

Article

# A Novel Architecture for Virtual Network Twin Deployment

Amir Hossein Banisadr  and Xavier Hesselbach \* 

Department of Network Engineering, Universitat Politècnica de Catalunya (UPC), Jordi Girona 1-3, E-08034 Barcelona, Spain; banisadr.amir.hossein@upc.edu

\* Correspondence: xavier.hesselbach@upc.edu

**Abstract:** In this paper, a novel architecture is proposed that enhances network connectivity by combining network virtualization and the digital twin approach. A virtual network twin (VNT) framework is designed to emulate the behavior of the original network within a virtualized environment. This framework provides an enhanced connection experience for users, mirroring the performance of the original network while avoiding the limitations of previous methods such as Telnet, SSH, and VPN. By integrating the network virtualization approach and the concept of digital twins, this framework can improve network visibility, security, and robustness in real-time connectivity through appropriate communication protocols and artificial intelligence (AI) methods. The application of this proposal can significantly impact key areas such as medical applications, autonomous driving, and space communications. This paper introduces the VNT architecture; its core components; requirements; and evaluation metrics, such as the accuracy of the VNT.

**Keywords:** virtual network twin; communication protocol; digital twins; network virtualization

## 1. Introduction

In the ever-evolving world of technology, network protocols play a critical role in facilitating communication among devices and networks. These protocols, which consist of sets of rules and conventions, enable devices to communicate effectively, regardless of differences in hardware, software, or network infrastructures. The Telnet protocol, for example, is a point-to-point, client/server, and simple terminal protocol that allows users to log into a computer across the Internet. Telnet is still utilized in some local private environments where security is not a concern. To mitigate these security risks, the Secure Shell (SSH) protocol was developed. SSH, also a point-to-point and client/server protocol, is widely used for remote access to systems, especially in environments where security is paramount, such as servers, networking devices, and cloud infrastructure [1]. Following the SSH protocol, in order to enhance productivity by extending business corporate networks and applications, providing flexibility and security, and reducing communication costs, a Virtual Private Network (VPN) is used by applying a tunnel created between the VPN–client and VPN–server over a public network [2]. Despite the advancements in communication methods, the existing communication methods have several drawbacks, including low synchronization, limited compatibility, integration concerns, and low privacy. Therefore, this paper explores a solution to these issues, particularly in light of the advent of network virtualization models as a promising approach to address the ossification problem on the Internet [3]. Additionally, the innovative concept of digital twin (DT) has been applied in several fields like manufacturing, industrial applications, and healthcare. DT, as a transformative approach, enables the modeling and simulation of real assets and systems within a digital environment to improve operational efficiency and reduce failure rates [4]. The novel architecture proposed in this paper is based on a virtual network twin (VNT) framework, as shown in Figure 1, and aims to provide users with a seamless connection experience as if they were directly connected to the original network. The primary focus of this research is the creation of a digital twin network (DTN) through virtualization,



**Citation:** Banisadr, A.H.; Hesselbach, X. A Novel Architecture for Virtual Network Twin Deployment.

*Electronics* **2024**, *13*, 5045. <https://doi.org/10.3390/electronics13245045>

Academic Editor: Alexandra Bousia

Received: 15 November 2024

Revised: 16 December 2024

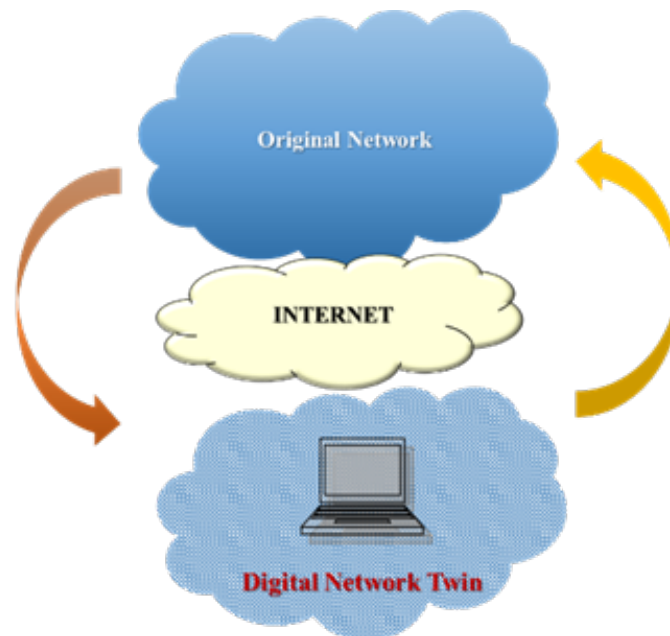
Accepted: 18 December 2024

Published: 22 December 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

where the digital network acts as a virtualized replica of the original. The virtual network twin architecture leverages the DTN concept as a digital representation of a live physical network, utilizing network virtualization. The VNT framework can play a significant role in several key areas, such as the healthcare industry by improving medical applications, in the field of autonomous, in remote driving by improving communication with vehicles, and in deep-space communication systems [5].



**Figure 1.** The digital twin network concept.

The motivations for proposing this framework are as follows:

- Providing the next generation of network connectivity: this is achieved by using a digital twin network and Virtual Network architectures.
- Enhancing network visibility and understanding: The virtual network twin encompasses all the features and elements of the original network, providing a comprehensive understanding of its real counterpart. Consequently, reviewing the network, identifying, and resolving issues in the digital replica becomes more achievable than in the physical realm.
- Enhancing the security and robustness of the network: One of the most critical issues in maintaining a network is detecting potential threats and failures in real time. The NVT can effectively mitigate these concerns with its extensive capabilities and high performance.
- Ensuring correct performance in the NVT: The application of artificial intelligence (AI) at various levels within the NVT significantly improves the performance of the network twin manager. This includes identifying risk levels, recognizing patterns to enhance efficiency, and reducing or eliminating disruptions and outages. Consequently, networks can be deployed in real time without service disruptions and can quickly respond to changing conditions or any threats or failures.
- Reducing network cost: By optimizing performance and resource utilization, the overall network costs can be reduced.

The rest of the article is organized as follows: In Section 2, the background and related research are presented. The proposed virtual network twin architecture is introduced in Section 3. Section 4 defines the metrics and key performance indicators (KPIs) to evaluate the performance of the VNT architecture, providing explanations and relevant indicators. In Section 5, applications of the VNT framework in critical industries are presented. Finally, Section 6 summarizes the conclusions and outlines the future work required.

## 2. Background and State of the Art

The Internet has rapidly and significantly evolved over the past few decades, driven by a variety of infrastructure technologies that support distributed applications and protocols. Unfortunately, this diversification has led to an impediment to further Internet development, commonly referred to as the ossification problem [6]. Since Internet service providers (ISPs) are the owners of the current architecture, any changes or adoption of new technologies require their agreement. These limitations have hindered the development of numerous potential applications and services. Network virtualization (NV) has been recognized as a promising approach to address the current network ossification [6]. Network virtualization has been proposed to advance the current Internet and stimulate innovation by enabling diverse network architectures to coexist on a shared physical substrate [6]. In other words, NV is defined by the decoupling of the roles of ISPs into two independent components, namely infrastructure providers (InPs), who manage the physical infrastructure, and service providers (SPs), who create virtual networks (VNs) by aggregating resources from multiple InPs to offer end-to-end services [7]. The deployment of VNs should be examined from two distinct perspectives: The first is that of InPs, which focus on maximizing their own revenue through the allocation of physical resources. The second perspective pertains to SPs, who aim to secure the contracted resources [8]. Consequently, NV includes two subsets, namely a physical network (also referred to as a substrate network), which is owned and operated by an infrastructure provider and consists of physical nodes connected by physical links that form the physical topology, and a virtual network, which is composed of a set of virtual nodes (each hosted on a physical node) and virtual links (each established over a physical connection) [9]. From an architectural perspective, network virtualization enables the coexistence of multiple virtual networks on the same physical network, as well as flexibility in their routing, forwarding functions, and control protocols. It also improves manageability, scalability, and security. These characteristics can be achieved through appropriate solutions [9]. Network virtualization has been evolving for over three decades, with related studies focusing on virtualization at various levels and scales within a network, including node, link, resource, and network levels. Early research includes virtual local area networks (VLANs), which facilitate different types of operations or services, provide flexible network control, and improve link utilization [9]. Both academia and industry have invested significant effort in network virtualization. However, existing studies have primarily concentrated on network infrastructure and resources, with less attention given to end-users. As a result, with the increasing diversity of end-user devices and resource-demanding services, it is more important than ever to consider the requirements of end-users and to develop innovative approaches [10]. Despite this need, only a limited number of researchers have explored end-user virtualization in the context of networking. For instance, network-hosted avatars, or virtual agents of end-users, have been proposed for applications such as file downloading when users are offline. One of the novel technologies that significantly stands out in enabling user virtualization is the digital twin. This approach must be presented to the end-user in a way that makes it appear indistinguishable from the physical network while also being easier and more intuitive to operate [11]. The digital twin (DT) concept was initially introduced by Michael Grieves at the University of Michigan in 2003. It is defined as a comprehensive software representation of a physical object (PO) [12], encompassing its properties, conditions, and behaviors in real life. NASA and the U.S. Air Force developed a digital twin paradigm for vehicles to predict their remaining usable life and the probability of mission success [11]. It is important to note that the early architecture of what would later evolve into the digital twin consisted of three main components [4]:

- The real space;
- The virtual space;
- The link serving as a communication medium between the two spaces.

In other words, a digital twin is a self-adapting, self-regulating, self-monitoring, and self-diagnosing system-of-systems identity. Overall, these properties highlight the

advanced capabilities of digital twins to operate autonomously and efficiently as a system-of-systems identity [11,13]. Most existing research on DT in the network field focuses on applications, such as distributed clock synchronization [14]. A digital twin-based, cloud-centric network architecture is proposed in [15], where digital twins of end-users hosted at the network edge serve as communication assistants or network data loggers. The application of DTs in 6G communication systems is also discussed, along with a set of challenging requirements and stringent key performance indicators recommended by standards development organizations (SDOs) [13]. These requirements are classified into two categories: functional requirements and service requirements. The functional requirements are defined as specific features and functions that a digital twin must possess to effectively accomplish its tasks. These include data collection tools and policies, data repositories, and data models. Service requirements are specified as characteristics that a digital twin should have to function optimally depending on different user demands, such as synchronicity, compatibility, flexibility, privacy, and security [13]. Communication protocols are essential in digital twins to facilitate the exchange of data and information among various interconnected components. Without these protocols, devices and systems within a digital twin environment would struggle to understand and interpret shared data, resulting in inefficiencies and communication breakdowns [5,11]. By meeting these requirements, communication protocols play a crucial role in enabling effective communication, data exchange, and collaboration within digital twins, ultimately enhancing their functionality and performance. Some of these protocols include the Transmission Control Protocol (TCP), User Datagram Protocol (UDP), QUIC, Inter-Planetary File System (IPFS), and Secure Reliable Transport Protocol (SRT). To select the most suitable communication protocol, it is essential to analyze their strengths and weaknesses in relation to the specified requirements. Virtual networks are based on network virtualization technologies, such as Software-Defined Networking (SDN), and Network Function Virtualization (NFV). These technologies emphasize resource abstraction and segmentation, enabling dynamic allocation, scalability, and network slicing. However, they do not focus on real-time mirroring, predictive analytics, adaptive to live changes, and comprehensive representation of the physical network layer [10,12]. In contrast, the digital twin network architecture focuses on creating real-time synchronization between a physical network and its digital encounter. This enables various use cases, including the safe validation of network configurations, user intent-based network automation, behavioral analysis, network optimization, and data collection for analytical purposes. However, these architectures face challenges, such as scalability issues and limited abstraction layers because DTNs focus on physical network replication and may not address logical or service-level abstractions effectively [16].

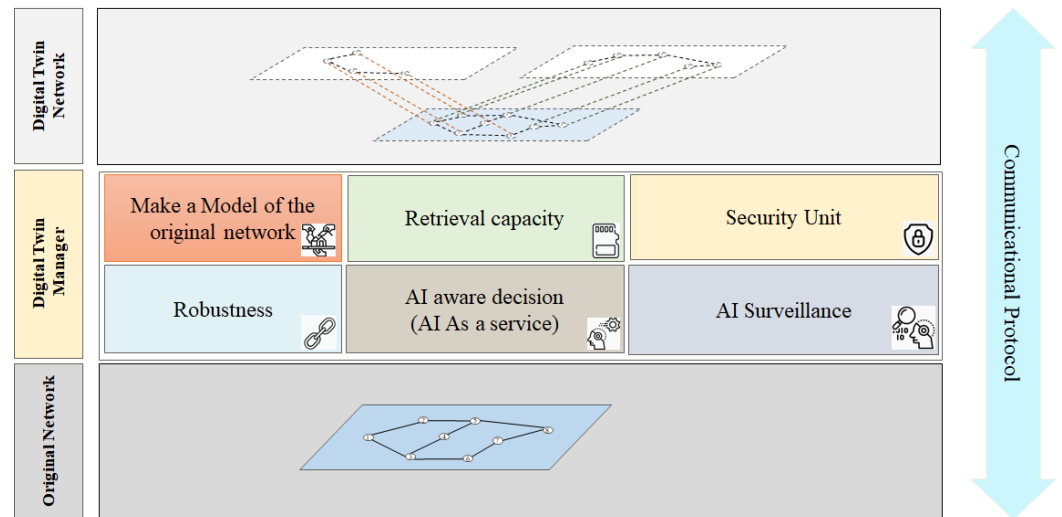
### 3. Virtual Network Twin Architecture Proposal

As discussed above, we explored architectures and protocols to develop a digital twin network using network virtualization strategies. Our proposed VNT architecture applies the digital twin network by leveraging the capabilities of virtual networks while addressing their limitations, including dynamic real-time virtualization, unified representation, scalable predictive management, and enhanced user experience. In this section, the architecture of the proposal based on the virtual network twin is explained.

#### 3.1. Description of the Main Goals

The new generation of connectivity is achieved through an innovative approach that enables users to experience seamless connectivity, mirroring the original network experience. This method provides the same feeling for any connection within the original network. To achieve synchronicity between the original network and its replica, this approach requires a suitable protocol, along with other essential components, including network capacity, computational requirements, and network services. A virtual network twin (VNT) is introduced as a virtualized replica of the original network, emulating its behavior while maintaining synchronization with the real network. A major challenge arises

from this virtualization process, particularly the synchronization between the network twin and the original. To address this issue, a digital twin manager was proposed. This unit plays a critical role in the VNT with several functionalities such as security and robustness. Figure 2 illustrates our proposed framework, referred to as virtual network twin, which can be divided into several sections: the original network, the digital twin network (DTN), the digital twin manager, and the communication protocol.



**Figure 2.** VNT framework.

- **Original Network:** The original network contains physical components, including routers, switches, and other devices that facilitate data transmission.
- **Digital Twin Network (DTN):** This refers to a digital replica of the original network that models its behavior and configuration. As illustrated in Figure 2, the DTN consists of two layers. The first layer is a digital twin layer, which represents the digital twin of the original network and is responsible for emulating its behavior, configuration, and processes. This layer is indirectly connected to the physical resources. The second layer encompasses various physical resources on the digital side that connect to the real network elements but exist in the digital realm, such as virtual routers and switches.
- **Digital Twin Manager:** The core component of the VNT framework is the digital twin manager, which is responsible for coordinating, managing, and maintaining the virtual network twin. This section comprises several units that perform various functions, including the following:
  - **Retrieval Capacity:** this ensures that real-time data are completely retrieved and effectively respond to the requests of the digital twin;
  - **Security Unit:** this ensures the security of the entire framework against various types of attacks and unauthorized access;
  - **Robustness:** this ensures resilience and sustains normal functionality in the event of failures or attacks;
  - **AI unit:** this is applied to optimize the performance of all components within the VNT framework.
- **Communication Protocol:** Another critical component is the communication protocol, which is responsible for maintaining a real-time connection between the original network and the digital twin network.

Each component, such as retrieval capacity, security, and robustness, is developed and operated independently, simplifying integration and debugging. This approach ensures that complexity is localized to specific subsystems, reducing the overall system's cognitive and operational load. Each component interacts with others via clearly defined APIs. This separation of concerns ensures that adding a new component does not introduce direct

dependencies or unpredictable interactions with existing ones. Metrics such as latency, throughput, and error rates are used as tools to continuously monitor the performance of individual layers and are measured in real time.

### 3.2. Modeling of Original Network

In the initial step, a processing unit is designed based on various requirements of the original network. This model ensures the continuous preservation of system-wide consistency, enabling the deployment of a functional replica wherever required. To optimize and adjust this unit, an evaluation algorithm is required. We propose using an adjacency matrix as a digital representation of the original network. The reasons for this are as follows:

- This matrix provides a concise representation of the network's topology by showing which elements are connected to each other and how;
- An adjacency matrix can be used as a data structure to represent network configurations and simulate their behavior;
- Using this matrix can facilitate efficient simulations of network operations and changes;
- A virtual twin can accurately replicate and represent the behavior of the physical network.

The adjacency matrix: For a network with  $n$  nodes, the adjacency matrix is an  $n \times n$  matrix. Each entry can represent a binary value, a parameter, or a set of values that store the properties or features of a specific element. The adjacency matrix is simple and general, and facilitates easy access to the information for reading or modification. More efficient structures can be explored in the future in order to optimize the performance of the specific strategies developed. The model must be applicable to scenarios of any size: small-scale, medium-scale, and large-scale networks. Therefore, scalability is one of the main considerations in the VNT architecture.

#### 1. Small-Scale Network with Tens of Nodes

An example of this scenario is a small home network with a few devices, including a router, a laptop, a smartphone, a smart TV, and a printer, all connected to each other. Regarding the topology, the devices are either fully connected or arranged in a partial mesh. Under these conditions, the performance of the adjacency matrix for modeling a virtual twin network is excellent, easy to compute, and requires minimal memory.

#### 2. Medium-Scale Network with Hundreds of Nodes

An example of this scenario is a university campus network with hundreds of nodes, including servers, routers, switches, and various endpoints such as computers and smart devices interconnected to provide both internet and intranet services.

In terms of topology, the network elements are hierarchical or partial mesh. In this condition, the performance of the adjacency matrix is good and manageable, but it starts to require more resources.

#### 3. Large-Scale Network with Millions of Nodes

An example of this scenario is a large ISP network with millions of nodes, including routers, switches, and various devices that provide connectivity to millions of users. The performance of the adjacency matrix significantly degrades. For large networks, without specialized hardware or algorithms, this method is relatively impractical.

To model a virtual network twin at a large scale, we can apply some commercial products from telecommunication vendors such as OpenStack which is an open source and powerful platform.

### 3.3. Suitable Communication Protocol

The communication protocol is responsible for establishing a suitable connection between the physical network and all virtual counterparts [11]. The primary functions of a communication protocol include data format and encoding, which determine how data are structured, encoded, and decoded. This ensures that data sent from the physical network are understood by their virtual counterparts and vice versa. Another critical role is error handling and correction, which involves implementing mechanisms for detecting and correcting errors in data transmission, thereby ensuring the reliability and integrity

of the data. In addition, flow control and congestion management are vital functions that regulate the rate of data transmission to prevent congestion and ensure efficient utilization of network resources [5]. To achieve a suitable communication protocol, two primary steps must be considered. The first step is to determine the requirements and constraints of the digital twin network. For instance, these requirements depend on different user demands, including synchronization, compatibility, flexibility, and privacy, as well as several applications and the system's behavior under specific conditions, such as data collection policies and tools [13]. Some main requirements for suitable communication protocols include [11] the following:

- **Low latency:** the capability of establishing a real-time connection with low latency, essential for data transfer, and ensuring that data exchange occurs in a synchronized manner;
- **Reliability:** the capability to ensure that data are transmitted accurately and consistently, without loss or corruption;
- **Scalability:** the protocol should be able to support the increasing volume of data and devices within the digital twin ecosystem;
- **Security:** security is paramount in digital twins to protect sensitive data and prevent unauthorized access or tampering. The communication protocol should incorporate robust security measures, such as encryption and authentication, to safeguard information exchange;
- **Interoperability:** this is essential for enabling seamless communication between diverse devices, systems, and platforms within the digital twin environment.

Then, various transport protocols, such as TCP and UDP, will be reviewed to select an appropriate communication protocol. As the first alternative, the Transmission Control Protocol (TCP), which is the most widely used protocol on the Internet, is selected. It is a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, as well as in interconnected systems of such networks with varying characteristics, including the following features:

- Broadband transmission;
- Connection models exported from the original network to the digital twin network;
- Mechanisms for congestion control and error control.

TCP has been used in research as a communication protocol for digital twins, particularly in the development of an innovative digital twin platform dedicated to water quality monitoring, ensuring reliable transmission of data packets over the network, albeit with slightly higher latency [17]. One of the main requirements of the selected protocol is synchronism, which is essential to maintain optimal connectivity between the real and digital twins. TCP includes mechanisms for error control, and its latency constraints render it unsuitable for our needs in terms of synchronism. User Datagram Protocol (UDP) provides minimal latency due to its lightweight design. In contrast, TCP ensures reliable data delivery by establishing a virtual connection and using retransmission mechanisms, which are facilitated through a three-way handshake involving synchronization and acknowledgment processes. While TCP enhances reliability, it can also introduce higher latency and jitter, potentially affecting real-time responsiveness compared to UDP [18]. DT communication must provide real-time responsiveness while ensuring reliable data delivery. The protocol that offers these characteristics is the Quick UDP Internet Connection (QUIC) protocol. The QUIC protocol was originally proposed by Google as a transmission protocol based on UDP rather than TCP. It is claimed that QUIC's new features can address the shortcomings of TCP. Some of these features are as follows [19]: Connection multiplexing and reduced handshake overhead are key features of QUIC. Unlike TCP, which requires a three-way handshake to establish a connection, QUIC minimizes latency by combining the handshake and data transmission processes. This allows for faster connection setup, which is essential for DTs that require real-time data exchange between physical and digital components [19]. Compared to TCP, QUIC provides security protocols as part of its fundamental design. It

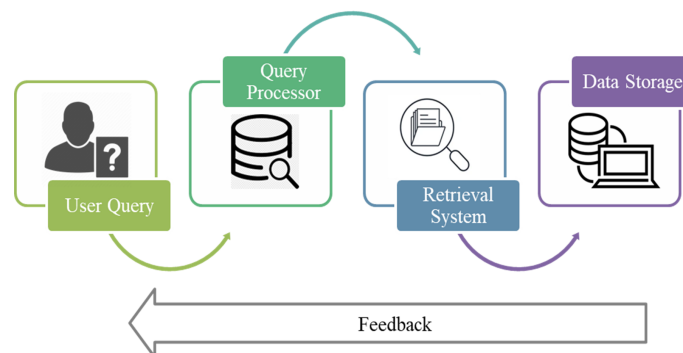
enhances performance by encrypting all payloads by default, thereby reducing the risk of eavesdropping and man-in-the-middle attacks. Additionally, QUIC employs advanced congestion control mechanisms that are more adaptable to changing network conditions. This adaptability is critical for the implementation of DTs in various environments, as it helps maintain data flow efficiency and prevents bottlenecks [20]. QUIC seems to be a more favorable candidate than TCP and UDP as a communication protocol for digital twins (DTs). However, other protocols, such as the Real-Time Streaming Protocol (RTSP), Real-Time Messaging Protocol (RTMP), and Secure Reliable Transport Protocol (SRT), may also be considered suitable based on an analysis of the time delay in data transmission and other critical requirements of digital twins in a network setup. According to the information presented above, the VNT architecture is protocol-agnostic. So, the suitable protocol will be selected in each scenario based on specific requirements. After determining the communication protocol, to mitigate all assigned requirements, the following strategies are employed within the VNT framework:

- To ensure real-time performance, the AI decision system dynamically improves routing paths, adjusts bandwidth allocation, and predicts congestion points.
- Continuous monitoring of network traffic patterns as AI surveillance identifies latency or jitter, enabling proactive measures to address potential disruptions.

### 3.4. Retrieval Procedures from Network Digital Twin

One of the major challenges in digital twin networks is ensuring low-latency retrieval in response to user queries. As the volume of data increases, this issue can arise due to the growing complexity of indexing, searching, and retrieving data. To address this challenge, various retrieval mechanisms have been proposed. These mechanisms consist of several key components, as illustrated in Figure 3.

- User Query: this process involves the user inputting a query into the system;
- Query Processor: the query processor analyzes and optimizes queries to improve their alignment with the stored data;
- Retrieval System: a retrieval system ranks and filters data using algorithms that take into account factors such as keyword matches;
- Data Storage: implementing indexing and caching strategies to enhance response times for common queries, along with fault tolerance measures to ensure data availability and system reliability;
- Feedback System: the feedback system is designed to learn from user interactions and adjust its processes and algorithms accordingly.



**Figure 3.** Retrieval mechanism concept.

### 3.5. Developing the Security Unit of Network Digital Twin

The security unit is one of the essential components of the digital twin manager, responsible for ensuring the privacy, safeguarding, and accessibility of the entire framework. Its primary role is to safeguard the VNT against a range of potential threats. These threats are classified into two types: digital and physical. Digital attacks encompass all vulner-

abilities related to software, including poor coding, inadequate upgrades, and default security settings, as well as all components that provide resources for distributed and centralized computation, such as the network itself and its information systems. Physical attacks involve security threats associated with access to endpoints, including CPS/IIoT nodes, communication infrastructures, and facilities [21]. Some of these threats include the following:

- Software attacks can occur due to critical bugs in various software components, including databases, machine learning (ML) models, applications, and firmware, as well as flaws in their own code and manipulations within computing sections. These threats can impact several aspects of operational performance in DTs, leading to issues such as desynchronization and connectivity problems.
- Rogue Human Machine Interfaces (HMIs): Attackers with full access rights may insert, replace, configure, or clone HMIs connected to the network digital twin. They can alter the final data representation to draw invalid conclusions and block or hinder the maintenance of HMIs, among other malicious activities.
- Tampering can occur in several areas, including data tampering, which affects data quality and management in critical contexts. Knowledge tampering is closely related to data, with a strong emphasis on database tampering and virtual resource tampering. These forms of tampering can manipulate sections and actions of digital twins by compromising their containers and the hypervisor.

### 3.6. Robustness of the VNT Structure

Robustness is a critical component of the VNT structure, ensuring that the framework sustains its normal functionality even when a portion of the network fails due to malfunctions or attacks. The damage caused by these incidents typically results in the disruption of essential network functions, such as connectivity, controllability, data transmission, and communication capabilities [22]. Therefore, two primary issues can compromise the system's functionality: attacks and failures. Both of these issues must be analyzed and addressed through appropriate strategies.

- Attacks, such as hacking and viruses, can compromise all the resources involved in the physical environment being mirrored. The security unit must cooperate closely with the resilience unit to ensure the normal functionality of the entire system.
- To ensure functionality in the face of failures, it is essential to select suitable structures within the VNT framework that offer high performance. For instance, when representing the original network as a graph, one can utilize either an adjacency matrix or an adjacency list as potential numerical representations, choosing the optimal option based on performance criteria.

According to these components, the VNT architecture offers several benefits, including the following:

- Proactive Network Management: The VNT framework enables users to predict issues before they occur. For example, using historical data, the twin can identify potential failures and recommend solutions preemptively.
- Risk-Free Testing and Optimization: New configurations, policies, and applications can be tested in the twin network environment without risking disruptions to the live network.
- Enhanced Network Performance: The twin environment allows for the safe testing of new configurations, policies, and security measures without disrupting live systems. Real-time synchronization and protocol adaptability enable precise performance evaluations.
- Accelerated Troubleshooting: Users can resolve problems in the twin environment, instead of troubleshooting directly in the physical network.
- Improved Security: The VNT architecture significantly enhances security by identifying and mitigating both digital and physical threats. This includes safeguarding

against software vulnerabilities, rogue HMIs, and tampering attempts. Cybersecurity measures can be tested and validated in the twin environment without impacting live operations, while anomalies detected in the twin provide early warnings to protect the live network.

#### 4. KPIs and Metrics for the VNT Architecture

The VNT is expected to be an exact replica of the original network. However, limitations in the capacity of the remote environment where the VNT is deployed, as well as the consequences of imperfect communication between the VNT and the original network, must be considered in order to assess the deviations and their impact on performance. Regarding the necessity of measuring the quality of the VNT in relation to the original network and communication capacity, a set of key performance indicators (KPIs) are established to evaluate the performance of the proposed VNT framework. These KPIs are determined based on the essential components of the digital twin manager.

- **Accuracy of the Digital Twin Network:** This indicator assesses the accuracy of the digital twin network model in representing the physical network. The model must ensure that the digital twin network closely mirrors the original network in terms of its components, links, and overall architecture. Additionally, it should effectively adapt to changes in network size without significant performance degradation. If the behavior of the digital twin network deviates substantially from that of the physical network, it may result in incorrect conclusions or even system failures. One of the primary purposes of a digital twin is to serve as a reliable, real-time representation of the physical network, enabling network administrators to make informed decisions based on the performance of the DTN and its analyses. The accuracy of the DTN is assessed by comparing various parameters, including latency, throughput, error rate, and storage capacity, between the physical and digital twin networks. The parameters are as follows:
  - Latency: the time taken to transmit data packets across the network;
  - Throughput: the volume of data transmitted successfully per unit of time;
  - Error Rates: the percentage of packets lost during transmission;
  - Storage: the ability to handle and store data through the network.

The normalized difference (ND) is used to compare differences for each parameter between the original network and the DTN. For an individual  $i$ th parameter, the related ND is calculated as follows:

$$ND_i = (C_{phy,i} - C_{vir,i}) / C_{phy,i} \quad (1)$$

where

- $C_{phy,i}$ : the  $i$ -th physical parameter;
- $C_{vir,i}$ : the  $i$ -th virtual parameter.

The accuracy of the digital twin network is evaluated through a weighted summation of all parameters. Each parameter is assigned a weight based on its relative importance within the framework. For example, if latency is considered more critical than throughput, it may be assigned a weight of 0.4, while throughput is assigned a weight of 0.3.

So, the accuracy of the DTN (AC) is calculated as follows:

$$AC = \frac{1}{n} \sum_{i=1}^n w_{ai} * (ND_i) \quad (2)$$

where

- $w_{ai}$ : weight assigned to  $i$ -th parameters;
- $n$ : total number of parameters.

This formula represents the absolute average differences between the performance values of the physical network and those of its digital twin. The simple numerical example is prepared and presented below to clarify this metric. The network comprises five nodes and six edges, as illustrated in Figure 4.

According to Figure 4, the simple DTN depicted is not exactly the same as the original network in terms of CPU capacity and throughput; however, their behavior is almost identical. The accuracy metric measures the differences between these two layers. In the first step, the Accuracy Network is defined based on the differences between these two layers, as shown in Figure 4. The accuracy network is represented in Figure 5.

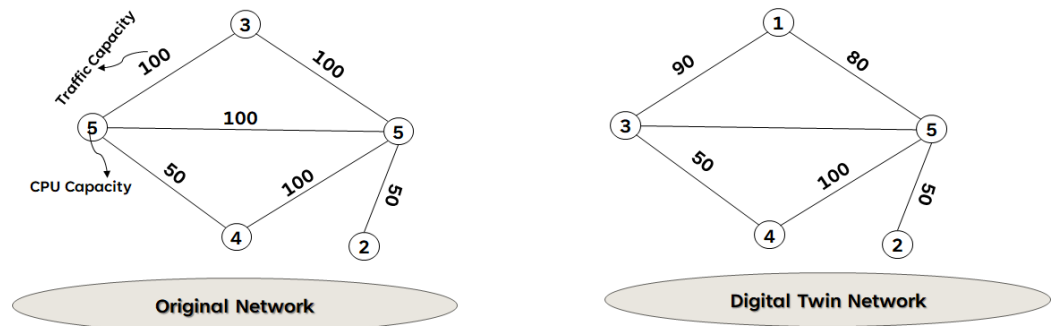


Figure 4. Numerical example: a small-scale network with five nodes.

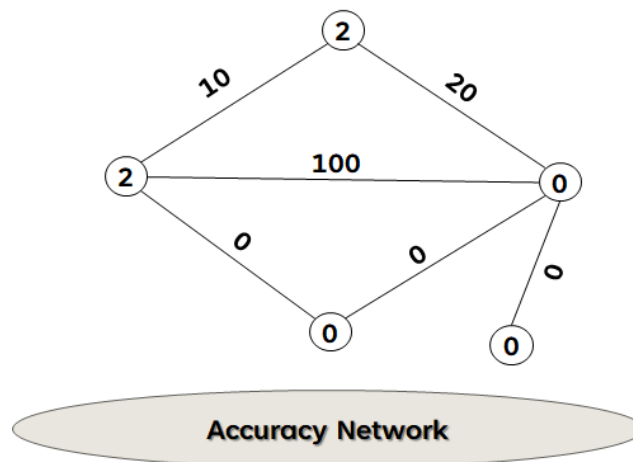


Figure 5. Numerical example: the accuracy network.

Then, the normalized differences for two parameters including CPU capacity (C) and throughput (T) are calculated.

$$ND_C = (C_{phy} - C_{vir}) / C_{phy} \tag{3}$$

$$ND_T = (T_{phy} - T_{vir}) / T_{phy} \tag{4}$$

The accuracy of the DTN based on the normalized differences and weight factors for two parameters is 1.21.

- **Retrieval Capacity:** This indicator refers to the efficiency of the retrieval system and data processing. To measure this, the total time taken to respond to requests, known as the response time (RT), is considered. This encompasses the time required for processing a request, communication between the digital twin network and the physical network, and the response to the user. The response time in retrieval capacity includes the following:
  - Request processing time: this refers to the time it takes to process a request;

- Retrieval time: this is the required time to retrieve data from the digital twin's storage;
- Latency: this refers to the time taken for communication between the original and digital twin networks.

The response time is one of the crucial metrics in our framework. It represents the sum of all the aforementioned components, measuring how quickly the DTN can deliver data when requested. In real-time network management, quick access to accurate data is critical. Slow response times can diminish the performance of the proposed framework, resulting in delays in troubleshooting, optimization, and proactive maintenance. Therefore, a low RT is essential to maintaining the high operational efficiency of the VNT, enabling quick reactions to network changes. The response time (RT) is calculated as the sum of processing, retrieval, and latency times.

$$RT = T_{\text{pro}} + T_{\text{ret}} + T_{\text{lat}} \quad (5)$$

where

- $T_{\text{pro}}$  : the processing time of the request;
- $T_{\text{ret}}$  : the retrieval time from the digital twin's storage;
- $T_{\text{lat}}$  : latency in communication between physical and DT networks.

Example: Let us consider a DTN deployed in a smart healthcare system within a hospital. The hospital is equipped with several Internet of Medical Things (IoMT) devices, such as heart rate monitors and oxygen level sensors, to monitor patients' vital signs in real time. These devices continuously collect data and communicate with the hospital's digital twin network, which mirrors the state of all connected medical devices and patients' health metrics. This system comprises five nodes within the VNT framework: Node 1 is the central digital twin processing server, Node 2 is the IoMT devices gateway, Node 3 is the historical data storage, Node 4 is the diagnostic and predictive analysis unit, and Node 5 is the monitoring interface. Additionally, there are seven edges that serve as communication links between these components. The response time metric is essential for assessing the system's performance during critical patient events, such as irregular heartbeats. In this scenario, we assume that a potential anomaly, such as a drastic drop in oxygen levels, is detected by a patient's device. Consequently, a request is automatically sent to the DTN to validate the alert and process the data.

- Request Processing Time: The initial step involves processing the alerts sent from the IoMT devices, which includes filtering out noise and, validating data integrity.  $T_{\text{pro}}$  is assumed to be 0.1 s.
- Data Retrieval Time: Historical patient data are retrieved from storage in Node 3 to compare current vital signs with past trends.  $T_{\text{ret}}$  is assumed to be 0.2 s.
- Latency: This involves complex computations and the transmission of data between the processing server and the diagnostic unit to run a predictive model that assesses the risk level of detected anomalies.  $T_{\text{lat}}$  is assumed to be 1 s.

The response time in this example is 1.3 s, reflecting the framework's capacity to respond to critical health events in real time. In healthcare, even a delay of a few seconds can be life-threatening, particularly in situations like cardiac arrest. Therefore, it is essential to analyze the components that contribute to response time, such as minimizing database query durations, to optimize both the response time and the overall responsiveness of the framework.

Security: Metrics for assessing security levels are essential for achieving proper framework functionality. In this regard, the following indicators should be considered:

- The number of security incidents detected and resolved within a specific period;
- The average time required to investigate and respond to detected intrusion attempts (ATIs);

- The percentage of incidents prevented due to proactive security (PIS) measures, such as endpoint protection, intrusion detection systems, and threat intelligence.

Using these metrics, we can evaluate and improve the security of the VNT architecture, ensuring that the framework remains resilient against potential attacks.

**Robustness:** This metric evaluates the resilience of the DTN in maintaining functionality under adverse conditions, such as hardware failures, network outages, or other uncontrolled situations. Robustness is crucial for ensuring the reliability of network services. Networks can be subject to various disruptions, and a robust DTN can effectively manage these events by rerouting traffic and recovering from failures with minimal impact on overall performance. This indicator allows for the assessment of the VNT framework's capability to sustain high availability and reliability. To calculate the robustness of the VNT framework, we propose two indicators: fault tolerance degree (FTD) and average recovery time (ART).

- **Fault Tolerance Degree:** This is a crucial measure of robustness and represents the digital twin network's capacity to maintain its functionality when certain components fail. The key components of this metric include the following:
  - **Redundancy Ratio (RR):** This refers to the proportion of backup resources that can assume control in the event of a failure of the primary component. For example, if one node fails, a redundant node can take over its operations to prevent interruptions in the transmission of data packets.
  - **Error Detection and Correction Rate (ER):** This refers to the ability of the DTN to quickly detect failures and correct them. For example, if a data packet is lost, the DTN will resend the data.

The fault tolerance degree (*FDT*) is calculated as follows:

$$FDT = w_{F,RR} * RR + w_{F,ER} * ER \quad (6)$$

where

- *RR*: the redundancy ratio is determined as follows:

$$RR = \frac{\text{Number of Backup Nodes/Links}}{\text{Total Primary Nodes/Links}} \quad (7)$$

- *ER*: the error detection and correction rate (*ER*) is determined as follows:

$$ER = \frac{\text{Number of Detected and Recovered Faults}}{\text{Total Faults Occurred}} \quad (8)$$

- $w_{F,RR}$ : the weight factor assigned based on the relative importance of redundancy component;
- $w_{F,ER}$ : the weight factor assigned based on the relative importance of error detection and correction component.
- **Total Average Recovery Time (TAR):** This indicator measures the time taken for the framework to recover from failures and disruptions within the network. It is defined as the average time required to restore normal operations after a failure occurs concerning various components of the digital twin manager. A lower average recovery time indicates that the VNT framework is highly resilient and capable of managing faults with minimal impact on operations. Depending on the strategies deployed in the system, the calculation method can be adjusted. For example, the mean absolute deviation (MAD) can be employed for a more robust measure of recovery consistency. This set of metrics offers a thorough assessment of the performance of the VNT architecture.

## 5. Applications of the VNT Framework in Critical Industries

In this section, several applications of the VNT framework are explained. This framework directly addresses the main challenges facing the identified industries.

- **Healthcare Industry:**
  - **Improving Medical Applications:** In the medical sector, the VNT framework can significantly improve medical applications by enabling real-time data monitoring and analysis.
  - **Remote Surgery and Diagnostics:** The VNT framework enables real-time video streaming and data transmission with minimal latency, which is critical for remote surgeries; thus, surgeons can perform more accurate procedures, even if they are not physically present.
- **Autonomous Driving:** VNT can play a key role in improving communication between autonomous vehicles and traffic management systems. It allows for real-time exchange of data, such as vehicle status, road conditions, and traffic signals, ensuring that autonomous vehicles operate safely and efficiently.
- **Deep Space Communication Systems:**
  - **Real-Time Data Transmission:** The VNT framework significantly enhances the capabilities of deep-space communication systems by minimizing latency in data transmission between Earth and space missions. This is crucial for tasks such as real-time monitoring of spacecraft, remote control, and data retrieval from planetary explorations.
  - **Adaptive Congestion Control:** The advanced congestion control mechanisms of the VNT framework allow for efficient data transmission even in environments with limited bandwidth and high noise levels, such as deep-space communication.

The VNT framework's ability to integrate various communication protocols, handle diverse data types, and optimize performance makes it an ideal solution for addressing the complex communication needs of these critical industries.

## 6. Conclusions and Future Work

In this article, we present the virtual network twin (VNT) architecture, a novel approach to network connectivity that creates a digital replica of a physical network to enhance performance, security, and reliability. One of the primary challenges within the VNT architecture is ensuring accurate synchronization between the original network and its digital twin. To address this challenge, the virtual network manager—a key component of the VNT—is designed with several units, including a model of the original network, retrieval capacity, security, robustness, and artificial intelligence (AI). We highlight the need for specific structures to support topology descriptions, such as the adjacency matrix, to effectively model the original network. To maintain an appropriate degree of synchronization and suitable time connections between the physical network and the digital network twin, we introduce open problems in communication protocols based on all defined VNT requirements. The VNT is expected to be an exact replica of the original network, but practical deployments aim to achieve this goal. Therefore, this paper proposes a set of key performance indicators (KPIs) to evaluate deviations and threats within the VNT framework. This architecture can be effectively utilized in critical fields, including medical applications, autonomous driving, and space communications. In future work, we plan to explore and propose suitable models for structures required to model the topology and parameters; analyze and select the suitable communication protocol based on VNT requirements, particularly considering the significant latencies of hard environments; and investigate the application of AI to expedite decision-making processes in order to provide optimal performance across the six blocks outlined in the architecture.

**Author Contributions:** Conceptualization, A.H.B. and X.H.; methodology, A.H.B. and X.H.; validation, A.H.B. and X.H.; formal analysis, A.H.B. and X.H.; investigation, A.H.B. and X.H.; resources, X.H.; writing—original draft preparation, A.H.B. and X.H.; writing—review and editing, A.H.B. and X.H.; supervision, X.H.; project administration, X.H.; funding acquisition, X.H. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work has been supported by the Agencia Estatal de Investigación of Ministerio de Ciencia e Innovación of Spain under project PID2022-137329OB-C41/MCIN/AEI/10.13039/501100011033.

**Data Availability Statement:** The data presented in this study are available in the article.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Coonjah, I.; Catherine, P.C.; Soyjaudah, K. Experimental performance comparison between TCP vs. UDP tunnel using OpenVPN. In Proceedings of the 2015 International Conference on Computing, Communication and Security (ICCCS), Pointe aux Piments, Mauritius, 4–5 December 2015; pp. 1–5.
2. Shen, X.; Gao, J.; Wu, W.; Lyu, K.; Li, M.; Zhuang, W.; Li, X.; Rao, J. AI-assisted network-slicing based next-generation wireless networks. *IEEE Open J. Veh. Technol.* **2020**, *1*, 45–66. [\[CrossRef\]](#)
3. Belbekkouche, A.; Hasan, M.M.; Karmouch, A. Resource discovery and allocation in network virtualization. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 1114–1128. [\[CrossRef\]](#)
4. Barricelli, B.R.; Casiraghi, E.; Fogli, D. A survey on digital twin: Definitions, characteristics, applications, and design implications. *IEEE Access* **2019**, *7*, 167653–167671. [\[CrossRef\]](#)
5. Mihai, S.; Yaqoob, M.; Hung, D.V.; Davis, W.; Towakel, P.; Raza, M.; Karamanoglu, M.; Barn, B.; Shetve, D.; Prasad, R.V.; et al. Digital twins: A survey on enabling technologies, challenges, trends and future prospects. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 2255–2291. [\[CrossRef\]](#)
6. Wang, C.; Wang, C.; Yuan, Y. Game based dynamical bandwidth allocation model for virtual networks. In Proceedings of the 2009 First International Conference on Information Science and Engineering, Nanjing, China, 26–28 December 2009; pp. 1745–1747.
7. Chowdhury, N.M.K.; Boutaba, R. Network virtualization: State of the art and research challenges. *IEEE Commun. Mag.* **2009**, *47*, 20–26. [\[CrossRef\]](#)
8. Zhou, Y.; Li, Y.; Sun, G.; Jin, D.; Su, L.; Zeng, L. Game theory based bandwidth allocation scheme for network virtualization. In Proceedings of the 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, USA, 6–10 December 2010; pp. 1–5.
9. Seddiki, M.S.; Frikha, M. A non-cooperative game theory model for bandwidth allocation in network virtualization. In Proceedings of the 2012 15th International Telecommunications Network Strategy and Planning Symposium (NETWORKS), Rome, Italy, 15–18 October 2012; pp. 1–6.
10. Chiosi, M.; Clarke, D.; Willis, P.; Reid, A.; Feger, J.; Bugenhagen, M.; Khan, W.; Fargano, M.; Cui, C.; Deng, H.; et al. Network functions virtualisation: An introduction, benefits, enablers, challenges and call for action. In Proceedings of the SDN and OpenFlow World Congress, Darmstadt, Germany, 22–24 October 2012; Volume 48, pp. 1–16.
11. Rasheed, A.; San, O.; Kvamsdal, T. Digital twin: Values, challenges and enablers from a modeling perspective. *IEEE Access* **2020**, *8*, 21980–22012. [\[CrossRef\]](#)
12. Kaur, K.; Mangat, V.; Kumar, K. Architectural framework, research issues and challenges of network function virtualization. In Proceedings of the 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 4–5 June 2020; pp. 474–478.
13. Vuković, M.; Mazzei, D.; Chessa, S.; Fantoni, G. Digital Twins in Industrial IoT: A survey of the state of the art and of relevant standards. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
14. Coonjah, I.; Catherine, P.C.; Soyjaudah, K.S. A VPN framework through multi-layer tunnels based on OpenSSH. In Proceedings of the International Conference on Computing, Communication & Automation, Greater Noida, India, 15–16 May 2015; pp. 1395–1401.
15. Wang, Y.; Su, Z.; Guo, S.; Dai, M.; Luan, T.H.; Liu, Y. A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects. *IEEE Internet Things J.* **2023**, *10*, 14965–14987. [\[CrossRef\]](#)
16. Raj, D.R.R.; Shaik, T.A.; Hirwe, A.; Tammana, P.; Kataoka, K. Building a Digital Twin Network of SDN Using Knowledge Graphs. *IEEE Access* **2023**, *11*, 63092–63106. [\[CrossRef\]](#)
17. Kabir, M.R.; Mila, S.A.; Ray, S. AQUATWIN: A Digital Twin Framework for Early Detection of Water Contamination. In Proceedings of the 2024 4th Interdisciplinary Conference on Electrics and Computer (INTCEC), Chicago, IL, USA, 11–13 June 2024; pp. 1–6.
18. Cakir, L.V.; Al-Shareeda, S.; Oktug, S.F.; Özdem, M.; Broadbent, M.; Canberk, B. How to synchronize digital twins? a communication performance analysis. In Proceedings of the 2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Edinburgh, UK, 6–8 November 2023; pp. 123–127.

19. Iyengar, J.; Thomson, M. QUIC: A UDP-based multiplexed and secure transport. In *RFC 9000*; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2021.
20. Langley, A.; Riddoch, A.; Wilk, A.; Vicente, A.; Krasic, C.; Zhang, D.; Yang, F.; Kouranov, F.; Swett, I.; Iyengar, J.; et al. The quic transport protocol: Design and internet-scale deployment. In Proceedings of the Conference of the ACM Special Interest Group On Data Communication, Los Angeles, CA, USA, 21–25 August 2017; pp. 183–196.
21. Alcaraz, C.; Lopez, J. Digital twin: A comprehensive survey of security threats. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1475–1503. [[CrossRef](#)]
22. Lou, Y.; Wang, L.; Chen, G. Structural robustness of complex networks: A survey of a posteriori measures [feature]. *IEEE Circuits Syst. Mag.* **2023**, *23*, 12–35. [[CrossRef](#)]

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.