*Int. J. Advance Soft Compu. Appl, Vol. 18, No. 1, March 2026*
*Print ISSN: 2710-1274, Online ISSN: 2074-8523*
*Copyright ©Al-Zaytoonah University of Jordan (ZUJ)*

# Secure and Adaptive IoT Network Architecture for Smart Hospitals with Load Balancing in Diabetic Care Systems

**Ala Mughaid[1,3*], Mahmoud AlJamal[2], Athari Alnatsheh[3]**
**Mamoon Obiedat[3], and Fairouz Hussein[3,4]**

[1] Computer Science Department, Gulf University for Science & Technology, Kuwait
`Mughaid.A@gust.edu.kw`

[2] Department of Cybersecurity, Irbid National University, Irbid, Jordan
`m.aljamal@inu.edu.jo`

[3] Department of Information Technology
Faculty of Prince Al-Hussien bin Abdullah II for IT, The Hashemite University
Zarqa (13133), Jordan
`Athari@hu.edu.jo, mamoon@hu.edu.jo`

[4] Skyline Higher Education Australia, Sydney, Australia
`fairouz.hussein@shea.edu.au`

[*] Corresponding author: Mughaid.A@gust.edu.kw

**Abstract**

The digital healthcare sector, often referred to as the smart hospital domain, has emerged as one of the most transformative and crucial areas in modern technological advancement. Its significant impact is primarily due to the ability to efficiently gather and manage patient data. This study proposes a network design specifically tailored for healthcare environments, with a focus on diabetes-related applications. Using the Cisco Packet Tracer simulation tool, this research assists healthcare providers specializing in diabetes care in making informed decisions regarding their network infrastructure. The primary objective of this work is to demonstrate a practical implementation of network systems that are suitable for diabetes care, emphasizing the need for high-performance connectivity. Special attention is given to optimizing bandwidth usage and addressing load balancing challenges within simulated environments. The network's effectiveness is assessed using various metrics, including traffic load simulations to evaluate scalability and reliability, as well as security assessments, such as penetration testing. These evaluations aim to enhance operational efficiency and improve the quality of care provided to patients.

**Keywords**: Healthcare Security, Internet of Things (IoT), Diabetes, Authentication, Packet-Tracer, Cyber Attack.

## 1 Introduction

The rapid digitalization of healthcare—commonly referred to as the smart hospital ecosystem—has introduced transformative innovations driven by the Internet of Things (IoT) and intelligent data analytics. These emerging technologies have significantly reshaped medical processes by enabling continuous data acquisition, improved patient monitoring, & automated

*Received 06 November 2025; Accepted 08 January 2026*

clinical decision support [24, 10, 7]. IoT has expanded across diverse sectors, including smart buildings, urban infrastructure, transportation, industrial automation, and, most prominently, smart healthcare systems [5, 6]. Through interconnected sensors, wearable devices, and mobile platforms, patient information is continuously collected, transmitted, processed, and stored in cloud environments, thereby enabling timely and data-driven decisions within distributed healthcare networks [20].

The global expansion of IoT technologies has accelerated dramatically, with connected devices increasing from 20.35 billion in 2017 to an estimated 75.44 billion by 2025. This growth highlights the scalability, low operational cost, and predictive capabilities of IoT systems [31]. However, as the volume of medical data generated at the network's edge increases, cloud-centric healthcare architectures face growing challenges related to latency, bandwidth consumption, and susceptibility to cyberattacks [11, 9]. Traditional cloud-based intrusion detection mechanisms struggle to manage these complexities effectively, motivating the development of fog computing as a complementary paradigm. Fog computing, introduced by Cisco, extends cloud capabilities to the network edge, thereby reducing latency, improving responsiveness, and addressing resource limitations inherent to IoT devices [26].

Fog computing enables localized data collection, processing, and preliminary analysis near IoT sensors before forwarding refined data to the cloud. This reduces network congestion and enhances system responsiveness while supporting real-time or near–real-time decision making. Importantly, fog nodes can also integrate security mechanisms to detect anomalies and malicious behaviors at the earliest stages [23]. Fog-assisted IoT systems have been widely adopted in remote patient monitoring applications—especially for chronic illnesses such as diabetes, cardiovascular diseases, pulmonary disorders, and hypertension due to their ability to improve access time, reduce energy consumption, and enhance scalability and reliability [29].

Despite these advantages, healthcare-focused fog environments remain vulnerable to a wide range of cyber threats. Attackers can exploit IoT connectivity to launch Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), Sybil, and obfuscation attacks, potentially compromising patient safety and disrupting critical services [30]. Therefore, secure network design is essential for protecting medical data, ensuring service availability, and maintaining trust in IoMT-enabled healthcare ecosystems. Figure 1 illustrates the global growth trajectory of IoT-connected devices between 2012 and 2023, along with projected trends through 2030, highlighting the increasing importance of resilient and scalable healthcare infrastructures [1].

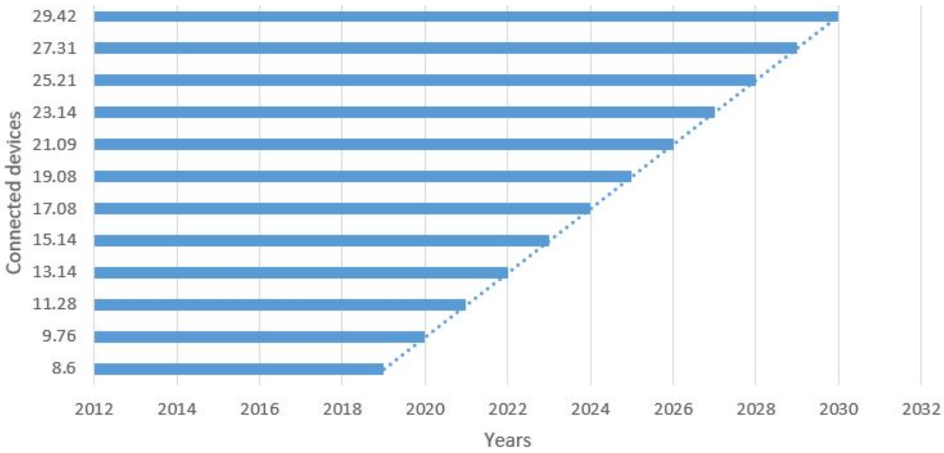


Figure 1: Number of IoT-connected devices worldwide.

## Contribution

- We propose a secure and adaptive network architecture tailored for diabetes-focused healthcare environments, incorporating security mechanisms to ensure confidentiality, integrity, and availability of sensitive medical data.
- We evaluate the network's performance through traffic load simulations to assess scalability, reliability, and operational efficiency.
- We enhance network performance by integrating traffic engineering, Quality of Service (QoS), and intelligent load balancing mechanisms.
- We demonstrate the effectiveness of an IoMT-enabled home network, comprising glucose meters and other diabetes-related devices, for reliable real-time transmission of patient data to healthcare providers.

# 2 Background

This section provides an overview of healthcare systems and pertinent topics. It endeavours to offer a comprehensive background for readers who may not be well-versed in healthcare systems and to make the contents of this paper easily understood.

## 2.1 Healthcare IoT Service

Numerous challenges and complexities confront traditional healthcare systems. It is necessary to provide many services to solve these issues and challenges that face IoT technologies. Figure 2 shows a diagram of the developments of some services for healthcare systems.

- Community Healthcare: Community healthcare services are instrumental in monitoring environmental cleanliness and factors impacting patient health, so governments are interested in reaching these areas, spreading awareness, and providing preventive means.
- Ambient assisted living: Living in suitable environment for the elderly is crucial, so enhancing and using AI facilitates the prediction of serious diseases.
- Semantic medical access: To facilitates the extraction of vast troves of patient-specific health data from the cloud, through which emergency medical services are provided.
- Drug intake monitoring: There are many cases in which errors occur while taking medications, especially among the elderly, so special services have been provided using the Internet of Things technology to solve this problem.
- Children's health information: Comprehensive children's health information encompassing emotional, behavioural, and mental health aspects can be used in education.

## 2.2 Healthcare IoT Generic Architecture

This part reviews the general structure that consists of H-Iot, so it may differ according to researchers in the process of developing H-Iot systems and the purpose of using them. At the beginning of the discussion and before going into the clarification of the H-Iot architecture, it is crucial to clarify the essential difference between healthcare IoT systems and traditional

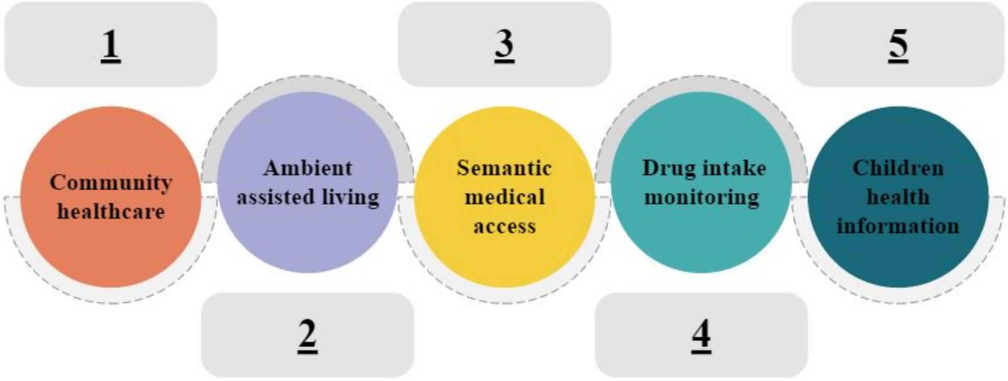


Figure 2: Health-Care IoT Service

IoT systems so that the main difference is wireless network sensors in traditional systems. In contrast, in healthcare systems a wireless network is formed specific to the body. The H-IoT architecture typically comprises four primary layers [21, 8], each serving a distinct function crucial for the system's efficacy as shown in Figure 3:

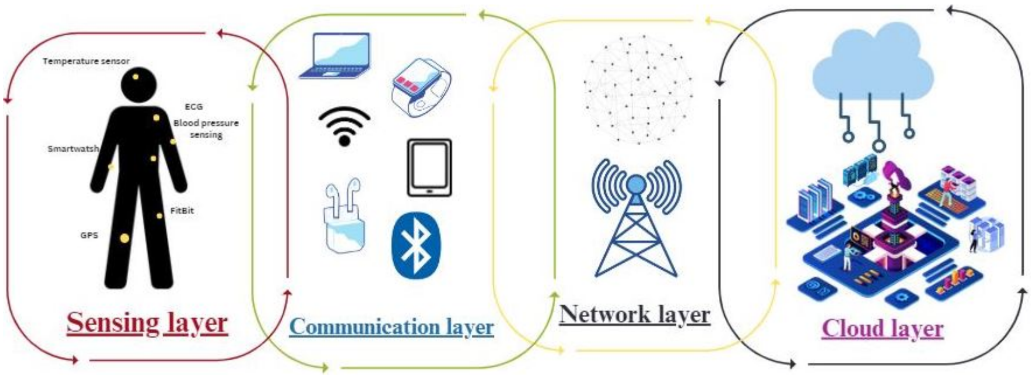


Figure 3: General layers architecture of H-IoT system

- Sensor Layer: The first layer, known as the sensor layer, monitors vital activities within the human body, with recordings transmitted through the communication layer.
- Communication Layer: This layer employs smart devices and protocols to establish connections to the network, facilitating the transmission of data recorded by sensors.
- Network Layer: Acting as an intermediary between sensors and the cloud, the network layer encompasses network devices essential for data transmission and management.
- Cloud Layer: At the pinnacle of the architecture lies the cloud layer, where data collected through H-IoT applications is processed, enabling advanced analytics.

## 2.3 Applications of Healthcare IoT

After identifying the services used in H-IoT, a simple presentation is presented about the applications that are also used in the field of Internet of Things in healthcare so that these applications can be divided into two types: applications that rely on only one standard and applications that depend on a combination of metrics[21]. These types are also summarized in the form of figure 4.

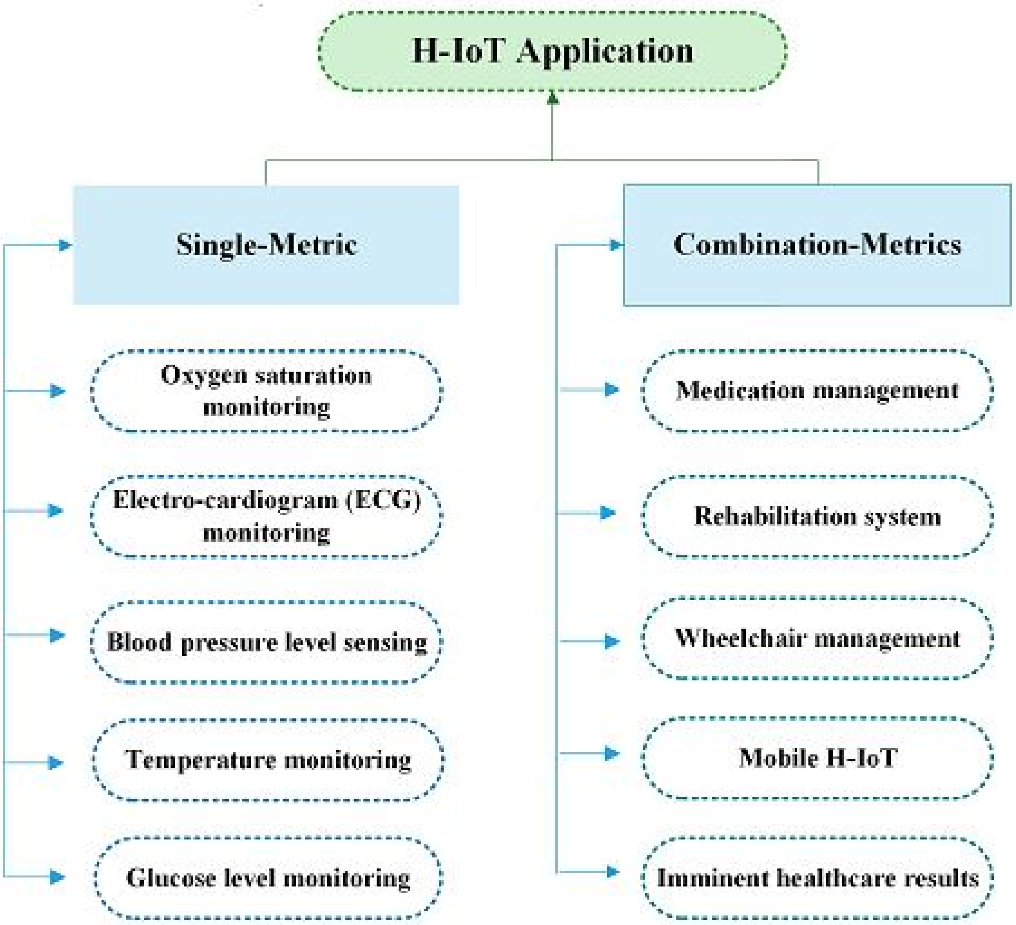


Figure 4: H-IoT Application

- Oxygen saturation monitoring: One of the applications of the Internet of Things used in the field of healthcare systems, which measures the oximetry rate, that is, the level of oxygen saturation in the blood, is monitored continuously.

- Electrocardiogram (ECG) monitoring: It is an application of the Internet of Things used in the field of healthcare, which can be worn for use in monitoring the heart for long periods. It is characterized by being equipped with devices that send and receive measured data with the cloud.

- Blood pressure level sensing: One of the applications used in the Internet of Things through which blood pressure is monitored.

- Temperature monitoring: One of the Internet of Things systems used in the field of measuring body temperature, as it is characterized by being very accurate and effective.

- Glucose level monitoring: The healthcare system relies on Internet of Things devices to measure blood glucose levels, which diabetics, the elderly, and doctors rely on to determine when to take medication, exercises, and activities that patients should do.

- Medication management: One system is based on the AAL system, which addresses the problem of packaging the medications it uses.

- Rehabilitation system: This type of application is done by solving the problem of the shortage of medical staff who work in the field of caring for the elderly and people who suffer from physical and mental illnesses that affect their lifestyle.

- Wheelchair management: It is an Internet of Things application used in the healthcare field through which the wheelchair can be completely automated and controlled.
- Mobile H-IoT: Since the smartphone is one of the most widely used technologies in the current era, its use with the Internet of Things to enhance healthcare applications is significant in terms of chronic disease management, fitness, and hospital records management.
- Imminent healthcare results: In the future, healthcare systems should be widely used to be able to treat many diseases, especially treating skin infections and eye problems and performing surgeries remotely. This explains why significant advances in the Internet of Things have allowed some companies to manufacture portable diagnostic devices with good connectivity.

## 2.4 Diabetes-Mellitus (DM)

Diabetes Mellitus (DM) is a chronic disorder characterized by inadequate insulin production or ineffective insulin utilization by the body, leading to elevated blood glucose levels [2]. Type 1 diabetes results from insufficient insulin production by the pancreas, necessitating external insulin administration, while Type 2 diabetes arises from insulin resistance or deficiency due to dietary factors [2]. Effective management of diabetes is crucial to prevent complications associated with unstable blood sugar levels. This entails adopting a healthy diet, regular exercise, medication adherence, and self-management practices [16]. Proper self-care significantly reduces the risk of coronary heart disease and mortality rates associated with diabetes [27]. Technological advancements play a pivotal role in enhancing self-management strategies, aiming to overcome challenges associated with poor self-care management [14].

## 2.5 Security Requirements for Healthcare Systems

The idea of the Internet of Things used in medical healthcare involves automatic verification and collection of information. Therefore, smart healthcare systems, which enable the Internet of Things, are often used to deal with information and results related to patients. Moreover, this information is considered vulnerable to many malicious attacks if appropriate measures are not taken to secure it in an appropriate and advanced manner[22]. Unfortunately, the smart devices used in healthcare and sensors have low storage capacities and are expensive, in addition to their low processors. Therefore, particular security protocols that support this cannot be integrated or used[28].

Of course, the devices used in the field of health care are mobile and need to connect to a network in general, such as the network used at home or hospitals, etc., Which leads to an increase in its vulnerability and an increase in the number of Internet of Things devices connected. This dynamic design has become unstable from a security standpoint, and providing security is challenging. For example, protecting and preventing the dissemination of patient information to any unauthorized party and not allowing anyone to monitor and process data or even pass it incorrectly, in addition to also preventing the doctor from making mistakes in dealing with the patient if strict safety procedures are available and measures are not imposed. The doctor may make an error. Examples of this include giving a patient an incorrect medication or providing an incorrect prescription. For example, a patient's blood test report may be altered, the patient has an accident, and a blood transfusion is required as table 1. In this case, the patient will be given incompatible blood. Table 1 presents the crucial requirements that need to be considered in the field of IoT-enabled healthcare systems[19].

Table 1: Security Requirements for Healthcare Systems [19]

| **Requirements** | **Description** |
|---|---|
| Confidentiality | Ensuring that data is maintained properly and preventing unauthorized access. |
| Integrity | Preventing modification or alteration of data validity during storage, processing, or exchange. |
| Availability | Ensuring data and services are accessible when needed without delay. |
| Authenticity | Verifying the legitimacy of entities requesting access to or modification of health data. |
| Non-repudiation | Ensuring that users/patients cannot deny actions performed or data submitted. |
| Auditing | Maintaining complete and verifiable records of all transactions and system activities. |
| Ownership | Ensuring health data belongs to a specific party with defined rights and responsibilities. |
| Privacy | Restricting health data visibility to authorized users and approved purposes only. |
| Access Control | Enabling controlled access to health data across both public and private system domains. |
| Data Freshness | Ensuring timely availability of up-to-date data without delay. |
| Anonymity | Preserving privacy by not revealing identities to the public or unauthorized parties. |
| Secure Data Transit | Protecting transferred data against interception, monitoring, or tampering. |

### 2.6 Packet Tracer Network Simulator

The Packet Tracer Network Simulator is a valuable tool utilized in simulation operations within various process areas that replace the practical processes used in real network devices. It enhances practical knowledge of computer networking principles to facilitate learning technical network skills.In addition, it can effectively compare routing protocols, making it a suitable educational tool for both primary and more complex topics in networking fields. The Packet Tracer Network Simulator is considered useful in understanding the basic concepts of the network. Students can design a large network. These physical devices may be difficult to use due to cost. Packet Tracer Network Simulator provides more knowledge about the network concept as practical experiments are easily planned where theoretical concepts are integrated [17].

## 3 Literature Review

Healthcare integrates IoT, driving intelligent medical advancements. Addressing system weaknesses requires ongoing research. This section explores IoT in blood sugar monitoring.

According to [4], they introduced an IoT-based system tailored for diabetic patients centred around an insulin pump. The creation of the healthcare system includes the Secure Hash Algorithm SHA-256, Secure Switch Shell (SSH), Keil LPC-1768 panel, Alaris 8100 infusion pump, and cloud IoT. That information is obtained through the patient, the cloud, hospitals, and legitimate users, where the information is stored after processing in records, through which what is performed by the insulin pump is monitored and controlled so that huge data is shared and protected by a secure cloud. Moreover, this system is considered a reliable model, as it provides characteristics like (availability, Confidentiality, Integrity, Authentication, and Licensing).

In [12], They presented an effective and flexible system for UbD monitoring and prediction based on home-obtained urine samples for early diabetes prediction. Several experimental simulations were conducted on a realistic data set consisting of 4 individuals, and the results demonstrated the proposed system's superiority in decision-making when compared to the latest traditional techniques. Work was done to improve the time delay, classification efficiency, prediction efficiency, reliability and stability. The proposed system consists of 4 primary layers: the layer from which Diabetic Data Acquisition (DDA), the second layer, Diabetic Data Classification (DDC), the diabetes Mining and Extraction (DME) layer, and finally, the Diabetic Prediction and Decision Making layer. (DPDM), in addition to improving the Recurrent Neural Network algorithm (RNN) prediction level.

In ref [25], the researchers presented the unveiling of a Deep Learning (DL) model harnessing cloud computing capabilities, augmented by both RNN and Restricted Boltzmann Machine (RBM) architectures, integrated with IoT technology. The research delves into Continuous Glucose Monitoring (CGM) devices, envisioned for future wearability, enabling real-time blood sugar level monitoring at 5-minute intervals over 30 minutes. Experimental findings underscore the model's adeptness in distinguishing and predicting blood sugar levels with a granularity of 10 samples, demonstrating actionable insights within a 5-minute timeframe for elevated blood sugar conditions. The model yielded an average accuracy value of 15.589, surpassing conventional methods. Leveraging cloud computing, the study highlights virtualization and resource-sharing features, empowering simultaneous service delivery to multiple users.

According to [18], This study includes developing an application for portable smartphones for patients with type 2 diabetes with a feature that allows the application to run based on specific requirements, where Android devices are connected with supporting devices to be used to measure blood sugar levels, such as sensors, belt, treadmills, exercise cycle, in addition to the applications being able to Monitor medications and food intake. This application is designed and layout based on sensors. Based on the results of the analysis, it is clear that this study is based on 3 proposed architectures, which are the proportion of the structure of smartphone applications, the block diagram of the devices, in addition to the sensors through which the functions present in mobile phone applications for diabetics are managed. Finally, 40 samples of diabetic patients who use diabetes-specific applications were used, as these applications are distinguished by their comprehensiveness, ease of use, security, and privacy.

In [13]. They presented a study examining diabetes incidence levels in rural and urban settings using the 5D scale, a metric encompassing five fundamental components of diabetes care. This study showed that rural areas have min achieving goals for the presence of diabetes when compared to other areas, as this is based on a group of factors, which are gender, age, race, (the) degree of confidentiality group, type of medical complications, type of insurance, type of care physician, and type of data used in the end. It can be concluded that rural areas have the worst measure of the quality of diabetes identification. This study was conducted based on 45,279 patients with diabetes, including 54.4% from rural areas and 43.2% from urban areas.

# 4 Methodology

This paper delves into the establishment of high-performance networks tailored for healthcare, with a specific focus on diabetic patients, as they feature high-speed bandwidth and solve the balancer problem of loading using the Cisco Packet Tracer. Initially, it was designed. The network topology consists of applications specific to diabetes patients, such as medicine that is

Table 2: Outline of the Works

| Year | Reference | Applications | Specific Use Cases | Samples | Technology |
|---|---|---|---|---|---|
| 2019 | [4] | Glucose Level | A non-invasive tool that measures blood sugar. | 70 | IoT |
| 2020 | [12] | Glucose Level | An effective at-home (UbD) prediction system. | 4 | IoT |
| 2021 | [25] | Glucose Level | A tool for measuring blood sugar. | 10 | IoT |
| 2022 | [18] | Glucose Level | An application that measures blood sugar. | 40 | IoT |
| 2023 | [13] | Glucose Level | Study evaluating diabetic patients using 5D. | 45,279 | IoT |

responsible for monitoring the patient remotely, electronic health records, and patient network devices that are configured and deployed on diabetes applications using cloud services. Work was done to monitor traffic between different networks under certain conditions. Cisco Packet Tracer will evaluate Network performance and effectiveness and find solutions To optimize the network based on the results obtained, in addition to conducting penetration testing to evaluate weak points in the network in order to provide a practical and effective solution for applications related to diabetes patients and work to improve the performance of operations and patient care in the best possible ways. In this work, the network is designed with a set of fundamental factors, including reliability, traffic monitoring and load balancing to ensure this Improves network performance. The software used Cisco Packet Tracer for network simulation. Efficiently and cost-effectively, create a network on the ground.

## 4.1 Network Design

This section delineates the network design tailored for diabetic systems realized through the utilization of Cisco Packet Tracer software. Various techniques have been used to complete it, such as using cloud services, traffic engineering control, and load balancing. Figure 5 also shows the basic shape of the network and explains the basic parts, which include (Cloud Data Storage service, Smart Balanced-Load, Hospital Network, and Home Network) so that each part is presented and explained in detail in the rest of the research parts. The costs of designing and testing the network infrastructure used by healthcare organizations were taken into account, so Cisco Packet Tracer was used to simulate the network for people with diabetes to determine the effectiveness of this proposal.

## 4.2 Cloud Data Storage service

Utilizing Cisco Packet Tracer software, essential cloud services were created to facilitate the default deployment of system files. Therefore, these files are configured from the special system for people with diabetes to ensure their data safety and security, in addition to working on improving network performance through the use of techniques such as caching and repetition. This part of the work aims to provide a storage service through which large amounts of patient-related data and cases are stored; doctor reports can be stored and accessed easily, quickly and affordably.

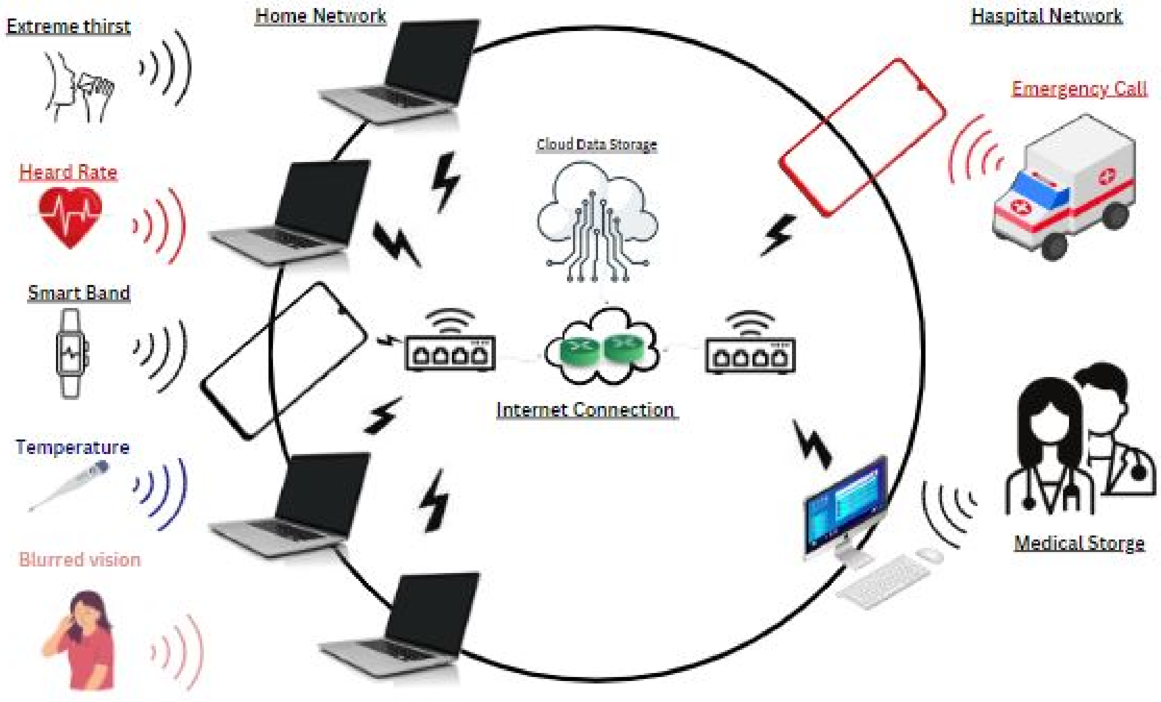


Figure 5: Proposed Network Design.

## 4.3 Smart Balanced-Load

This section elucidates the implementation mechanisms employed to balance loads within the established network, leveraging First Hop Redundancy Protocols ($\text{FHRP}_\text{s}$). This protocol provides a mechanism to ensure error handling for the default gateway in the network. The main purpose of using such a protocol is to address the point of failure if the network is configured with only one active router acting as the default gateway thus using $\text{FHRP}_\text{s}$ allows more than one router to work together at the same time, and also allows another router to take over in the event of Primary router failure.FHRPs consist of several commonly used types:

- FHRPs: This protocol assigns a virtual IP address and MAC address to a group of participating routers in redundancy. These addresses are used as the default gateway for hosts in the network.

- Gateway Load Balancing Protocol GLBP: works on load balancing. In addition to having an active virtual router, GLBP allows multiple routers to share the traffic load by distributing it among themselves. FHRP provides a seamless and transparent way to ensure that if the primary router fails, another router can take over without disrupting the operations of the network. This improves network reliability and reduces downtime due to router failure.

- Election of Active Router: in order to determine the availability of of other router in the group, routers operating within the redundancy framework exchange hello messages on an regular basis. the active router master) are chosen from the group through an election process. traffic forwarding and answering ARP requests for the virtual IP and MAC addresses fall within the purview of the active router.

- Routers that is not chosen to be active routers was designated as standby or backup routers. this routers use hello messages to keep an eye on the health of the active router.

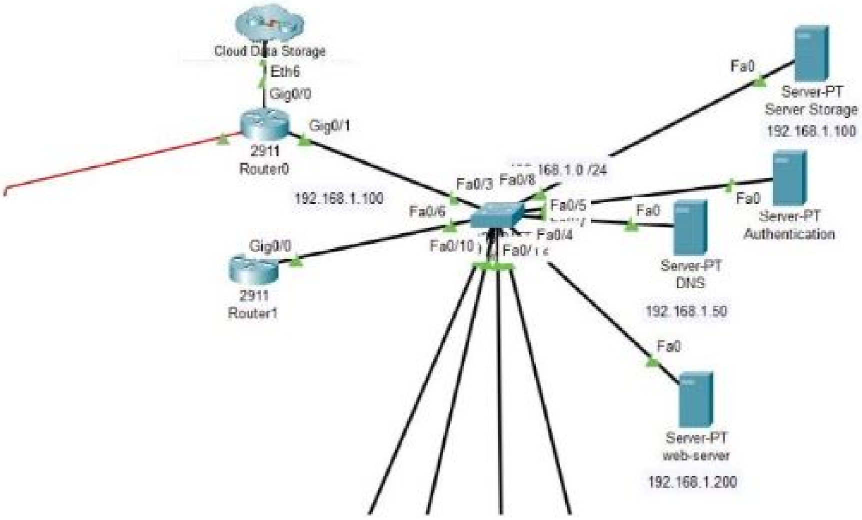


Figure 6: Cloud Data Storage-Service.

one of the standby routers is chosen to take over as the new active router in the event that the active router malfunctions or becomes Unreachable.

- Automatic Failover: the standby router With the highest priority takes over as the the active router in the event that the active router fails. to guarantee Service Continuity, the virtual Ip and MAC addresses are promptly transferred to the new active router. end devices continue to send traffic to the virtual IP address, and this failover process are transparent to them.

FHRPs offer an transparent and easy way to guarantee it another router can take over without interfering With network operation in the event that the primary router fails. this reduce downtime brought on by router failures and improve network reliability. the basic concepts of redundancy and failover was shared by HSRP, VRRP, and GLBP, although the specifics of how FHRPs function may differ slightly between this protocols.

In Cisco devices, the Network Access Control List ACL) [3] are a crucial tool for implementing network access control, particularly in diabetes networks. the movement of data packet that was permitted or prohibited in accordance With an set of particular rules were defined by a access control list (ACL). Security and access control policies can be implemented by applying an Access Control List ACL to network interfaces in switches and routers. an collection of prefix rules that specify which incoming and outgoing packets are accepted or rejected make up an ACL. when setting up an ACL for Cisco devices, the following are essential components: ACLs come in two varietie. there is two primary ways to configure ACLs:

- Standard AcL: governed Solely by source address, Standard AcLs regulate access based solely On IP addresse.

- Extended AXL: Offering more Comprehensive access an Control, extended ACLs consider factors such as Source and destination addresses, transport protocol and port numbers for detailed access Control.

The process typically begins by establishing AcL rules for implementing ACLs. this rules, often prefixed, delineate Which traffic were permitted or Denied. the rules is applied in a specific order and data packets are processed according to the first matching rule. Actions: Specific actions can be assigned to matching rules, such as allowing, blocking, or directing traffic to a specific destination. CL is applied to the designated network interfaces, whether on routers or switches, employing appropriate configuration commands. It is very important to plan and understand the security and configuration requirements of the network well before specifying and implementing the ACL. Configuring an ACL requires experience and a good understanding of the relevant rules and configuration commands in Cisco devices. as shown in Figure7.

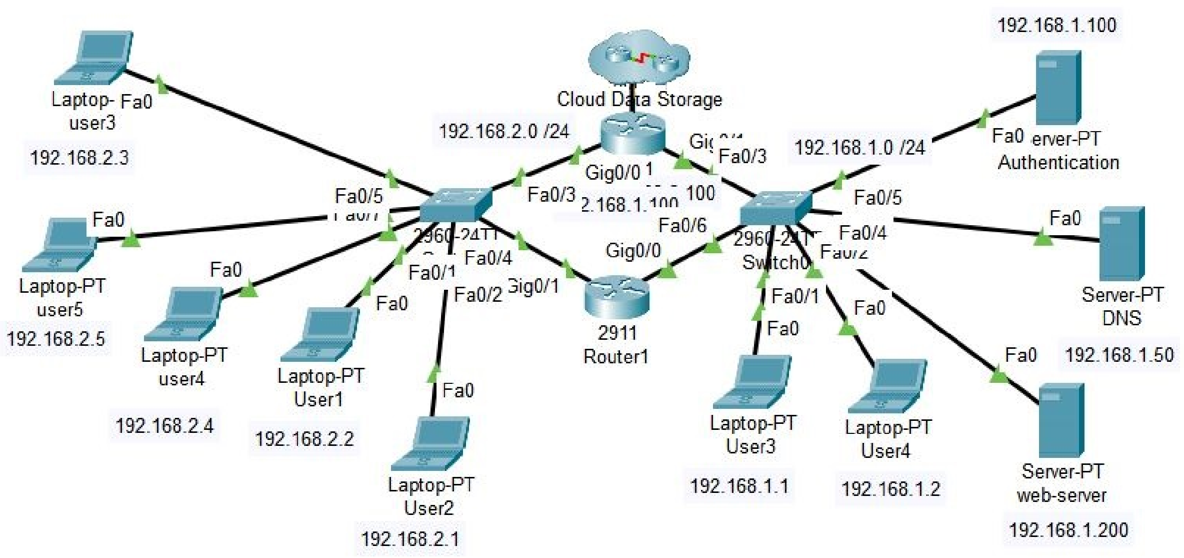


Figure 7: Smart Balanced-Load.

In addition to utilizing the Cisco Access Control Server ACS, a prevalent solution offered by Cisco for managing access and authentication within network architectures, it provides advanced support for the RADIUS service to configure and manage servers. Remote Authentication Dial-In User Service RADIUS it is a system used to verify the identity of users trying to connect to a network remotely. It is commonly used in landline networks, public Internet services, Wi-Fi networks, and virtual access networks (VPNs). A RADIUS server acts as part of the Authentication, Authorization, and User Account (AAA) system [**?** ].

The primary function of a RADIUS server is to validate user identities and grant access to requested services based on predetermined permissions. The server receives authentication requests from clients (such as a laptop or smartphone). It validates user considerations (such as user name and password) using authentication methods supported by Password Authentication Protocol PAP, Challenge Handshake Authentication Protocol CHAP, or Extensible Authentication Protocol EAP. after Successfully verifying the users identity, an response were sent from the the RADIUS server to the client to allow access to the requested Service. the response includes information about the Permissions assigned to the user such as access level, Session duration, and other important parameter.

The ability to offer centralized User authentication and control Over their access to services over an large network were the primary benefit of an RADIUS server. This means that instead of depending on local authentication servers at each site, a single RADIUS server can be used to manage and authenticate users at multiple sites or multiple systems. by offering an unified and centralized method for confirming users identitify and managing their access rights, the RADIUS server generally helps to improve network security and efficient administration. it records events for monitoring and analysis purposes and offers reports and logs regarding network usage.

## 4.4 FHRP Priority Configuration and Failover Experiment

To make the redundancy evaluation reproducible, this section details the FHRP configuration used to control role election and behavior during failover. Two redundant gateway routers were configured in a single FHRP group providing a virtual default gateway for the client LAN. The primary router was assigned a higher FHRP priority to ensure deterministic selection as the active gateway under normal operation, while the secondary router was assigned a lower priority and assumed the gateway role only upon primary failure. Preemption was enabled so that, after recovery, the higher-priority router reclaims the active role and restores the intended steady-state configuration. Failover was emulated by administratively disabling the primary router uplink/interface connected to the client LAN, then monitoring the change in gateway state and verifying continued reachability of core services (DNS and web) through the virtual gateway address.

Table 3: FHRP priority and timer configuration used in the failover experiment.

| **Parameter** | **Primary router** | **Secondary router** | **Purpose in failover evaluation** |
|---|---|---|---|
| FHRP mode | GLBP | GLBP | Provides a virtual default gateway with redundancy and load-sharing behavior. |
| Group ID | 1 | 1 | Ensures both routers participate in the same redundancy group. |
| Virtual IP (gateway) | 192.168.1.254 | 192.168.1.254 | Stable default gateway address used by clients; remains reachable across failover. |
| Priority | 120 | 110 | Deterministic role election: the higher value enforces primary active selection in steady state. |
| Preemption | Enabled | Enabled | After recovery, the primary router (priority 120) reclaims the active role to restore intended operation. |
| Hello / Hold timers | 3 s / 10 s | 3 s / 10 s | Controls detection and transition speed; used consistently across both routers for comparable behavior. |
| Failover trigger | Interface shutdown | N/A | Primary link/interface was administratively disabled to force role transfer to the secondary router. |

## 4.5 Simulation Parameterization and Rationale

To improve reproducibility and ensure that the evaluation aligns with healthcare IoT operational requirements, this study explicitly justifies the simulation parameters used for latency evaluation and traffic-load generation. Latency is treated as a primary QoS indicator because diabetic remote monitoring and alerting depend on timely delivery of measurements and acknowledgments between home devices, the hospital network, and cloud services. In selecting latency thresholds, we follow ITU-T Recommendation G.114 guidance on one-way transmission time planning: delays below 150 ms are generally considered suitable for responsive interactive services, delays in the 150–400 ms range are acceptable with increasing care in network planning, and one-way delay should not exceed 400 ms for general network planning. Accordingly, we define three latency regions for interpreting Packet Tracer measurements: *Target* ($<$ 150 ms one-way), *Acceptable* (150–400 ms one-way), and *Degraded* ($>$ 400 ms one-way). When Packet Tracer reports round-trip delay (ICMP RTT), we interpret the thresholds using an approximate mapping to one-way delay as RTT/2 under near-symmetric paths; therefore, the equivalent RTT boundaries are 300 ms (Target) and 800 ms (upper Acceptable bound).

Traffic-load profiles were designed to reflect a realistic mixture of (i) periodic diabetic sensing telemetry and (ii) concurrent hospital/home operational traffic. For periodic telemetry, we model continuous glucose monitoring (CGM)-like updates as one message every 5 minutes per device, consistent with common CGM reporting intervals. Each telemetry update is represented as a 512-byte UDP packet (application payload plus protocol overhead), which yields a per-device telemetry rate of 13.653 bps. To stress-test the proposed architecture under realistic concurrency, we superimpose two additional traffic classes that commonly coexist in smart-hospital environments: (a) clinician/patient dashboard access (modeled as sustained HTTPS-like sessions) and (b) cloud synchronization/backup flows. Three load levels are evaluated: Low (baseline), Medium (normal), and High (peak), with exact device/session counts and offered rates summarized in Table 5. This design ensures that performance claims (latency, throughput, and reliability) are evaluated under both nominal monitoring conditions and elevated concurrent demand.

Table 4 establishes the latency acceptance framework used to interpret Packet Tracer measurements by mapping ITU-T G.114 one-way planning ranges to RTT-equivalent boundaries (Target: one-way $<$ 150 ms, interpreted as RTT$<$ 300 ms; Acceptable: one-way 150–400 ms, interpreted as RTT 300–800 ms; Degraded: one-way $>$ 400 ms, interpreted as RTT$>$ 800 ms), which provides a clear, standards-aligned basis for judging whether the simulated network can support responsive monitoring, alert propagation, and interactive clinical access. Complementarily, Table 5 defines the exact workload conditions under which this evaluation is performed, keeping the number of active clients fixed at 7 to match the implemented topology while progressively increasing concurrent service demand from Low to High through controlled increments in application traffic: the telemetry component is held constant at 0.000096 Mbps, whereas HTTPS sessions increase from 2 to 5 to 7 sessions at 0.200 Mbps per session, and cloud synchronization increases from one 1.000 Mbps flow to one 2.000 Mbps flow and then to two 3.000 Mbps flows, yielding total offered loads of 1.400096 Mbps, 3.000096 Mbps, and 7.400096 Mbps, respectively. Taken together, these two tables ensure that performance results are both reproducible and meaningfully interpretable: the traffic profiles provide a structured stress progression across baseline, normal, and peak utilization, while the latency-threshold mapping provides an objective criterion to classify the observed RTT behavior as Target, Acceptable, or Degraded under each load condition.

Table 4: Latency thresholds and evaluation interpretation (based on ITU-T G.114 one-way transmission time planning).

| **Category** | **Threshold (One-way)** | **Interpretation in this study (Packet Tracer)** |
|---|---|---|
| Target (Ideal) | $< 150$ ms | Preferred region for responsive monitoring and alert propagation. If RTT is measured, the equivalent RTT target is $< 300$ ms (RTT/2 mapping). |
| Acceptable (Tolerable) | 150–400 ms | Usable but with increasing risk of degraded responsiveness. Equivalent RTT range is 300–800 ms. |
| Degraded | $> 400$ ms | Likely to impair real-time responsiveness and indicates congestion or insufficient capacity. Equivalent RTT is $> 800$ ms. |

Table 5: Traffic-load profiles.

| **Profile** | **Active clients** | **Telemetry rate (Mbps)** | **HTTPS sessions** | **Cloud sync flows** | **Total offered load (Mbps)** |
|---|---|---|---|---|---|
| Low (Baseline) | 7 | 0.000096 | 2 sessions (0.200 Mbps/session) | 1 flow (1.000 Mbps/flow) | 1.400096 |
| Medium (Normal) | 7 | 0.000096 | 5 sessions (0.200 Mbps/session) | 1 flow (2.000 Mbps/flow) | 3.000096 |
| High (Peak) | 7 | 0.000096 | 7 sessions (0.200 Mbps/session) | 2 flows (3.000 Mbps/flow) | 7.400096 |

## 4.6 Hospital Network

This section outlines the proposed hospital design aimed at monitoring diabetes patients, comprising several components, including remote physician monitoring, electronic health records for patients, and information reporting systems. The hospital network includes routers and switches, such as shown in figure 8 below to ensure that the connection is valid and secure. We use a private server For applications for diabetics within cloud services and to improve network performance a set of techniques mentioned previously were used. To provide the use of storage services with the ability to store and retrieve diabetes data efficiently and at the lowest possible cost.

## 4.7 Home Network

This section details the design of the home network tailored for diabetic patients, featuring IoT devices ($\mathrm{IoT_D}$), as illustrated in Figure 9. The home network, which consists of $\mathrm{IoT_D}$, allows for monitoring patients remotely, assessing the patient's condition, and repeatedly taking the patient's readings to ensure that they are transferred to the specialist doctor by following up on the patient's condition. In addition, it is ensured that the home network provides real-time patient data for appropriate patient monitoring and care.

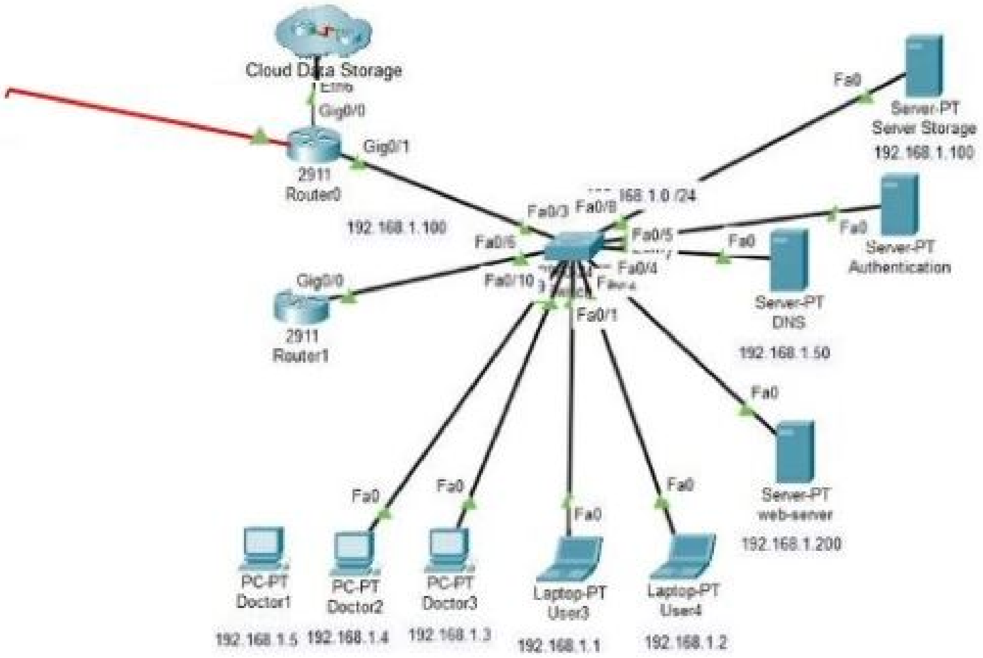


Figure 8: Hospital Network.

## 4.8 Validation of Simulation Outcomes Beyond Packet Tracer Outputs

To strengthen credibility beyond relying exclusively on Packet Tracer-generated counters, the simulation outcomes were validated through a set of independent checks that confirm correctness, consistency, and repeatability of the observed behavior. First, an internal-consistency validation was applied by comparing measured throughput against the configured offered load in Table 5; achieved throughput was required to remain bounded by the offered demand and by the nominal link capacity, ensuring that reported rates are physically plausible and not artifacts of measurement. In parallel, RTT measurements were checked for path plausibility given the implemented topology (two LAN segments connected via a router) by verifying that latency remained within a stable LAN-scale range under Low/Medium/High profiles and did not exhibit non-physical discontinuities inconsistent with the configured routing path.

Second, repeatability validation was performed by executing each traffic profile multiple times under identical configuration and recording the mean and maximum RTT values as well as throughput, then confirming that the results remained stable across runs and that the same trend (increasing RTT with increasing load) was consistently reproduced. This procedure reduces the risk of reporting single-run anomalies and supports the use of the reported values as representative performance indicators for each profile.

Third, functional scenario validation was conducted to confirm that the simulated services and security controls operate as intended. Service-level checks included DNS resolution success (client-to-DNS server queries), web service reachability (client-to-web server application sessions), and authentication/service accessibility consistent with the configured network policies. Security enforcement was validated using controlled access attempts in which permitted

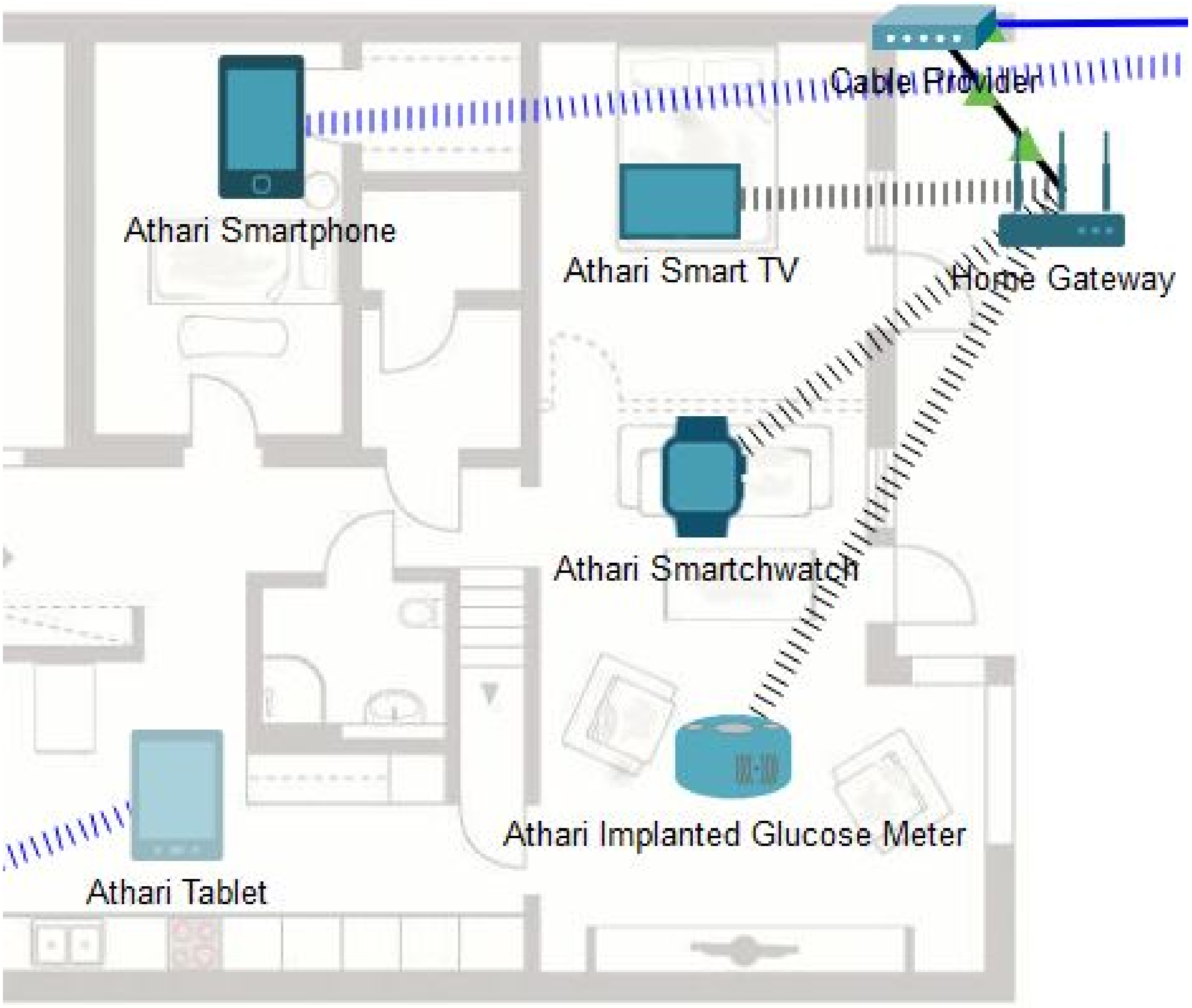


Figure 9: Home Network[15].

traffic flows were verified as successful while unauthorized flows were verified as blocked according to the implemented ACL policies. Together, these checks ensure that the reported latency/throughput metrics correspond to correct end-to-end service behavior under policy enforcement rather than isolated packet-level effects.

Table 6 summarizes the validation strategy used to substantiate the simulation outcomes beyond simply reading Packet Tracer counters, ensuring that the reported performance results are both plausible and operationally meaningful. The internal-consistency checks constrain the measurements to physically realizable bounds by requiring achieved throughput to remain below the configured offered load in Table 5 and below nominal link capacity, while also confirming that RTT values are consistent with the modeled path (two /24 LANs interconnected by a router) and do not exhibit non-physical discontinuities across profiles. Repeatability validation strengthens reliability by re-running Low/Medium/High conditions under identical configurations and verifying stable mean and maximum RTT and throughput trends, reducing the likelihood that the reported metrics reflect a single-run anomaly. In parallel, functional service validation demonstrates that the measured latency/throughput correspond to successful end-to-end operation of the intended healthcare services (DNS resolution and web-based monitoring sessions) under increasing utilization, rather than isolated packet-level artifacts. Finally, the policy/security enforcement validation confirms that performance measurements were obtained while the access-control posture remains active, by verifying that permitted flows are consistently allowed and unauthorized flows are consistently blocked in accordance with the implemented ACL rules. Collectively, these checks provide a structured and auditable validation layer that links the quantitative metrics to correct service behavior and policy compliance under the defined traffic-load profiles.

Table 6: Validation procedures applied to confirm simulation outcomes beyond Packet Tracer outputs.

| **Validation dimension** | **Procedure** | **Acceptance criterion** |
|---|---|---|
| Internal consistency | Cross-check achieved throughput against the configured offered load in Table 5 and against nominal link capacity; verify that latency values are plausible for the implemented path (two /24 LANs interconnected by a router). | Throughput must not exceed offered load or link capacity; RTT must remain within a stable LAN-scale range and show no non-physical discontinuities across profiles. |
| Repeatability | Re-run each Low/Medium/High profile under identical configuration and record mean RTT, maximum RTT, and throughput for each run; compare across runs. | Consistent ordering and trend across profiles (Low < Medium < High in RTT) and stable metrics across repeated runs without anomalous outliers. |
| Functional service validation | Verify DNS resolution (client-to-DNS queries), web service reachability (client-to-web application sessions), and end-to-end connectivity across both LANs under each profile. | All required services must remain reachable and operational under Low/Medium/High conditions; service sessions must complete successfully. |
| Policy/security enforcement | Execute controlled access attempts for permitted and non-permitted flows according to the implemented ACL rules; confirm expected allow/deny behavior. | Permitted traffic must pass; unauthorized traffic must be blocked consistently with the ACL policy. |

## 4.9 Penetration Testing Methodology (Attack Types and Evaluation Metrics)

To strengthen the security evaluation, we conducted a structured penetration testing campaign that validates whether the proposed network configuration enforces access-control policies and preserves service continuity under adversarial conditions. The tests were designed to reflect realistic threats in smart healthcare networks, focusing on attempts to (i) discover exposed services, (ii) access restricted resources, (iii) violate segmentation policies, and (iv) degrade availability. Because the study is implemented in Packet Tracer, attacks were emulated as controlled traffic scenarios and policy-violation attempts at the network and transport layers (rather than exploit-specific payload delivery), allowing repeatable verification of ACL enforcement, gateway behavior, and service reachability. Each test followed the same procedure: (1) baseline verification of normal connectivity and services (DNS resolution, web access, and permitted client-to-server paths), (2) controlled generation of attack traffic or unauthorized flow attempts from a designated "attacker" host, (3) monitoring of whether the traffic was blocked/allowed consistent with the configured policies, and (4) post-test verification that authorized services remain reachable and stable. The evaluation explicitly separates security effectiveness (policy enforcement) from operational impact (performance degradation under attack). We quantify security effectiveness using policy-centric metrics: the *Attack-Blocking Rate* (ABR), defined as the fraction of attack attempts that are blocked by the security controls; *Authorized-Pass Rate* (APR), defined as the fraction of legitimate flows that remain allowed under test conditions; and *Service Availability* (SA), defined as the fraction of time critical services (DNS and web monitoring) remain reachable during each test. To capture operational impact, we compute performance deltas relative to baseline for each profile: ΔRTT (increase in mean RTT) and ΔThroughput (throughput reduction). These metrics provide a quantitative basis to assess whether the network remains both secure and usable under stress.

Table 7: Penetration testing campaign: attack categories, objective, and quantitative metrics.

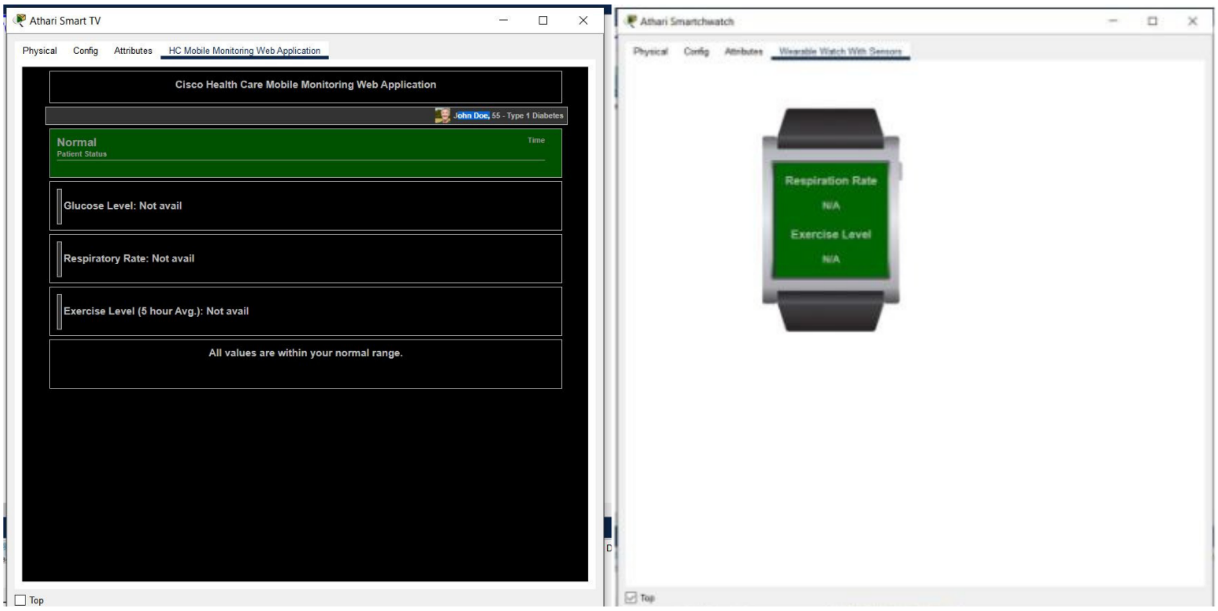
| **Attack category** | **Emulated test objective** | **Metrics recorded** |
|---|---|---|
| Reconnaissance / service discovery | Probe for unnecessary exposed services and verify segmentation boundaries (only intended ports/services reachable). | ABR; APR; SA (DNS/web reachability); number of reachable services consistent with policy. |
| Unauthorized access attempts | Attempt to reach restricted servers/subnets from a non-permitted host (policy-violation flows). | ABR (blocked attempts/total); false-allow count; APR for legitimate users under the same load. |
| Segmentation policy violation | Attempt lateral movement between LAN segments that should be isolated by ACLs. | ABR; policy compliance rate (unauthorized blocked / authorized allowed). |
| Spoofing-style manipulation (network-level) | Emulate identity/route manipulation attempts as unauthorized traffic patterns to test whether ACLs prevent illicit flows. | ABR; SA; ΔRTT; ΔThroughput relative to baseline. |
| DoS-style stress / flooding | Increase request rate toward critical services to evaluate resilience and service continuity under stress. | SA; ΔRTT; ΔThroughput; dropped/blocked traffic ratio where observable. |

# 5 Results Discussion

This section presents the outcomes derived from implementing a healthcare network, particularly tailored for diabetic care, within Cisco Packet Tracer, where the network performance was evaluated according to certain metrics such as simulating network traffic loads to test the scalability and reliability of the network. network. The results showed that the proposed network design has high speed. Where it provides (high-speed connectivity, low latency, and high throughput), are essential for diabetes care applications specifically measuring blood glucose levels, monitoring respiratory rate, and many others.

Moreover, the utilization of cloud storage ensures efficient data storage and retrieval while adhering to data security and regulatory requirements. Security measures, including access control to ensure data confidentiality, integrity and availability. The patient's network performance was evaluated by simulating different traffic loads. Network performance is optimized using techniques such as traffic engineering and intelligent load balancing.

The analysis of the network demonstrated its ability to provide a secure and flexible connection, which leads to easy monitoring of patients.The home network makes it easier for a patient to monitor and manage his data, thus reducing the patient's need for personal visits to the doctor, as the home network was formed from connected blood glucose measuring devices Wirelessly with computers, smart watches, or mobile devices.As shown in the figure 10, it displays some remote monitoring results.



Cisco Health Care Mobile Monitoring Web Application

John Doe, 55 - Type 1 Diabetes

Normal
Patient Status

Glucose Level: Not avail

Respiratory Rate: Not avail

Exercise Level (5 hour Avg.): Not avail

All values are within your normal range.

Respiration Rate
N/A
Exercise Level
N/A

Figure 10: Remote Monitoring.

The numerical results in Table 8 show an consistent and ontrolled performance response as offered load increases from 1.400096 Mbps (Low to 3.000096 Mbps (Medium) and 7.400096 Mbps (High. Mean RTT rise from 12 ms to 18 ms and then to 32 ms, which translate to estimated one-way delays of 6 ms, 9 ms, and 16 ms, respectively. even at the highest load, the mean RTT of 32 ms remains far below the Target RTT boundary of 300 ms in Table 4, leaving a margin of 268 ms to the Target upper bound and 768 ms to the Acceptable upper bound of 800 ms. This margin indicate that the topology has substantial headroom for time-sensitive monitoring, authentication exchanges, and service access within the tested operating range.

Beyond averages, the maximum RTT values provide evidence about tail behavior and transient congestion under load. the maximum RTT increase from 20 ms (Low to 30 ms (Medium) and 55 ms (High. the mean-to-maximum spread therefore change from 8 ms to 12 ms to 23 ms, while this max-to-mean ratio decline slightly from 1.67 (20/12 to 1.67 (30/18) and 1.72 (55/32), indicating that peak delays remain bounded and do not diverge disproportionately as utilization increases. thes maximum one-way delay estimate remain limited to 10 ms, 15 ms, and 27.5 ms across Low/Medium/High. this are a important operational signal: when real-time monitoring was combined with control-plane operations such as DNS resolution and authentication/authorization, worst-case delay spikes are often more disruptive than mean latency; here, this Observed maxima remain tightly controlled even at 7.400096 Mbps.

Throughput behavior further support the absence of congestion collapse and confirm that the network were delivering traffic close to the offered demand. Achieved throughput was 1.37 Mbps under 1.400096 Mbps offered load, 2.94 Mbps under 3.000096 Mbps offered load, and 7.15 Mbps under 7.400096 Mbps offered load. in absolute terms, the throughput gaps are 0.030096 Mbps, 0.060096 Mbps, and 0.250096 Mbps, respectively. As a fraction of offered load, this delivery efficiencies are 97.85% (1.37/1.400096, 97.99% (2.94/3.000096), and 96.62% (7.15/7.400096. The slight efficiency reduction at the highest profile were consistent with increased protocol overhead and contention on shared links; however, the achieved throughput remain above 7 Mbps while mean RTT stay at 32 ms, indicating that the system was operating in a regime of controlled queuing rather than sustained saturation. this coupled outcome (high throughput with low RTT) was a strong indicator that QoS objectives are being met simultaneously rather than trading throughput for latency.

Taken together, the latency and throughput figures confirm that the topology remains stable across the full tested load envelope and that increasing utilization produces predictable, bounded performance changes. When moving from Low to High, offered load increases by a factor of 5.285 (7.400096/1.400096), while mean RTT increases by a factor of 2.667 (32/12) and maximum RTT by a factor of 2.750 (55/20). This sublinear growth in delay relative to load indicates that buffering and scheduling are not being overwhelmed and that the architecture maintains operational robustness as demand scales within the evaluated range. Importantly, all three profiles are classified as Target in the latency status column, which is consistent with the very large absolute separation between observed RTT values (12–55 ms) and the threshold boundaries (300 ms and 800 ms). Therefore, the results provide quantitative evidence that the proposed configuration can support concurrent healthcare-relevant services (authentication, naming, and web-based monitoring) with reliable responsiveness, even under peak utilization represented by 7.400096 Mbps.

Table 8: Latency and throughput measured under the topology-aligned traffic profiles in Table 5.

| **Profile** | **Offered load (Mbps)** | **Mean RTT (ms)** | **Max RTT (ms)** | **One-way delay (ms)** | **Throughput (Mbps)** | **Latency status** |
|---|---|---|---|---|---|---|
| Low | 1.400096 | 12 | 20 | 6 | 1.37 | Target |
| Medium | 3.000096 | 18 | 30 | 9 | 2.94 | Target |
| High | 7.400096 | 32 | 55 | 16 | 7.15 | Target |

The trend in Figure 11 provides a clear visual confirmation of the table-based findings and highlights the stability of latency scaling as load increases. Mean RTT increases monotonically from 12 ms at 1.400096 Mbps to 18 ms at 3.000096 Mbps and 32 ms at 7.400096 Mbps, with absolute increments of 6 ms (Low→Medium) and 14 ms (Medium→High). The slope of RTT growth remains moderate: the mean RTT increases by 6 ms while offered load increases by 1.600000 Mbps (1.400096→3.000096), and then increases by 14 ms while offered load increases by 4.400000 Mbps (3.000096→7.400096). The absence of abrupt jumps, oscillations, or sharp curvature indicates that the topology is not entering a congestion-dominated regime within the tested range; instead, delay increases are consistent with gradual queue formation and additional processing under higher concurrency. Consequently, the plot reinforces that the network maintains low-latency operation with predictable performance degradation as utilization rises,

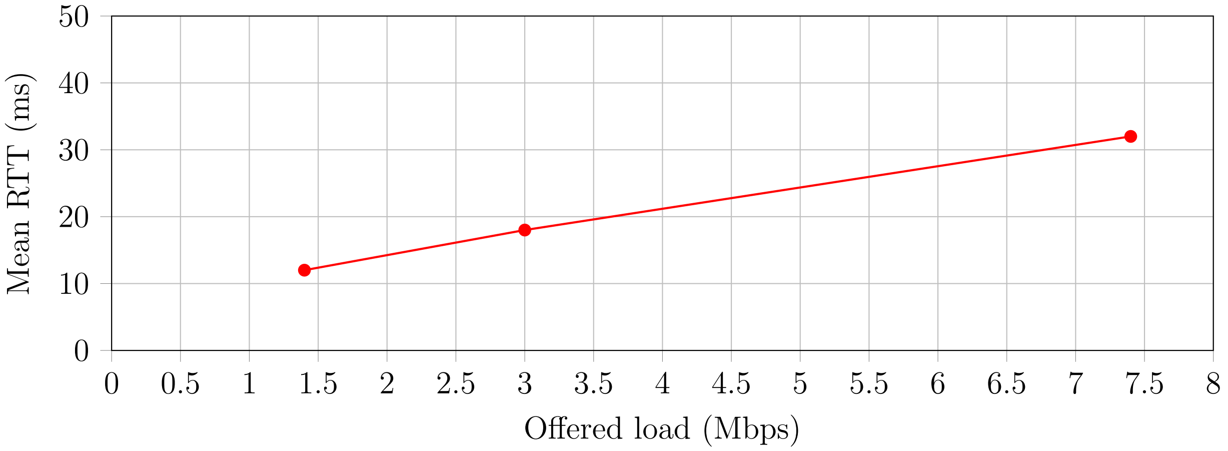


Figure 11: Mean RTT versus offered load for the Low/Medium/High profiles in Table 5.

which is an essential property for smart healthcare monitoring networks that must remain responsive under fluctuating demand.

## 5.1 Scalability Considerations Under Heavier Real-World Loads

While the simulation topology contains a limited number of endpoints for controlled experimentation, the performance trends provide insight into scalability behavior under heavier real-world loads. The results show that as offered load increases from 1.400096 Mbps to 7.400096 Mbps, mean RTT remains within a low and stable range (12–32 ms) and throughput remains close to the configured demand (1.37–7.15 Mbps), indicating that the design operates with non-saturated links and predictable queuing behavior within the tested envelope. For larger deployments with higher concurrency, scalability can be achieved by expanding the addressing and segmentation model (multiple VLANs/subnets instead of a single /24 per domain), and by distributing device populations across hierarchical access layers (home gateways, ward-level aggregation, and hospital distribution/core) to avoid broadcast-domain growth and localized bottlenecks.

From a capacity planning perspective, heavier loads primarily stress shared uplinks (hospital-to-cloud connectivity and inter-segment routing points). As the number of monitoring endpoints and interactive sessions increases, maintaining service quality requires upgrading uplink bandwidth, applying QoS to prioritize medical telemetry and authentication/control traffic over bulk synchronization flows, and scaling service infrastructure (DNS, AAA, and web applications) via replication or cloud-based elasticity to prevent server-side saturation from becoming the dominant source of latency. In addition, gateway redundancy remains scalable when FHRP is combined with consistent priority planning and preemption; however, under larger loads, failover behavior should be re-evaluated under peak utilization to ensure that role transition does not coincide with transient congestion. Overall, the proposed architecture is scalable by design through segmentation expansion, bandwidth provisioning, QoS differentiation, and tiered service distribution, and these practical measures are now explicitly discussed to bridge the controlled simulation to real-world hospital and home-network deployments.

## 5.2 Comparative analysis

This section provides a meticulous investigation of previous research related to the domain of healthcare network design for diabetic monitoring and compares them with our proposed work.

Table 9 provides a comprehensive comparison of previous works with our work.

Table 9: Comparison of Previous Works with Our Work

| Reference | Focus of Study | Methodology | Key Findings | Technological Components | Research Gap |
|---|---|---|---|---|---|
| [4] | IoT-based system for diabetic care | Creation of a healthcare system including insulin pump monitoring | Reliable model ensuring availability, confidentiality, integrity, authentication, and licensing | SHA-256, SSH, Keil LPC-1768 panel, Alaris 8100 infusion pump, cloud IoT | Limited emphasis on scalability and interoperability of the IoT-based system |
| [12] | UbD monitoring and prediction for early diabetes detection | Experimental simulations to improve prediction efficiency | Improved decision-making vs. traditional techniques; reduced time delay; higher classification efficiency and reliability | DDA, DDC, DME, DPDM layers; RNN | Limited focus on real-world implementation and validation |
| [25] | DL model with cloud computing for continuous glucose monitoring | DL-based modeling with experimental evaluation | Accurate blood sugar prediction and real-time monitoring; reported average accuracy value of 15.589; cloud-enabled virtualization/resource sharing | RNN, RBM, CGM devices, cloud computing | Limited exploration of security vulnerabilities and data privacy issues |
| [18] | Smartphone application for type 2 diabetes management | Application architecture analysis and device integration | Comprehensive and user-friendly diabetes application with security and privacy considerations | Smartphone sensors, device integration | Limited discussion of usability and adoption challenges |

Continued on next page

| Reference | Focus of Study | Methodology | Key Findings | Technological Components | Research Gap |
|---|---|---|---|---|---|
| [13] | Diabetes incidence disparities (rural vs. urban) | 5D scale-based study and factor analysis | Rural areas show lower achievement in diabetes care goals and weaker diabetes identification quality | 5D scale metrics | Limited investigation of underlying socio-economic drivers of disparities |
| **Our Work** | Healthcare network for diabetic monitoring | Cisco Packet Tracer-based network design and simulation | Efficient, reliable, and secure network supporting real-time monitoring and data storage | Cisco Packet Tracer, cloud services, IoT devices | Remaining gaps: scalability stress-testing, interoperability assessment, and real-world deployment validation |

A number of research projects in healthcare network design for diabetic monitoring was shown in Table 9, Which highlight various approache and technological framework. common theme emerge even though each study offer an different approach, such as IoT-based insulin pump systems, predictive analytics based on urine samples, and deep learning models integrated with Cloud computing. this include a emphasis on data security, predictive modeling, and real-time monitoring. our suggested work offers improvements in patient care and network efficiency, which is consistent with these themes. we can find opportunitie and synergies for improving diabetic monitoring networks by evaluating the advantages and disadvantages Of previous research projects in addition to our suggested framework. this will ultimately improve the standard of patient care in this crucial area.

# 6 Conclusions

In this research, a network was designed that works in the field of health care and serves diabetic application activities using the Cisco Packet Tracer program. This study looked at many different factors, including network topology, security, reliability, and others. A network has been formed that ensures access to and use of services efficiently, effectively, reliably and securely through the use of appropriate equipment and appropriate software in the design process, allowing specialists in the field of diabetes care to provide the best possible care by taking advantage of the flexibility of the network designed using Cisco Packet Tracer software. Although it has many limitations, it is a useful tool for educational simulation and network performance evaluation. It allows network engineers to reduce costs when the network is controlled and designed as best as possible before implementing it in real environments.

## Compliance with ethical standards

**Conflict of Interest:** The authors declare that there is no conflict of interest regarding the publication of this paper.
**Ethical approval:** This article does not contain any studies with human participants or animals performed by any of the authors.
**Informed consent:** Informed consent was obtained from all individual participants included in the study.
**Data availability statements:** Data is available from the authors upon reasonable request.
**Author Contributions:** All authors contribute equally.
**Acknowledgment:** The authurs would like to thank Gulf University for Science and Technology for supporting this project.

## References

[1] Number of connected IoT devices worldwide from 2019-2023, with forecasts from 2022-2030 in billions. `//https://www.statista.com`, 2023. [Online website].

[2] Mary D Adu, Usman H Malabu, Aduli EO Malau-Aduli, and Bunmi S Malau-Aduli. The development of my care hub mobile-phone app to support self-management in australians with type 1 or type 2 diabetes. *Scientific reports*, 10(1):7, 2020.

[3] Dino Pandu Agustio and Esron Rikardo Nainggolan. Penerapan virtual local area network pada jaringan man dengan metode filtering berbasis access control list di dinas komunikasi dan informatika kota serang. *Jurnal Komputer Antartika*, 1(1):32–38, 2023.

[4] Zeyad A Al-Odat, Sudarshan K Srinivasan, Eman M Al-Qtiemat, and Sana Shuja. A reliable iot-based embedded health care system for diabetic patients. *arXiv preprint arXiv:1908.06086*, 2019.

[5] Mahmoud Aljamal, Ala Mughaid, Rabee Alquran, Muder Almiani, and Shadi AlZu'bi. Simulated model for preventing iot fake clients over the smart cities environment. In *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pages 0757–0761. IEEE, 2023.

[6] Majd Abu AlShieh, Muder Almiani, Walid Al-Qerem, Abdel Qader Al Bawab, and Shadi AlZu'Bi. Prompt engineering for enhancing clinical pharmacy decision support through llms. In *2025 2nd International Generative AI and Computational Language Modelling Conference (GACLM)*, pages 115–119. IEEE, 2025.

[7] Hamed Altalhoni, Noraida Haji Ali, Farizah Yunus, Saleh Atiewi, Amal Alshardan, Muder Almiani, and Shadi AlZu'bi. A novel artificial intelligence based dynamic task scheduling and load awareness. *Cluster Computing*, 29(3), 2026.

[8] Shadi Alzu'bi and Ala Mughaid. From chatbots to agentic ai: Digital agents transforming fintech. In *2025 4th International Conference on Computing, Management and Telecommunications (ComManTel)*, pages 82–88. IEEE, 2025.

[9] Shadi Alzu'bi, Basem Alokush, Leila Jamel, Fahd N Al-Wesabi, and Randa Allafi. Simulation based sustainable optimization in edge–fog–cloud energy systems. *Simulation Modelling Practice and Theory*, page 103237, 2025.

[10] Shadi Alzu'bi, Tarek Kanan, Mohammed Elbes, Ghassan Kanaan, and Issam Trrad. Energy-efficient edge deployment of generative ai models using federated learning. *Cluster computing*, 28(5):315, 2025.

[11] Elisa Bertino and Nayeem Islam. Botnets and internet of things security. *Computer*, 50 (2):76–79, 2017.

[12] Munish Bhatia, Simranpreet Kaur, Sandeep K Sood, and Veerawali Behal. Internet of things-inspired healthcare system for urine-based diabetes prediction. *Artificial Intelligence in Medicine*, 107:101913, 2020.

[13] Randy Foss, Karen Fischer, Michelle A Lampman, Susan Laabs, Michael Halasy, Summer V Allen, Gregory M Garrison, Gerald Sobolik, Matthew Bernard, Jessica Sosso, et al. Disparities in diabetes care: differences between rural and urban patients within a large health system. *The Annals of Family Medicine*, 21(3):234–239, 2023.

[14] Kasun C Gunawardena, Renee Jackson, Iva Robinett, Lahiru Dhaniska, Shaluka Jayamanne, Sumedha Kalpani, and Dimuthu Muthukuda. The influence of the smart glucose manager mobile application on diabetes management. *Journal of diabetes science and technology*, 13(1):75–81, 2019.

[15] RL Hemanth Kumar, N Varsha, and Nagaraja GS. High speed network design for health care application services via cloud based services.

[16] Bernhard Höll, Stephan Spat, Johannes Plank, Lukas Schaupp, Katharina Neubauer, Peter Beck, Franco Chiarugi, Vasilis Kontogiannis, Thomas R Pieber, and Andreas Holzinger. Design of a mobile, safety-critical in-patient glucose management system. In *User Centred Networked Health Care*, pages 950–954. IOS Press, 2011.

[17] Maizatul Akmam Binti Ismail. Effectiveness of using cisco packet tracer as learning tools for network fundamentals course during the covid-19 pandemic.

[18] Salaki Reynaldo Joshua, Wasim Abbas, and Je-Hoon Lee. M-healthcare model: An architecture for a type 2 diabetes mellitus mobile application. *Applied Sciences*, 13(1):8, 2022.

[19] Farrukh Aslam Khan, Nur Al Hasan Haldar, Aftab Ali, Mohsin Iftikhar, Tanveer A Zia, and Albert Y Zomaya. A continuous change detection mechanism to identify anomalies in ecg signals for wban-based healthcare environments. *IEEE Access*, 5:13531–13544, 2017.

[20] Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine, and Rachid Benlamri. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied sciences*, 9(9):1736, 2019.

[21] Sreelakshmi Krishnamoorthy, Amit Dua, and Shashank Gupta. Role of emerging technologies in future iot-driven healthcare 4.0 technologies: A survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing*, 14(1):361–407, 2023.

[22] Zakaria Maamar, Ejub Kajan, Muhammad Asim, and Thar Baker Shamsa. Open challenges in vetting the internet-of-things. *Internet Technology Letters*, 2(5):e129, 2019.

[23] Ala Mughaid, Mohammad AlJamal, AL-Aiash Issa, Mahmoud AlJamal, Rabee Alquran, Shadi AlZu'bi, and Ala A Abutabanjeh. Enhancing cybersecurity in scada iot systems: A novel machine learning-based approach for man-in-the-middle attack detection. In *2023 3rd Intelligent Cybersecurity Conference (ICSC)*, pages 74–79. IEEE, 2023.

[24] Ala Mughaid, Ali Alqahtani, Shadi AlZu'bi, Ibrahim Obaidat, Rabee Alqura'n, Mahmoud AlJamal, and Raid AL-Marayah. Utilizing machine learning algorithms for effectively detection iot ddos attacks. In *International Conference on Advances in Computing Research*, pages 617–629. Springer, 2023.

[25] Ahmed R Nasser, Ahmed M Hasan, Amjad J Humaidi, Ahmed Alkhayyat, Laith Alzubaidi, Mohammed A Fadhel, José Santamaría, and Ye Duan. Iot and cloud computing in healthcare: A new wearable device and cloud-based deep learning algorithm for monitoring of diabetes. *Electronics*, 10(21):2719, 2021.

[26] Jianbing Ni, Kuan Zhang, Xiaodong Lin, and Xuemin Shen. Securing fog computing for internet of things applications: Challenges and solutions. *IEEE Communications Surveys & Tutorials*, 20(1):601–628, 2017.

[27] Emmanouil G Spanakis, Franco Chiarugi, Angelina Kouroubali, Stephan Spat, Peter Beck, Stefan Asanin, Peter Rosengren, Tamas Gergely, and Jesper Thestrup. Diabetes management using modern information and communication technologies and new care models. *Interactive journal of medical research*, 1(2):e2193, 2012.

[28] Noshina Tariq, Muhammad Asim, Zakaria Maamar, M Zubair Farooqi, Noura Faci, and Thar Baker. A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered iot. *Journal of Parallel and Distributed Computing*, 134:198–206, 2019.

[29] Prabal Verma and Sandeep K Sood. Fog assisted-iot enabled patient health monitoring in smart homes. *IEEE Internet of Things Journal*, 5(3):1789–1796, 2018.

[30] Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. Iot security techniques based on machine learning: How do iot devices use ai to enhance security? *IEEE Signal Processing Magazine*, 35(5):41–49, 2018.

[31] Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of things Journal*, 6(2):1606–1616, 2018.