a dynamic and adaptive semantic sphere. It is not a simple improvement of H-DIR², but an architectural re-conception that transforms the sequential pipeline into an enveloping and stratified system.

6.1 Name Decomposition: A Declaration of Intent

The name H-SPHERE³ is not merely catchy but constitutes a declaration of intent that defines its foundational pillars. Its synergistic power is symbolized by the cube elevation:
H (Hybrid): This element represents the hybrid core of the framework, inherited and enhanced from H-DIR². It defines the synergistic fusion of two intelligence paradigms:

- **Sub-Symbolic Intelligence (Machine Learning)**: Implemented by the Adaptive Risk Neural Network (ARNN), it specializes in recognizing complex patterns and subtle anomalies in raw data, providing the capability to detect zero-day attacks based on statistical deviations from the learned norm.
- **Symbolic Intelligence (Logical Reasoning)**: Implemented by the semantic layer (RDF, SPARQL, OWL), it provides the capability to formally represent knowledge, apply business rules, and, most importantly, explain decisions in a format interpretable by a human operator or other systems.

SPHERE (Semantic Pipeline for Holistic Entropy-based Risk Evaluation): This element describes the method and operational form. It defines a processing pipeline that is:

- **Semantic**: Based on formal knowledge, explainable and queryable;

- **Risk-Oriented**: Whose final output is a holistic risk assessment;
- **Entropy-based**: Whose primary and characterizing trigger mechanism is the analysis of entropy variation (ΔH) on DT flows.

6.2 Transition from H-DIR² to H-SPHERE³: Architectural Evolution for Digital Twins

The transition from H-DIR² to H-SPHERE³ can be visualized as a shift from a linear model to a spherical one:
H-DIR² - Pipeline Model: The O1-O6 operators are arranged in a linear sequence. Data flows from input (O1) to output (O6) mostly unidirectionally. It is an efficient but hierarchical architecture.
H-SPHERE³ - Orbital Model: The same operators are reorganized into concentric layers surrounding the DT. This organization introduces critical emergent properties:

- **Inner Orbit (Hybrid Detection - O2, O4)**: A high-frequency sensor layer that includes the calculation of contextualized entropy (ΔH) and neural evaluation (ARNN). It operates in direct contact with DT data.
- **Median Orbit (Semantic Interpretation - O1, O5)**: A "brain" layer that builds and queries the knowledge representation (RDF Graph). It transforms alerts from lower layers into semantically enriched events.
- **Outer Orbit (Orchestration and Mitigation - O6)**: An "action" layer that translates semantic decisions into operational commands on the DT.

This orbital model supports defense-in-depth: each layer provides a distinct protection, and the failure of one does not cause the collapse of the whole system.

Evolution of Application Scope and Security Focus

While H-DIR^2 primarily operates in Cloud-IoT Data Center environments with a focus on network attacks like SYN Flood, DAO-DIO, and NTP Amplification, H-SPHERE^3 expands the application domain to Digital Twins in distributed and mission-critical environments. This shift requires a reorientation of the security focus towards preventive defense against Zero-Day and reflective attacks specifically targeting digital twin vulnerabilities, where consequences can have direct impacts on the corresponding physical system.

Enhancement of Predictive Engine and Semantic Layer

The predictive engine in H-DIR^2 already relied on ARNN (Adaptive Random Neural Network) for risk scoring. In H-SPHERE^3, this engine is refined and contextualized, enabling adaptive risk prediction directly tailored to Digital Twin environments and their operational flows. Similarly, H-DIR^2 employed RDF/SPARQL with OWL ontologies to provide explainability and rule-based reasoning. In H-SPHERE^3, the semantic layer evolves towards domain-specific OWL ontologies dedicated to Digital Twin entities and interactions, allowing for personalized semantic reasoning aligned with the unique behaviors of digital twins.

Contextualization of Entropic Trigger and Pipeline

Entropy analysis, which in H-DIR^2 identified anomalous variations in network traffic distribution, is reconceptualized in H-SPHERE^3 to monitor Digital Twin-specific flows, including command patterns, sensory data, and simulated events. The processing pipeline evolves from the six deterministic operators of H-DIR^2 towards an extended semantic-adaptive architecture, incorporating orchestration mechanisms and feedback tightly integrated into the operational cycles of Digital Twins.

Advanced Mitigation and Optimized Scalability

Mitigation strategies in H-DIR^2 included general actions such as rate limiting, rerouting, and edge caching. H-SPHERE^3 evolves these into sophisticated runtime coordination between Digital Twins and defensive modules, leveraging real-time semantic-statistical evaluations. Scalability, already validated in H-DIR^2 along vertical (nodes) and horizontal (data) axes, is further optimized in H-SPHERE^3 to handle the high-frequency demands of Digital Twins in domains such as smart grids, healthcare, and automotive systems.

Validation and Performance Metrics

H-DIR^2 provided validation in Cloud-IoT environments with standard detection metrics such as AUC and latency. H-SPHERE^3 extends the reproducibility framework into containerized Digital Twin simulations, contextualizing performance to metrics directly relevant for DTs, including Packet Delivery Ratio, mitigation of operational loops, and pre-failure alerting.

Progressive Implementation and Roadmap

The implementation presented in this thesis constitutes the functional core of H-SPHERE^3, demonstrating the feasibility of the hybrid pipeline in a containerized environment. The path towards full realization involves integration with industrial DT platforms, the development of specialized ontologies, and the design of context-aware mitigation policies. This evolution positions H-SPHERE^3 as a reference framework for holistic Digital Twin security, uniting statistical detection, entropy-based analysis, semantic reasoning, and neural prediction in an explainable and adaptive architecture designed for the cyber-physical challenges of Digital Twin systems.

Chapter 7

Experimental Analysis and Evaluation

This chapter presents the experimental design and performance evaluation of the H-SPHERE³ framework against targeted attacks in the context of Digital Twins, analyzing data to determine the robustness of the solutions.

7.1 Case study 1: NTP Amplification Attack - H-DIR² Validation

The first case study validates the effectiveness of the H-DIR² pipeline in detecting and mitigating NTP (Network Time Protocol) amplification attacks, demonstrating the framework's capabilities in a real-world security scenario before its extension to H-SPHERE³ for Digital Twin environments.

7.1.1 Experimental Configuration

The validation was conducted through a complete implementation of the H-DIR² pipeline on a synthetic network traffic dataset. The experimental configuration includes:

- **Dataset**: 100 simulated traffic records with balanced distribution between normal traffic (label: *normal*) and malicious traffic (label: *anomaly*).
- **NTP attack parameters**: Typical amplification attack configuration (UDP port 123, monlist/readvar/version commands).
- **Operational thresholds**: $\Delta H \geq 1.5$ bits for entropy detection, $R_i > 0.55$ for automatic mitigation activation.
- **Test environment**: O1-O6 pipeline implemented in Python 3.10 with specialized libraries (rdflib, scikit-learn, pandas).

7.1.2 H-DIR² Pipeline Implementation

The experiment faithfully followed the six-stage architecture of the H-DIR² pipeline:

O1 – RDF Serialization

Each record was transformed into RDF triples according to the specially developed NTP ontology. Example serialization:

```
ex:Packet12 a ntp:Packet ;
    ntp:hasBandwidth "258000"^^xsd:integer ;
    ntp:hasLabel "normal"^^xsd:string .
```

O2 – Entropy Evaluation

The calculation of entropy on moving windows of 10 records analyzed the distribution of traffic labels. Entropy variations (ΔH) identified statistical anomalies in traffic patterns.

O3 – Feature Vectorization

Critical network features (IP addresses, UDP ports, NTP commands) were simulated and encoded using one-hot encoding, generating numerical vectors for subsequent processing.

O4 – ARNN Risk Scoring

The simulation of the Adaptive Risk Neural Network generated risk scores $R_i \in [0.2, 0.95]$ for each record using a temporal window of 5 records for contextual risk assessment.

O5 – Semantic Graph Injection

The risk scores generated by the ARNN were injected into the RDF graph as semantic triples, enabling automatic reasoning and contextual querying through properties such as `ntp:hasRiskScore` and `ntp:underMitigation`.

O6 – Dynamic Update Loop

The dynamic update cycle was implemented through SPARQL queries that extract and prioritize at-risk records based on risk scores and mitigation states:

```
SELECT ?packet ?riskScore WHERE {
    ?packet ntp:hasRiskScore ?riskScore ;
            ntp:underMitigation "true"^^xsd:boolean .
} ORDER BY DESC(?riskScore)
```

7.1.3 Experimental Results

SPARQL Mitigation Output

The execution of the mitigation query produced the following significant results:

```
Packets under mitigation (R_i > 0.55):
http://example.org/example#Packet12 -> Risk Score: 0.9461
http://example.org/example#Packet86 -> Risk Score: 0.9197
```

```
http://example.org/example#Packet58 -> Risk Score: 0.9180
http://example.org/example#Packet65 -> Risk Score: 0.9087
http://example.org/example#Packet31 -> Risk Score: 0.9047
http://example.org/example#Packet35 -> Risk Score: 0.9023
http://example.org/example#Packet30 -> Risk Score: 0.8934
http://example.org/example#Packet88 -> Risk Score: 0.8831
http://example.org/example#Packet36 -> Risk Score: 0.8686
http://example.org/example#Packet37 -> Risk Score: 0.8642
[...]
http://example.org/example#Packet100 -> Risk Score: 0.5703
http://example.org/example#Packet99 -> Risk Score: 0.5684
```

Quantitative Performance Analysis

The numerical results demonstrate the operation of the H-DIR² pipeline:

Table 7.1: Experimental results of the H-DIR² pipeline

Metric	**Value**	**Interpretation**
Total records analyzed	100	Complete dataset
Records under mitigation ($R_i > 0.55$)	61	61% identified for mitigation
High-risk records ($R_i > 0.75$)	16	16% with high risk
Critical records ($R_i > 0.90$)	6	6% with critical risk
Risk score range	0.5684 - 0.9461	Actual distribution
Applied entropy threshold	$\Delta H \geq 1.5$ bits	H-DIR² paper configuration

Pattern Analysis

The analysis of results revealed significant correlations:

- Bimodal distribution of risk scores reflecting the separation between normal and anomalous traffic;
- Effective application of operational thresholds defined in the H-DIR² framework;
- Functional integration between semantic components and risk analysis.

7.1.4 Results Discussion

The experimental results confirm the effectiveness of the H-DIR² architecture in the simulated context, They demonstrate a complete operational pipeline for detecting and mitigating NTP amplification attacks.

Detection Effectiveness: The pipeline identified 61 out of 100 records (61%) as candidates for mitigation, successfully applying the operational thresholds defined in the framework. The distribution of risk scores from 0.5684 to 0.9461 shows a clear separation between normal and anomalous traffic, with a risk gradient reflecting the complexity of attack patterns. The 6 records classified as critical ($R_i > 0.90$) represent the most severe cases that would require immediate intervention in a production environment.

Pipeline Integration: All six operators O1-O6 demonstrated synergistic operation.

Entropy analysis (O2) provided an independent first layer of detection, while neural evaluation (O4) added precision in risk classification. Semantic integration (O1, O5, O6) transformed numerical results into queryable knowledge, enabling contextually informed mitigation decisions.

Explainability and Audit Trail: The SPARQL output provided a complete and structured audit trail, allowing not only the identification of at-risk records, but also their prioritization based on score. The ability to extract and sort results by risk severity demonstrates the practical value of the semantic layer in real operational scenarios.

Performance and Scalability: The proof-of-concept implementation operated with computational efficiency, handling the entire dataset without significant overhead. The modular architecture proved suitable for future extensions, particularly for integration with Digital Twin environments where data complexity requires hybrid and scalable approaches.

Validation of Operational Thresholds: The thresholds $\Delta H \geq 1.5$ bits and $R_i > 0.55$ proved effective in balancing sensitivity and specificity. The resulting distribution (61% mitigation, 16% high risk, 6% critical) suggests a good balance between aggressive detection and false positives, although fine optimization requires validation on larger datasets.

The main limitations concern the simulated nature of the dataset and the simplification of the ARNN model, which however do not compromise the architectural validation. The results demonstrate that H-DIR[2] provides a solid framework for hybrid security, particularly suitable for extensions towards H-SPHERE[3] in Digital Twin environments where the integration between statistical analysis, machine learning, and semantic reasoning becomes crucial for protecting complex cyber-physical systems.

The pipeline confirms itself as a promising approach for proactive security, combining statistical early-warning through entropy analysis with precise decisions based on neural models, all while maintaining transparency and explainability through the semantic layer.

7.2 Case study 2: Hybrid Detection Simulation in Dockerized Environment

To validate the entire pipeline in a reproducible and controlled scenario, a complete experimental environment was orchestrated using Docker. This case study aims to demonstrate the synergistic operation of all six operators (O1-O6) of the pipeline in the face of a dynamic transition from physiological to malicious traffic, simulating a Zero-Day or NTP Amplification type attack.

7.2.1 Experimental Configuration

The experimental campaign was conducted using the replay framework based on YAML configuration files, ensuring full reproducibility. The configuration included:

- **Seed:** 42 (fixed to ensure experiment repeatability).
- **Baseline Phase (Normal):** Duration of 180 seconds. Traffic generated with 2.0 second interval between packets, packet size between 60 and 200 bytes, simulating regular IoT sensor traffic.

- **Attack Phase:** Duration of 180 seconds. Traffic generated with accelerated interval of 0.5 seconds and packet size between 400 and 1200 bytes, simulating the volumetric payload typical of an NTP amplification attack.
- **Entropy Threshold:** The ΔH value was calculated on multiple windows (100, 200, 500 packets) and the dynamic threshold was set at the 95th percentile (θ_H = P95) of the baseline.
- **Devices:** 10 simulated IoT devices with IP addresses 192.168.1.1-192.168.1.10.

The Docker infrastructure, composed of the mqtt-broker, iot-simulator, digital-twin, and fuseki services, ensured an isolated and consistent execution.

7.2.2 Results and Performance Analysis

The simulation execution produced a complete set of metrics confirming the effectiveness of the hybrid pipeline.

a) Learning and Performance of the ARNN Model

The ARNN model demonstrated excellent discriminative capabilities after training on 200 epochs. The results of the performance report (`performance_report.json`) indicate:

- **AUC (Area Under the ROC Curve):** 0.993 (95% Confidence Interval: [0.991, 0.995]). A value close to 1.0 denotes an almost perfect ability to distinguish between the two classes.
- **F1-Score:** 0.978. This value, which balances precision and recall, confirms the model's accuracy in classifying packets.
- **False Positive Rate (FPR):** 0.021. Only 2.1% of normal traffic was erroneously classified as attack, demonstrating low impact on false alarms.
- **Accuracy:** 0.982.

These metrics highlight that the model not only learned effectively but is also ready for operational deployment with a high degree of reliability.

b) Anomaly Detection based on Entropy

The analysis of the temporal trend of entropy variation (ΔH) revealed significant patterns. During the baseline phase (0-180 seconds), the value of $|\Delta H(t)|$ remained contained within a range of 0.2-0.5 bits, steadily below the dynamic threshold θ_H = 0.013 bits calculated on the 95th percentile of the baseline.
At the instant $t = 180$ seconds, corresponding to the beginning of the attack phase, a significant peak of $|\Delta H(t)| = 1.83$ bits was recorded for the 100-packet window, exceeding the critical threshold by over 14000%. This peak was followed by anomalous oscillations between 1.2 and 1.8 bits throughout the duration of the attack.
The net transition from physiological values ($\Delta H < 0.5$ bits) to pathological values ($\Delta H > 1.2$ bits) confirms the ability of the entropy module to function as an effective early-warning system, capable of detecting statistical anomalies even of previously unseen attacks (zero-day).

c) System Temporal Performance

Real-time performance is crucial for a defense system. Log analysis revealed:

- **Average inference time (τ_{inf}):** 2.1 ms (95% CI: [1.8, 2.4] ms). The time taken by the ARNN to classify a single packet is negligible, demonstrating the model's efficiency.
- **Average end-to-end detection time (τ_{det}):** 15.3 ms (95% CI: [12.8, 17.8] ms). This time includes MQTT reception, RDF serialization, entropy calculation, vectorization, and inference.
- **Average mitigation time (τ_{mit}):** 10.5 ms (95% CI: [9.8, 11.2] ms). The time to apply the mitigation policy (e.g., marking in the RDF graph) is extremely reduced.

These values demonstrate that H-SPHERE^3 operates with an extremely low total latency (approximately 25.8 ms for the complete O1-O6 cycle), making it suitable for real-time applications even in high-speed traffic environments.

d) Explainability through SPARQL Diagnostics

Confirming semantic explainability, diagnostic queries were executed correctly during the simulation.
The high-risk-hosts-window query identified all source IP addresses (192.168.1.*) that generated high-risk packets during the attack window.
Query RPL Loops did non identify loops.
The results were stored in json format, providing an immediate and queryable audit trail for a security analyst.

e) Verification of RDF Serialization

The experimental validation included direct verification of the correct generation of RDF triples through SPARQL queries on the Fuseki endpoint:

```
-- Real-time verification query
SELECT * WHERE { ?s ?p ?o } LIMIT 10
```

Verified result:

```
<http://example.org/packet/device_2_1758891289745> a ntw:Packet ;
    ntw:src "192.168.1.2" ;
    ntw:dst "10.0.0.1" ;
    ntw:hasRiskScore "0.996396005153656"^^xsd:float ;
    ntw:port "123"^^xsd:integer ;
    ntw:timestamp "1758891289745"^^xsd:long ;
    ntw:risk "high" ;
    ntw:proto "UDP" ;
    ntw:size "782"^^xsd:integer .
```

This empirical verification confirms the correct functioning of the O1 operator (RDF Serialization) and the persistence of semantic knowledge in the triplestore.

7.2.3 System Architecture and Technology Integrations

The proposed architecture, based on the principles of H-DIR², is designed to be inherently distributed, modular, and containerized. This architectural choice guarantees the fundamental requirements of scalability, resilience, and reproducibility, essential for a security system intended to operate in dynamic and potentially critical Digital Twin environments.
The system consists of four main technological components that interact through well-defined interfaces:

Containerization and Orchestration: Docker and Kubernetes

The infrastructural core of the framework is its deployment strategy based on Docker containers and orchestrated by Kubernetes. This "infrastructure-as-code" approach allows packaging each component (the Digital Twin, the semantic database, the messaging broker) into isolated and self-consistent units. Kubernetes manages the lifecycle of these containers, ensuring high availability, automatic scaling based on load, and simplified network configuration management. This model ensures that the entire environment is easily replicable, a fundamental requirement for experimental validation and production deployment.

Real-Time Communication: MQTT Protocol

Asynchronous real-time communication between components, particularly for data input from sensors or the DT, is entrusted to the MQTT (Message Queuing Telemetry Transport) protocol. Chosen for its lightness and reliability, de facto standard in IoT, MQTT operates on a publish-subscribe model. Data producers (simulators or real sensors) publish messages on specific "topics," while consumers (the Digital Twin's analysis module) subscribe to them. This decoupling ensures efficient communication even in high-load scenarios and allows easy integration of new data sources.

Semantic Knowledge Base: Apache Jena Fuseki

The "semantic brain" of the system is implemented using Apache Jena Fuseki, a SPARQL server that functions as an RDF triplestore. This component is responsible for persisting and querying the system's knowledge. All events, network packets, risk scores, and DT metadata are represented as RDF triples and stored in Fuseki. It provides an endpoint for executing diagnostic, investigative SPARQL queries and for updating knowledge, thus enabling the explainability and reasoning capabilities of the framework.

The Processing Core: The Digital Twin

The central component is the Digital Twin itself, which encapsulates the security logic. Inside it resides the implementation of the hybrid analysis pipeline (O1-O6). This module receives event streams via MQTT, executes RDF serialization, entropy calculation, neural network evaluation, and finally updates the knowledge graph and triggers any mitigation actions. Its containerization makes it a scalable and independent processing unit.

The interaction between these components creates a coherent and robust architecture: data flows via MQTT to the Digital Twin, which processes them and enriches the Knowledge Base in Fuseki. Mitigation decisions, based on semantic queries, can in turn be communicated to the DT control system always via MQTT, closing the control loop.

7.2.4 Case Study Discussion

The results of this end-to-end simulation experimentally validate the proposed architecture. In particular:

- **Hybrid Synergy:** The entropy (O2) and ARNN (O4) modules operated synergistically, providing two independent but complementary defense layers. Entropy provides alarms, while ARNN provides high-precision classifications.
- **Zero-Day Detection:** The ΔH peak coinciding with the attack demonstrates the system's resilience to threats not known a priori, provided they modify the statistical properties of network traffic.
- **Operational Efficiency:** The temporal metrics (τ_{det}, τ_{mit}) demonstrate that the overhead introduced by semantic and neural processing is minimal, making the pipeline feasible for production deployment.
- **Explainability and Audit Trail:** The output of SPARQL queries transforms the detections of the neural "black box" into actionable and understandable information for a human operator, bridging the critical gap between detection and response.

7.2.5 The Simulation as Validation of the H-SPHERE³ Core

The experimental campaign conducted in this thesis has validated the functional hybrid core of H-SPHERE³. Although the input was simulated network traffic, the implementation successfully demonstrated:

- The synergistic operation of the H and SPHERE elements.
- The effectiveness of the semantic pipeline (O1-O6) in detecting a known threat (NTP amplification) in an explainable and automatic manner.
- The system's ability to operate in real time with reduced latencies (τ_{det}, τ_{mit}).

This implementation constitutes the proof of concept on which to build the entire H-SPHERE³ ecosystem. The next step, in a real operational context, would consist of complete contextualization: extending the internal orbit to calculate entropy on DT-specific metrics (e.g., command frequency, sensor states) and specializing the external orbit to execute mitigation actions directly on the state of the digital twin.
In conclusion, H-SPHERE³ is not just a simple security tool, but a meta-architectural framework for the engineering of Digital Twin resilience, uniting in a single hybrid model the speed of statistical detection, the power of symbolic knowledge, and the sensitivity of entropy analysis, all orchestrated in an orbital architecture that ensures holistic and explainable protection.

Chapter 8

Conclusions and Future Directions

8.1 Original Contributions

This thesis builds upon the H-DIR^2 framework and introduces original contributions primarily in its adaptation to Digital Twin environments:

- **Orbital re-conception of the pipeline**: whereas H-DIR^2 organized the six-stage pipeline (O1–O6) in a linear sequence, this work reconceptualizes it as a stratified "orbital architecture" surrounding the Digital Twin. The inner orbit integrates entropy and ARNN detection, the median orbit manages semantic reasoning, and the outer orbit enables orchestration and mitigation. This reorganization enhances resilience through defense-in-depth.
- **Entropy-based early-warning perspective**: whereas H-DIR^2 employed entropy variation to identify anomalous traffic distributions, this thesis emphasizes its role as a potential early-warning indicator for zero-day vulnerabilities in Digital Twins, where deviations in entropy may precede critical failures or novel attack patterns.
- **Containerized reproducibility**: the framework was implemented in a containerized environment, ensuring reproducibility of results and demonstrating its feasibility for scalable, portable deployments across hybrid IoT–Digital Twin infrastructures.
- **Semantic reasoning for Digital Twins**: RDF/SPARQL and OWL ontologies were employed as in H-DIR^2, but this thesis identifies the creation of specialized ontologies for Digital Twins as a crucial step forward, positioning it as both a limitation of the current work and a contribution to future development directions.

8.2 Limitations and Challenges

Firstly, the experimental validation was carried out on datasets of limited size and under controlled conditions, which may not fully reflect the complexity and variability of industrial-scale deployments. Although containerized validation demonstrates reproducibility, large-scale testing on thousands of Digital Twin instances with high-frequency data exchange remains an open challenge. Secondly, although RDF/SPARQL

and OWL reasoning were integrated, the development of domain-specific ontologies for Digital Twins was not implemented in this work; it remains an essential step for contextualized reasoning. Finally, the computational cost of semantic reasoning could pose constraints for deployment on edge or resource-limited devices, requiring further optimization.

8.3 Final Considerations

In conclusion, this thesis has demonstrated the efficacy of the H-SPHERE^3 framework in addressing critical security challenges within Digital Twin ecosystems, particularly by integrating entropy-based risk evaluation with hybrid semantic pipelines. Evolving from the foundational H-DIR^2 architecture, H-SPHERE^3 has shown the ability to mitigate NTP amplification and zero-day vulnerabilities, improving detection accuracy, response times, and semantic orchestration in heterogeneous environments. These contributions establish a robust foundation, while also revealing the limitations of current hybrid methods in adapting to rapidly evolving zero-day threats under distributional shifts.

Building on these findings, future research can advance toward neurosymbolic architectures such as Ψ-Risk-DT, which extend entropy-driven detection through the integration of recurrent neural inference and semantic reasoning. By coupling ARNN activations with RDF/SPARQL updates under entropy modulation, Ψ-Risk-DT promises enhanced adaptability, reduced false positives, and improved stability supported by formal analysis. This progression from hybrid to neurosymbolic frameworks represents a natural continuation of the work presented here, opening avenues for explainable, resilient, and scalable cybersecurity solutions in safety-critical Digital Twin domains.

Bibliography

[1] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, others, Challenges for securing cyber physical systems. Workshop On Future Directions in Cyber- Physical Systems Security, 2009.

[2] T.Y. Melesse, V. Di Pasquale, S. Riemma, Digital Twin Models in Industrial Operations: a Systematic Literature Review, Procedia Manuf. 42 (2020) 267–272, https://doi.org/10.1016/j.promfg.2020.02.084.

[3] Z. Liu, A. Li, Z. Sun, G. Shi, X. Meng, Digital Twin-Based Risk Control during Prefabricated Building Hoisting Operations, Sensors 22 (2022), https://doi.org/10.3390/s22072522.

[4] L. Hou, S. Wu, G.(Kevin) Zhang, Y. Tan, X. Wang, Literature Review of Digital Twins Applications in Construction Workforce Safety, Appl. Sci. 11 (2021), https://doi.org/10.3390/app11010339.

[5] S. Suhail, R. Jurdak, S. Member, Towards Trusted and Intelligent Cyber-Physical Systems: a Security-By-Design Approach, 2021. https://arxiv.org/abs/2105.08886v3.

[6] S. Suhail, R. Jurdak, R. Hussain, D. Svetinovic, Security Attacks and Solutions for Digital Twins, 2022.

[7] E.A. Patterson, M.P. Whelan, A framework to establish credibility of computational models in biology, Prog. Biophys. Mol. Biol. 129 (2017) 13–19, https://doi.org/10.1016/j.pbiomolbio.2016.08.007.

[8] E. Karaarslan, M. Babiker, Digital Twin Security Threats and Countermeasures: an Introduction, in: 2021 International Conference on Information Security and Cryptology (ISCTURKEY), 2021, pp. 7–11, https://doi.org/10.1109/ISCTURKEY53027.2021.9654360.

[9] D. Tosi, R. Pazzi, H-DIR Design and Experimentation of a Distributed Information Retrieval-Hybrid Architecture in Cloud IoT Data Centers, IFIP International Internet of Things Conference, 2024.

[10] D. Tosi, R. Pazzi, H-DIR^2: A Scalable Entropy-Based Framework for Anomaly Detection and Cybersecurity in Cloud-IoT Data Centers, Technical Report, University of Insubria, 2024.

[11] Zero-Day attack according to CIL-NIDS, Technical Document, University of Insubria, 2024.

[12] Zero-Day attack according to H-DIR^2, Technical Document, University of Insubria, 2024.

[13] S. R. Jeremiah, A. El Azzaoui, N. N. Xiong, and J. H. Park, "A comprehensive survey of Digital Twins applications, technologies," Journal of Systems Architecture, vol. 151, p. 103120, 2024.

[14] Cerasuolo F., Bovenzi G., Ciuonzo D., Pescape A. (2025). Attack-adaptive network intrusion detection systems for IoT networks through class incremental learning. Computer Networks, 263, 111228.