## **King Fahd University of Petroleum and Minerals**

Project Title

**An SDN/NFV-based Next-Gen Smart Hospital Network**

Term: 242

Course No: COE 546

Course Name: Computer Network Design

Submitted By

**Nafisa Tabassum (g202424600)**

**Tazeen Khan (g202317010)**

Instructed By

**Dr. Tarek Rahil Sheltami**

**Professor, Dept. of COE, KFUPM**

## Abstract

Modern hospitals rely heavily on digital tools for patient monitoring, including electronic health records (EHRs), telemedicine, and Internet of Things (IoT) devices. However, typical hospital networks are not designed to meet the increasing demands for speed, security, and adaptability, particularly during emergencies such as the COVID-19 epidemic. This project demonstrates a smart hospital network that is more elastic, secure, and robust thanks to Software-Defined Networking (SDN) and Network Function Virtualization (NFV). The network can detect cyberattacks, respond rapidly with an automated strategy, and modify resources such as firewalls or virtual routers in response to real-time traffic. It also connects seamlessly with healthcare applications and IoT devices. While this is a theoretical architecture, tools like as Mininet, Docker, and machine learning might be employed in the future to assess how the system operates in high-traffic situations or under assault. The resulting network design can help keep healthcare services running, increase performance, and deliver better patient care now and in the future.

## Introduction

Software-Defined Networking (SDN) is a modern way of managing networks by using software to control how data moves through the system. Unlike traditional networks that rely on dedicated hardware like routers and switches to make traffic decisions, SDN shifts that control to a central software-based controller. This controller communicates with the network hardware using protocols like OpenFlow and has a complete view of the network, which allows it to make smarter, more efficient decisions. By separating control and data layers, SDN simplifies network management, improves flexibility, and makes it easier to adapt to changing demands [1].

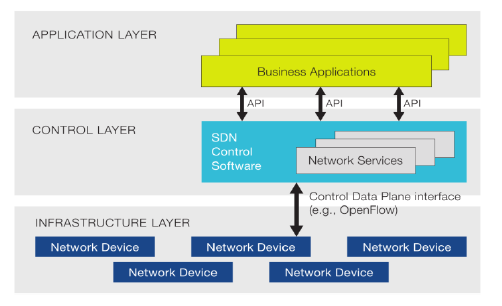


Fig. 1: Basic SDN architecture

A method for virtualizing network services that were previously run on proprietary hardware, such as load balancers, firewalls, and routers, is called network functions virtualization, or NFV. These services are packaged as virtual machines (VMs) on commodity hardware, allowing service providers to run their networks on standard servers instead of proprietary ones. With NFV, specific hardware is no longer needed for any network operation. NFV improves scalability and flexibility by allowing service providers to introduce new network services and applications as needed without needing additional hardware resources. According to [1], NFV also works well with SDN, helping make networks more resilient by allowing virtual functions (VNFs) to be deployed or replaced on demand. For example, if an intrusion detection system (IDS) isn’t enough, it can be swapped for a firewall, or extra VNFs can be added automatically to balance traffic or recover from failures.

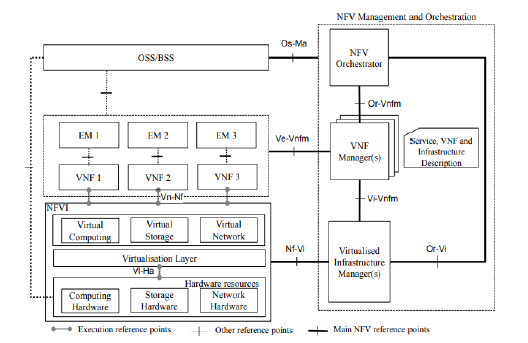


Fig. 2. NFV Architecture

In paper [2], the authors propose a model that introduces an elastic router capable of adjusting hardware resources dynamically based on real-time changes in demand or resource availability (as shown in Fig. 3). The system continuously monitors key performance indicators (KPIs) to determine how many and what types of network functions (NFs) are needed at any given time. This helps optimize resource usage while maintaining network performance. When service needs shift or in worst-case scenarios, the model can rearrange resources automatically to ensure continued service quality.

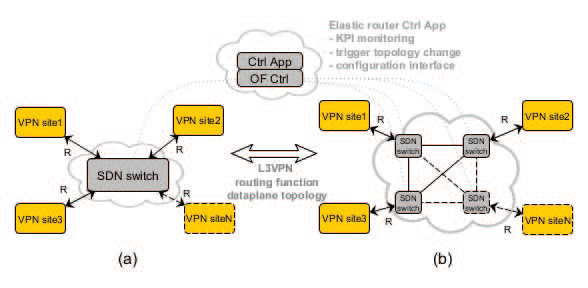


Fig. 3. VPN service with an elastic router providing N ports. The dynamic

creation of extra ports is illustrated by the dashed links/blocks.

In paper [3], the authors propose a robust resilience strategy for SDN/NFV-based networks, centered around a smart feedback control loop (illustrated in Fig. 4). This loop continuously monitors the network’s behavior and collects real-time data after different protection strategies are applied, allowing the system to adapt and improve. Each Virtual Network Function (VNF)—such as a firewall or load balancer—can respond quickly to issues by redirecting traffic or adjusting its function. Meanwhile, SDN features help detect problems like sudden traffic spikes or service disruptions. If VNFs alone aren’t enough, SDN takes further action, like isolating affected servers or network segments, to maintain stability and security.

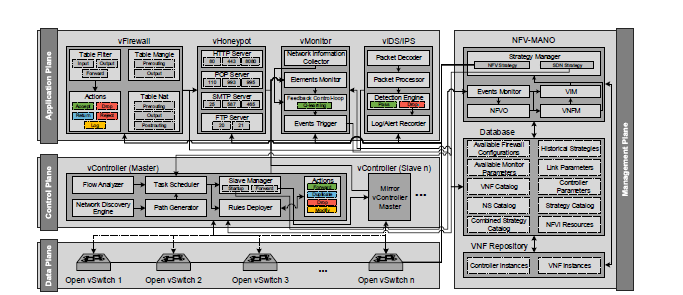


Fig. 4. Overall Network Resilience Architecture

Hospitals nowadays need networks that are secure and sophisticated. These networks need to grow to meet demand for services like telemedicine, electronic health records, and smart patient devices. This project builds a smart hospital network using SDN and NFV. The system will be flexible, easy to expand, and problem-resistant. It will also continue to ensure that healthcare services are delivered in a timely, safe, and effective manner.

## Description of the problem

As healthcare systems increasingly depend on digital technologies to deliver essential services, the need for robust, scalable, and intelligent network infrastructures has become more critical than ever. Modern healthcare environments must support real-time communication, secure and fast data exchange, and seamless integration across diverse systems and connected devices. Unfortunately, many existing hospital networks lack the flexibility, resilience, and adaptability required to meet these demands, especially during emergencies or in remote and underserved areas. The challenges outlined below highlight some of the major limitations faced by current healthcare networking infrastructures.

* **Inaccessibility for Remote and Isolated Patients**

Patients who live in remote or rural areas typically struggle to receive timely medical care due to a lack of nearby healthcare services. These limitations were worsened by the challenging or impossible nature of in-person consultations during the COVID-19 epidemic [4] [5]. Scalable remote healthcare delivery cannot be maintained by standard healthcare infrastructures, resulting in missed diagnoses, inadequate monitoring, and preventable complications.

* **Fragmented Healthcare Information Systems**

Most hospitals use a variety of diverse, segmented systems, including billing platforms, laboratory information systems, radiology systems, and electronic health records (EHR). This incompatibility results in delayed clinical judgment because of incomplete data, human mistakes are increased by redundant data entering, and inefficient departmental and caregiver communication [6].

* **Increased Risk of Cyber Threats**

Large volumes of sensitive data, such as patient demographics, medical histories, and insurance information, are managed by healthcare providers. Cyberattacks like ransomware, phishing, and data breaches frequently target these records [7]. Patient safety and trust are at risk because legacy network designs lack the flexibility and real-time security measures required to fend off these changing threats.

* **Inflexibility Toward Technological Advancements**

Large volumes of sensitive data, such as patient demographics, medical histories, and insurance information, are managed by healthcare providers. Cyberattacks like ransomware, phishing, and data breaches frequently target these records [8]. Patient safety and trust are in danger because legacy network designs lack the flexibility and real-time security measures required to fend off these changing threats.

## Literature survey

The combination of Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) marks a major shift in how modern networks are designed and managed. SDN separates the control logic from the hardware, while NFV allows network services to run as software on standard servers, eliminating the need for specialized devices. Together, these technologies have transformed network operations, making them more flexible, programmable, and efficient. This review explores recent advancements in SDN and NFV, with a particular focus on how they enhance network resilience and support healthcare systems in delivering smarter, more reliable digital services.

Recent research highlights the powerful combination of SDN and NFV in improving network resilience and adaptability. For example, the ANSwer architecture proposed by Machado et al. (2016) introduces a smart feedback control loop that allows real-time reconfiguration of the network. This approach is particularly effective in detecting and mitigating DDoS attacks, providing fast and automated responses to network anomalies.

Van Rossem et al. (2015) explored **elastic routing**, demonstrating how dynamically scaling VNFs and migrating their state can help maintain service continuity under changing loads. Their work emphasizes the importance of **VNF profiling**, though it also points out the challenges of optimizing performance under **high-traffic conditions**.

In the context of **5G networks**, Bouras et al. (2017) examined the role of SDN and NFV in managing technological diversity and standardization. Their comparative study of **OpenRadio, OpenRAN, and SoftRAN** highlights practical deployment challenges, especially in ensuring interoperability and managing network complexity.

The integration of SDN/NFV has also shown promising results in **radio resource management** and **quality-of-service (QoS)** optimization. However, dense network environments and complex handover scenarios remain areas that require further research and refinement.

In the **healthcare sector**, Boudlal et al. (2021) proposed a **multi-layer SDN/NFV architecture** tailored for Hospital Information Systems. Their framework significantly improves network flexibility and performance, especially in response to the high demands, such as remote care, telemedicine, and increased data exchange.

### Critical Analysis and Research Implications

The reviewed studies present diverse yet complementary approaches to SDN/NFV implementation. While Machado et al. (2016) emphasize dynamic resilience strategies, Van Rossem et al. (2015) focus on function scalability. Bouras et al. (2017) and Boudlal et al. (2021) provide domain-specific insights into 5G and healthcare applications, respectively.

Several recurring themes emerge:

* The crucial role of centralized network control
* Virtualization's impact on operational flexibility
* The necessity of adaptive network management
* Persistent challenges in standardization and security

Requirements and specifications

SDN and NFV must be integrated to fulfill the increasing demand for scalable, secure, and responsive healthcare services. These technologies provide dynamic service supplies, effective resource allocation, and flexible control across healthcare services and hospital information systems (HIS). The following requirements are necessary for our system:

1. Elasticity

The system must support real-time dynamic resource scaling to handle unpredictable workloads in patient monitoring, teleconsultation, and data sharing.

*Specification*:

* Deploying virtual routers, firewalls, and load balancers that scale horizontally.
* Utilizing elastic network functions to respond to spikes in healthcare data traffic, especially during pandemics.
* Implementing SDN-controlled traffic engineering for load balancing and adaptive routing.

1. Resilience

By identifying and reacting to malfunctions or attacks (such as DDoS or equipment failure), we can guarantee the ongoing availability of vital healthcare services.

*Specification:*

* Integrating resilient design principles to dynamically reroute traffic and reconfigure network paths on failure.
* Maintaining controller redundancy and fault-tolerant NFV orchestration layers.
* Using SDN-enabled anomaly detection for preemptive mitigation of cyber and operational threats.

1. Automation

Enabling real-time, policy-driven automation to optimize performance, security, and scalability with minimal human intervention.

*Specification*:

* Feedback control loop to monitor performance metrics and trigger automatic reconfiguration or scaling.
* Automating VNF lifecycle management (deployment, migration, scaling) via NFV MANO.
* AI-assisted orchestration to predict resource needs and optimize service delivery.

1. Security and Privacy

Protect sensitive health data and comply with security and privacy regulations (e.g., HIPAA).

*Specification*:

* Fine-grained access control and micro-segmentation using SDN flow rules.
* VNF-based firewalls and IDS/IPS at network edges and data centers.
* Enabling real-time security policy enforcement using SDN controllers.
* Support end-to-end data encryption and secure tunneling.

1. Centralized Monitoring and Control

Providing unified visibility and centralized management for network operations across all departments.

*Specification*:

* A central SDN dashboard for monitoring traffic patterns, latency, and health devices.
* Multi-tenant control for managing network slices per department or service unit.
* Log and visualize network metrics for auditing and optimization.

## Discussion of different design approaches and how we have arrived at the design in our project

As shown in Fig. 5, a WLAN-enabled architecture combined with a wired backbone network is a frequently used network configuration in hospitals. This configuration makes sure that only people with the right credentials and accountability can access critical data by controlling access to the main network using authorization and verification mechanisms. Studies such as [9], [10], and [11] report successful adoption of these mechanisms across various healthcare institutions. Given the reliance on wireless communication, this architecture typically includes a wireless system analyzer to monitor signal strength and maintain stable radio connections. On the server side, tools like Wavelink’s Mobile Manager are used to efficiently manage Access Points (APs), perform firmware updates, monitor configurations, and alert administrators of unauthorized changes. Furthermore, only authorized individuals can access security credentials and configuration data since they are kept in tamper-resistant memory. While this model provides basic security and network accessibility, it lacks the dynamic adaptability, real-time resource elasticity, and integrated resilience required for today’s healthcare environments, particularly in times of high demand or during critical service disruptions.

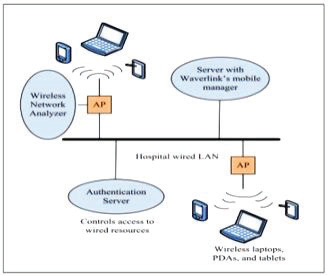


Fig. 5. Typical Hospital Network System [12]

Figure 6 displays a normal hospital networking system that relates to the A&E room, radiology, and ICU unit. Each situation requires multiple programs, which are all connected to the wired networking system architecture that provides high-speed connection and centralized control as stated in [12].

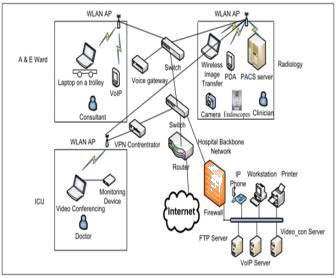


Fig. 6. Traditional Hospital Network System [12]

Another new research strategy is to integrate IoT with cloud-based infrastructures for remote healthcare monitoring [14]. This concept involves linking electronic equipment at the patient's home and hospital online, transmitting data to cloud platforms for storage and immediate access by family members and medical experts, as illustrated in Figure 7. This architecture still relies on traditional networking components and requires dependable end-to-end communication, despite the inclusion of mobile apps and sensors to improve patient lifestyle and remote monitoring.

This type of traditional networking involves manual configuration and management of individual devices such as routers, switches, and firewalls. While the models have served well in smaller or static environments, they pose significant challenges in scalability and efficiency for larger networks. Key limitations in typical networks include time-consuming manual configuration, device-by-device troubleshooting, and a lack of centralized management.

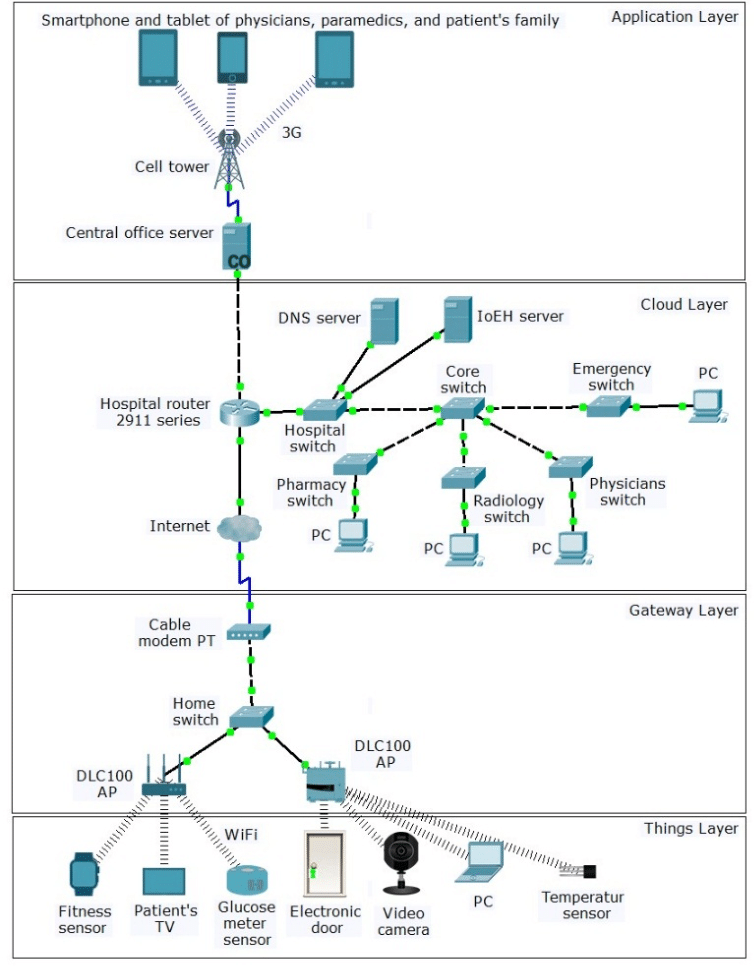


Fig. 7. Simulated IoT healthcare network [14]

As this traditional networking struggles to meet the demands of modern, dynamic environments, it highlights the need for more flexible and automated solutions like Software-Defined Networking (SDN). Hospitals and healthcare systems particularly need real-time communication for telemedicine, secure access to electronic health records, and seamless integration with IoT-based patient monitoring systems. These requirements cannot be efficiently met with static, hardware-centric architectures.

To address these challenges, this project proposes an SDN/NFV-based smart hospital network architecture that provides:

* Centralized control and automation through SDN, reducing manual errors and operational complexity.
* Dynamic Resource Scaling via NFV, allowing the network to elastically adjust to traffic demands—critical during health emergencies like pandemics.
* Enhanced Resilience and Security, using programmable policies and real-time anomaly detection.
* Seamless integration with healthcare applications, IoT devices, and third-party platforms.

By leveraging the programmability and virtualization capabilities of SDN and NFV, the proposed architecture ensures a scalable, resilient, and secure network infrastructure tailored to the evolving needs of modern healthcare systems.

## Design and Methodology

### **System Architecture Overview**

The proposed smart hospital network is structured into four key layers, as shown in **Figure 7**. This layered approach provides modularity, flexibility, and clear separation of responsibilities for managing healthcare services in an elastic and resilient manner.

#### **Application Layer (Healthcare Services Layer)**

This topmost layer includes critical healthcare applications such as telemedicine, e-health, PMS, EHRs, and third-party integration.

#### **SDN/NFV Control Layer**

This layer introduces SDN and NFV technologies to manage the network dynamically. The NFV Orchestrator manages the deployment and lifecycle of VNFs such as virtual firewalls and IDS. SDN Controller controls the network centrally, enabling dynamic routes, traffic optimization, and security enforcement. Elastic routers are dynamically instantiated to scale with demand. Cloud resources provide virtual infrastructure for flexible resource allocation. This layer also handles protection mechanisms such as attack detection, traffic rerouting, and auto-scaling.

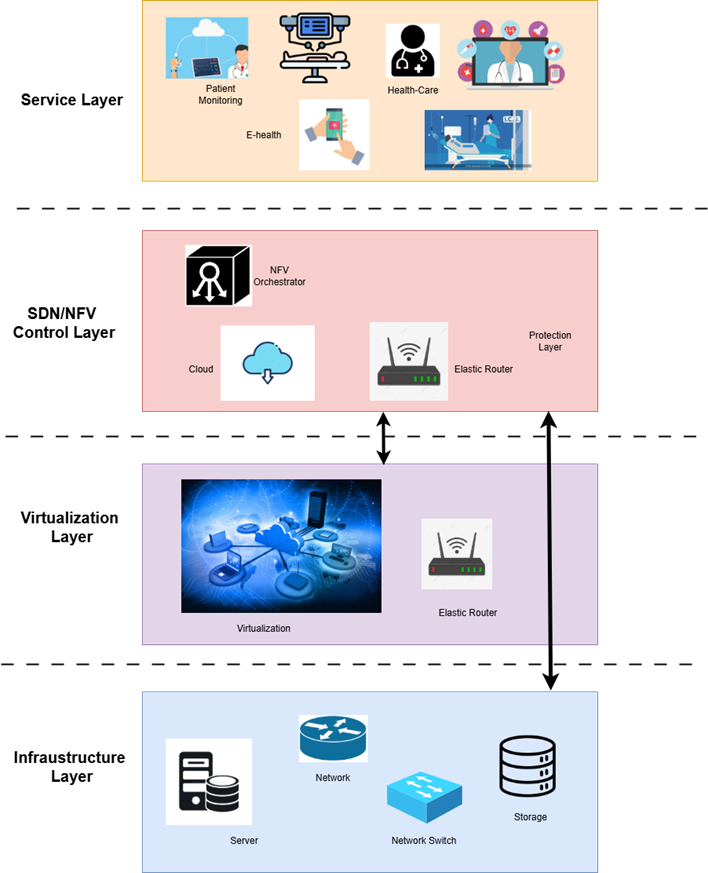


Figure 7: System Architecture of the SDN/NFV-Based Smart Hospital Network

#### **Virtualization Layer**

This layer provides virtualized resources through technologies like OpenStack. Network services (e.g., virtual routers, firewalls) are abstracted from hardware, enabling elasticity. This layer supports the seamless deployment of healthcare-specific VNFs.

#### **Physical Infrastructure Layer**

This foundational layer includes servers, network devices, storage systems, etc.

### **Methodological Approach**

#### **Design and Setup**

The system can be designed with layered modularity for scalability and resilience. An SDN controller like Ryu can manage flow control. An NFV orchestrator like OpenStack can provide VNFs on demand.

#### **VNF Deployment and Management**

VNFs such as Snort for IDS, Open vSwitch for router, and HAProxy for load balancer can be deployed in containers. Resource profiling can be used to define scaling thresholds.

#### **Elasticity and Feedback Control Loop**

Network traffic and resource metrics can be monitored in real-time using tools like Prometheus and Grafana. An ML-based anomaly detection system can trigger automated scaling or mitigation actions. A feedback control loop can be used to continuously optimize the system state.

#### **Simulation and Testing**

The network can be emulated in **Mininet** to validate real-world performance under:

* + Normal operation
  + Sudden traffic spikes
  + DDoS attack scenarios

#### **Evaluation**

Performance can be measured by

* + **Scalability**: VNF scaling, latency, and efficiency.
  + **Resilience**: Time to detect and mitigate attacks.
  + **Availability**: Service uptime during stress.

## Discussion of the findings

The proposed SDN/NFV-based smart hospital network presents a forward-thinking solution to many of the limitations faced by traditional healthcare network infrastructures. Although this study is theoretical, the design is based on existing research and current technology capabilities, allowing us to assess its potential usefulness.

1. **Expected Improvements in Elasticity and Scalability**

One of the key strengths of this architecture is its ability to dynamically scale network resources through virtualized functions. The system can scale down during off-peak hours and install more virtual routers or load balancers to accommodate traffic in high-demand scenarios, such as a spike in telemedicine use during a medical emergency. This elastic characteristic offers more resource efficiency and performance than static, hardware-based networks.

1. **Enhanced Resilience and Threat Response**

The architecture is built to react rapidly to network anomalies like cyberattacks or service interruptions by incorporating a feedback control loop and anomaly detection methods. This design offers automated techniques that improve network resilience, such as traffic redirection, isolating affected nodes, and dynamic VNF reconfiguration, in contrast to existing systems that mostly rely on manual intervention.

1. **Seamless Integration with Healthcare Applications**

The design places a strong emphasis on third-party services, including telemedicine platforms, IoT-based patient monitoring, and integration with current hospital information systems (HIS). It is simpler to control many healthcare services across a single network when SDN is used because it enables flexible traffic routing and policy enforcement.

1. **Operational and Security Benefits**

While NFV lowers dependency on expensive physical hardware, centralized control through SDN streamlines network administration and lowers the possibility of misconfiguration. Security is also enhanced through real-time monitoring and programmable policies that can enforce data privacy standards and respond to threats proactively.

Overall, the proposed architecture addresses critical shortcomings in traditional hospital networks, offering a scalable, secure, and resilient alternative. Although the architecture is theoretical, it aligns well with existing SDN controllers (like Ryu or ONOS) and NFV orchestrators (such as OpenStack or Kubernetes), which are already in use in various industries. This suggests that the proposed design is technically feasible and can be implemented using currently available tools and frameworks.

## Comparison with traditional networks

Conventional hospital networks are based on manual device management and static hardware configurations, which can be rigid and unsteady to adjust to abrupt shifts in demand or security risks. On the other hand, our suggested SDN/NFV-based architecture offers virtualized network services and a programmable, centralized control system, enabling real-time flexibility, automated scaling, and proactive security measures. Critical Healthcare services like telemedicine, patient monitoring, and electronic health records require high availability, resilience, and integration, all of which are supported by this modern architecture.

Table 1 shows the key difference between a traditional network and our proposed network.

Table 1: Comparison between Traditional and SDN/NFV-based network

|  |  |  |
| --- | --- | --- |
| **Feature** | **Traditional Network** | **SDN/NFV-Based Smart Hospital Network** |
| **Control Mechanism** | Distributed, manual configuration | Centralized, programmable via SDN controller |
| **Scalability** | Limited and hardware-dependent | Highly scalable with dynamic VNF deployment |
| **Security Management** | Static firewalls and manual monitoring | Real-time threat detection and automated response |
| **Resilience** | Reactive and slow to adapt | Proactive, with a feedback loop and self-healing |
| **Integration with Healthcare Apps** | Difficult, often siloed systems | Seamless integration via APIs and virtual services |
| **Resource Utilization** | Often under- or over-provisioned | Optimized via VNF profiling and elastic scaling |
| **Maintenance and Upgrades** | Manual and time-consuming | Automated and remotely managed |
| **Adaptability to Emergencies** | Poor (slow scaling and response) | High (on-demand resource scaling and fast reconfiguration) |
| **Deployment Time** | Long - due to manual setup and hardware dependency | Fast – due to automated provisioning of virtual functions |
| **Mobility Support** | Weak support for mobile/IoT devices | Native support for IoT and mobile health devices |

## Conclusions

This project presents a theoretical design for a smart hospital network based on Software-Defined Networking (SDN) and Network Function Virtualization (NFV) to meet the growing demands of modern healthcare environments. By adding centralized control, dynamic resource allocation, and real-time threat response mechanisms, the suggested architecture provides a versatile, scalable, and robust alternative for conventional static network infrastructures. Key features such as automated elasticity, integrated resilience strategies, and seamless support for healthcare services like telemedicine and IoT-based patient monitoring demonstratethe potential of this architecture to transform hospital networking.The solution increases operational efficiency, strengthens data security, and guarantees high service availability, especially in times of crisis like pandemics, by utilizing virtualized network services and a layered design. For future analysis, we can enhance the anomaly detection system with predictive models using ML to anticipate network issues before they occur. Moreover, we can extend the network design to support 5G and edge computing for low-latency applications such as remote surgery or real-time diagnostics. Additionally, we can explore blockchain-based mechanisms for secure and verifiable access to patient data. Although this work is theoretical, it highlights a clear path forward for modernizing healthcare networks using currently available technologies and frameworks.

## References

1. H. Boudlal, M. Serrhini and A. Tahiri, "Towards an SDN/NFV based Network Infrastructure for Hospital Information Systems and Healthcare Services," 2022 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5g//6G-based Interconnected Digital Worlds (NISS), Bandung, Indonesia, 2022, pp. 1-5.
2. S. Van Rossem et al., "Deploying elastic routing capability in an SDN/NFV-enabled environment," 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, USA, 2015, pp. 22-24, doi: 10.1109/NFV-SDN.2015.7387398.
3. J. Hatim, S. Chaimae and C. Habiba, "SDN/NFV Security Challenges and Proposed Architecture," 2023 7th IEEE Congress on Information Science and Technology (CiSt), Agadir - Essaouira, Morocco, 2023, pp. 145-149, doi: 10.1109/CiSt56084.2023.10409955. keywords: {Information science;Organizations;Network function virtualization;Security;Software defined networking;Resilience;sdn;nfv;security},
4. C. C. Machado, L. Z. Granville and A. Schaeffer-Filho, "ANSwer: Combining NFV and SDN features for network resilience strategies," 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 2016, pp. 391-396, doi: 10.1109/ISCC.2016.7543771.
5. R. G. Hollander and R. Carr, “Virtually perfect? Telemedicine for COVID-19,” New England Journal of Medicine, vol. 382, no. 18, pp. 1679–1681, 2020.
6. [2] World Health Organization (WHO), “Maintaining essential health services: operational guidance for the COVID-19 context,” June 2020. [Online]. Available: [https://www.who.int](https://www.who.int/)
7. [3] J. Adler-Milstein and A. Jha, “No evidence found that hospitals are using new electronic health records to increase Medicare reimbursements,” Health Affairs, vol. 33, no. 7, pp. 1271–1277, 2014.
8. [4] Verizon, “2023 Data Breach Investigations Report,” 2023. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir>/
9. [5] S. M. Riazul Islam et al., “The Internet of Things for health care: a comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, 2015.
10. Hneiti, W. and N. Ajlouni. Performance enhancement of wireless local area networks. in Information and Communication Technologies, 2006. ICTTA'06. 2nd. 2006: IEEE.
11. Dar, H. and A. Shah, Evaluating the Effect of using IP version and Physical Media on the ICMP Throughput of a LAN. Journal of Advanced Computer Science & Technology Research, 2013. 3(1).
12. Rajput, P.S., Maximising the Shared Bandwidth for Classroom Quiz Conduct Scenario in Wireless Environment. 2013, Indian Institute of Technology, Bombay.
13. Algaet, Mustafa & Muhamad Noh, Zul Azri & Basari, Abd Samad & Shibghatullah, A. & Milad, Ali & Mustapha, Aouache. (2015). A Review of Service Quality in Integrated Networking System at the Hospital Scenarios. Journal of Telecommunication, Electronic and Computer Engineering. Vol. 7 No. 2. 61-69.
14. Al-Joboury, Istabraq & Al-Hemiary, Emad. (2018). Internet of Things Architecture Based Cloud for Healthcare. Iraqi Journal of Information and Communications Technology (IJICT). 1. 18-26. 10.31987/ijict.1.1.7.