Multimedia Tools and Applications
https://doi.org/10.1007/s11042-023-15678-2

SDN-based multi-level framework for smart home services

Syed Mushhad Mustuzhar Gilani[1] · Muhammad Usman[1] · Saqib Daud[2] · Asif Kabir[3] · Qamar Nawaz[4] · Oláh Judit[5,6]

Received: 15 July 2021 / Revised: 15 June 2022 / Accepted: 22 April 2023

Abstract
The smart home is a field that uses smart devices and gadgets to automate tasks and operations in the house, and it is expected that this study subject will become a focal point in future civilizations. The adoption of smart home services faces significant obstacles in terms of reliability and stability. The Software Defined Networking (SDN) paradigm offers up novel approaches and trends to embrace smart technologies to tackle the issues of smart homes. To avoid accidents, we developed a vertical SDN-based multi-level structure consisting of two controllers with a parent-child connection. It enables smart homes to make optimal use of current services while also providing new services to smart homes and buildings, opening the path for future smart services. In addition, we created an Application Programming Interface (API) for the smart home to make it easier to use current services and pave the path for future smart services. We designed numerous jobs depending on their categorization to give smart services, which is beneficial for smart homes. Local topologies, cloud topologies, and cloud-local topologies have all been compared in the evaluation section. The performance of POX, NOX, and Flood Light controllers is measured using three performance metrics: mean throughput, Round-Trip Time (RTT), and packet loss across all three topologies. Our findings revealed that the cloud-local topology had the lowest packet loss ratio of 1.4%, while the local and cloud topologies had 1.9% and 2.3%, respectively.

Keywords SDN · Smart home API · Smart services · Smart home framework

1 Introduction

The notion of making items smarter with intelligence is growing fast in the recent era, thanks to the rapid innovation and exponential expansion of the Internet of Things (IoT). The smart house is now one of the most popular IoT applications. According to a report [30], 90 million people throughout the globe will live in smart houses in the future. Many writers have defined the smart house in the literature. Smart houses, on the other hand, maybe divided into two categories: (1) smart houses and (2) smart

✉ Oláh Judit
olah.judit@econ.unideb.hu

Extended author information available on the last page of the article

buildings. Devices (home appliances), sensors, and a communication network make up a smart house. These gadgets can monitor and access the users, who are the residents of the house, remotely based on their requirements [5]. Smart buildings, on the other hand, place a greater emphasis on the energy system. These energy systems are capable of effectively producing and using energy [10]. Both definitions emphasize the significance of communication networks in connecting smart devices and sensors, with one focusing on people and the house itself and the other on using energy services effectively in buildings. The crucial services that sit in the driver's seat of the smart home are smart automated services. The key services provided by smart homes include smart security, energy lighting, entertainment networking, and health services. The development of a self-management solution to existing smart home customers' difficulties with automation and smart services is still in its early phases. The growing number of smart devices and smart services introduces new challenges, such as complexity. The present solutions are insufficient to meet the demands of these services and smart home customers. Another key issue with smart home networks is the setup of low-level parameters necessary for improved service delivery [3]. For example, managing bandwidth among various devices and smart services seems to be an easy task in smart houses. This job requires an understanding of low-end choices as well as ongoing monitoring of bandwidth use by various sorts of services. When enjoying entertainment services in smart homes, most consumers do not want to let their security down. A security service that minimizes reaction time is known as guard down. As a result, a system that handles whole services operating in smart homes rather than individual devices must exist.

Different organizations often supply gadgets with various types of intelligent characteristics and data collecting modules. Different communication protocols and network interfaces are used by these devices. To create a cohesive system, the smart home assumes that every gadget and sensor in this highly isolated environment will operate together via some form of smart service. The authors of [6, 27] developed a centralized architecture for managing many types of gadgets in a smart home setting. This approach focuses on devices rather than services. To avoid interoperability issues, the smart home design relies on services rather than individual devices to solve problems. In the article [21] they used SDN and cloud-based technologies to work on auto-configuration and administration of residential networks. Although this research is a first step in the right path, it cannot offer a service-centric strategy and delivery of various services.

Our goal is to address the issues surrounding smart home services, a potential SDN framework paradigm was presented for improved administration of future smart home automation services. SDN is a networking design that tries to make networks more adaptable. SDN-based architectures are capable of swiftly and readily adapting to changes. It's a relatively new paradigm that allows a centralized console with distinct control and data planes to influence traffic (forwarding plane). It can make abstract decisions, allowing us to govern any network component via a centralized administration tool. To avert catastrophes, we want to build a vertical SDN-based multi-level architecture with two controllers that are connect as parents and children. It allows smart homes to make the most of existing services while also introducing new services to smart homes and buildings, paving the way for future smart services. We also established a smart home API to make existing services simpler to use and pave the way for future smart services. We created a variety of professions based on their classification in order to supply smart services that will benefit smart homes. For communication between wired and wireless devices, Open Flow switches and routers are employed. Second, studies were carried out in a simulated environment built-in Mininet, a discrete event based SDN emulator. For all three topologies, we will use three

performance measures to calculate the performance of POX, NOX, and Flood Light controllers: mean throughput, Round-Trip Time (RTT), and packet loss.

The remainder of the paper is laid out as follows: Section 2 discusses the literature review. Section 3 presents the proposed framework. Section 4 contains details about the prototype. The experiments and findings are described in Sections 5 and 6 concludes the discussion.

2 Background and literature review

The IoT networks are hampered by security flaws that hackers may exploit to launch attacks in a variety of settings, including smart homes, industries, and healthcare systems. To get over this stumbling block, researchers [18, 31] have devised a variety of intrusion detection and prevention technologies (IDPSs). Machine Learning (ML) has emerged as the most promising method among all the employed technologies. As a result, most ML-based intrusion detection systems concentrate only on finding relevant ML algorithms in order to enhance detection accuracy. As a result, the authors investigated the attributes of several smart home security assaults, as well as the quality of the features that can be extracted and used in machine learning algorithms to effectively identify each of these attacks. Additionally, this study offered effective intrusion prevention measures as well as an SDN-based deployment architecture for IDPSs inside residential networks. Different feature sets and ML models are used to perform experimental assessments of the suggested solution.

The authors in [20] presented an SDN-based security architecture for smart homes. They used a small collection of parameters to classify IoT devices and identify DDoS attacks, such as the proportion of ICMP, TCP, and UDP flows, packet size, packet count, and IP diversity ratio. They also looked at the KNN, LK-SVM, and RF machine learning models. By lowering the training dataset size, choosing an acceptable machine learning model, providing stateless and easy-to-calculate features, and raising the polling period to decrease overhead on the SDN controller, their suggested solution fulfills the memory, latency, and security criteria.

They find that KNN outperforms LK-SVM and RF for the suggested feature set and longer polling intervals (i.e., more non-cumulative statistics). KNN also achieves higher than 95% accuracy with an average latency of 1.18 milliseconds for 1820 data points and a 24-second optimum polling period.

To overcome the challenges of smart homes, the SDN paradigm is the most suitable and ideal option. In this research [22], a novel architecture for the software defined network was suggested to provide a safe smart home environment (SHSec). Used a simulation to verify the suggested model's performance and viability in a real-world setting, including connection failures and switching. Also, assessed the suggested model's performance using a variety of metric factors. The simulation findings demonstrate that SHSec management is capable of detecting and mitigating assaults, as well as securing the system, ensuring user security, and improving the heterogeneous local network. When it comes to forecasting harmful occurrences, the suggested model has an accuracy of 89.9% and a sensitivity of 91.1%.

Edge computing, a novel computing paradigm in which data is processed from edges, is the key to the expansion of the IoT and the capacity to gather, analyses, and offer big data in the cloud. In the last two years, Edge Computing has gotten a lot of attention as one of the top ten strategic technological developments, and it has a lot of revolutionary

potentials. The researchers in [9] introduced the concepts, backgrounds, and advantages and disadvantages of edge computing in this paper, explained how it works and how it is structured hierarchically using artificial intelligence concepts, listed examples of its applications in various fields, and finally suggested some improvements and discussed the challenges of its application in three representative technological fields. They want to explain diverse assessments and viewpoints on artificial intelligence and edge computing.

Tens of IoT devices with a broad range of functional capabilities are installed in each smart house. The authors suggested a bandwidth allocation framework based on the potential software defined networking (SDN) architecture for improving bandwidth allocation on both internal and external Internet traffic. The whole system architecture is divided into two parts: SDN Smart Home Cloud and Massive Smart Homes, with the OpenFlow protocol connecting them. The researchers [39] tweaked the 3GPP LTE QoS Class Identifier (QCI) to make it more adaptable to smart home services. They developed a bandwidth allocation method that takes into account fairness, latency, and service priority all at once. With this approach, ISPs may efficiently improve Quality of Service (QoS) and user experience by aggregating hundreds of categorized smart home services and thereby optimizing bandwidth allocation (QoE).

Smart City (SC) has brought with it a plethora of possibilities as well as new obstacles. One of the most significant difficulties with SC networks is network security. Due to the possibility of a single point of failure, Software-Defined Networking (SDN) is more likely to be the target of Distributed Denial of Service (DDoS) attacks. To better protect against DDoS assaults, the author in [25] focused on tracing the source and proposed a statistics-based traceback system that makes use of the SDN architecture's capabilities. They calculated the eigenvalue and established the anomaly tree by analyzing the variations inflow via the Base Station (BS) nodes. The assault route was then pruned using a DDoS detection technique. They discovered the best parameters for making the suggested strategy more flexible and effective via trials. It was shown that the technique uses fewer network resources and saves time than standard ones while maintaining a high degree of DDoS protection accuracy.

Figure 1 shows the various use cases for smart home networks using SDN. Researchers are currently concentrating their efforts on integrating SDN with smart home networks [23, 38]. The authors [19] presented an SDN-enabled smart home design with the potential to link to other platforms through an open interface. For an SDN-based house, the researchers [37] designed a data transmission distribution system. SDN engineering is required for the transmission capacity assignment system presented in this study. An Internet Service Provider (ISP) is responsible for assigning IoT-based devices to each smart building and house. ISPs are responsible for streamlining the data transmission distribution of inward home network traffic and outside network traffic for the internet separately. The authors, on the other hand, did not address the adaptability of using an SDN-based architecture in conjunction with sensors and smart devices.

Network Function Virtualization (NFV) is a similar new technology that is used to manage networks. It gives network equipment and solutions like security firewalls, Generally Deep Packet Inspection (DPI), and Intrusion Detection Systems (IDS) a way to function (IDS). These are virtual components that are included into hardware systems and are placed in applications as virtual components. The physical components of wireless networks used in smart buildings and cities may be virtually divided into several pieces for the convenience of operators using NFV. The network operators gained various benefits in terms of network resources, scheduling, cache space allocation, and processing space as a result of this split. Although NFV technology produces superior outcomes, it also has its own set of restrictions.

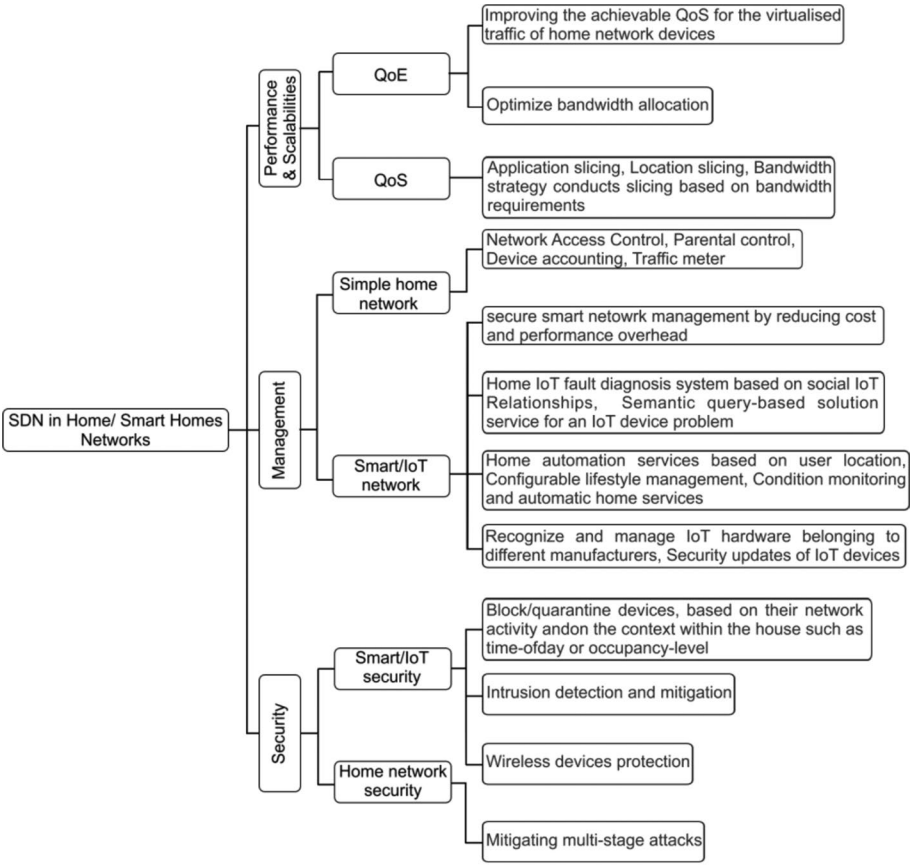


Fig. 1 Taxonomy of SDN in Smart Homes

Slicing methods are the new contemporary networking front that guarantees that the needs of customers are met [2, 11]. The multiple route environment is used in the home domestic network optimization, which increases the network's overall performance [12]. A smart house is a collection of Internet of Things (IoT) gadgets. Independence, object connection, resource management, privacy protection, and data security are the fundamental characteristics of an IoT platform. The IoT management and control part connects to a disconnected network application and provides services for smart devices controlled by the cloud.

One of the most important developing technologies for smart homes is the IoT. In many smart IoT applications, routing protocols like DSDV and AODV are utilized to communicate between devices [7, 8]. The researchers [16] offered a possible methodology and key technologies for developing a people-centric IoT-based civilization. They also outlined the major issues and obstacles. Dynamic QoS aware queuing in the smart home for heterogeneous traffic was presented by the authors in [35]. The home network users connect to manage the tasks via their own networks to conduct the new user centered management architecture. The new services' usability and accessibility have increased as a result [33]. There are two aspects to the home network management applications: The first section is concerned with the front end, which is interactive and

runs on the user's preferred device, such as a PC, laptop, or smartphone. Both SDN and NFV models are included in the second section.

In [14, 36] researchers presented a home setup strategy based on SDN technology. This method of setting is based on network automation without the use of in-between devices and home gateways. They also said that the number of IoT-enabled devices-based apps employed in smart homes is quickly expanding.

The authors of [34] highlighted automatically controlled and assistive appliance services for improving life quality, which is a popular smart home application. IoT devices may collaborate and improve their users' comfort levels by applying context-specific limitations and awareness. People who live in a heterogeneous data integration environment might find comfort and security in smart homes. Ontologies that enable semantic translation of events and establishing attentiveness are used to execute data integration. Furthermore, metaphysics-based data semantic structure and application are proposed to accommodate the ever-increasing amounts of heterogeneous data in smart home devices. Cloud-centric IoT solution [15, 26] that explains how to integrate with their framework for different smart home devices that function in the environment. Furthermore, they freely discuss the issues and limitations that various communication protocols utilized in smart homes face.

The deployment of multi controller environments in current smart home design is lacking, despite its importance for fault tolerance and system effectiveness. As smart homes become increasingly integrated and complex, having a single controller may no longer suffice to meet the needs of the system. The authors of [17, 32] presents a software defined alert management system for smart communities as a solution. However, one limitation of this method is that it does not offer a fault-tolerant multi-controller design. This means that if one controller fails, the entire system may become non-functional, leading to potential downtime and reduced system reliability. There is a dearth of smart home research connected to smart services framework, which might be critical in advancing the smart house and smart city age. The authors [28, 29] offered a distributed control strategy for the controller placement issue, however, it lacks work with merely the built-in shortest route. It lacks resilience, which is critical in a multi-controller scenario.

A smart house is a home with internet-connected gadgets that allow for remote monitoring and control of appliances and systems like lighting and heating. Smart home technology, also known as home automation or domotics (from the Latin "domus" meaning "home"), allows homeowners to manage smart equipment through a smart home app on their smartphone or other networked device, providing security, comfort, convenience, and energy efficiency. Smart home systems and gadgets, which are part of the internet of things (IoT), often work together, exchanging consumer use data and automating activities depending on the homeowners' preferences.

Our objective is to provide a vertical SDN-based multi-level architecture with two controllers that have a parent-child connection to avoid disasters. It enables smart homes to make optimal use of current services while also providing new services to smart homes and buildings, opening the path for future smart services. We'll also create an API for the smart home to make it easier to use current services and pave the path for future smart services. We will design numerous jobs depending on their categorization to deliver smart services, which will be beneficial to smart homes. To calculate the performance of POX, NOX, and Flood Light controllers, we will utilize three

performance metrics: mean throughput, Round-Trip Time (RTT), and packet loss for all three topologies.

3 Proposed framework

We defined the key principle underlying SDN (central control, openness, virtualization) and its difficulties and challenges connected to smart homes experienced during the provisioning of new smart services, taking into account earlier existing solutions. Figure 2 shows the abstract level of the framework.

A Primary SDN Controller (PSC) on the cloud lies on top of the framework and is responsible for high-level operations such as dealing with third-party external service providers that communicate with the cloud controller. It has the ability to detect security risks and flaws. It may also improve the overall experience of using that service in the future. PSC has a Primary Data Storage (PDS) that serves as both a cache and a database. It is utilized as a cache to speed up the service delivery process and minimize latency.

LSC is the second controller on the local area network that works under PSC and manages local smart service systems of many sorts, such as smart health, energy, security, and entertainment. LSC issues directives and proactive rules to the primary open flow switch. Under the supervision of PSC, it directly controls different modules such as bandwidth management, device status management, and so on. LSC has its own Local Data Storage (LDS) database, which stores settings as well as data received from PSC.

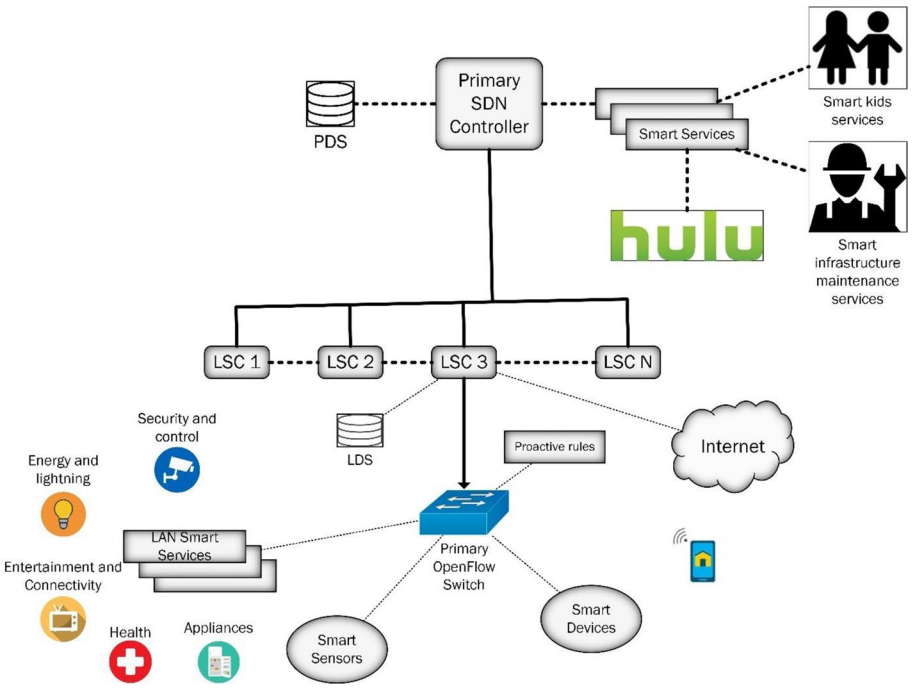


Fig. 2 Framework for Smart Home Services

A built-in SDN controller is connected to the home gateway. One main controller makes up the SDN controller system that works as a parent-child connection. The general modules in the system of framework are in the form of a tree structure to accommodate diverse job scheduling and arrangements to the architecture. When an emergency happens, such as floods or smoke, the controller detects it and sends signals to the LSC. The controller promptly notifies the PSC, who in turn notifies the police. This means that even if our local controller is damaged in a fire, the answer will be sent. LSC is a local smart home service and module that operates on a LAN network and contains local smart home services and modules for security, traffic management, and access control. LSC has a database system (LDS) that stores configuration and policies. The Primary Open Flow switch uses proactive controls to provide quicker communication and lower latency.

In the data layer, local and cloud controllers that operate as the network's operating system, cutting off the intelligence of devices in networks has been utilized for routing and switching reasons. The proposed framework makes use of [1, 13] primary two components that offer security functionality while still being lightweight. At different layers of SDN-based frameworks, these modules identify and mitigate security issues. Orchestrator protects the controller of a smart home network against upper-level threats such as application-layer malware and viruses, which may be highly dangerous to the controller and the whole network. KNOT is in charge of assisting in the analysis of threats that come. It's helpful for packet openers, flow graph creators, and attack mitigation.

For flawless smart home service execution, home gadgets such as smart TVs, ovens, sound systems, and other devices must be in a live real-time state [24]. For automated smart home services and smart focused framework services, this is critical. The method of real-time state management of home network devices is shown in Fig. 3. Connections with devices identify any status changes when updating in real time. LSC submits state requests to AP regularly. The message is then sent to all connected home devices at that time. The home device receives the request and responds to the AP in real time with its current condition. The link between the home AP and the devices is similar to the Keep-Alive technique.

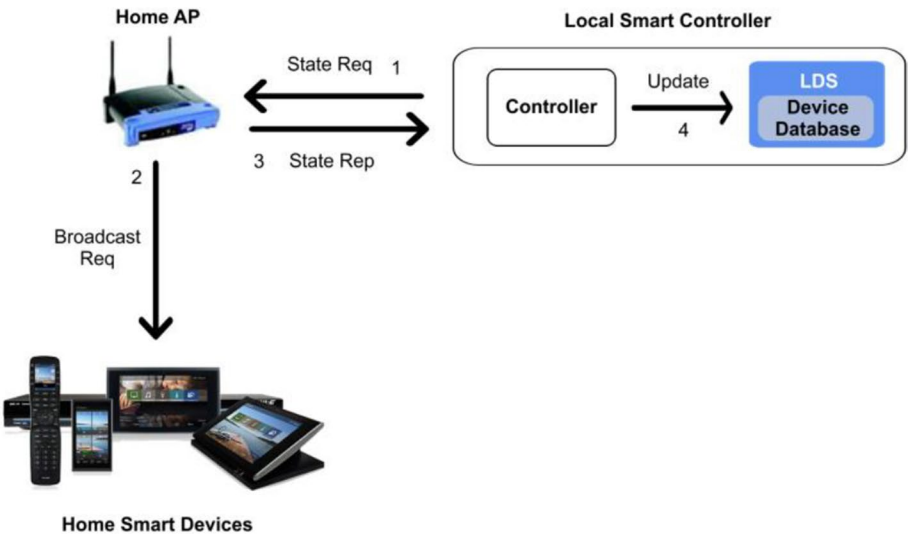


Fig. 3 Real Time State Management in Smart Home

If a device does not respond, it is considered disconnected from the network. Finally, after verifying the device database in LDS updates, AP sends each message to the controller.

In order to identify issues in the smart home, there should be a diagnostic system that takes into account fault tolerance design. Using several domains relating to smart devices is the best method to accomplish this aim. Parent object connection, co-location object relationship, co-work object relationship, owner object relationship, and social object relationship are some of the relationships between IoT devices described by the authors [4]. These domain specific correlations are very useful in identifying faults in smart homes. Both consumers and service providers have a tough time locating issues in the service domain or network domain. The controller automatically finds flaws in the framework to simplify the process and decrease complexity for home users. The controllers create the four fundamental relationships after recognising them. Figure 4 depicts the flow diagram of the Primary SDN controller. The process of recognising

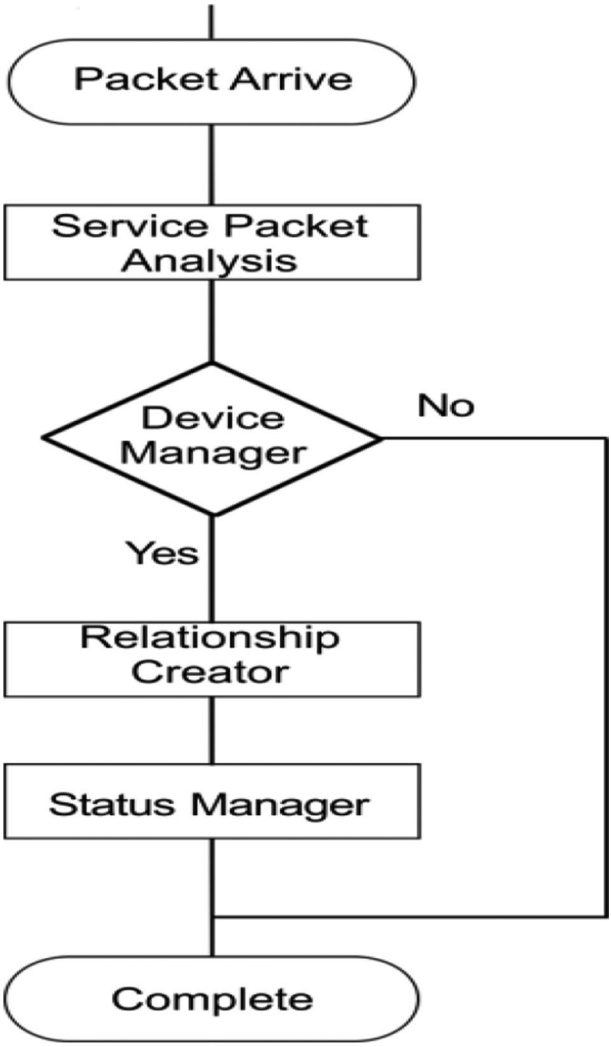
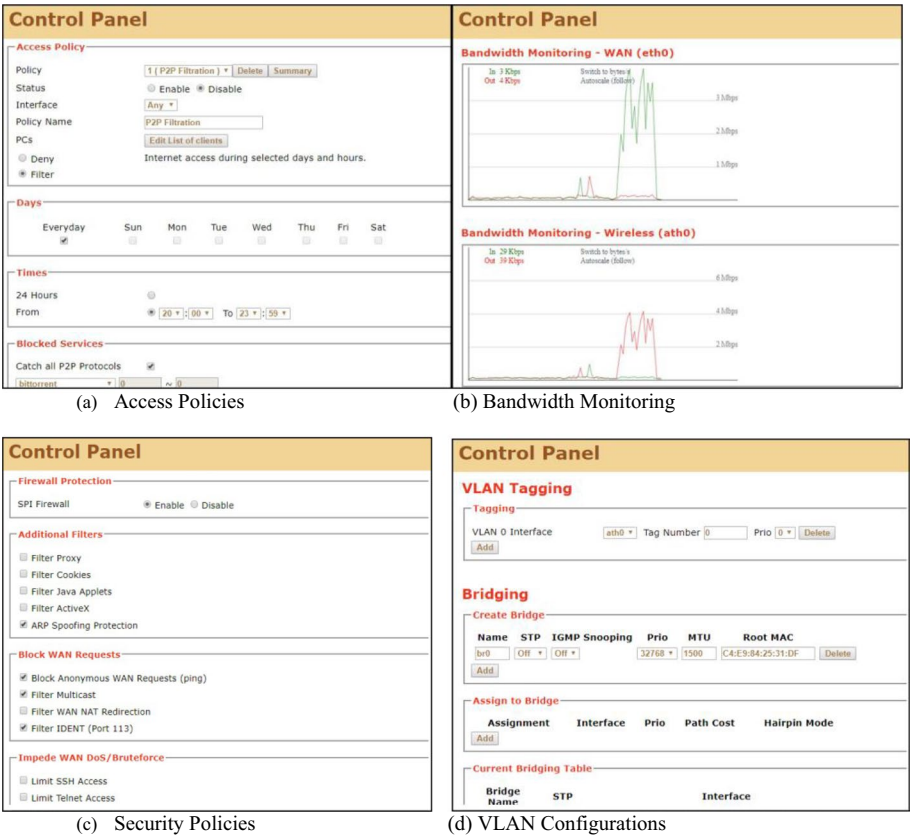


Fig. 4 Flow Diagram

Smart Devices begins with Service Packet Analysis (SD). Following this, Relationship Creator begins the automating relationship phase. These freshly created connections are saved in Status Manager.

The Primary SDN Controller benefits from the Cloud platform, which can address all challenges and jobs that the LSC cannot, such as tasks that need very high-power resources for various types of services, data-oriented tasks, or processing power for third-party service providers. PSC plays a critical role in ensuring that smart services work smoothly and to their full potential. It is also capable of providing data solutions.

The proposed framework's most basic features are implemented using a main Open Flow TP-LINK WR1043ND v2.1 switch deployed in the test bed. Figure 5 depicts the web interfaces. These interfaces provide the option to customize settings and monitor processes. The setup page may be used to adjust the settings, and the status menu can be used to monitor them. The ability to implement user rules on a need-to-know basis is provided by the access page. Different forms of access rules may be applied simultaneously with priority given to the most important. The firewall and other security-related features are available on the Security page. The Services page contains settings for VLAN, bridge, and other networking parameters.



(a) Access Policies (b) Bandwidth Monitoring

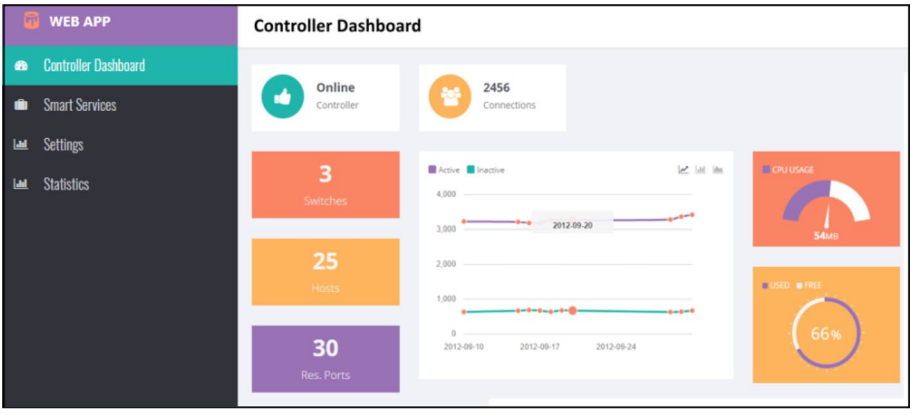
(c) Security Policies (d) VLAN Configurations

Fig. 5 Primary Open Flow Switch Interfaces

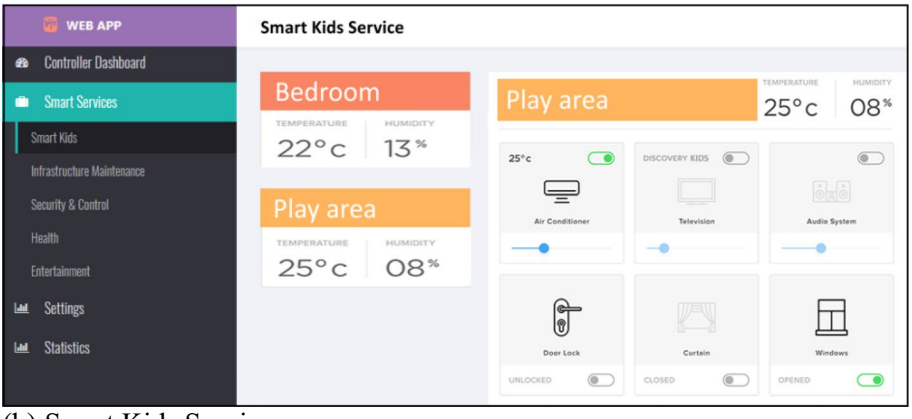
4 Prototype for smart home

We created a smart home prototype, which is essentially an application that allows the network to monitor and manage all linked devices, mostly using computers or smart phones. Smart home apps may now control and manage numerous systems in smart homes through a local area network or a wide area network. Users may monitor the status of smart homes using an application included within the framework architecture. It allows the user to operate smart services and get alerts. In the application, each smart service has its own control interface. The user may make changes to the settings or see the current state, as well as receive any service-generated warnings. The application may be accessed both on a computer and on a mobile device. The application's interface is seen in Fig. 6.

The application's dashboard displays several information, such as the controller's condition, the number of switches installed in the smart home, the number of hosts presently connected, reserved ports, CPU consumption, RAM utilization, and the overall number of connections. The Smart Services page displays all of the smart services that are available. It is possible to access and administer each smart services interface. The user may manage



(a) Dashboard



(b) Smart Kids Service

Fig. 6 Screenshot of Build API

every part of the service using a smart application, for example, while mom is doing her laundry, she can check on her kids who are playing in their play area and take active safety precautions such as setting limits and playing cartoons. As a result, the kids are occupied with cartoons, and she can wash her clothes in peace. Users may design bulk actions for certain scenarios. For example, if a user leaves for work, many actions may be required, such as locking the doors, shutting off the lights, activating the security system, and turning off the cooling/heating system. Coming home after work necessitates rational behaviour.

In today's society, we can see how technology influences our everyday lives in terms of employment, entertainment, security, and children's activities, among other things. Different types of smart services that employ smart items are one of the primary elements that make this feasible. Many duties are automated by these smart services and gadgets. Smart service is the use of specialized skills in acts, processes, and performances that are made possible by smart goods. Whether it's during recreation or when studying, children may be challenging to manage. Parents desire to conduct their job while keeping an eye on their children in these times. The Smart Kids Service was introduced to assist parents and guardians. This application offers an active atmosphere for children in which technology assists them in physical activities and keeps them occupied in their studies. This application also sends out notifications to parents or guardians anytime anything out of the ordinary occurs at a certain time. Smart Infrastructure Service is another significant smart service. For improved home care, the application provides timely maintenance warnings, data on infrastructure status, and material consumed. This service will assist in decreasing the costs and damage that are often incurred as a result of poor housekeeping. Some entertainment services, such as Hulu, Netflix, and iFlix, have become indispensable in modern living. Smart Entertainment Service will integrate with intelligent services in smart homes to give high-quality entertainment. To deliver next-generation smart home services, several kinds of online services may be combined with the proposed framework. Integrating intelligent online services with smart homes is an intriguing concept.

5 Performance evaluation

The performance assessment of our suggested framework was covered in this part. The studies were carried out using the Mininet simulation software. There are two SDN controllers in the proposed ecosystem. One controller serves as a remote controller, often known as a main controller, while the other serves as a local controller. We tested various performance factors with two alternative SDN topologies: local and cloud-based. Using the iPerf command, simulations were run for 15 s to assess network and smart service performance. The connection speed has been set to 100Mbps.

First, we evaluated the throughput of our proposed cloud-tree topology to SDN topologies based on local and cloud resources. In these topologies, we also tested the performance of three controllers. Using the pingFull approach, Fig. 7 demonstrates the RTT of POX, NOX, and flood light in local, cloud-based, and cloud-local tree hierarchical topologies. Our cloud-local tree topology produced the best RTT delay in all three POX, NOX, and Flood Light controllers, according to the data. When compared to local and cloud-based topologies, the reaction times of all three controllers in our cloud-Local topology are lower: 92 msec for POX, 22 msec for NOX, and 19 msec for Flood Light RTT. POX controllers are utilised in small networks, whereas NOX and flood lights are used in complicated and huge networks. Table 1 represent the RTT comparison results.

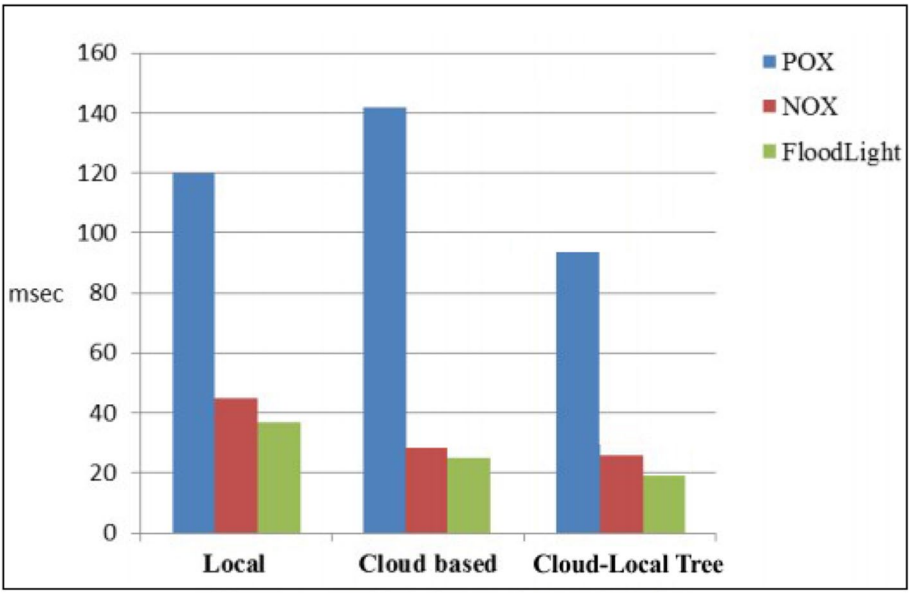


Fig. 7 RTT Comparison

The throughput performance of services employing the TCP and UDP protocols is shown in Fig. 8. The average throughput for smart services using the UDP protocol was 97 Mbps, whereas the average throughput for TCP was 88 Mbps.

Experiments are also carried out to demonstrate the framework's capability in the event of a connection breakdown. When a connection failure occurs, the LSD controller sets the connection timeout parameter to collect the data and decides whether or not to redirect the current streams. The link layer discovery protocol is used to obtain information about available connections. Simulations revealed that the average downtime in UDP and TCP is 3 and 9 s, respectively. This offers the controller the concept of how to manage these types of link down circumstances and make appropriate decisions.

In terms of process rate of packets in messages and replies. Table 2 illustrates the results of mean throughput in different toplogies, Fig. 9 shows the mean throughput of topologies such as local, cloud-based, and our cloud local tree. The mean throughput of our cloud local tree topology is 10.5Mbps, which is slightly higher than the cloud based topology.

Table 1 RTT Comparison

RTT (msec) in different Topologies			
Controllers	Local	Cloud based	Cloud tree
POX	120	142	: 92 msec
NOX	45	25	22 msec
Floodlight	38	22	19 msec

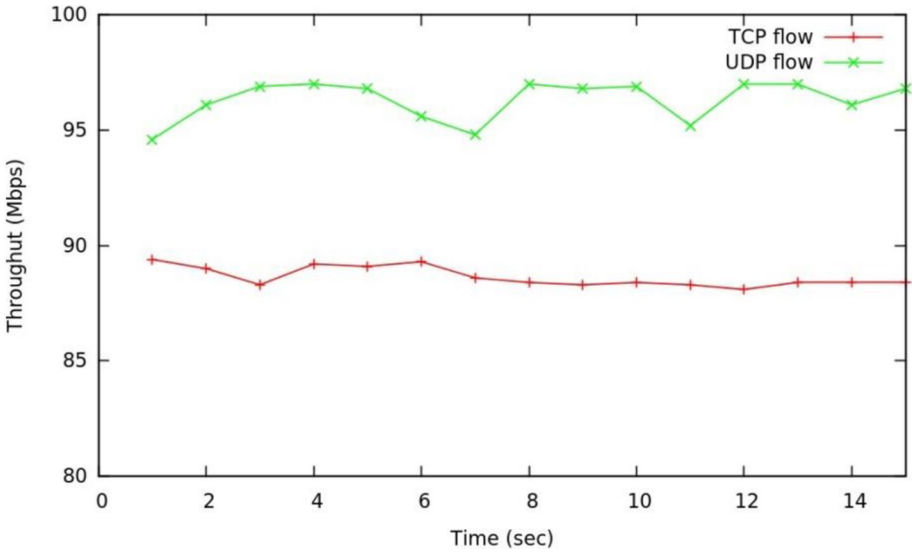


Fig. 8 TCP/UDP Services Throughput

Following simulations were run to evaluate the bandwidth priority module after activating the smart kids services. The graph in Fig. 10 depicts bandwidth allocation priorities. The bandwidth allocation priorities change based on the requirements of each service. A normal, non-smart device used up to 17Mbps of bandwidth.

Using iPerf, we discovered that a typical device received UDP data on a shared bandwidth of 20 Mbps at a rate of 90% until the smart kid's service was enabled. When smart kids services were enabled on the device, however, the internet rate on a regular home device dropped to 7 Mbps. We obtained data up to 14 Mbps when the smart kids service gadget was given priority. Because all devices must first register under services, this aim may be accomplished with the aid of the LDP device database. In order to examine the overhead performance of the proposed framework, the memory, processing, and bandwidth performance of the controller were monitored. Figure 11 depicts the performance of the proposed framework, which comprises processor, bandwidth, and memory. The findings indicated that when packet loss increased, the usage rate of the CPU, bandwidth, and memory increased linearly.

Table 2 Throughput (Mbps) in different Topologies

Throughput (Mbps) in different Topologies			
Topologies	Throughput (Mbps)	Maximum Throughput with TCP flow (Mbps)	Maximum Throughput with UDP flow (Mbps)
Local	8.5	97	88
Cloud based	10.9	97	88
Cloud tree	11	97	88

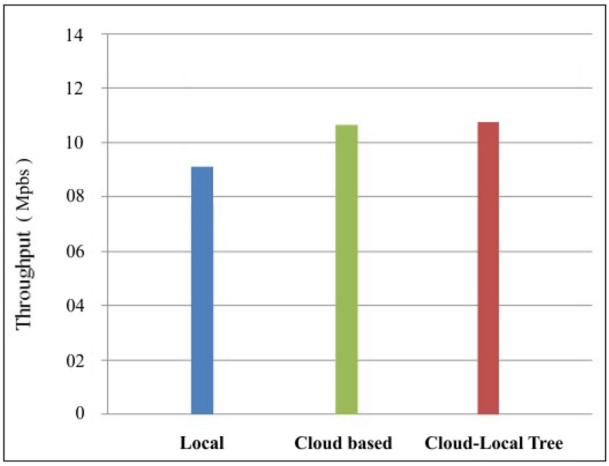


Fig. 9 Topologies Throughput

In all three topologies, Fig. 12 depicts the rate of packet loss when various smart services transmit packets at varying speeds and there are pre-existing links between sender and recipient. The bandwidth is set at 300Mbps for this experiment, and services transfer data at varying speeds. When a controller is engaged in building the pathways between transmitter and receiver, the experiment is repeated. Table 3 represents the packet loss ratio of all topologies.

For all three controllers, i.e., POX, NOX, and Flood light, Fig. 13 shows a comparison of flow installation time vs. the number of switches. When the number of switches

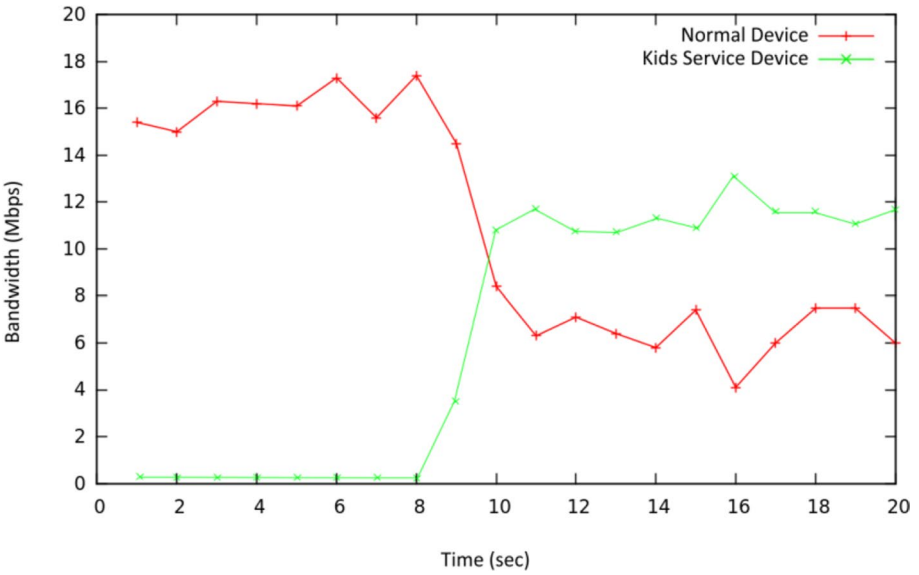


Fig. 10 Bandwidth Priority

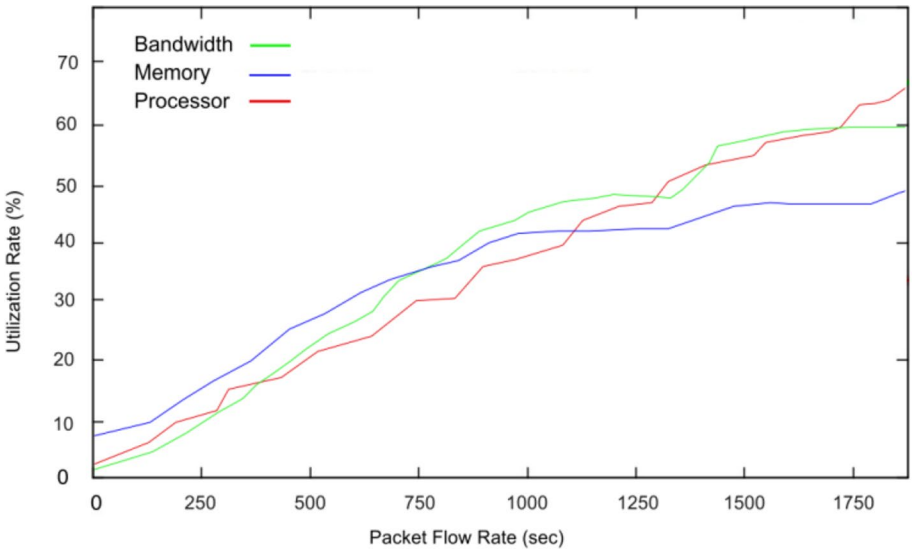


Fig. 11 Controller Utilization

is set to 2, the flow installation time for NOX is 80ms, while it is 70ms and 39ms for POX and Flood light, respectively. The flow time changes as the number of switches increases. When the number of switches reaches 16, the flow installation time for NOX and POX is 80 milliseconds, whereas the flow installation time for Flood light is 36 milliseconds.

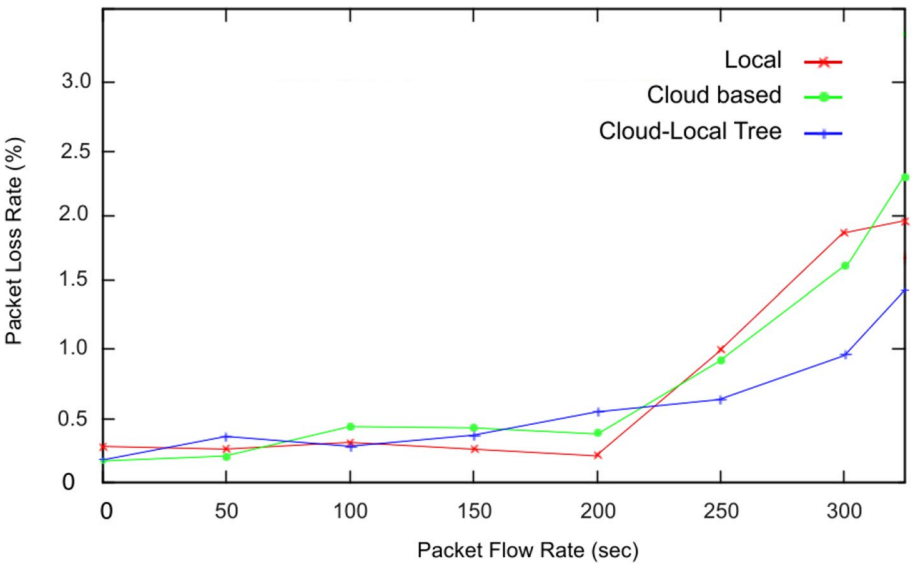


Fig. 12 Packet Loss Ratio

Table 3 Packet loss rate (%) in different Topologies

	Packet loss rate (%) in different Topologies		
	Flow Rate in secs		
Topologies	50	200	300
Local	0.4	0.5	0.7
Cloud based	0.28	0.4	1.8
Cloud tree	0.2	0.2	1.9

6 Conclusion and future directions

This article presented a framework for smart services in smart homes based on SDN. The multi-level structure, which consists of two controllers, is the primary contribution of this study. One is a remote controller that acts as the main controller. This remote controller ensures that external and internal services are delivered in a consistent manner. Our suggested framework's security and performance were also prioritized. With the addition of several additional smart home services to the proposed framework, the smart home environment will be improved. Mininet is used to assess the performance of the proposed framework for evaluation purposes. Smart houses and services are critical to providing homeowners with efficient services. One of the key concepts for delivering smart home services is software-defined networking (SDN). In this study, we presented a multilayer SDN-based system for providing internal and external services in a seamless manner. We concentrated mostly on services and smart services systems. We want to enhance multi-level

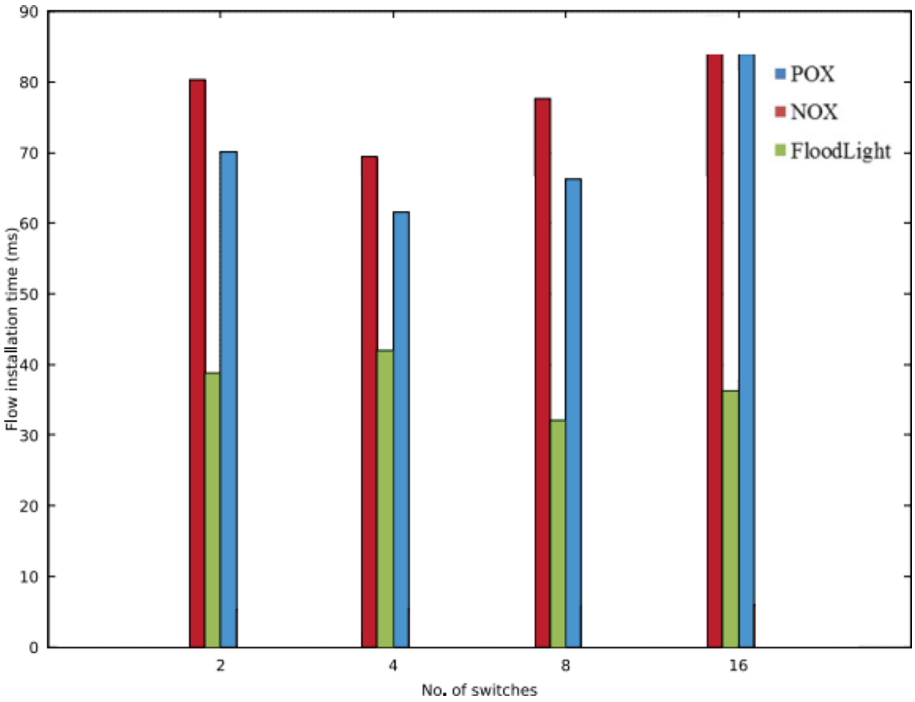


Fig. 13 Comparison of flow installation time vs. no of switches

cloud-based apps in the future. We have created an API for smart homes to make it easier to provide current and new services. Finally, in this work, a comparison of local, cloud, and cloud-local topologies is offered. POX, NOX, and flood light were the SDN controllers.

we employed in our assessment part for all three topologies. Three performance indicators were used to evaluate the system: mean throughput, round trip time, and packet loss. For the cloud-local topology, we obtained the lowest packet loss of 1.4%. Future studies will involve evaluating the performance of multiple cloud frameworks for smart homes that are integrated with AI. Future development will involve the use of an AI-enabled tiered cloud infrastructure for smart homes. In some application domains, such as smart healthcare monitoring for patients, the performance of a tiered cloud infrastructure integrated with AI algorithms may be assessed. Cyber security is another significant need that may be solved in the future.

Author contributions Syed Mushhad M. Gilani and Muhammad Usman conceived and designed the proposed scheme and prepared the initial draft version. Saqib Daud and Asif Kabir performed the experiments. Qamar Nawaz analyzed the results and wrote the results of manuscript, Oláh Judit performed the editing and proofreading of the manuscript, and also supports in funding for this research work. All authors read and approved the final manuscript.

Funding Open access funding provided by University of Debrecen.

Data availability Data sharing not applicable to this article.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Abhishek R, Zhao S, Tipper D, Medhi D (2017) SeSAMe: software defined smart home alert management system for smart communities. In: IEEE Workshop on Local and Metropolitan Area Networks 2017–June. https://doi.org/10.1109/LANMAN.2017.7972142
2. Almási B, Harman A (2013) An overview of the multipath communication technologies. In: Proc. Conf. on Advances in Wireless Sensor Networks, pp 7–11
3. Alshnta AM, Abdollah MF, Al-Haiqi A (2018) SDN in the home: a survey of home network solutions using Software defined networking. Cogent Eng 5(1):1–40. https://doi.org/10.1080/23311916.2018.1469949
4. Atzori L, Iera A, Morabito G, Nitti M (2012) The social internet of things (SIoT) - when social networks meet the internet of things: concept, architecture and network characterization. Comput Networks 56(16):3594–3608. https://doi.org/10.1016/j.comnet.2012.07.010
5. Balta-Ozkan N, Boteler B, Amerighi O (2014) European smart home market development: public views on technical and economic aspects across the United Kingdom, Germany and Italy. Energy Res Soc Sci 3:65–77. https://doi.org/10.1016/j.erss.2014.07.007

6. Banerjee A, Sufyanf F, Nayel MS, Sagar S (2018) Centralized framework for controlling heterogeneous appliances in a smart home environment. In: 2018 International Conference on Information and Computer Technologies (ICICT). IEEE, pp 78–82. https://doi.org/10.1109/INFOCT.2018.8356844
7. Ben Attia M, Nguyen KK, Cheriet M (2019) Dynamic QoE/QoS-aware queuing for heterogeneous traffic in smart home. IEEE Access 7:58990–59001. https://doi.org/10.1109/ACCESS.2019.2914658
8. Boavida F, Kliem A, Renner T, Riekki J, Jouvray C, Jacovi M, ... Triviño A (2016) People-centric Internet of Things—challenges, approach, and enabling technologies. In: Intelligent Distributed Computing IX: Proceedings of the 9th International Symposium on Intelligent Distributed Computing–IDC'2015, Guimarães. Springer International Publishing, pp 463–474. https://doi.org/10.1007/978-3-319-25017-5_44
9. Chen W, Xiao S, Liu L, Jiang X, Tang Z (2020) A DDoS attacks traceback scheme for SDN-based smart city. Comput Electr Eng 81:106503. https://doi.org/10.1016/j.compeleceng.2019.106503.)
10. Darby, S. J. (2018). Smart technology in the home: time for more clarity. Building Res Inform 46(1):140–147. https://doi.org/10.1080/09613218.2017.1301707
11. Daud S, Gilani SMM, Riaz MS, Kabir A (2019) DSDV and AODV protocols performance in internet of things environment. In: 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), pp 466–470. https://doi.org/10.1109/ICCSN.2019.8905256
12. Daud S, Gilani SMM, Hamid I, Kabir A, Nawaz Q (2020) Dsdv and Aodv protocols performance in internet of things based agriculture system for the wheat crop of Pakistan. Pakistan J Agric Sci 57(X):1–9. https://doi.org/10.21162/PAKJAS/20.9249
13. Demetriou S, Zhang N, Lee Y, Wang X, Gunter CA, Zhou X, Grace M (2017) HanGuard: SDN-driven protection of smart home WiFi devices from malicious mobile apps. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp 122–133. https://doi.org/10.1145/3098243.3098251
14. Eghbali H, Wong VW (2015) Bandwidth allocation and pricing for SDN-enabled home networks. In: 2015 IEEe international conference on communications (ICC). IEEE, pp 5342–5347. https://doi.org/10.1109/ICC.2015.7249173
15. Flores Moyano R, Fernández D, Bellido L, González C (2017) A software-defined networking approach to improve service provision in residential networks. Int J Netw Manag 27(6):e1984. https://doi.org/10.1002/nem.1984
16. Flores Moyano R, Fernández D, Cambronero L, Bellido Triana (2017) A user-centric SDN management architecture for NFV-based residential networks. Comput Stand Interfaces. https://doi.org/10.1016/j.csi.2017.01.010
17. Hernando ABG, Farina ADS, Triana LB, Pinar FJR, Cambronero DF (2017) Virtualization of residential IoT functionality by using NFV and SDN. In: 2017 IEEE international conference on consumer electronics (ICCE). IEEE, pp 86–87. https://doi.org/10.1109/ICCE.2017.7889240
18. Gordon H, Batula C, Tushir B, Dezfouli B, Yuhong L (2021) Securing smart homes via software-defined networking and low-cost traffic classification. In: 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, pp 1049–1057. https://doi.org/10.1109/COMPSAC51774.2021.00143
19. Han B, Gopalakrishnan V, Ji L, Lee S (2015) Network function virtualization: challenges and opportunities for innovations. IEEE Commun Mag 53(2):90–97. https://doi.org/10.1109/MCOM.2015.7045396
20. Huh J, Seo Y (2019) Understanding edge computing: engineering evolution with artificial intelligence. IEEE Access 7:164229–164245. https://doi.org/10.1109/ACCESS.2019.2945338
21. Illy P, Kaddoum G, Kaur K, Garg S (2022) ML-based IDPS enhancement with complementary features for home IoT networks. IEEE Trans Netw Service Manag 19(2):772–783. https://doi.org/10.1109/TNSM.2022.3141942
22. Jang H-C, Lin J-T (2017) SDN based QoS aware bandwidth management framework of ISP for smart homes. 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp 1–6
23. Jang HC, Huang CW, Yeh FK (2016) Design a bandwidth allocation framework for SDN based smart home. In: 2016 IEEE 7th annual information technology, electronics and mobile communication conference (IEMCON). IEEE, pp 1–6. https://doi.org/10.1109/IEMCON.2016.7746320
24. Jiménez Y, Cervelló-Pastor C, García AJ (2014) On the controller placement for designing a distributed SDN control layer. In: 2014 IFIP Networking Conference. IEEE, pp 1–9. https://doi.org/10.1109/IFIPNetworking.2014.6857117

25. Jo J, Lee S, Kim J (2014) Software-defined home networking devices for multi-home visual sharing. IEEE Trans Consum Electron 60(3):534–539. https://doi.org/10.1109/TCE.2014.6937340
26. Kim Y, Lee Y (2015) Automatic generation of social relationships between Internet of Things in smart home using SDN-based home cloud. In: 2015 IEEE 29th International conference on advanced information networking and applications workshops. IEEE, pp 662–667. https://doi.org/10.1109/WAINA.2015.93
27. Lee M, Kim Y, Lee Y (2015) A home cloud-based home network auto-configuration using SDN. In: 2015 IEEE 12th International conference on networking, sensing and control. IEEE, pp 444–449. https://doi.org/10.1109/ICNSC.2015.7116078
28. Luo S, Wu J, Li J, Guo L (2016) A multi-stage attack mitigation mechanism for software-defined home networks. IEEE Trans Consum Electron 62(2):200–207. https://doi.org/10.1109/TCE.2016.7514720
29. Nobakht M, Sivaraman V, Boreli R (2016) A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. In: 2016 11th International conference on availability, reliability and security (ARES). IEEE, pp 147–156. https://doi.org/10.1109/ARES.2016.64
30. Oracle (2014) The internet of things: manage the complexity, seize the opportunity, pp 1–12
31. Sharma PK, Park JH, Jeong YS, Park JH (2019) SHSec: SDN based secure smart home network architecture for internet of things. Mob Networks Appl 24(3):913–924. https://doi.org/10.1007/s11036-018-1147-3
32. Sivaraman V, Gharakheili HH, Vishwanath A, Boreli R, Mehani O (2015) Network-level security and privacy control for smart-home IoT devices. In: 2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob). IEEE, pp 163–167. https://doi.org/10.1109/WiMOB.2015.7347956
33. Stojkoska BLR, Trivodaliev KV (2017) A review of internet of things for smart home: challenges and solutions. J Clean Prod 140:1454–1464. https://doi.org/10.1016/j.jclepro.2016.10.006
34. Stolojescu-Crisan C, Crisan C, Butunoi BP (2021) An IoT-based smart home automation system. Sensors 21(11):3784. https://doi.org/10.3390/s21113784
35. Tao M, Ota K, Dong M (2017) Ontology-based data semantic management and application in IoT- and cloud-enabled smart homes. Futur Gener Comput Syst 76:528–539. https://doi.org/10.1016/j.future.2016.11.012
36. Wang S, Wu X, Chen H, Wang Y, Li D (2014) An optimal slicing strategy for SDN based smart home network. In: 2014 International conference on smart computing. IEEE, pp 118–122. https://doi.org/10.1109/SMARTCOMP.2014.7043848
37. Wood T, Ramakrishnan KK, Hwang J, Liu G, Zhang W (2015) Toward a software-based network: integrating software defined networking and network function virtualization. IEEE Netw 29(3):36–41. https://doi.org/10.1109/MNET.2015.7113223
38. Xu K, Wang X, Wei W, Song H, Mao B (2016) Toward software defined smart home. IEEE Commun Mag 54(5):116–122. https://doi.org/10.1109/MCOM.2016.7470945
39. Yan Q, Yu FR, Gong Q, Li J (2015) Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Commun Surv Tutorials 18(1):602–622. https://doi.org/10.1109/COMST.2015.2487361

Authors and Affiliations

Syed Mushhad Mustuzhar Gilani[1] · Muhammad Usman[1] · Saqib Daud[2] · Asif Kabir[3] · Qamar Nawaz[4] · Oláh Judit[5,6]

Syed Mushhad Mustuzhar Gilani
mushhad@uaf.edu.pk

Muhammad Usman
ranamusman92@gmail.com

Saqib Daud
saqibmirza.daud@gmail.com

Asif Kabir
asifkabirumsit@outlook.com; asif.kabir@uajk.edu.pk

Qamar Nawaz
mqamarnawaz@hotmail.com

1 UIIT, PMAS, Arid Agriculture University, Rawalpindi, Pakistan

2 Shaheed Zulfikar Ali Bhutto Institute of Science & Technology, Islamabad, Pakistan

3 Department of CS & IT, University of Kotli, Azad Jammu & Kashmir, Kotli, Pakistan

4 Present Address: Department of Computer Science, Agriculture University, Faisalabad, Pakistan

5 Faculty of Economics and Business, University of Debrecen, Debrecen 4032, Hungary

6 College of Business and Economics, University of Johannesburg, Johannesburg 2006, South Africa