Journal of Intelligent Systems and Internet of Things
Vol. 12, No. 02, PP. 75-88, 2024
DOI: https://doi.org/10.54216/JISIoT.120206

Securing Pervasive Computing Networks: Enhancing Network Security via Network Virtualization in Wireless Communications Infrastructure

Ali Kadhim Nsaif
Department of Software Engineering, South Tehran Azad University, Tehran, Iran

*Corresponding Author: alikadem.2025@gmail.com

Abstract

The seamless integration of technology for computing into everyday items and environments is known as pervasive computing. To protect against cyber threats and vulnerabilities, robust security mechanisms are necessary. Conventional security measures, including gateways and the use of encryption, may not be sufficient to address the unique challenges encountered in ubiquitous computing systems. But these techniques are still vital. In addition to the variety of devices, resource limitations, mobility needs, and the possibility of large-scale distributed attacks, these obstacles also include the potential for attack. Network virtualization, that abstracts and separates network facilities and functions, is a promising way to increasing security in pervasive computing deployments: it abstracts and isolates network resources and processes. Wireless communication play a significant part in the development of a digital infrastructure that is both resilient and trustworthy. The processes of dynamic resource allocation, isolation, and management of network bandwidth are made possible through the utilization of virtualization, leads to the proposal of Secure Wireless Virtual Resource Allocation and Authentication Algorithm(SWVRA3) to make the abstraction of the network's physical resources into virtualized entities By using network virtualization, pervasive computing applications and services can be secured with logically segregated virtual networks. The cross-contamination and security breaches can be reduced by this separation. Furthermore, flexible *configuration, dynamic allocation of resources, and centralized virtual control are allowed by* network visualization that improves threat incidence response, enforcement of policies, and security surveillance.

Received: March 02, 2024 Revised: Aprial 03, 2024 Accepted: April: 19, 2024

Keywords: Network security; Computing network; Authentication accuracy; Wireless sensor network; Virtualization; Resource utilization.

1. Introduction

Virtualization is efficient and well-established, allowing the sharing of similar hardware resources by several users [1]. Also, the technique allows numerous users to efficiently share, access and use the physical resources of logical representation created by the technique [2]. Virtualization revolves around the abstraction and distribution of resources [3]. Virtualization can significantly reduce equipment and management costs compared to traditional approaches by increasing hardware utilization, decoupling functionality from infrastructure, facilitating the move to more current services and products, and allowing for more versatile management [4]. "virtualization" refers to a wide range of technologies that have become increasingly popular in the information and communications technology sector [5].

A framework that includes devices, software, maintenance, and safety procedures to manage and distribute communications via wireless networks. Therefore, communication via wireless network is necessary. By network of networks the virtualization process, the system mean the process of encapsulation the capabilities of a network from its core hardware components. A rising trend in computing is the integration of processing capablities, usually processors into ordinary items so that they can communicate effectively and carry out beneficial functions, thereby

reducing the need for the end user to interact with computers directly. The ever-present internet connectivity of our devices is used by a form of pervasive computing. Consequently, virtualization necessitates a ubiquitous system-based computing architecture.

In IoT devices, implementing verified higher layer security techniques is challenging due to limited communication and compute capabilities. The physical layer security framework offers a long-term safety measure by utilizing associated physical layer capabilities and settings, in addition to chaotic channel-related computing, to secure communications without conventional encryption methods [6]. Microelectromechanical systems (MEMS), wireless networking, and digital electronics all come together in these WSN nodes, allowing them to collect data from their surroundings, process it, and share it with other nodes in the network [7]. When WSNs are virtualized, several applications can share the same network without disrupting performance [8]. It makes network virtualization a promising technique for maximizing the value of WSN installations [9]. As a technique fundamental to realizing the Future of the Internet, virtualization bears serious investigation in the context of WSNs [10].

WSN virtualization is a crucial enabling technology that relies on citizen-generated sensors to collect the necessary data rather than deploying and operating specialized sensors [11]. The physical layer between central stations and the devices of consumers is vulnerable to data fraud and eavesdropping. The least secure layer cannot provide enough security alone. Each layer of the wireless networks infrastructure has its own technologies, thus they must work together to provide virtualized communications safety and reliability[12]. The term pervasive computing refers to integrating all the digital and computational tools used in our daily lives, not just those accessed on our desktop computers [13].

Deploying pervasive computing applications in the wild relies heavily on reliable, safe, and rapid middleware installation on multiple workstations [14]. They use a heterogeneous collection of input/output (I/O) devices, runtime libraries, software platforms, and rusty bits of code [15]. Soon, the embedded computers that regulate environmental equipment may be little more than cloaked smartphones [16]. Accurate computers and smartphones can communicate with, command, and coordinate with other gadgets in their immediate vicinity [17]. Sensors and actuators are quickly becoming a standard component in pervasive computing architectures [18]. The time has come to think about how to better use and distribute these resources through virtualization [19]. Due to WSN virtualization, several programs can use the same WSN hardware and software [20]. When it comes to virtualizing WSNs, there are two options. The first is to have one set of sensor nodes run one application while another group runs the second set of applications simultaneously (or nearly simultaneously) [21]. There is some flexibility in the size and number of these subgroups to accommodate different uses. The second method takes advantage of the unique qualities of each sensor node to perform several additional application works. Other sensor node handles each application duty, while the physical nodes are identical [22].

A physical server can be split up into several "virtual servers," each of which appears to end users as if it were running on its separate computer despite sharing the original physical server's hardware resources (CPU, memory, network interface card, and storage). Allocating physical resources to virtual ones to achieve maximum utilization of the former while still satisfying the latter's performance needs is a complex problem. Virtualization's benefits are increased hardware efficiency, simpler transition to new goods or technologies while maintaining legacy products, and lower equipment and management costs [23]. This infrastructure allows for the rapid transmission of information while maintaining its security and dependability. Utilizing network virtualization presents a possible method to strengthening security inside wireless networks that are supporting deployments of pervasive computing that are being implemented. This research also examines wireless network virtualization's structures, difficulties, and future prospects, giving a comprehensive framework for understanding and tackling pervasive computing security issues. This research uses network virtualization's flexibility and isolation to create secure, resilient, and reliable pervasive computing environments that effortlessly incorporate into our daily lives and protect against cyber threats.

The key contributions are as follows:

- To improve pervasive computing security, create a Secure Wireless Virtual Resource Allocation and Authentication Algorithm (SWVRA3) to abstract and isolate network resources for improving resource utilization, and authentication accuracy.
- Improving security monitoring, and incident response to threats can be achieved through the use of network virtualization, which allows for dynamic resource allocation, flexible setup, and centralized virtual control.
- Logically segregating virtual networks improves pervasive computing application and service security, minimizes security breaches, and makes the digital infrastructure resilient and trustworthy.

The following is the structure of this paper: Background information for the study will be presented in Section 2, and Section 3 will introduce a model that improves and provides an optimal solution for SWVRA3 for network virtualization control, etc. Section 4 evalautes the proposed model and presents outcomes with metirc evaluation authentication accuracy, resource utilization, and false acceptance rate and false rejection rate, while Section 5 provides a endnote and a brief overview.

2. Related Works

This study reviewed several strategies for improving virtualization through the wireless communication infrastructure. Future research on the subject should make heavy use of these methods.

Xue, P., & Jiang [24] aimed to secure Network Functions Virtualization (NFV) networks, where traditional network services have been virtualized into Virtualized Network Function that rely on standard Hardware Applications(HA), against multiple threats, including the Sybil attack. The intricate VNF-HA mapping link makes dependability and security difficult throught the developed NFV network. VNF-HA mapping strategies to optimize allocation of resources and security.SecRouting, a multi-path safe routing technique, efficiently routes data packets via the NFV infrastructure while preventing Sybil attacks.Security and traffic capacity are evaluated to show that SecRouting improves security and network performance.

Wang et al. [25] highlighted the predicted paradigm shifts that are expected to occur with 6G, such as the utilization of additional spectrum, the incorporation of artificial intelligence and machine learning technologies, and the establishment of an integrated network that spans numerous domains through dynamic Trust Evaluation Platform(dTEP-FL) through Federated Learning. The study emphasized the wireless network infrastructure, xenogenesis and sustainable trust of wireless network environment. With the use of asymmetric crypto and tamper proof security through blockchain. The study was evaluated with e-health sector using 6 trust paradigm for making decision in network trust for secure communication.

El-Haggar et al., [26] promoted secure Ubiquitious Learning (secU-Learn) for enhancing learning behavior, motivation, creativity and providing authentication and privacy of user data within the wireless signals. This includes IoT devices like smart cards, sensor network nodes, radio frequency identifiers plays a major role in preventing unauthorized access and denial of service attacks in this network. This framework consists of 3 phases like perception, network and application also addressed privacy preserving measures for these phases. Using smart locks on doors, digital surveillance cameras, and school bus tracking to keep students and teachers safe. Learning platform or mobile device data leaks or cyberattacks can cause identity, financial, and IP theft. To protect systems and data, organizations encryption and firewalls were employed.

Khan et al. [27] explored WSN virtualization [WSN-VIoT] in which the Internet of Things (IoT) is a paradigm shift that relies heavily on Wireless Sensor Networks (WSNs). In most cases, organizations deploy WSNs to back up a single app. Installing middleware remotely on embedded computers that can be found on these machines is challenging. Virtualization technology may facilitate this sharing. The first step was to define and differentiate between node-level, network-level, and hybrid WSN virtualization. WSN virtualization is highly relevant in the setting of the IoT, where a record number of small-scale devices are anticipated to offer amenities for numerous applications at the same time and where a critical analysis of the existing state-of-the-art in each category is given and assessed based on a set of demands derived from the inspiring scenarios.
Alam et al. [28] provide a comprehensive and organized analysis of Virtualization Methods [VM] developed for IoT networks. More complex, effective, and flexible approaches for administration, arrangement, and flow scheduling are required as the physical architecture of networked devices evolves. Network virtualization models have garnered much interest as possible answers to the challenges posed by the Internet of Things. This method brings to light many open issues and research obstacles connected to the widespread implementation of the software-defined Internet of Things.

The existing works related too wireless network virtualization and security research addresses issues and opportunities in this industry. One study proposes resource allocation optimization and SecRouting to secure NFV systems toward vulnerabilities like the Sybil attack. Another study emphasises how artificial intelligence and machine learning will change 6G networks and how trust evaluation systems will provide secure wireless connection. For IoT devices, secure Ubiquitous Learning (secU-Learn) addresses authentication, privacy, and security problems by improving learning behavior and privacy in wireless signals. Another study examines Wireless Sensor Network (WSN) virtualization for IoT applications, emphasizing resource sharing among devices to support different applications. Finally, an in-depth examination of Virtualization Methods (VM) for IoT networks shows how software-defined networks (SDNs) and network function virtualization (NFVs) can address evolving IoT network architecture challenges and outline key research obstacles to their widespread implementation. These research expand wireless network virtual and secure knowledge and methods.

3. Secure Wireless Virtual Resource Allocation and Authentication Algorithm(SWVRA3):

Pervasive computing, as computing features are effortlessly integrated into common products and situations, has enabled digital innovation and improved user experiences. There are risks to security and flaws caused by the ubiquitous and linked nature of these technological goods. The network resilience and safety are of the utmost importance due to the increasing reliance of pervasive computing devices upon a wireless network communication structure for the transmission and collaboration of information.

The advent of the fifth generation of wireless networks will mark the beginning of a new age characterized by ubiquitous connectivity, wireless applications that are aware of their surroundings, and extremely individualized customer experiences. Nevertheless, for fifth-generation to fulfill its potential, it must offer networks far more connectivity, allow for dense communication between endpoints with little latency and cost, generate a lot of power, and be more affordable than existing wireless standards. There are several areas that WSN virtual could offer cost-effective and efficient approaches, including smart cities, smart homes, smart health, sustainable technology, and pervasive computing. The advent of omnipresent computing has made it simpler for consumers to combine affordable gadgets with innovative settings. Intelligent gadgets, which contain incorporated processors have made it possible to integrate various pieces of hardware, such as mobile devices, machines, and even ordinary appliances for the kitchen, into complex data networks.

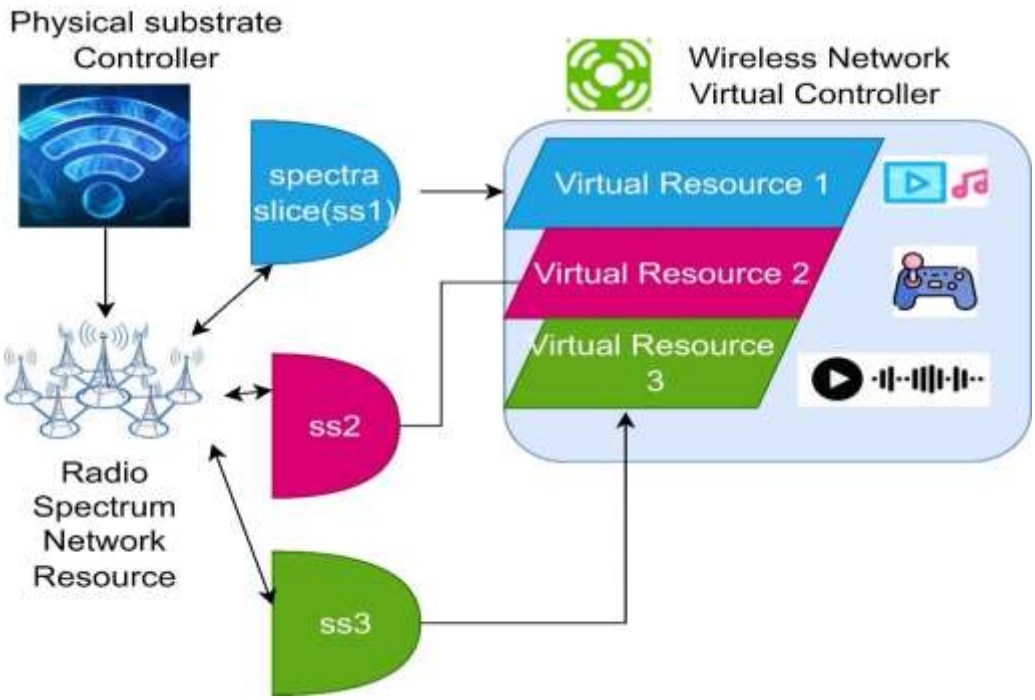

Figure 1: Wireless virtualization of networks paradigm

Figure 1 shows the foundation paradigm for wireless network virtualization with physical substrate controller. A dedicated virtualization layer is used to virtualize the network functions, which helps to improve efficiency, resilience, agility, and flexibility by uncoupling service design from service implementation. The NFV reference architecture allows for the deployment and operation of VNFs across various types of hardware, including servers, storage devices, and networks. Pooling and connecting hardware for processing and storing data is standard practice. Virtualized 5G network functions (VNFs) can be integrated with preexisting technologies using other network resources that link the VNFs to external networks and non-virtualized operations. The benefits of NFV can be realized through resource provisioning modules, which are part of NFV management.

VNF managers are responsible for two primary tasks: running the service and allocating resources. Infrastructure management, fault management, performance management, and capacity planning and optimization are all part of running a virtual network function. Resource provisioning guarantees optimal resource allocation (virtual machines, VMs, servers), connectivity between virtual network functions (VNFs), optimal energy conservation, and resource reclamation. Resource managers can locate infrastructure resources such as computers, storage spaces, and networks.

$$\vartheta_j = \sum_{j=1}^{P} S\,[M_j]^m * (D) \quad (1)$$

From equation (1), ϑ_j is the virtualization function, D indicates the data point, M_j indicates the degree of membership function, m represents the cluster's centroid. S denotes the similarity of data points.

$$C_s = \frac{D_f * \sum_{j=1}^{P} V_R}{\sum_{j=1}^{P} M_j} \quad (2)$$

Equation (2) shows the cluster centers, which are represented by C_s, D_f is the function of data points, V_R is the virtual resources.

$$M_P = \frac{1}{\sum_{L}^{i=1} \frac{D_f - C_j}{D_f - C_i}} \quad (3)$$

In the above equation (3), M_P is the partition matrix, D_f is data function, j denotes the initial cluster, C_i is the cluster iteration process, i denotes the number of iterations. Signal monitoring is done majorly in equation (3).

$$V_L = V_c + V_s + V_n \quad (4)$$

The V_L denotes the virtual layer, which is the combination of V_c which is virtual computing, V_s is the virtual storage, V_n represents the virtual network in equation (4). Throughput is achieved maximum from the above equation.

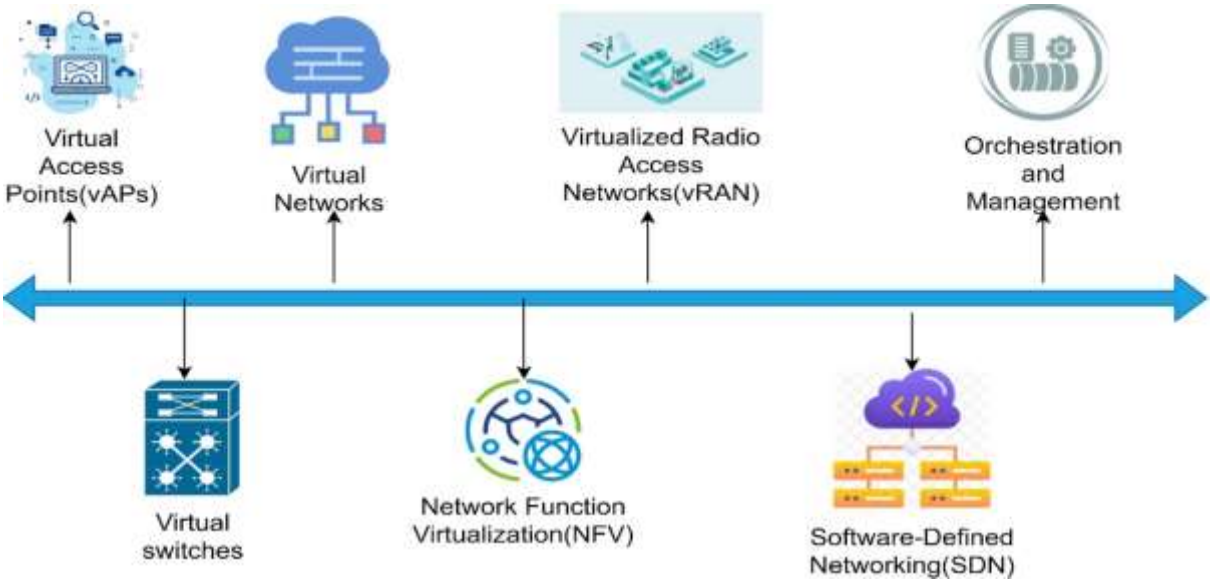

Figure 2: Integration of Network Security Components in Wireless Network Virtualization Infrastructure

A graph representing the concept for adding network security components in the virtualization-based infrastructure of wireless networks is presented in Figure 2. A wireless network virtualization architecture integrates network security components as shown in the system block diagram. Each component is vital to network cyberdefense. Through the use of cryptography along with access authority, virtualized connection points ensure the security of wireless communication. Virtual LANs allow for the separation of network traffic, and virtual switches can safeguard ports. By utilizing segmentation and firewalls, virtual networks are able to control traffic between segments and enforce security requirements. Anomaly detection, secure virtualization gadgets, and the use of virtual network functions strengthening all work together to keep Virtualized services and facilities safe. The process of authentication, proof of identity, the use of encryption, and detection of anomalies are features of virtual radio accessibility networks that help to protect communication channels and maintain the integrity of architecture. By employing access control as well as communication data encryption controllers for SDN can thwart attempts at man-in-the-middle attacks and configuration alterations. Orchestrating and control systems incorporate authorization, encryption of information, and monitoring to safeguard management of network activities. All of these parts work together to form a strong security structure that can ward off cybercriminals targeting virtualized wireless networks.

The network deployment and administration procedures can be made more secure by including the authentication process, encryption, and auditing into management and control platforms with the consideration of the Management Overhead (MO) .

For wireless networks simulation to be effective, a number of prerequisites must be satisfied. These requirements can be categorized as either fundamental or advanced communications based on the level of virtualization implementation required. System separation control, agility, and concurrent existence are the fundamentals. Ability to adapt, reconsideration, diversity, regularity, and advancement, accessibility, and accessible sources are further factors to consider.

The virualized access points security and key management encrypting and monitoring utilization of wireless networks is the capability of virtual access points, which guarantees the security of communications over wireless networks. Quantification of the encryption strength is possible through the utilization of metrics such as the Encryption Ratio (ER) using equation(5).

$$ER = (No.of\ encrypted\ communications)/(total\ communications) \quad (5)$$

Both virtual networking switches and virtual networks have the capability to perform network segmentation through the utilization of virtual local area networks (VLANs) and to impose privacy regulations through the utilization of firewalls in order to regulate communication between portions and the Firewall Efficiency (FE) measure takes into account using equation (6).

$$FE = (No.of\ blocked\ malicious\ packets)/(total\ malicious\ packets) \quad (6)$$

3.1 Framework of Virtualization:

Figure 3: The Network Virtualization for secure wireless Communication Infrastructure

An overview of a secure infrastructure for virtualizing wireless communication networks is provided in the above figure 3 . This paradigm for wireless network virtualization captures the essential principles, components, and relationships established by past research; it may not be universally applicable because each architecture is designed to accomplish a specific goal and is the result of different inspirations. The figure depicts the major components of a wireless network virtualization framework: electromagnetic spectrum, actual wireless hardware, a wireless virtual source of power, and a wireless virtual machine controller.

Radio Spectrum Resource:

In wireless communication, the radio spectrum plays a crucial role. The terms "licensed spectrum" and "dedicated free spectrum" are frequently used interchangeably with the term "radio spectrum resource" (e.g., IEEE 802.11). White spectrum refers to radio frequencies that are not actively used by their owner and are therefore available for use by other parties; their availability has been made possible by the development of cognitive radio. Cognitive radio technology and the advent of heterogeneous networks are changing the relatively rigid nature of spectrum access in cellular networks, allowing for more adaptive and efficient spectrum use.

$$N_s = \left[\frac{\vartheta_j - C_s}{V_L}\right] * M_P \quad (7)$$

Substituting all the above factors in the previous equations, equation (7) obtained the net result for spectrum analysis.

$$N_s = \left[\frac{\left[\sum_{j=1}^{P} S\,[M_j]^m * (D)\right] - \left[\frac{D_f * \sum_{j=1}^{P} V_R}{\sum_{j=1}^{P} M_j}\right]}{V_c + V_s + V_n}\right] * \left[\frac{1}{\sum_{L}^{i=1} \frac{D_f - C_j}{D_f - C_i}}\right] \quad (8)$$

Net output for spectrum is denoted by N_s is calculated as shown above in equation (8).

The concept of making all available to many providers underneath a single contract is known as frequency pooling. By pooling their spectrum goods, A and B may enhance their bandwidth sequencing and heterogeneity profit, thereby improving the ability as well as efficiency of their respective networks. Through the many levels, for example, ranging from one to N, depending on the devices that are wireless linked per the suggested model, the entire virtualization is now a reality. This virtualization removes any access mediums and treats the radio frequency as a single resource. As a result of network wireless the use of virtualization the idea of efficient exchange of spectrum comes to mind and is being promoted.

Infrastructure constructed on Wireless Network:

The physical parts of a wireless network, encompass elements including locations (high towers and broadcasters), central systems, points of entry in wireless networks, wireless transmission networks, and network infrastructure components. Because mobile telephone companies are inherently competitive with one another or with each other over the same network segment, there is neither no sharing at all or very little sharing in certain wireless regions. Virtualization in this framework is thus limited to what is called restricted intra-infrastructure integration. The term infrastructure sharing can describe anywhere from the operation of a single wireless network to the sharing of certain towers and other pieces of hardware. When considering wireless networks from a cloud perspective, network sharing emerges as a crucial method for enabling virtualization. Infrastructure sharing and full network sharing are the two succeeding methods that needs to be analyzed in depth here.

Sharing the Network Infrastructure:

Here, rather than exchanging information through radio signals, customers trade tangible goods. Multiple organizations engage in inactive interaction when they integrate resources like an organization, a location, or a transmission tower. As it stands, "tower companies" are in charge of passive sharing and work with operators to supply passive Radio Access Network (RAN)infrastructures.

When discussing the process of sharing individual components of a mobile network, the term "active sharing" is typically applied to (a) radio frequency (RF) antennas and eNode Base stations in radio access networks (RANs), (b) the transmission networks' backbone and backhaul (c) a network's central components, including routers, switches, and databases (such a visitor's location register, or VLR).

Full network sharing:

When multiple mobile network operators (MNOs) agree to share radio resources and network infrastructure, this is called "full network sharing." It can be applied to several architectures, such as the MOCN and GWCN configurations. In MOCN, the radio access networks (RANs) serve as the communal components. With GWCN, not only may mobile switching centers (MSCs) and serving aggregation and serving nodes (SGSNs) be shared, but also radio access nodes (RANs).

Because of the increased efficiency and adaptability of the underlying physical substrate networks made possible by full network sharing, virtualization has the potential to become ubiquitous. It is meant by the term called "universal virtualization."

$$E_{VR} = \sqrt{\frac{P_m}{L_r - 1}} \sum_{n=1}^{N} \frac{{E_{avg}}^{L}}{E_{avg}} \quad (9)$$

The above equation (9) indicates the percentage of energy for virtual resources, P_m indicates the percentage, E_{avg} is the energy required for the data, r denotes the cluster region. E_{VR} is the energy for virtual resources. Energy efficiency has achieved the maximum in the above equation.

$$Lat = [D_{prop} - D_s] * D_a \quad (10)$$

Equation (10) shows the latency of the network, which is denoted by Lat, D_{prop} is the propagation delay and D_s represents the serialization of data, D_a is the delay in data sent to the network.

Wireless Virtual Resource analysis using SWVRA3

The SWVRA3 method guarantees that virtual resources are allocated to service requests in a secure and efficient manner, taking into account the availability of such resources. The incorporation of an authentication system allows for the verification of the authenticity of requests prior to the allocation of resources. Initialize the set of available virtual resources $VR = \{vr_1, vr_2, .. vr_n\}$ and initialize the set of service requests $SR = \{sr_1, sr_2, .. sr_n\}$ .For each request sr_i in SR extract the required virtual resource set $VReq$ and check the condition for below available resources and trigger authentication process for sr_i using digital certificates and protocols like kerberos for providing enhanced network security. Virtual slices of wireless network infrastructure and spectrum are used to create virtual pieces of wireless resources like resource 1, resource 2, and resource 3. A perfect world would have one virtual entity slice that contained all the virtual entities segmented by the various nodes in a wireless network. Virtualization requirements for wireless resources are thus context-dependent. Spectrum slicing, architecture slicing, network slicing, and flow slicing are the four types of network slicing. The term $VReq$ defines the set of required virtual resources and VR defines the set of available virtual resources using equation 11.

$Sum(VReq) \leq sum(VR)$ (11)

The above equation helps to identify whether sufficient virtual resources are available for a service request in a wireless network. After successful authentication, the allocated virtual resources are instantiated for the requested service. The remaining available resources are updated using equation (12)

$$VR = VR - VReq \quad (12)$$

Authentication and Identification measure of a network security emphasize the Virtualized Radio Access Network (vRAN) components have the ability to authenticate users and devices and identify malicious elements by utilizing protocols for authentication and methods for detecting anomalies during the authorization procedure while entering the netwokr. Quantification of this can be found in the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) from equations 13 and 14.

$$FAR = No.of\ threats\ accepted/total\ threat\ scores \quad (13)$$

$$FRR = No.of\ legitimates\ rejected/total\ legitimate\ scores \quad (14)$$

The accuracy of the authentication accuracy(AA) can be computed using equation (15)

$$AA = 1 - (FAR + FRR) \quad (15)$$

The resource utilization can be identified from virtual resources and derived using the below equation 16.

$$RU(\%) = (sum\ of\ allocated\ virtual\ resources)/(total\ available\ virtual\ resources) \quad (16)$$

Analysis of the effectiveness of the allocation of resources and identification of prospective excessive provisioning or inadequate use events are both possible outcomes that might be aided by this indicator.

***Pseudocode*1**: Service Wireless Virtual Resource Allocation and Authentication Algorithm

Input: Initialize virtual resources and service requests

$VR = \{vr_1, vr_2, .. vr_n\}$ // Set of available virtual resources

$SR = \{sr_1, sr_2, .. sr_n\}$ // Set of service requests

***Step* 1**: Function to authenticate a service request

function AuthenticateRequest(sr) **returns**

Step* 1*a: Perform authentication

return authentication_successful

***Step* 2**: Main algorithm

for each sr in SR ***do***

VRreq = GetRequiredResources(sr) // Get required resources for sr

if $Sum(VRreq) <= Sum(VR)$ ***then***// Check resource availability

Allocate($VRreq, sr$) // Allocate required resources

if AuthenticateRequest(sr) ***then***/ // Authenticate the request

InstantiateService($sr, VRreq$) // Instantiate service

VR = VR - VRreq // Update available resources

else:

ReleaseResources(VRreq) // Release allocated resources

AddToDeniedList(sr) // Add to denied requests list

else:

AddToPendingQueue(sr) // Add to pending requests queue

***Step* 3**: Compute metrics

FAR = ComputeFAR() // False Acceptance Rate

FRR = ComputeFRR() // False Rejection Rate

AuthAccuracy = 1 - (FAR + FRR)

PendingRequestWaitTimes = []

for each pr in PendingRequestsQueue ***do***

PendingRequestWaitTimes.append(GetWaitTime(pr))

AvgWaitTime = Sum(PendingRequestWaitTimes) / len(PendingRequestsQueue)

The pseudocode 1, involves initializing virtual resource sets and service requests, defining an authentication function, implementing an algorithm for iterating over requests, allocating resources, and releasing resources if authentication fails, computing metrics for authentication accuracy and resource utilization, and calculating the average wait time for pending requests.

3.2 Wireless Virtualization Controller:

A wireless virtualization controller can improve the service providers' virtual slices' scalability, control, and programmability. Wireless virtualization controllers make the separation of the control and data planes possible; service providers are given more leeway in organizing their virtual infrastructure under their own "virtual slices." An essential part of wireless virtualization is the controller, which has two counterparts: the substrate and the virtual.

Mobile network operators utilize substrate controllers to virtualize and administer the underlying physical network substrate. Mobile virtual network operators and service providers use a virtual controller to help their respective virtual networks.

Remote hardware can take use of the fact that the virtualization platform automatically regulates the transfer of information between actual and virtual endpoints. The active / passive of multiplexors and the standard layer of virtualization inverter are prerequisites. More complex user-facing software is developed specifically to address the needs of specific applications. For example, with a well-designed transformer system, inbound controls can go in either direction. It is possible to instruct the transformer to use the actual machine, disseminate information, or a remote device through the logic of the management program. The next operation is indicated by the unique collection of method parameters for each transformer.

The ubiquitous computing software of a virtualization machine includes both customer-level and secure deployments at the level of the virtualization. Depending on the software, consumer applications may work best when run as a virtual appliance that limits its impact to a subset of endpoints' data sources. The number of instances and versions on a machine may vary from pervasive computing application to application; for simplicity, assuming a single sample and version throughout. Both static and dynamic configurations of the transformer network are possible.

In the absence of a virtualization layer that insists on passing I/O device streams through SWVRA3 it serves little purpose. The homeowner is, therefore, more likely to approve of its installation. In addition, the virtual appliance doesn't care whether an operating system or runtime libraries are installed on the host computer; it runs on any computer with the necessary virtualization infrastructure. A laptop can download PerCom- VA from a centralized, universal repository or get a copy from a machine close to it that started the pervasive computing application. Although virtualization should help keep things separate, there might still be a requirement for a different SWVRA3 signature.

$$D = \frac{1}{2}\left[\partial_{D,L}\right] * \frac{w_{D,L}}{\emptyset_{D,L}} \tag{9}$$

where D is the delay, $W_{D,L}$ is the arrival date, $\emptyset_{D,L}$ is the processing rate of data on the network, which reduces delay in the network. If the lag can be contained, their network connectivity becomes superior.

The main challenges are establishing trust levels and deciding who controls the I/O stream within a single machine. It is challenging to maintain data security from an I/O device through SWVRA3. A virtual machine's I/O device stream may be incorrectly routed to a different PerCom-VA instance, even if the virtualization software and device drivers are trusted implicitly or explicitly. Any manipulation involving a transformer, such as addition, subtraction, modification, activation, or deactivation, is significant since it breaks the machine's trustworthiness, safety, isolation, and integrity. Unfortunately, a mobile device has many resources. Embedded systems and the need for more lightweight solutions are feasible due to the mediation, making it device flows, not any old flows machine monitoring in a virtual environment.

The virtual sensor networks are taken into consideration they are A and B. They all have different sensor devices connected to the wireless sensor network (WSN) hub. Network-level virtualization can be accomplished with virtual networks and application overlays central to virtual network/overlay-based solutions. A virtual or overlay is a logical network superimposed on a physical network.

The nodes of a physical network are organized into related groups (clusters) in cluster-based solutions. Clustering is more analogous to the network's physical partitioning, in which different parts serve other purposes than a virtual network or overlay. Different nodes within a cluster exist, such as a cluster leader and regular cluster nodes. It's the user's option to choose either cluster-based or network-based virtualization.

Layered virtualization architecture for wireless sensor networks is described in this research to optimize spectrum utilization and resource allocation. VNF is a set of methodologies created to analyze the strategy above, aiming to manage the signal via evaluating energy efficiency and performance.

4. Results & Discussion

For maximum performance, the research is evaluated using metrics like authentication accuracy, resource utilization, FAR and FRR advocated the adoption of SWVRA3 through various number of user requests from 0 to 500 and number of user requests upto 100 simulations by analyzing existing models such as VNF-HA[24], dTEP-FL[25], and secU-

Learn[26]. The dataset is sourced from the provided URL purposes https://www.grapecity.com/componentone/docs/win/online-flexgrid/data-virtualization.html.

4.1 Authentication Accuracy Analysis:

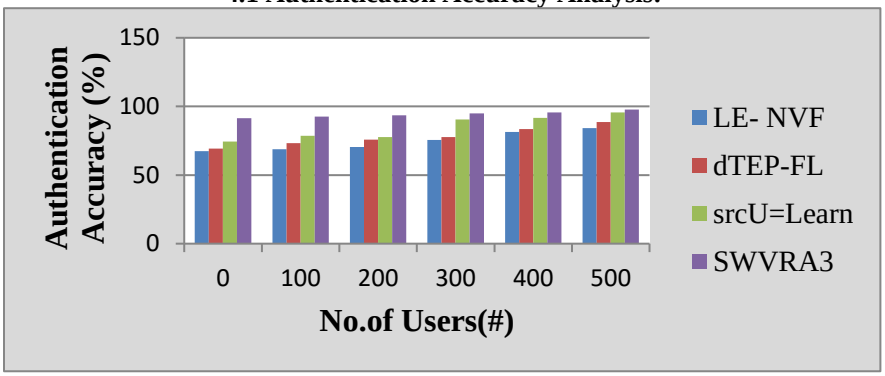

Figure 4: Authentication Accuracy Analysis

Figure 4 shows the accuracy of authentication is an essential parameter that quantifies the efficiency of the authentication processes that are utilized within the framework of wireless network virtualization from equation (15). It assesses the performance of the authentication system in terms of its ability to differentiate between genuine users and devices and impostors, with the goal of reducing the number of false acceptances and false rejections. In the process of calculating authentication accuracy, the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are taken into consideration. A larger value implies that the authentication performance is significantly improved. For an authentication process, the direct influence of the entire correctness that embed with the SWVRA3 algorithm, depends on access control lists, database consultation and protocols that are the function of multi-factor authentication process. Elements that are having the effects on accuracy, includes the database quality, protocol robustness, strength of authentication factors, and vulnerable potential. To improve the security posture, monitoring and analysis of accuracy provided managers to enhance the authentication process of the virtualized infrastructure environment, are currectly utilized and evaluated.

4.2 FRR Vs FARAnalysis:

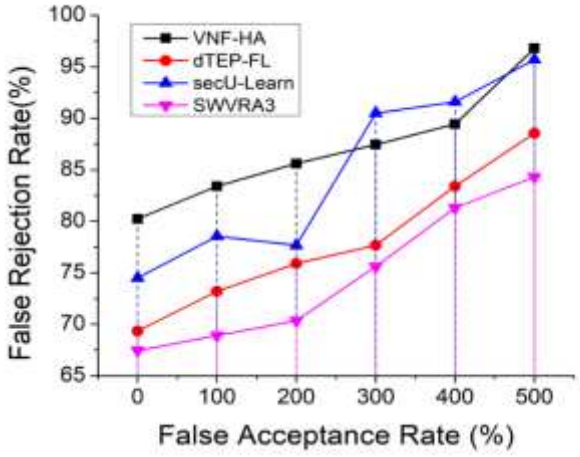

Figure 5: FRR Vs. FAR Analysis

Figure 5 depicts the FAR, also, Equations (13) and (14) gives legitimate analysis of authentication system that gives the measurement to determine the percentage of illegitimate service request. The total count of authentication attempts by the total count of requests were falsely accepted is the measure of required calculation. For decreasedFAR values, there will be reduced risk of unapproved access. For approving the system's capacity, this will be the better indication to correctly differectaite the illegitimate and legitimate requests. At th same time, due to incorrect authentication, FRR measures the rate at which thr legitimate service requests get rejected. The measurement based on it includes, ratio of total count of legitimate attempts of authentication to the number of requests rejected due to mistakes. The decreased

FRR proposed a increased rate of reliability to identify legal requests, that results in decreased likelihood of user rejection, those who are permitted to access the system.

4.3 Resource Utilization Analysis:

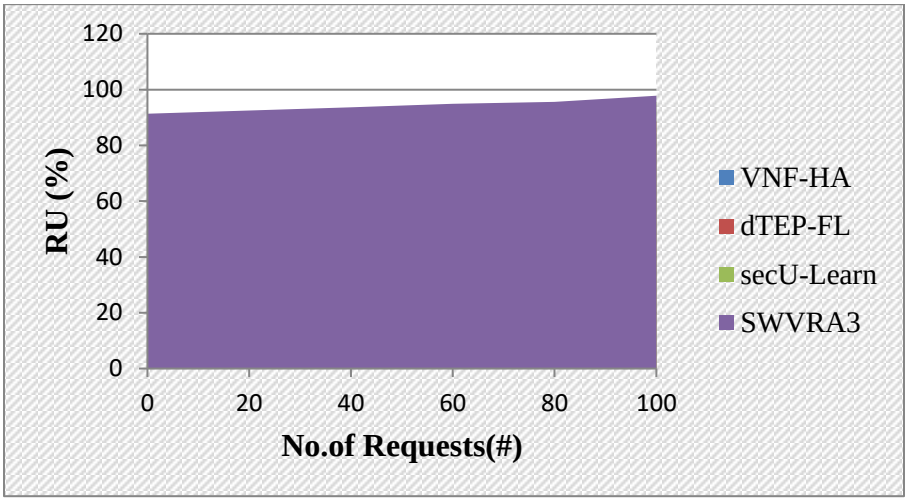

Figure 6: Resource Utilization Analysis

Figure 6 depicts a virtualized infrastructure, resource utilization is an important indicator that indicates how effectively resources are distributed across the various components identified from equation (16). The proportion of allotted virtual capacity compared to all resources on hand is utilized to compute it. Before allocating service requests, the SWVRA3 algorithm's resource allocation step verifies that there are excess computational resources available. The available pool of resources is refreshed using this method in accordance towards the virtualized allocate of resources. With a high rate of resource consumption, therefore can see that what is available is being put to good use, and may put an end to wastage and excess supply. Simultaneously, inefficient underutilized resources and allocation strategies are indicated by decreasing efficiency in using resources. Not only do assignment procedures, patterns of demand, and resources breakdown affect resource consumption, but scaling processes are also variables. In the context of the virtualized communication facilities this lets operators optimize utilization strategies, find insufficiently utilized assets or prospective challenges, and make educated judgments on resource scheduling . All of this is within the realm of possibility for administrators that monitor checks on resource usage.

5. Conclusion

The SWVRA3 is a sophisticated technology that may be used in pervasive computing settings to increase the safety and efficiency of wireless network virtualisation. SWVRA3 ensures the validity of service requests via authentication methods like Kerberos and encrypted certificates, resulting in a high level of verification accuracy. The main target of this mechnicm is make the network security more reilblr and trust for distributed sources tasks. cyber-attack defense identification include establish certain of SWVRA3's detailed security measures and the FAR and FRR. For matching SWVRA3 to additional simulations on the prevous studies, the current average effectiveness in terms of verification precision, resources consumption, and security measures is validated. For agility and scalability, SWVRA3 provided pronounced appropriate for numerous WSN states, containing smart communities and smart medical sets.

References

[1] Darch Abed Dawar, A. (2024). Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks. International Journal of Mathematics, Statistics, and Computer Science, 2, 183–198. https://doi.org/10.59543/ijmscs.v2i.9073

[2] Ren, J., & Li, X. (2022). Wireless Network Virtualization Resource Sharing Based on Dynamic Resource Allocation Algorithm. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/5654188

[3] Wu, W., Zhou, C., Li, M., Wu, H., Zhou, H., Zhang, N., ... & Zhuang, W. (2022). AI-native network slicing for 6G networks. IEEE Wireless Communications, 29(1), 96-103.

[4] Slimani, K., Khoulji, S., & Kerkeb, M. L. (2023). Advancements and Challenges in Energy-efficient 6G Mobile Communication Network. In E3S Web of Conferences (Vol. 412, p. 01036). EDP Sciences. https://doi.org/10.1051/e3sconf/202341201036
[5] Taşkin, D., & Taşkin, C. (2021). Container-based virtualization for bluetooth low energy sensor devices in internet of things applications. Tehnički vjesnik, 28(1), 13-19. https://doi.org/10.17559/TV-20180528134139
[6] Niyato, D. (2024). Editorial First Quarter 2024 IEEE Communications Surveys and Tutorials. IEEE Communications Surveys & Tutorials, 26(1), i-vi. https://doi.org/10.1109/COMST.2024.3356268
[7] Wang, Y., & Li, W. (2022). International Trade Transportation Cost Based on Internet of Things-Assisted Wireless Network Virtualization. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/3591338
[8] Saad, A., Al-Ma'aitah, M., & Alwadain, A. (2020). 6G technology based advanced virtual multi-purpose embedding algorithm to solve far-reaching network effects. ComputerCommunications, 160,749-758. https://doi.org/10.1016/j.comcom.2020.07.025
[9] Chamola, V., Patra, S., Kumar, N., & Guizani, M. (2020). Fpga for 5g: Re-configurable hardware for next generation communication. IEEE Wireless Communications, 27(3), 140-147. https://doi.org/10.1109/MWC.001.1900359
[10] Nazir, M., Sabah, A., Sarwar, S., Yaseen, A., & Jurcut, A. (2021). Power and resource allocation in wireless communication network. Wireless Personal Communications, 119(4), 3529-3552. https://doi.org/10.1007/s11277-021-08419-x
[11] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Blockchain for 5G and beyond networks: A state of the art survey. Journal of Network and Computer Applications, 166, 102693. https://doi.org/10.1016/j.jnca.2020.102693
[12] Parashar, J., Jain, A., Meena, L., & Kapoor, S. (2023). 5G Network Security Challenges and Solutions. JOURNAL OF INTELLIGENT SYSTEMS AND COMPUTING, 4(2), 1-13. https://n2t.net/ark:/47543/JISCOM2023.v4i2.a36
[13] El Amri, A., & Meddeb, A. (2021). Optimal server selection for competitive service providers in network virtualization context. Telecommunication Systems, 77(3), 451-467. https://doi.org/10.1007/s11235-021-00764-3
[14] Liu, B., & Han, C. (2022). Research on wireless network virtualization positioning technology based on next-generation agile IoT technology. Journal of Interconnection Networks, 2150029. https://doi.org/10.1142/S0219265921500298
[15] Nguyen, T., Tran, N., Loven, L., Partala, J., Kechadi, M. T., & Pirttikangas, S. (2020). Privacy-aware blockchain innovation for 6G: Challenges and opportunities. 2020 2nd 6G WirelessSummit(6GSUMMIT),1-5. https://doi.org/10.1109/6GSUMMIT49458.2020.9083832
[16] Tariq, F., Khandaker, M. R., Wong, K. K., Imran, M. A., Bennis, M., & Debbah, M. (2020). A speculative study on 6G. IEEE Wireless Communications, 27(4), 118-125. https://doi.org/10.1109/MWC.001.1900488
[17] Chen, Y., Liu, W., Niu, Z., Feng, Z., Hu, Q., & Jiang, T. (2020). Pervasive intelligent endogenous 6G wireless systems: Prospects, theories and key technologies. Digital communications and networks, 6(3), 312-320. https://doi.org/10.1016/j.dcan.2020.07.002
[18] Cano, L., Capone, A., & Sansò, B. (2020). On the evolution of infrastructure sharing in mobile networks: a survey. ITU Journal on Future and Evolving Technology, 1(1), 21. https://publications.polymtl.ca/9467/
[19] Akyildiz, I. F., Kak, A., & Nie, S. (2020). 6G and beyond: The future of wireless communicationssystems. IEEEaccess, 8,133995-134030. https://doi.org/10.1109/ACCESS.2020.3010896
[20] AlQahtani, S. A., & Alhomiqani, W. A. (2020). A multi-stage analysis of network slicing architecture for 5G mobile networks. Telecommunication Systems, 73(2), 205-221. https://doi.org/10.1007/s11235-019-00607-2
[21] Chang, Z., & Chen, T. (2021). Virtual resource allocation for wireless virtualized heterogeneous network with hybrid energy supply. IEEE Transactions on Wireless Communications, 21(3), 1886-1896. https://doi.org/10.1109/TWC.2021.3107867
[22] Benomar, Z., Longo, F., Merlino, G., & Puliafito, A. (2021). Cloud-based network virtualization in iot with openstack. ACM Transactions on Internet Technology (TOIT), 22(1), 1-26. https://doi.org/10.1145/3460818
[23] Alshammari, A. R. (2020). Resilient Wireless Network Virtualization with Edge Computing and Cyber Deception (Doctoral dissertation, Howard University). https://www.proquest.com/openview/7305e6e268b0faab81fa1d69b328d69f/1?pq-origsite=gscholar&cbl=18750&diss=y
[24] Xue, P., & Jiang, Z. (2021). SecRouting: Secure routing for network functions virtualization (NFV) technology. IEEE Transactions on Circuits and Systems II: Express Briefs, 69(3), 1727-1731. https://doi.org/10.1109/TCSII.2021.3119938
[25] Wang, Y., Kang, X., Li, T., Wang, H., Cheng, C., & Lei, Z. (2023). SIX-Trust for 6G: Towards a Secure and Trustworthy Future Network. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3321114
[26] El-Haggar, N., Amouri, L., Alsumayt, A., Alghamedy, F. H., & Aljameel, S. S. (2023). The Effectiveness and Privacy Preservation of IoT on Ubiquitous Learning: Modern Learning Paradigm to Enhance Higher Education. Applied Sciences, 13(15), 9003. https://doi.org/10.3390/app13159003

[27] Khan, I., Belqasmi, F., Glitho, R., Crespi, N., Morrow, M., & Polakos, P. (2015). Wireless sensor network virtualization: A survey. IEEE Communications Surveys & Tutorials, 18(1), 553-576. https://doi.org/10.1109/COMST.2015.2412971

[28] Alam, I., Sharif, K., Li, F., Latif, Z., Karim, M. M., Biswas, S., ... & Wang, Y. (2020). A survey of network virtualization techniques for internet of things using sdn and nfv. ACM Computing Surveys (CSUR), 53(2), 1-40. https://doi.org/10.1145/3379444