Available online at www.qu.edu.iq/journalcm

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)

# Development a Software Defined Network (SDN) with Internet of Things (IoT) Security for Medical Issues

*Ahmed Shihab Ahmed* [a], *Hussein Ali Salah* [b*]

[a] *Department of Basic Sciences, College of Nursing, University of Baghdad, IRAQ, , Email: ahmedshihabinfo@conursing.uobaghdad.edu.iq*

[b,*] *Department of Computer Systems, Technical Institute- Suwaira, Middle Technical University, IRAQ, , Email: hussein_tech@mtu.edu.iq;*

ARTICLE INFO

*Article history:*
Received: 10 /06/2023
Rrevised form: 30 /07/2023
Accepted : 02 /08/2023
Available online: 30 /09/2023

*Keywords:*

IoT Internet of Things
software defined networking
Medical networks
network security
Healthcare systems

ABSTRACT

Because providing billions of objects with network connectivity, the Internet of Things (IoT) enables the collection and transfer of real-time data for intelligent applications. Therefore, IoT enables remote access and control of connected devices when there is a sufficient network infrastructure. Additionally, the introduction of software-defined networking (SDN) presents capabilities that allow internet providers and users to control and connect network equipment wirelessly, even as enabling a global perspective on the network, that has previously become a soaring interest area due to its extensive use for various applications and systems, including wireless sensor nodes, medical equipment, delicate home sensor systems, and some other connected IoT devices. In order to create worldwide connectivity between the Internet of Things (IoT) and based on the SDN architecture in the medical contexts, this paper's contribution is to outline some relevant directions. Additionally, we provide a model based on software defined network principles that depicts interactions between a group of people each of whom have a Nano network within their bodies and the medical services via the local network of a medical institution. For everybody electrical engineers to data engineers the requirement to integrate everything in a global setting is a significant problem. As a result, the cloud is useful for handling the instantaneous sharing of information. In terms of health care, the effort is also stated in terms of IoT architecture and services. IoT's current prospects for the healthcare sector are quite promising. Due to its capacity for sensing and measuring, it is also highly well-liked. From the smallest sensor to the massive amounts of data gathered, this revolution is completely changing how we view healthcare.

MSC.

https://doi.org/ 10.29304/jqcm.2023.15.3.1268

## 1. Introduction

The (IoT) Internet of Things have advanced rapidly in recent years, convincing some who were first dubious of the technology as it was just beginning to take off over and over again. Applications for the Internet of Things today include monitoring environmental conditions, both in locally relevant areas and at the urban scale, as well as monitoring and automatic data collecting from a variety of sensors in the electricity and water sectors. An entire class of networks, including ad hoc networks, wireless sensor systems, etc., were created as a result of the construction of connectivity and the accompanying methods for communication between nodes.

[*] **Hussein Ali Salah**[b,*]

Email addresses: hussein_tech@mtu.edu.iq

Communicated by 'sub etitor'

Advance detection can prevent many crises that are brought on by human activity or unusual natural events (Floods, hurricanes, earthquakes, etc.) Furthermore, a new path for IoT development recently emerged within the scope of all these applications connected to the idea of the IoT, realizing the so-called Smart Devices. The transition to a Nano world [1].

The network of things has many uses in the medical industry, including remote monitoring, cutting-edge sensors, and the coordination of therapeutic devices. It may help keep patients healthy and safe while also enhancing how doctors communicate. Human resources IoT can help patients feel more engaged and satisfied by enabling them to spend more time working with their doctors. The development of digital physical smart unavoidable systems is seriously hampered by the Internet of Things (IoT), which gives rise to strong objections. There are several applications for the IoT, including healthcare. With bright mechanical, economical, and social prospects, the IoT uprising is revolutionizing the current medical services [2].

Numerous healing applications, such as mobile healthcare evaluation, exercise programs, never-ending illnesses, and elder care, may find growth with the IoT. Another crucial potential use is to continue receiving treatment and prescriptions at home from social insurance providers. In this sense, various medicinal devices, sensors, and analytic and Viewing imaging devices is possible as intelligent devices or items that IoT's fundamental components. Social insurance services powered by the Internet of Things are anticipated to lower costs, improve client involvement, and boost happiness levels. The Internet of Things (IoT) may decrease device downtime through distant setting, according to providers of medical services. Additionally, the IoT is capable of accurately identifying the best conditions for recharging different devices' batteries to ensure continuous and smooth operation. Additionally, by verifying their optimal use and the care of more people, the IoT enables the efficient use of limited resources. [3].

Applications for medical networks and Nano-networks focus primarily on the analysis of the body and the localization of potential anomalies (problems) through communication between the framework for managing fundamental healthcare services of the human body and the corresponding actuators realized as components of Nano machines. By putting these mechanisms in place, epidemics of all kinds can be prevented as well as the early detection of threats to the body. Naturally, there are numerous problems regarding how to organize the secured these connections and how to uphold the principle of a patient's personal autonomy private life because this notion is still in its infancy. The interaction between Nano things and things in the actual world at the level of network architecture, algorithms, and protocols. In generally, the evolution of this idea can be broken down into a number of abstract layers of interactions, each of which has a defined interface. This research focuses on the investigation of the viability of processing Nano machine-generated traffic both in low-traffic systems and traditional connections under excessive bandwidth utilization [4,5,6].

Through 2020, Cisco Systems predicts that there will be 50 billion Internet-connected devices, and it is anticipated that a large number of physical items, including computers and detector controllers, will have individual locations and the ability to securely transfer data, ranging from daily routines to private healthcare data. The Internet of Things (IoT) is a technology that provides a framework for all these physical things with intelligent devices to be coherently connected and enables them to interact, experience, or interact with the physical world as well as with one another [7]. The term "Internet of Things" (IoT) refers to a concept that connects everyone, everything, everywhere, at any time, with any service, over any network [8]. Healthcare is one of the most alluring IoT application areas since it offers us the chance to use several uses in medicine for chronic illnesses, exercise regimens, and health monitoring, and senior care [9].

Software-defined networking (SDN), a novel idea, is put out as an alternative to conventional networks. Communication network can now be autonomous of traditional equipment because of a brand-new type of network architecture called SDN [10]. The main objective of the SDN is to separate the control and data planes including the set to transform. As an outcome, the hardware objects are able to instantly construct appropriate control logic in line with software requirements. Infrastructure, control, and application make up the three levels that make up SDN in general [11]. There is numerous application program interfaces (APIs) northbound, southbound, eastbound, and westbound in addition to the layer-wise design of SDN. The application layer and the control layer are connected via the northbound API so that they can communicate with one another. The application layer is also given access to the network's abstracted view via the northbound API. In order for controllers to install various rules in forwarding devices like routers and switches and for those devices to be able to interact with the controller in real-time, the southbound API is in charge of bridging the gap between the control and infrastructure levels.

The easterly and westerly APIs are in charge of interacting with various controllers so they can make decisions in unison. The most popular protocol for facilitating communication across the control and data planes is Open Flow.

The internet of things (IoT), which is currently undergoing rapid technical development, enables various objects, including sensor nodes, embedded systems, and intermediary devices, to gather and share data in the near future in order to realize the goals of a completely linked world. In order to overcome some of the major problems that wireless networks face, the authors highlighted the use of the SDN concept [12]. SDN in the context of IoT presents a variety of opportunities and problems, and research has shown that SDN-based technologies will significantly affect IoT to make sure it succeeds in a networked world [13].

In recent years, the Internet of Things (IoT) health-based framework has grown significantly in terms of consumers, services, and applications across numerous academic fields. As a result, a large or restricted region seems to distrust hundreds of wireless gadgets. SDN was considered to be a good candidate to handle this enormous number of wireless users in order to deliver a more effective network. After being presented for the medical context, a distinctive SDN algorithm is constructed and incorporated into an Internet of Health Things (IoHT) framework. As a brand-new responsive interconnect method based on adaptively choosing between the already-used Go-Back-N and Selected Repeat strategies, the innovative algorithm known as adaptive switching (AS) is proposed. The throughput performance of wireless body sensor decentralized control in hospital-based healthcare applications is examined. For e-health services, a new model for the SDN-driven Internet of Things is suggested. since the SDN is thought to be a good option for regulating such a network because it clearly distinguishes between the control plane and the data plane [14,15].

The main contributions of this article are as follows:

- The suggested framework combines SDN with security in IoT medical systems from a multifaceted historical viewpoint. In IoT healthcare systems, SDN and security are discussed separately in the current studies and multi-dimensional data is not taken into account.
- We suggest a lightweight authentication strategy to protect the IoT-enabled healthcare system. The server authenticates wearable and IoT devices using this method. These devices share data with the servers after authentication.
- The suggested architecture enables collaboration across servers to address real-time and high-bandwidth challenges in terms of load balancing and effective network utilization with the aid of SDN controller, overcoming the limitations of a single server.
- The SDN controller is set up to send the crucial data on schedule in order to utilize network resources efficiently.
- Lastly, we run comprehensive to assess how well the suggested architecture performs. The results show that the suggested framework performs better with regard to average response time, packet delivery ratio, average delay, throughput, and control overhead, thus offering a superior solution for SDN computing in an IoT-enabled medical system.

The organization of this manuscript is as the following. Section 2 discussed the relevant related work. In section 3 discuss the SDN and IoT. Section 4 describe the benefits of IoT in healthcare. In section 5 we present the proposed model. Section 6 describes the experimental analyses. Section 7 illustrates the conclusions.

## 2. Related Work

The Internet of Things (IoT) is a system of intelligent, resource-limited devices that can perceive and process data. It links a sizable number of heterogeneous networks and smart sensing things, or things. There are many applications for IoT, including smart grid, smart home, smart health, etc. In various nations where healthcare facility pilot projects are being examined, the idea of smart healthcare has developed [16]. The security of IoT devices and the data they generate is crucial in IoT-enabled healthcare systems, and edge computing is a potential architecture that can address their computational and processing issues. By increasing the connection and calculation IoT system efficiency in a medical environment, Data processing can deliver fast data services and is cost-effective. Edge computing powered by SDN is useful for making the most of IoT devices' meager resources. These low-powered gadgets, together with the data they are connected to (private, sensitive patient data), are vulnerable to a number of security risks.

In order to implement Health insurance system using IoT and SDN-based Edge computing, the authors created a safe framework. The Edge servers of the proposed framework use a simple authentication technique to verify the IoT devices' authenticity. These devices capture patient data after authentication and transfer it to the edge servers for archiving, processing, and analysis. An SDN controller that manages the healthcare system's load balancing, network optimization, and effective resource usage is connected to the Edge servers. The suggested framework is assessed using simulations that are run on computers. The outcomes show that the suggested framework offers superior IoT-enabled healthcare system solutions [17].

In the context of the (IoT), internet connectivity has been expanded Besides common electronics like desktops, laptops, cellphones, and iPad, to any variety of traditionally dormant or internet-incompatible physical technologies and everyday objects. IoT has largely taken over the industrial sector in recent years, particularly in automation and control [18,19]. IoT is also applicable to other significant industries, particularly the health sector, since it presents several chances to enhance health services and also empowers medical professionals (such as doctors and nurses) to base their judgments on accurate data. Several additional health applications are offered by the IoT with the express purpose of tracking patient development and giving physicians information to aid in decision-making. Based on a thorough review of prior material, this report presents IoT health problems and future potential. Examining the findings reveals that several health-related services are still in need of further development. Interestingly, there is little literature on these services and little information on the application of IoT in the health sector. This work makes an effort to fill the knowledge vacuum in the IoT healthcare industry, and it also offers intriguing suggestions for future studies on the application of patient data [20].

Given the increasing growth of the Internet of Things, developing an IoT architecture that supports control instructions and device access is both a fascinating and challenging research field (IoT). The improvement of a methodical framework for remotely (re)programming a variety of IoT frameworks poses difficult technical problems in terms of interoperability, scalability, and adaptability. The IoT network architecture has recently been thought of as needing a solution based on (SDN) technologies. The authors begin by reviewing the most cutting-edge SDN remedies and ongoing work on remotely (re)programming IoT devices [21]. The recent study out present state-of-the-art systems on Application technologies and over-the-air (OTA) reprogramming strategies in IoT devices as well as highlights the current issues that promote conducting more and more suitable strategies to meet the needs of the future Internet. The SDIoT reprogramming (SD-IoTR) framework is then put forth. Based on SDN architecture, the proposed SD-IoTR framework places a strong emphasis on OTA programming IoT systems. The dynamic adaptation and scalability requirements for this system are considerable. Two case studies are additionally provided as proofs-of-concept to demonstrate the viability of using the suggested framework for actual installations [22].

The applications of the (IoTs) in the healthcare fields are the main focus of this study. The medical field of health care includes a variety of skilled doctors who provide patient care. As technology advances daily, internet-based technology will manage health care, and doctors will be able to take advantage of their patients at anytime and anyplace. Patients' chances of survival will increase thanks to this IoT technology, and the cloud is becoming an essential component of everyone's daily lives. As a result, the cloud is useful for handling the instantaneous sharing of information. In terms of health care, the effort is also stated in terms of IoT architecture and services [23].

This study provides an outline of certain IoT's effects on the healthcare industry. Medical care must adhere to this framework given the rise of IoT technologies. The purpose of this study is to provide guidelines for achieving worldwide connectivity between medical environments and the (IoT). The necessity to integrate everyone in a global setting is a significant issue for everyone (from electrical engineers to data engineers). From the smallest sensor to the massive amounts of data amassed, this transformation is revolutionizing the way we view healthcare [24].

IoT's support for the healthcare sector are quite promising. Due to its capacity for sensing and measuring, it is also highly well-liked. We have narrowband Internet of Things in low energy version (NB IoT). Due of its low energy consumption, it is preferred in the healthcare industry. Several plans exist for implementing NB IoT in the medical care industry. The NB IoT has been formalized and is completely compatible with LTE and other cellular technologies. NB IoT is an excellent option for applications relating to healthcare in the present day. The largest concerns to NB IoT, meanwhile, are protection precautions and additional framework challenges. It might be among the most appropriate. and well-liked strategies for implementing medical care in low power vast areas if these problems and difficulties are adequately resolved. These are the primary problems and difficulties now existing in the NB IoT regime, according to the authors of this study. They also offer some suggested fixes for these issues [25].

The authors [26] discussed how novel advancements, such as big data, contextual knowledge, and wearables, can be used in a healthcare setting, addressed various IoT and eHealth arrangements and directions around the world to decide how they can encourage economies and social orders to the greatest extent possible improvement, and provided some avenues for future research on IoT-construct human services. According to author [27], exciting new applications of Internet of Things (IoT) technology are emerging, particularly in the field of human services, where their combined effects might improve patients' well-being while resolving the issue of scarce resources. The authors discuss some of the most promising uses of IoT in social insurance as well as the formidable challenges that lie ahead. The paper [28] describes the design and implementation of a clever framework for checking wellbeing. Here, a patient can be checked using a collection of small, wearable sensor hubs for continuous detection and analysis of several important health parameters. It is possible to gather record and decipher information thanks to the devices' constant data accumulation, sharing, and storing.

The authors in [29] introduced a WBSN framework for the healthcare paradigm that is built on the SDN paradigm and uses a unique energy-aware routing algorithm. As a result, an innovative energy-aware routing algorithm is developed and implemented for the e-healthcare sector together with a WBSN architecture built on the SDN method. The software-defined WBAN (SDWBAN) framework presented by [30] incorporates SDN technology into WBAN applications.

The IoT applications in the e-healthcare sectors are examined and provided in [31], demonstrating the intelligentization trend of upcoming research in IoT-based e-healthcare approaches.

[32] addresses and studies the impact of Choosing a power source and a packet size on the operation of a wireless medium-based e-healthcare IoT system. The paper proposes three protocols: a global link decision, an efficacy and package size option, and a power level decision. In [33], a brand-new, smart hospital system that is IoT-aware is unveiled. The suggested system is successful in managing emergency situations. For IoT researchers and developers, interoperability has been a significant hurdle. However, in [34], an IoT-based paradigm for semantic interoperability is put forth, allowing semantic interoperability for heterogeneous IoT devices. Due to the semantic interpretation and meaningful communication of the acquired data, doctors are able to interact with their patients.

The "EdgeSDNI4COVID" architecture was proposed in [17] for the intelligent and effective management of the smart industry during COVID-19 taking into account the IoT networks. The authors also provided the data, control, and application layers that are SDN-enabled, allowing for efficient and automatic monitoring of the IoT data from a distance. Additionally, an effective control mechanism for handling the data from IoT sensors is provided by the proposed convergence of SDN and NFV. Additionally, it gives the tools needed for Industry 4.0 throughout the COVID-19 epidemic, as well as strong data integration on the surface. The study supported the aforementioned contributions with specific performance assessments based on the right simulation process and conditions [17].

## 3. SDN and IoT

### *3.1. Internet of Things*

Internet connectivity numbers in the billions. According to Gartner [35], who estimates that 8.4 billion systems were persistently online and connected expanding. Due to the Internet of Things (IoT) idea, which appears to be the foundation of the connected world of the future, this number climbed by 2.5 times during the following two years. According to Gartner, there will be 20.4 billion Internet-connected IoT devices by the end of 2020 [35]. The (IoT) is a new model for communication that involves connecting current items and giving them more intelligence. Through the internet, these gadgets process the data that has been felt and talk to other gadgets [36], [37]. First, Bluetooth and ZigBee technologies were used to operate IoT devices in the unlicensed spectrum. IoT implementation currently uses 4G and 5G mobile networks. In addition to these devices' short-range transmission limitations, the IoT gadgets have clogged up the unlicensed airwaves. It has thus given the research community access to a variety of research concerns and opportunities. For instance, IoT devices can take advantage of opportunities to use wireless medium by utilizing cognitive radio ideas (CR). Since a CR may use the wireless medium when it's available, IoT devices will be appropriate for long-range applications. Another unexplored topic is the idea of Licensed Spectrum Access (LSA), which is how the CR concept is implemented in 5G. In this way, IoT applications are being used in a wide range of industries, which presents a number of issues, such as ensuring the security and privacy of IoT networks and equipment.

### *3.2. Security in The (IoT)*

IoT devices with limited resources are susceptible to a variety of threats that have a negative impact on their performance. Standard encryption technologies do not function well to secure IoT-enabled networks, leading to significant security challenges [38], [39]. Each of the three IoT layers—the perception layer, the network layer, and the application layer is susceptible to security risks. These dangers can come from both inside and outside the network and can be either aggressive or passive. However, Denial of service (DoS) attacks and sybil are more hazardous since they exhaust the resources of the device and the network [40]. IoT architecture based on cloud-fog technology that utilizes various cloud and fog properties. For efficient resource usage, they have put forth a data offloading technique that is both economical and energy-efficient [41].

An overview of SDN, its structure, and how it interacts with the Internet of Things (SDN). The Internet of Things (IoT) is a term coined by the International Telecommunication Union (ITU) to describe a collection of physical or digital devices that may be recognized and connected into communication networks. Then a real-world illustration was provided. IoT technology makes it possible for regular physical objects to communicate online, allowing them to be aware of distant events or respond to a situation that they are unable to physically detect. Compared to individual portable devices, IoT has less computational power, bandwidth, and volatile memory. Therefore, connecting to a Cloud Infrastructure or Cloud Network may be essential for extra data processing. IoT functions are enabled by three key components:

- Hardware is a network of interconnected items and equipment with smart wearables.
- Software: A software used to collect, store, transport, process, and give instructions to equipment.
- Data communication: the technologies and protocols used to communicate data [42].

The majority of Internet of Things (IoT) devices have an uncomplicated design that is based on the notion that they may be utilized quickly and easily or that conventional devices can be made into IoT by adding Internet service. Sometimes, non-visible elements like security and stability are ignored in the rush to release a product [43]. It is clear that when developing IoT devices, from the platforms to the hardware/software modules, safety issues are not always taken into consideration. Security specialists claim that modern IoT devices depend on cloud services for transmission, which is recognized to have system vulnerabilities and might leave IoT applications open to attack. The most of (IoT) products run on insecure, newly developed platforms. Many IoT devices lack the capacity to upgrade their hardware and software, which makes the problem worse and leaves them very vulnerable to future faults and attacks [44,45]. The two primary types of IoT attacks on the architect layers and threats against the data phases [46].

The fact that content and data on traditional internet are produced by human activities is another difference between IoT and old internet. The Internet of Things (IoT) is a network of connected devices that regularly produce and collect data (sensors, actuators). Machines do not lie, even though they can be programmed to send or receive misleading information. The OWASP (2018) Internet of Things Project has compiled a list of the top 10 security concerns with IoT devices [47]:

1. Passwords that are easily guessable or hardcoded.
2. Services on unsecured networks.
3. ecosystem interfaces that lack security.
4. Insufficient safe updating mechanisms.
5. Utilization of outmoded or insecure components.
6. inadequate privacy safeguards.
7. Unsafe secure data and transmission.
8. Insufficient system design.
9. standard configurations that are unsafe.
10. Physical adaptation is insufficient.

### *3.3. Applications of Internet of Things*

Everyday items like baby monitors, smartphones, speech devices, and smart freezers are a few instances of IoT. Additional examples include less resource-intensive, more sophisticated devices like self-driving cars and wireless body sensor networks (WBAN) and medical wireless sensor networks (MWSN). Simply put, Figure 1 demonstrates that IoT-connected devices can be found not just in our houses, places of employment, streets, neighborhoods, and cities, but also in our bodies.

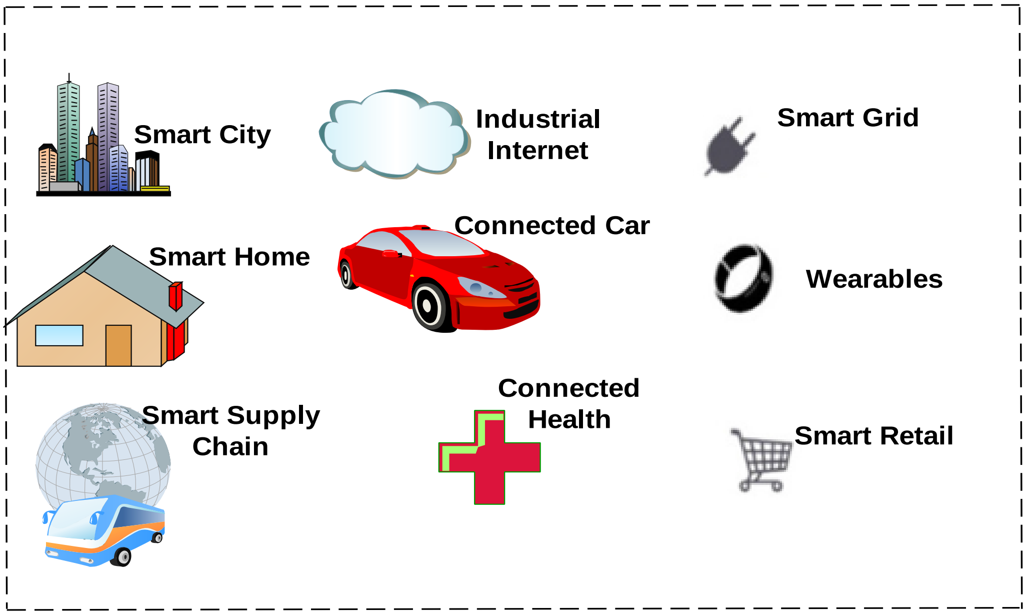

**Fig. 1 - Demonstrates that IoT-connected devices can be found not just in our houses, places of employment, streets, neighborhoods, and cities.**

Even while IoT is crucial to our daily lives now, it is clear that IoT utilization will be essential to the development of technology in the years to come [48]. According to a recent forecast, Figure 1. There will be over 80.45 billion linked devices worldwide in 2030. Unfortunately, security sometimes takes a backseat as businesses race to create new IoT devices with innovative uses. Businesses could employ outdated security requirements [49].

### *3.4. Architecture of Internet of Things*

For an IoT network, there isn't yet an official standard architecture or design. However, the IoT network may be separated into four primary levels (Table 1) depending on the data flow and various functions:

1. Detection and perspective layer.
2. Networking/transport layer.
3. Service/management layer.
4. Application/interface layer [50,51].

**Table 1 - IoT network layers.**

| Layer Function | Layer Function |
|---|---|
| Application, interface layer | Presentation and user involvement |
| Service, management layer | Business software |
| Networking, transport layer | processing and analysis of data |
| Detection and perspective layer | Information generation and transfer through wired or wireless networks Integration of hardware |

Perception nodes and networks are part of the layer for perception, sensing, and data collection. Access network, core network, and LAN are only a few of the sub-layers that make up the networking/transport layer. Data is collected at the application/interface layer and processed and evaluated at the service/management layer. In order to facilitate decision-making, processed information is consumed and presented in business applications [50, 51].

### *3.5. Software Defined Networking (SDN)*

An approach to network design known as SDN places programmable switches between the networking devices to enable the control and administration of diversified communication. SDN is a good substitute for conventional networks for a number of factors. First of all, because traditional networks depend on physical equipment like switches and routers for their infrastructure, they have some speed and maneuverability restrictions. SDN, however, may be virtually governed via the control plane because it is software-based. The software of SDN can be quickly and readily adjusted as needed rather than having fixed functions. Second, the routers in conventional networks need sophisticated algorithms to figure out where to send the packets. In SDN, the controller interacts with the network devices to manage data packet centrally in compliance with settings [52,53].

The fundamental objective of (SDN) is to isolate control instructions from routing operations, or the control and data planes, separately [54]. In SDN, every networking component transfers packets of data in accordance with the rules that have been designed for that device. The control plane is in charge of establishing the guidelines for network devices and regulating network activity. In particular, Cloud technology, automation, control devices, and the Internet of Things benefit most from the SDN's ability to streamline control and management [55]. The number of heterogeneous devices connected to the internet has increased exponentially as a result of these technologies [56, [57]. Furthermore, protection management of the SDN is a serious difficulty that poses security threats, especially with the introduction of IoT that connects heterogeneous devices with their various access protocols. Due to its single point of failure, the SDN technology's conceptually centrally controlled logic also presents a number of challenges. [58], [59]. It continues to be the key barrier that might destabilize the entire network and expose it to numerous known and unknown security threats and assaults. The most glaring difficulty for the industry and academia in SDN is security because it is still in its infancy [60].

Software-defined network (SDN) is regarded as a promising idea for the next-generation network design among the profusion of networking technologies. SDN-based solutions are particularly helpful in the IoT, which comprises of billions of connected equipments, to meet its requirements for variable programmability, availability, and portability [61]. An up-to-date report that SDN-based solutions can meet a number of important needs for IoT applications, encompassing resource use, energy generation, safety, and confidentiality as well as network administration and module of an application. Under these circumstances, network management is very challenging due to the intricate design and broad variety of IoT devices. Many SDN-related academics have recently invested a lot of time in designing and developing an appropriate SDN-based architecture for successfully managing the IoT network [62].

## 4. Benefits of IoT in Healthcare

Using IoT in healthcare has a number of advantages across a variety of use cases, including:

### *4.1. Patient satisfaction involvement*

Patients can participate more actively in their healthcare journey thanks to the IoT. The way patients obtain data is changing, in addition to how devices are developing to better fulfill the requirements of far observation (smaller form factors, less weight, etc.). Via applications and software, patients may now follow their progress and evaluate the impact of the healthcare system on their health [63].

### *4.2. Best results for patients*

The IoT gives physicians access to real-time patient data, empowering them to make wise decisions and thus provide better care. Everyone benefits when a healthcare professional can quickly diagnose a patient using evidence. The advantage: Patients who can be followed remotely can avoid going to the doctor, staying in the hospital, and being readmitted [64].

### *4.3. Reduction of mistakes*

Error rates decrease when data is automatically collected and transferred through automated workflows as opposed to human gathering and reporting [65].

### *4.4. Better outcome for the patient*

The requirements of the patient always should appear firstly because they are focus of healthcare. By providing quick diagnosis, improved accuracy, proactive therapies, and superior therapeutic outcomes, the IoT contributes to enhancing that experience. However, the IoT can be challenging, particularly in the healthcare industry where the need to improve patient outcomes ranks right up there with security and privacy concerns. The security of the data being captured and transferred is highlighted by the sorts of remote monitoring situations previously outlined. From the device, via the network, and to the receiving end, security must be prioritized from beginning to end. In order to create the best IoT experiences for healthcare practitioners and patients that are the appropriate fit and at the right cost, Numerous healthcare providers appoint to focus on medical safety as one of their primary priorities while using third-party controlled IoT internet services. A managed IoT services provider can evaluate a healthcare business holistically to decide the best course of action, including device management, connection, network management, deployment, and logistics. Security is given top attention across all devices and networks thanks to this end-to-end strategy. As a result, healthcare organizations are experiencing improved business agility, decreased cost and risk, and higher security in addition to better outcomes for patients [65].

### *4.5. Healthcare Security*

The (IoT) is transforming the medical industry. However, both clinical engineering and business technology struggle with security. Furthermore, these smart gadgets could be connected to global information networks to deliver for 24/7 access. As a result, hackers could have their sights set on the IoT healthcare arena. In order to encourage the full adoption of IoT in the healthcare domain, it is critical to identify and evaluate certain areas of IoT safety and privacy, including security demands, vulnerabilities, threat models, and countermeasures [66].

#### *4.5.1. Protection Factors*

Security requirements for IoT-based healthcare systems are equivalent to those in traditional communications contexts. In order to achieve secure services, consideration must be given to the following security standards [67].

- **Security -** The privacy of medical information guarantees that illegitimate users cannot access it.
- **Preservation -** Supports complete data integrity while data is being transferred between devices.
- **Verification -** Verification - When talking with peers, Authentication is checked.
- **Accessibility -** Whether local, regional, or cloud-based, all IoT medical services must be reachable to authorized individuals when required, including during denial-of-service assaults.
- **Data novelty -** Data integrity is made up of key novelty and data freshness. Each communication needs to be fresh due to the fact that each Smart healthcare network provides a few time-varying measures [67].
- **Non-Repudiation -** A node cannot retract a message it has already sent, according to non-repudiation.
- **Permission -** Approval makes sure that only nodes that have been given permission can access network resources or services.
- **Reliability -**: A security plan should still shield the network, equipment, and data from an attempt even if certain linked health devices are compromised.
- **Safety policy -** A safety policy should continue to offer the necessary security services even in the event of a malfunction (e.g., a software glitch, a device compromise, or a device failure).
- **Personality -** In an IoT healthcare network, a medical device could malfunction or run out of power. Then, the rest of the devices should enable a basic level of security.
- **Protected net boot -**: Using encryption keys produced digital signatures, the validity and integrity of the software on the device are checked when it is powered on for the first time.
- **Accessibility -** Accessibility is when many elements work together to deliver the intended service at the appropriate moment.
- **Security concerns -** are a must due to the network's flow of sensitive data.

### *4.5.2. Safety Issues*

IoT must overcome new obstacles in order to meet its security requirements because they cannot be met by existing security measures. The features for IoT security are listed in the items that follow.

- **Limitations of data processing**: IoT medical devices come with low-speed CPUs. The central processor (CPU) of such devices is not extremely powerful in terms of speed. Additionally, these gadgets are not designed to handle computationally demanding tasks. They merely act as a detector or an operator, in other words. It is quite challenging to find a security solution that maximizes security performance while using fewer resources.
- **Memory Restrictions**: Most IoT healthcare products have a little amount of memory. To activate such devices, system software, an application binary, and an embedded operating system (OS) are used. They might not have adequate memory as a result to perform intricate security procedures.
- **Energy Restrictions**: Small medical devices with low battery life are typically part of an IoT healthcare network (e.g., body temperature and BP sensors). When there is no need to report sensor readings, these devices save energy by activating the power saving mode. Additionally, if there are no vital tasks to be completed, they run at a low CPU speed.
- **Mobility**: Most medical devices are accessible rather than stationary. These devices are linked to the Internet through IoT internet services. For instance, a wearable heart monitor or body temperature sensor may be connected to the Internet and alert the user's worried caregiver of their circumstances.
- **Extensibility:** The gradual advancement of IoT devices has led to an increase in the number of devices being associated to the global data network. As a result, it is challenging to create a highly expandable safety system without compromising security requirements.
- **Media Communications**: In generally, medical appliances are connected to regional and international networks using a variety of wireless technologies, including WiFi, GSM, WiMax, Bluetooth, Bluetooth Low Energy, Zigbee, and 3G/4G. Traditional wired security solutions are less suitable in these networks because of the wireless channel characteristics. As a result, finding an all-encompassing security mechanism that can treat the wired and wireless channel characteristics equally is challenging.
- **The availability of equipment**: An IoT health network includes a variety of health equipment, from PCs to inexpensive RFID tags. The capabilities of these devices in terms of compute, power, memory, and embedded software vary. Designing a security system that can work with even the most basic gadgets is therefore a challenge.
- **An evolving architecture**: A new topology that may be based on the current ones but is dynamic is required since the IoT-based healthcare network must be accessible anywhere and at any time [69].
- **Network with Several Procedures**: A medical sensor may use a customized network protocol to connect to other hardware on the local network.
- **Privacy of information**: We must create an identity management or stream access control system since medical data are a sensitive topic.
- **Structures of Confidence:** A trust negotiation mechanism, negotiation language, or object identity management system must be used to sustain communication between peers [69].

## *4.6. Applications in Medical*

The occurrence of population disorders and the requirement for an immediate reaction from the medical community guided the selection of the following applications [70].
Diabetes Therapy: Diabetes mellitus is a metabolic a multifactorial disease characterized by recurrent diabetes and modifications in the breakdown of proteins, sugars, and fats as a result of issues with insulin secretion, action, or both. Numerous organs are permanently harmed, become inefficient, and collapse as a result of diabetes mellitus. By tracking each patient's unique blood glucose patterns and assisting them in organizing their meals, activities, and prescription schedules, sugar levels measurement can help patients avoid all the hazards that this illness may provide.

**Watching a heart**: Many deaths, according to report [70], are caused by issues with the circulatory system, such as arrhythmias, myocardial ischemia, or prolonged QT intervals. This highlights the significance of electrocardiogram (ECG) watching of our vital signs. Electrocardiography records the heart's electrical pulse and includes measurements of heart rate, rhythm, and the identification of extended QT intervals, cardiac hypoxia, and arrhythmia. In fact, IoT-based systems for ECG watching have the ability to provide information to medical staff and provide the most information possible [71].

**Heart Rate Tests:** Since the prevention of circulatory system issues includes blood pressure monitoring, IoT-based apps can remotely procedure in order between a health post and a hospital system [70].
Detecting Body Heat: Homeostasis—the way the human body regulates a range of incredibly complicated interactions to preserve equilibrium or repair systems—is an important part of healthcare services since body temperature is a vital sign. The use of a body temperature sensor incorporated in a TelosB device enables the retrieval of body temperature fluctuations and reporting them to a temperature measurement system based on a home gateway through the IoT [70].

**Measure Oxygen Concentration**: A non-invasive and continuous monitoring system called pulse oximetry can be used to detect blood oxygen saturation. Monitoring of oxygen saturation can be supported by the incorporation of a pulse oximeter in an IoT-based implementation [72].
Pharmacology Administration: The medicine poses are one of the major issues in public health and a significant cost burden. IoT guarantees a new instrument to address this problem [70].

**Mobility Administration**: IoT's reaction to the speeding up of work is the development of fully automated smart wheelchairs for the disabled [70]. The Remote Monitoring and Management Platform of Healthcare Information (RMMP - HI) is a framework that can be used for practical applications; it can monitor and manage these lifestyle diseases to achieve the goals of early detection and prevention. A data sharing center that propagates data to medical personnel or hospital facilities depending on regulations, such as an urgent notice derived to a hospital, can collect, discard, and update data from body medical sensors about human body health [73].

## 5. Proposed Model

IoT technology is today one of the industries with the fastest rates of growth, and new IoT devices are introduced every day. These devices are autonomous and have connectivity to the Internet. Because of this dynamic environment, traditional networks are not the best option to meet IoT requirements. A more adaptable and secure network infrastructure is needed to support IoT operations. SDN is a cutting-edge technology that, as was previously said, allows complete control over the network's general behavior and protects against system congestion. The IoT ecosystem can use the SDN controller's useful debugging tools to increase security [74,75]. The IoT with SDN topology is shown in Figure 2, and the SDN controller allows for the network to be divided into isolated subnets [74]. Additionally, the SDN Controller communicates with the network of IoT applications through separate subnets [74]. Furthermore, a unique application programming interface is used by the SDN Controller to communicate with the IoT application (API). The latter conducts actions in accordance with configured rules after analyzing network traffic. On the other hand, the controller communicates with the network switches using a different API in accordance with set up regulations [76]. IoT operations and security are improved overall because to the integration of SDN with IoT, which enables complete remote control over network setup without having to engage.

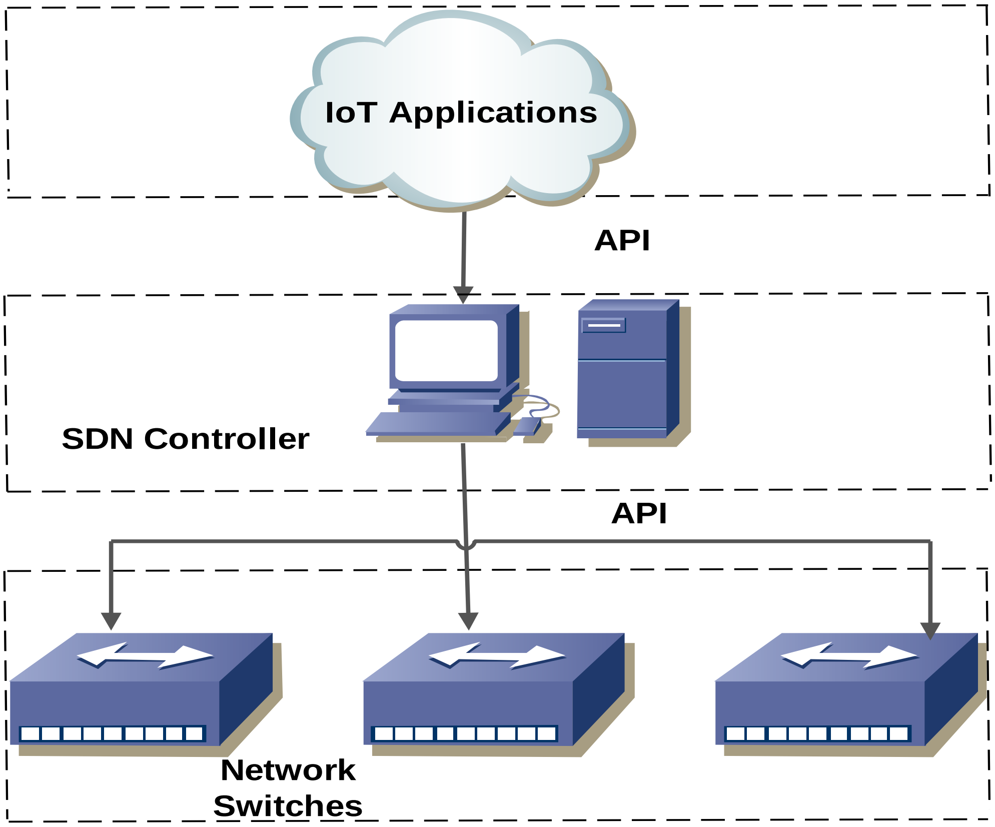

**Fig. 2 - SDN and IoT Structure.**

In our model system, SDN was constructed utilizing the Packet Switching. The SDN switch operates using a flow table, which is equivalent to the routing table used by traditional routers. It allows for chaining and allows for the matched of a broader range of fields because each flow has related actions. As a packet enters a switch, it is compared to the flow table, and if a match is found, the corresponding actions are taken. If a match is found, which is likely to happen for an addition of the new component, the received packet is sent to the SDN controller via the API. The control system then looks over the packet and decides what to do. It can build a new flow on the switch to make it possible for packets to be routed in the future without the controller being involved. Through API [77], information will be sent to the SDN application.

The network can be continuously managed and (re)programmed in accordance with the system administrators' detailed instructions. Deal with the scalability and availability of an IoT-based system in the core network and data center. Fundamental connection SDN-based techniques can offer a variety of functions, including dynamic resource and equipment interaction, and network traffic monitoring, from the perspective of IoT requirements. The data center is in charge of coordinating the deployment of services and virtual machines as well as network flow management. Since this study focuses on creating an IoT system structure utilizing SDN, which addresses needs on limit our discussion to the fundamental communication and information center when it comes to continuous controller (re)programming IoT devices at the edge network and the access network. [78].

**Proposed SDN-based framework for IoT reconfiguration (Case Study):**

The suggested architecture for remotely (re)programming IoT systems from an SDN-based architectural perspective. The middleware layer, the application layer, and the system layer are the three layers that make up the framework vertically. Executing programmes on end devices connected to various IoT networks are included in the system layer. Every sub-system in this tier has the sub-service for facilitating installation developed and pre-activated in order to support the remote (re)programming capability. The middleware layer, which doubles as the controller layer, offers a wide range of subservices, including data-related services, services for integrating circumstance and argumentation, and services for managing reconfiguration. This middleware layer, which supports APIs as well, is comparable to a SDN technology's SDN operator. The APIs give the system layer a mechanism to interface with various IoT subsystems, and they help the upper levels quickly deploy applications. The application layer is the final layer in the suggested structure, where users may effectively attempt to control, installing, and administering IoT-based systems. These levels will be thoroughly revealed in the ensuing sub-systems (Fig. 3).

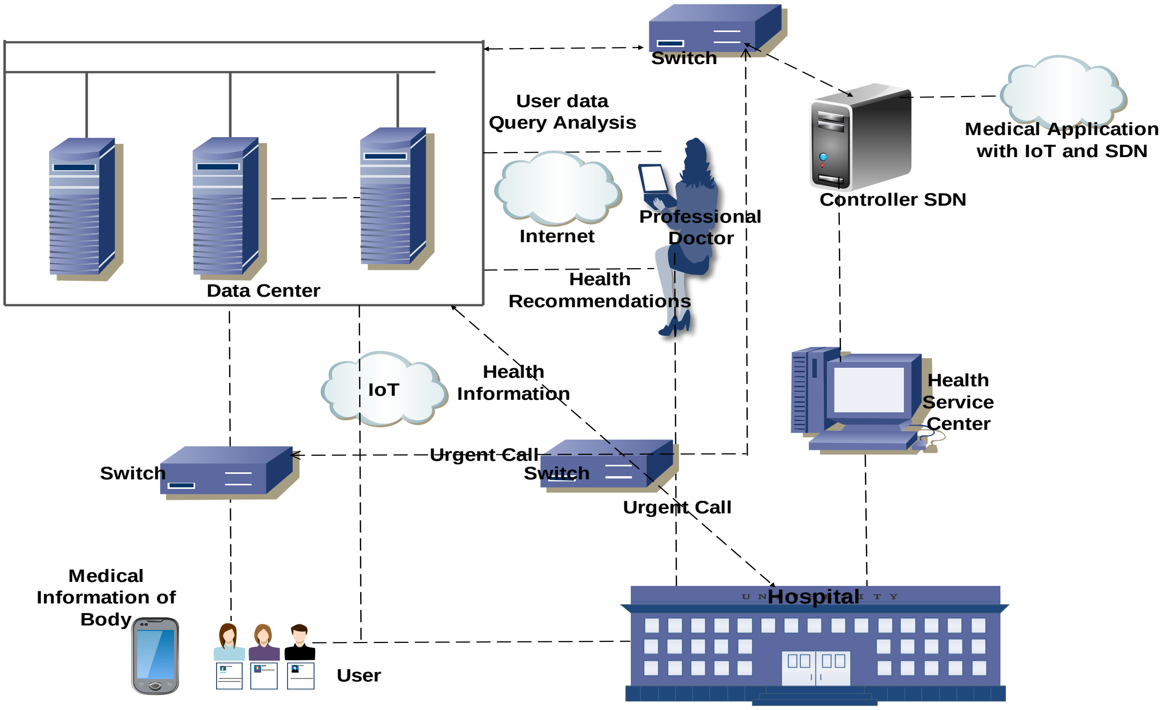

**Fig. 3 - The frame work of medical service with IoT and SDN Structure.**

The Remote Monitoring and Management Platform of Healthcare Information (RMMP - HI) is a framework that can be used for practical applications; it can monitor and manage these lifestyle diseases to achieve the goals of early identification and prevention [79,80]. Body medical sensors can store, remove, and update data across an IoT-based network. They then gather medical data about the human body and send it to a data sharing center, which then distributes it to medical professionals or hospital facilities in accordance with rules, like sending an urgent notice to a hospital as shown in figure 3.

## 6. Experimental Analyses

A local body area gateway and the traffic caused by a hospital facility network (Nano-network) connecting to an external network were both studied within the framework. The research's goal was fulfilled by realizing the imitation model. This model assumes that the user is within the boundaries of a healthcare facility with an SDN-based data transmission network. The body area gates of the user are linked to the medical facility's local area network and send information to a dedicated medical server that is also a part of the facility's communications network.

**Description of the experiment:**

1. **goal.** It is necessary to carry out an experiment using software defined network (SDN) as the network architecture and transfer data from a body area gateway (data produced by a Nano network).
2. **practical investments**: A traffic generator (client/server) for a software-defined network infrastructure on a lab stand.
3. **Features of the model** that was used Early studies, the results of which are reported, suggested the adoption of the basic circumstances listed below, which were incorporated into the traffic generator's parameters:
   When the IP header is taken into consideration, the packet length from one sensor is 32 bytes. Data is generated every second. The following parameters are listed in the case study simulation model:

- Twelve customers are concurrently connected to the local network. Each client has 128 Nano machines (sensors), and each client has a 30-minute network stay period (Test Time).

Figure 2 depiction of the interaction's structural plan provides a visual representation of the model.
A single aggregation switch connects the clients to the SDN network in this scenario, and the traffic generator is utilized to generate the essential characteristics of the traffic from the nanonetworks, as shown in Fig. 3, which depicts the interaction model in our experiment. Additionally, as the UDP protocol is regarded as the transport layer protocol, traffic duplicate transmission was taken into account in this model. This means that before delivering a second packet containing the identical data to the network, data from one sensor (nanomachines) was duplicated on the gateway. We simultaneously observed the presence of 12 people in a medical institution's building using our model under consideration. It is possible to expand the time of simultaneous discovery to a longer length of time; the time was chosen at 30 minutes.

Three steps made up the experimental phase of this work, which sought to compare how well this kind of traffic was transmitted via a network with various channel load characteristics. The subsequent tests were run:

1. Testing on channels with low demand and packet length L=32 bytes:
2. Testing when rival traffic (traffic encountered to the one under examination) is present on a network with a high level of congestion and packets L=32 bytes in length:
3. The second test results indicated that the interaction model's packet length L=64 should be increased while keeping the flow intensity constant. This testing was likewise conducted on a channel that was heavily congested with competing traffic of the same nature as in the second scenario (traffic encountered to the considered one). Through the TCP layer and at a rate of 78–80 Mbit/s, with a maximum throughput of 100 Mbit/s for the provided link, competing traffic was also generated using the traffic generator.
4. In the model structure, it was advised to increase the packet length L=128 while retaining the same flow intensity as stated in table 4 in accordance with the findings of the second test. In Table 2, the test results for the initial test are shown.

**Table 2 - The test results.**

| Person ID | Lost datagrams, % | Lost/Total datagrams | Jitter, ms | Bandwidth, Kbit/s |
|---|---|---|---|---|
| Patient.1 | 0.45 | 0/300032 | 0.223 | 32.0 |
| Patient.2 | 0.85 | 0/300032 | 0.294 | 32.0 |
| Patient.3 | 5.7 | 11081/300032 | 0.708 | 32.0 |
| Patient.4 | 1.001 | 3/300032 | 0.353 | 32.0 |
| Patient.5 | 1.25 | 0/300032 | 0.409 | 32.0 |
| Patient.6 | 4.9 | 12732/300032 | 0.642 | 32.0 |
| Patient.7 | 2.1 | 5339/300032 | 0.503 | 32.0 |
| Patient.8 | 0.25 | 838/300032 | 0.807 | 32.0 |
| Patient.9 | 7.2 | 17554/300032 | 0.901 | 32.0 |
| Patient.10 | 3.8 | 26315/300012 | 0.469 | 32.0 |
| Patient.11 | 4.7 | 13325/300012 | 0.547 | 32.0 |
| Patient.12 | 7.3 | 12314/300012 | 0.880 | 32.0 |

The test results according to the second test are displayed in the Table 3.

**Table 3 - The test results.**

| Person ID | Lost datagrams, % | Lost/Total datagrams | Jitter, ms | Bandwidth, Kbit/s |
|---|---|---|---|---|
| Patient.1 | 34 | 96738/300032 | 1.793 | 64.0 |
| Patient.2 | 60 | 180927/299809 | 1.957 | 64.0 |
| Patient.3 | 40 | 128456/297844 | 0.424 | 64.0 |
| Patient.4 | 22 | 66122/300021 | 2.942 | 64.0 |
| Patient.5 | 11.2 | 33748/300032 | 0.616 | 64.0 |
| Patient.6 | 45 | 154336/298927 | 0.208 | 64.0 |
| Patient.7 | 42 | 168057/300032 | 2.764 | 64.0 |
| Patient.8 | 28 | 183385/300032 | 0.268 | 64.0 |
| Patient.9 | 48 | 145938/2989808 | 1.716 | 64.0 |

| | | | | |
|---|---|---|---|---|
| Patient.10 | 35 | 155072/300020 | 2.045 | 64.0 |
| Patient.11 | 28 | 284640/290030 | 2.350 | 64.0 |
| Patient.12 | 55 | 167820/297503 | 1.990 | 64.0 |

The test results according to the third test are displayed in the Table 4.

**Table 4 - The test results.**

| Person ID | Lost datagrams, % | Lost/Total datagrams | Jitter, ms | Bandwidth, Kbit/s |
|---|---|---|---|---|
| Patient.1 | 46 | 138091/300025 | 6.301 | 128.0 |
| Patient.2 | 82 | 288764/299826 | 5.348 | 128.0 |
| Patient.3 | 44 | 170340/299566 | 2.317 | 128.0 |
| Patient.4 | 63 | 19935/300032 | 3.76 | 128.0 |
| Patient.5 | 73 | 215138/299983 | 5.71 | 128.0 |
| Patient.6 | 58 | 184044/299732 | 5.355 | 128.0 |
| Patient.7 | 2.7 | 88167/300032 | 3.086 | 128.0 |
| Patient.8 | 3.4 | 11157/300032 | 2.068 | 128.0 |
| Patient.9 | 68 | 198075/299496 | 0.643 | 128.0 |
| Patient.10 | 24 | 83693/299916 | 4.672 | 128.0 |
| Patient.11 | 28 | 73453/299916 | 3.428 | 128.0 |
| Patient.12 | 35 | 93253/299916 | 2.899 | 128.0 |

We can infer that when a network is heavily congested, the majority of packets are lost when competing for link space with rival traffic of same priority. However, the combined traffic from 12 customers was no more than 750 kbit/s. It is also notable that this method does not significantly reduce losses in the link with heavy rival traffic even with a halving of the packet length increase. The following algorithm can be used to represent the interaction on this model:

1. The gateway creates a registration message that includes its identity as well as information about the type of Internet of Things applications (Nano-network), the necessary QoS requirements, the range of potential deviations for those requirements, and the number of connected Nano machines. features of them
2. The gateway connects to its service and waits for a response.
3. The medical service refers to the network controller's application through a secured, previously designated channel after receiving the registration request. The network controller is in charge of managing health traffic.
4. In order to verify data, the SDN application layer service examines the current database for certain gateway identities (statistics). It then replies with a message to the medical service about the solution and addresses the appropriate controller modules that are in charge of network QoS regulation policy, depending on whether it is possible or impossible to deliver the necessary resources (with a successful solution, for example, a 200 OK message). If it is not possible to allocate the required resources, the medical service analyzes the prospective characteristics obtained with a potential range that was provided in the Internet of Things registration message. The service responds in this case by sending prospective characteristics (parameters) that it can assign to the message.
5. If the gateway experiences a failure in this functioning method, the service then concurrently sends a permission/denial message about the defined parameters to the service provider and the client gateway.

## 7. Conclusion

Over the past few years, the Internet of Things (IoT) has had a big impact on how we live our daily lives. The global community strongly want more smart devices. As more devices connect to the internet, information security will become more crucial because it is feasible for sensitive data to be accessed. The Internet of Things has an impact on the healthcare industry, increasing productivity, lowering costs, and refocusing attention on improving patient care. While this is happening, the Internet of Things is growing from the smallest detectors to the fundamentals of automation and equipment communication. We also take into account how IoT may be utilized to improve healthcare and how it can assist citizens and governments in enhancing daily activities on both a private and public level. Giving out location data has security drawbacks, but we can nevertheless give users some latitude in order to provide safeguards against abuse. To fully utilize this IoT technology, however, there are still many tasks to be completed. These applications must expand in the future so that society achieves the required level of health. We investigated merging SDN with IoT to strengthen security measures. Better network performance is the end outcome, including decreased network management overhead, packet delivery ratio, reduced latency, and average response time. The effectiveness of the suggested system has been confirmed by three distinct network scenarios' simulation results. In the future, we hope to improve the framework that has been proposed by safeguarding patient data and privacy. In order to forecast dangerous activity in the network, additionally, we want to use a machine-learning method and preserve the data patterns in a dataset. This suggested framework is still being built out in its entirety. Therefore, a viable direction is to finish all of the framework's capabilities as well as develop more useable experiments to thoroughly assess system efficiency.

## References

[1] Volkov, Artem, et al. "SDN approach to control internet of thing medical applications traffic." *International Conference on Distributed Computer and Communication Networks*. Springer, Cham, 2017.

[2] Amin, Syed Umar, and M. Shamim Hossain. "Edge intelligence and internet of things in healthcare: a survey." *IEEE Access* 9 (2020): 45-59.

[3] Javdani, Hamideh, and Hooman Kashanian. "Internet of things in medical applications with a service-oriented and security approach: a survey." *Health and Technology* 8.1 (2018): 39-50.

[4] Dhanvijay, Mrinai M., and Shailaja C. Patil. "Internet of Things: A survey of enabling technologies in healthcare and its applications." *Computer Networks* 153 (2019): 113-131.

[5] Thilakarathne, Navod Neranjan, Mohan Krishna Kagita, and Thippa Reddy Gadekallu. "The role of the internet of things in health care: a systematic and comprehensive study." *Available at SSRN 3690815* (2020).

[6] Usak, Muhammet, et al. "Health care service delivery based on the Internet of things: A systematic and comprehensive study." *International Journal of Communication Systems* 33.2 (2020): e4179.

[7] Asghari, Parvaneh, Amir Masoud Rahmani, and Hamid Haj Seyyed Javadi. "Internet of Things applications: A systematic review." *Computer Networks* 148 (2019): 241-261.

[8] Nasiri, Somayeh, et al. "Security requirements of internet of things-based healthcare system: a survey study." *Acta Informatica Medica* 27.4 (2019): 253.

[9] Ratta, Pranav, et al. "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives." *Journal of Food Quality* 2021 (2021).

[10] Priyadarsini, Madhukrishna, and Padmalochan Bera. "Software defined networking architecture, traffic management, security, and placement: A survey." *Computer Networks* 192 (2021): 108047.

[11] Yao, Haipeng, et al. "NetworkAI: An intelligent network architecture for self-learning control strategies in software defined networks." *IEEE Internet of Things Journal* 5.6 (2018): 4319-4327.

[12] Schaller, Sibylle, and Dave Hood. "Software defined networking architecture standardization." *Computer standards & interfaces* 54 (2017): 197-202.

[13] Singh, Sanjeev, and Rakesh Kumar Jha. "A survey on software defined networking: Architecture for next generation network." *Journal of Network and Systems Management* 25.2 (2017): 321-374.

[14] H. B. Mahajan, A. S. Rashid, A. A. Junnarkar et al., “Integration of Healthcare 4.0 and blockchain into secure cloudbased electronic health records systems,” in Applied Nanoscience, pp. 1–14, Springer, 2022.

[15] N. Zahid, A. H. Sodhro, U. R. Kamboh et al., “AI-driven adaptive reliable and sustainable approach for Internet of Things enabled healthcare system,” Mathematical Biosciences and Engineering, vol. 19, no. 4, pp. 3953–3971, 2022.

[16] Li, Junxia, et al. "A secured framework for sdn-based edge computing in IOT-enabled healthcare system." *IEEE Access* 8 (2020): 135479-135490.

[17] Rahman, Anichur, et al. "SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic." *Cluster Computing* 25.4 (2022): 2351-2368.

[18] Li, Wei, et al. "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system." *Mobile Networks and Applications* 26.1 (2021): 234-252.

[19] Sengupta, Souvik, and Suman Sankar Bhunia. "Secure data management in cloudlet assisted IoT enabled e-health framework in smart city." *IEEE Sensors Journal* 20.16 (2020): 9581-9588.

[20] Wahab, Fazal, et al. "An AI-driven hybrid framework for intrusion detection in IoT-enabled E-health." *Computational Intelligence and Neuroscience* 2022 (2022).

[21] Javed, F., Afzal, M.K., Sharif, M., *et al.*: ‘Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review’, *IEEE Commun. Surveys Tutor.*, 2018, **20**, (3), pp. 2062– 2100.

[22] Huynh-Van, Dang, and Quan Le-Trung. "SD-IoTR: an SDN-based Internet of Things reprogramming framework." *IET Networks* 9.6 (2020): 305-314.

[23] Chakraborty, Chinmay, et al., eds. *Internet of things for healthcare technologies*. Springer, 2021.

[24] Ahmadi, Hossein, et al. "The application of internet of things in healthcare: a systematic literature review and classification." *Universal Access in the Information Society* 18.4 (2019): 837-869.

[25] Anand, Sharath, and Sudhir K. Routray. "Issues and challenges in healthcare narrowband IoT." *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*. IEEE, 2017.

[26] Tallapragada, V. V., et al. "Significance of Internet of Things (IoT) in Health Care with Trending Smart Application." *Smart Systems: Innovations in Computing*. Springer, Singapore, 2022. 237-245.

[27] Yang, Dawei, et al. "Application of Internet of Things in Chronic Respiratory Disease Prevention, Diagnosis, Treatment and Management." *Clinical eHealth* (2022).

[28] Mohana, J., et al. "Application of internet of things on the healthcare field using convolutional neural network processing." *Journal of Healthcare Engineering* 2022 (2022).

[29] M. Cicioğlu and A. Çalhan, “SDN-based wireless body area network routing algorithm for healthcare architecture,” ETRIJournal, vol. 41, no. 4, pp. 452–464, 2019.

[30] K. Hasan, X. W. Wu, K. Biswas, and K. Ahmed, “A novel framework for software defined wireless body area network,” in 2018 8th International conference on intelligent systems, modelling and simulation (ISMS), pp. 114–119, IEEE, Kuala Lumpur, Malaysia, 2018, May.

[31] Sahoo, Kshira Sagar, et al., eds. *SDN-Supported Edge-Cloud Interplay for Next Generation Internet of Things*. CRC Press, 2022.

[32] Ja’afreh, Mohammed Al, et al. "Toward integrating software defined networks with the Internet of Things: a review." *Cluster Computing* (2021): 1-18.

[33] Abid, Muhammad Aneeq, et al. "Evolution towards smart and software-defined internet of things." *AI* 3.1 (2022): 100-123.

[34] Othman, Soufiene Ben, Faris A. Almalki, and Hedi Sakli. "Internet of things in the healthcare applications: overview of security and privacy issues." *Intelligent Healthcare* (2022): 195-213.

[35] Gartner. *8.4 Billion Connected `Things' Will Be Use in 2017, Up 31 Percent From 2016*. Accessed: Apr. 7, 2019. [Online]. Available: https://www.gartner.com/newsroom/id/3598917

[36] G. Yang, M. A. Jan, V. G. Menon, P. G. Shynu, M. M. Aimal, and M. D. Alshehri, ``A centralized cluster-based hierarchical approach for green communication in a smart healthcare system,'' *IEEE Access*, vol. 8, pp. 101464_101475, 2020.

[37] F. Khan, A. U. Rehman, A. Yahya, M. A. Jan, J. Chuma, Z. Tan, and K. Hussain, ``A quality of service-aware secured communication scheme for Internet of Things-based networks,'' *Sensors*, vol. 19, no. 19, p. 4321, Oct. 2019.

[38] S. Zeadally, A. K. Das, and N. Sklavos, ``Cryptographic technologies and protocol standards for Internet of Things,'' *Internet Things*, Jun. 2019, Art. no. 100075. [Online]. Available: https://www.sciencedirect.com/ science/article/pii/S2542660519301799

[39] X. Li, J. Li, Y. Liu, Z. Ding, and A. Nallanathan, ``Residual transceiver hardware impairments on cooperative NOMA networks,'' *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 680_695, Jan. 2020.

[40] F. Khan, A. U. Rehman, and M. A. Jan, ``A secured and reliable communication scheme in cognitive hybrid ARQ-aided smart city,'' *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106502.

[41] J. Dizdarevi¢, F. Carpio, A. Jukan, and X. Masip-Bruin, ``A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration,'' *ACM Comput. Surveys*, vol. 51, no. 6, pp. 1_29, Feb. 2019.

[42] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, ``Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance,'' 2020, *arXiv:2004.14563*. [Online]. Available: http://arxiv.org/abs/2004.14563

[43] V. G. Menon, S. Jacob, S. Joseph, and A. O. Almagrabi, ``SDN-powered humanoid with edge computing for assisting paralyzed patients,'' *IEEE Internet Things J.*, vol. 7, no. 7, pp. 5874_5881, Jul. 2020.

[44] A. J. Ferrer, J. M. Marquès, and J. Jorba, ``Towards the decentralised cloud: Survey on approaches and challenges for mobile, ad hoc, and edge computing,'' *ACM Comput. Surveys*, vol. 51, no. 6, pp. 1_36, Feb. 2019.

[45] S. Rajesh, V. Paul, V. G. Menon, S. Jacob, and P. Vinod, ``Secure brainto- brain communication with edge computing for assisting post-stroke paralyzed patients,'' *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2531_2538, Apr. 2020.

[46] W. Gong, H. Liu, J. Liu, X. Fan, K. Liu, Q. Ma, and X. Ji, ``Channelaware rate adaptation for backscatter networks,'' *IEEE/ACM Trans. Netw.*, vol. 26, no. 2, pp. 751_764, Apr. 2018.

[47] P. Zhang, T. Taleb, X. Jiang, and B. Wu, ``Physical layer authentication for massive MIMO systems with hardware impairments,'' *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1563_1576, Mar. 2020.

[48] Szymanski, T.H. Security and privacy for a green internet of things. IT Prof. **2017**, 19, 34–41.

[49] Alam, T. A Reliable Communication Framework and Its Use in Internet of Things (IoT). Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. **2018**, 2456–3307.

[50] Abiodun, Oludare Isaac, et al. "A review on the security of the internet of things: challenges and solutions." *Wireless Personal Communications* 119.3 (2021): 2603-2637.

[51] Bhatt, Shobha, and Prakash Rao Ragiri. "Security trends in Internet of Things: A survey." *SN Applied Sciences* 3.1 (2021): 1-14.

[52] Javeed, Danish, et al. "A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of Things (IoT)." *Sensors* 21.14 (2021): 4884.

[53] Harbi, Yasmine, et al. "Recent security trends in internet of things: A comprehensive survey." *IEEE Access* (2021).

[54] Zeleke, Esubalew M., Henock M. Melaku, and Fikreselam G. Mengistu. "Efficient intrusion detection system for SDN orchestrated Internet of Things." *Journal of Computer Networks and Communications* 2021 (2021).

[55] Babbar, Himanshi, et al. "Load balancing algorithm on the immense scale of internet of things in SDN for smart cities." *Sustainability* 13.17 (2021): 9587.

[56] Urrea, Claudio, and David Benítez. "Software-defined networking solutions, architecture and controllers for the industrial internet of things: A review." *Sensors* 21.19 (2021): 6585.

[57] Yungaicela-Naula, Noe M., et al. "Towards security automation in software defined networks." *Computer Communications* 183 (2022): 64-82.

[58] Muthanna, Mohammed Saleh Ali, et al. "Towards SDN-Enabled, Intelligent Intrusion Detection System for Internet of Things (IoT)." *IEEE Access* 10 (2022): 22756-22768.

[59] Wang, Shupeng, et al. "A multi-task learning-based network traffic prediction approach for SDN-enabled industrial Internet of Things." *IEEE Transactions on Industrial Informatics* (2022).

[60] Manocha, Prabhjot Singh, and Rajiv Kumar. "Improved spider monkey optimization-based multi-objective software-defined networking routing with block chain technology for Internet of Things security." *Concurrency and Computation: Practice and Experience* 34.11 (2022): e6861.

[61] Bhuyan, Monowar, et al. "A survey on blockchain, SDN and NFV for the smart-home security." *Internet of Things* (2022): 100588.

[62] Latif, Sohaib A., et al. "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems." *Computer Communications* 181 (2022): 274-283.

[63] Huo, Ru, et al. "A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges." *IEEE Communications Surveys & Tutorials* (2022).

[64] Ahmad, Md Oqail, and Shams Tabrez Siddiqui. "The Internet of Things for Healthcare: Benefits, Applications, Challenges, Use Cases and Future Directions." *Advances in Data and Information Sciences*. Springer, Singapore, 2022. 527-537.

[65] Friha, Othmane, et al. "Internet of things for the future of smart agriculture: A comprehensive survey of emerging technologies." *IEEE/CAA Journal of Automatica Sinica* 8.4 (2021): 718-752.

[66] Li, Wei, et al. "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system." *Mobile Networks and Applications* 26.1 (2021): 234-252.

[67] Hariharakrishnan, Jayaram, and N. Bhalaji. "Adaptability Analysis of 6LoWPAN and RPL for Healthcare applications of Internet-of-Things." *Journal of ISMAC* 3.02 (2021): 69-81.

[68] Bhuiyan, Mohammad Nuruzzaman, et al. "Internet of things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities." *IEEE Internet of Things Journal* 8.13 (2021): 10474-10498.

[69] Radwan, Neyara, and Maged Farouk. "The Growth of Internet of Things (IoT) In The Management of Healthcare Issues and Healthcare Policy Development." *International Journal of Technology, Innovation and Management (IJTIM)* 1.1 (2021): 69-84.

[70] Kumar, Priyan Malarvizhi, et al. "Clouds proportionate medical data stream analytics for internet of things-based healthcare systems." *IEEE Journal of Biomedical and Health Informatics* 26.3 (2021): 973-982.

[71] Kishor, Amit, Chinmay Chakraborty, and Wilson Jeberson. "Intelligent healthcare data segregation using fog computing with internet of things and machine learning." *International Journal of Engineering Systems Modelling and Simulation* 12.2-3 (2021): 188-194.

[72] Singh, Prabh Deep, Gaurav Dhiman, and Rohit Sharma. "Internet of things for sustaining a smart and secure healthcare system." *Sustainable computing: informatics and systems* 33 (2022): 100622.

[73] Kadhim, Kadhim Takleef, et al. "An overview of patient's health status monitoring system based on Internet of Things (IoT)." *Wireless Personal Communications* 114.3 (2020): 2235-2262.

[74] Restuccia, Francesco, Salvatore D'Oro, and Tommaso Melodia. "Securing the internet of things in the age of machine learning and software-defined networking." *IEEE Internet of Things Journal* 5.6 (2018): 4829-4842.

[75] Kaur, Kuljeet, et al. "Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay." *IEEE communications magazine* 56.2 (2018): 44-51.

[76] Mubarakali, Azath, et al. "Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems." *Computational Intelligence* 36.4 (2020): 1580-1592.

[77] Zhao, Yanling, et al. "A survey of networking applications applying the software defined networking concept based on machine learning." *IEEE Access* 7 (2019): 95397-95417.

[78] Al-Heety, Othman S., et al. "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet." *IEEE Access* 8 (2020): 91028-91047.

[79] Cabaj, Krzysztof, Marcin Gregorczyk, and Wojciech Mazurczyk. "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics." *Computers & Electrical Engineering* 66 (2018): 353-368.

[80] López, César, et al. "Reviewing SDN adoption strategies for Next Generation Internet of Things networks." *Smart Systems: Innovations in Computing*. Springer, Singapore, 2022. 619-631.