ITEJ December-2024, Volume 9 Number 2 Page 62 - 71

ITEJ

Information Technology Engineering Journals

eISSN : 2548-2157

Url: https://syekhnurjati.ac.id/journal/index.php/itej
Email: itej@syekhnurjati.ac.id

Design and Implementation of Network Security Systems on Virtualized Networks

Akmal Baharuddin Syam
Information Systems
Bacharuddin Jusuf Habibie Institute of Technology
Parepare
baharuddinsyamakmal@gmail.com

Rakhmadi Rahman
Information Systems
Bacharuddin Jusuf Habibie Institute of Technology
Parepare
rakhmadi.rahman@ith.ac.id

Abstract— This report, entitled "Design and Implementation of Network Security Systems on Virtualized Networks," was prepared to fulfill the final assignment of the Network Security course at the Bacharuddin Jusuf Habibie Institute of Technology (ITH). This research aims to design, implement and identify network security vulnerabilities in a virtualization environment using Proxmox Virtual Environment (Proxmox VE) in VirtualBox. The research results show that Proxmox VE in VirtualBox is less successful in optimizing software-hardware resources by implementing security mechanisms such as firewalls, encryption, IDS/IPS, VPN, and IAM. Even though it has several shortcomings, Proxmox VE has proven to be effective in managing virtual networks safely and efficiently when carried out outside of VirtualBox. This research also provides practical experience for students in implementing and identifying network security vulnerabilities, preparing them for real-world challenges.

Keywords— Encryption, Firewall, IAM, IDS/IPS, Proxmox VE, VirtualBox

I. INTRODUCTION

Network security is a series of actions to protect computer networks from threats, unauthorized access, hacking, and damage[1][2]. Its goal is to maintain the integrity, confidentiality, and availability of data[3]. Its main components include firewalls to control network traffic, encryption to prevent unauthorized access, as well as intrusion detection[4][5] and prevention systems (IDS/IPS)[6] to detect and prevent attacks[7]. Technologies like VPNs provide secure network connections[8], while antivirus and antimalware software detect and remove malicious software. Identity and Access Management (IAM) ensures that only authorized users can access network resources. Additionally, endpoint security protects individual devices connected to the network. Network security practices also include software updates, security training, and disaster recovery planning to minimize risks and maintain information integrity

At the Bacharuddin Jusuf Habibie Institute of Technology (ITH), a higher education institution focused on technology, network security is crucial for every student. Challenges arise in network system management and limited resources. Technology systems are constrained by space for server provision, storage provision, and hardware capability enhancement, which require significant costs. Moreover, servers, which are fundamental hardware, cannot be utilized to their full potential. Therefore, to prevent server damage, integrated network security is needed.

Cloud computing technology depends heavily on virtualization technology[9]. Virtualization simplifies management and backup in case of physical server damage, reducing downtime and eliminating the need for reinstallation[10]. Server virtualization, applied on multi-core processor servers, can be utilized to run applications and services virtually[11].

The use of hardware resources in the Software Laboratory at the Bacharuddin Jusuf Habibie Institute of Technology provided by the server machines has not been fully optimized. Thus, adding new server machines is not an efficient step. To optimize existing hardware resources in the Software Laboratory, virtualization technology is needed, which involves dividing a server into several machines called virtual machines (VM) using VirtualBox software to install Proxmox as the tool[12]. Network virtualization is a technology that enables the management and operation of multiple virtual networks within a single physical infrastructure. With the growing need for efficiency and flexibility in IT resource management, virtualization becomes an essential solution. Proxmox Virtual Environment (Proxmox VE) is an open-source virtualization platform that provides the ability to manage virtual machines (VMs) and containers, allowing the configuration of complex virtual networks[13].

Through this final project, we, as students, aim not only to understand the theory provided but also to gain soft skills through experience in implementing and identifying network security vulnerabilities. Therefore, my research focuses on the design and implementation of a network system in a virtualized network using Proxmox software.

II. RELATED WORKS

A. Network Security

Network security is a field of cybersecurity focused on protecting computer networks from cyber threats. Network security has three main goals: to prevent unauthorized access to network resources; to detect and stop ongoing cyber-attacks and security breaches; and to ensure that authorized users have secure access to the network resources they need when they need them[14].

Computer network security involves four different relationships, namely potential relationships with four main aspects when describing forms of threats to computer network security[15]. There are four main forms of threats to computer network security: misuse of Internet of Things information, denial of service background attacks, damage to the integrity of the computer network environment, and computer information leakage. First Internet of Things Misinformation, Usually, in the process of using computers, many users are calmer when clicking on websites and downloading images, files, and so on, and will not use them after use.

This will cause big hidden dangers to computer network security, because every website, file, link, and so on is very likely to contain viruses or hidden files and other dangerous things, if there is no application to filter viruses or hidden files, it can cause information leaks or infection of the computer. The second attack on background services, the so-called denial of service background attack is that the user deliberately delays or illegally suspends network services in the process of visiting websites or downloading files as usual, thereby causing certain damage to the security of the computer network. Third, destruction of the integrity of computer network security, hackers or other people who do not comply with the code of ethics deliberately uses various illegal means to destroy the security of computer networks, thereby affecting the integrity of computer security[16][17].

Fourthly informing computer information, when information in a computer network is transmitted directly to an unauthorized entity without the permission of the user, then the information is certain to become vulnerable. Common forms of computer information that are vulnerable due to these holes include the following aspects: virus intrusion or Trojan horse to the computer, vulnerability of the user's system, radio frequency interception of computer information, installation of monitoring equipment, and security of computer networks[18].

The practice of preventing and recognizing unauthorized use of a computer network is known as computer network security. The purpose of computer network security is to predict dangers to computer networks in the form of physical and logical threats that can disrupt computer network operations directly or accidentally. In addition, to protect computer system data from various risks.

B. Virtualization

Virtualization is a technology that can be used to create virtual representations of servers, storage, networks, and other physical machines. Virtual software mimics the functions of physical hardware to run multiple virtual machines simultaneously on one physical machine. Businesses use virtualization to efficiently leverage their hardware resources and achieve greater returns on their investments. Virtualization also supports cloud computing services, helping organizations manage their infrastructure more efficiently[19]. Virtualization is a technique or way to create something in virtualized form, unlike existing reality. Virtualization is also used to emulate physical computer devices, by making it appear as if the device does not exist (hidden) or even creating a device that does not exist.

Virtualization is the opposite of physical machines or physical machines. A physical machine is a form of server that has various components such as a power supply, mainboard, memory, disk, and so on. Virtualization is an application that appears to be running alone on one machine but is virtualized running on another machine, together with other applications[20]. Virtualization is a technique for hiding the physical characteristics of computer resources from the way other systems, applications, or users interact with those resources. This includes making a single resource such as a server, an operating system, an application, or a storage device appear to function as multiple logical resources, or it can also include definitions for making multiple physical resources (such as multiple storage devices or servers) appear to be a single logical resource. Looking at the historical records the term virtualization began to be developed in the mid-20th century when it was only used for industrial circles.

There are three types of virtualization approaches to building virtual servers, namely:

1. Partial Virtualization. is a form of virtualization on a portion of hardware. Partial virtualization software will emulate as if our computer device had this tool.
2. Full Virtualization means making it appear as if there is another computer inside the computer. By installing Linux on your Windows, you will also install Windows on Linux.
3. Hardware-assisted Virtualisation. This is virtualization that is supported by hardware, so there is special hardware that is useful for increasing the performance of the virtualization process. Hardware-assisted virtualization has a lot of overhead so that the guest OS's scalability doesn't drop too much, it is assisted by hardware

The concept of virtualization has become a key pillar in the evolution of information technology, providing a revolutionary way to manage and use IT infrastructure resources. Basically, virtualization is a technology that allows a physical machine to be used as a shared resource that can be shared and used by several services at once. With technology With virtualization, these services can be configured independently without affecting the configuration of other services even on the same physical machine.

C. Proxmox Virtual Environment (Proxmox VE)

Proxmox VE is an open-source virtualization platform that provides capabilities to manage virtual machines (VMs) and containers. Proxmox VE allows the configuration of complex virtual networks, supports various virtualization scenarios, and comes equipped with security features[21]. Proxmox is an open-source virtualization platform that combines KVM (Kernel-based Virtual Machine) virtualization technology for virtual machines and LXC (LInux Containers) for containers. Proxmox also provides a resource management and web interface that makes it easy for users to manage virtual machines, storage, networking and other computing resources. This platform is often used to build virtual servers and cloud infrastructure[22]. Proxmox is a virtual OS built from the Debian Linux operating system with a modified RHEL kernel. Proxmox VE supports two types of virtualization, namely OPENVZ container-based virtualization and full virtualization with KVM.

Here are the advantages and disadvantages of using Proxmox in the design and implementation of network systems on virtualized networks:

1. Advantages of Proxmox:
   - **Open Source:** Proxmox is a free open-source solution that does not require licensing fees, reducing implementation costs.
   - **Comprehensive Features:** Proxmox offers comprehensive virtualization features, including KVM for virtual machines and LXC for containers, as well as support for clustering, live migration, and high availability.
   - **Centralized Management:** A user-friendly web interface simplifies the centralized management of the entire virtualization infrastructure.
   - **Scalability:** Proxmox can easily scale to handle increased workloads and resource needs.
   - **Active Community:** Proxmox has an active and large user community that provides support, documentation, and valuable resources.
   - **Hardware Compatibility:** Proxmox is compatible with a wide range of hardware, including servers, workstations, and embedded devices.
   - **Integration with Networking Technologies:** Proxmox can integrate with various networking technologies such as virtual switches, virtual routers, and virtual firewalls.
2. Disadvantages of Proxmox :
   - **Learning Curve:** Proxmox has a relatively steep learning curve, especially for new users unfamiliar with virtualization and Linux environments.
   - **Limited Vendor Support:** As an open-source solution, Proxmox does not have the same vendor support as proprietary solutions like VMware or Hyper-V.

- **Cloud Service Integration:** Proxmox does not natively integrate with cloud services like AWS or Azure, which can be a drawback for organizations using cloud services.
- **Performance:** Although Proxmox is quite efficient, virtualization performance on proprietary solutions like VMware ESXi or Hyper-V can be better, especially for intensive workloads.
- **Limited Documentation:** Official Proxmox documentation can be limited for certain cases, so you might need to rely on the community and third-party resources.

Considering these advantages and disadvantages, you can evaluate whether Proxmox meets your organization's needs and requirements for designing and implementing network systems on virtualized networks.

D. Servers

A server is a computer or system designed to manage network resources and provide services to other computers or devices on the network. The server will act as a central hub used to store, process, and distribute data and applications. Servers are usually more powerful and have higher specifications compared to personal computers because servers need to handle several client requests and perform tasks efficiently. A server is a set of computers that contains programs that are capable of producing information and information is distributed to client computers that access it. Servers in simple terms can be one computer for several application services, or if the network is more complex and complicated, the server can be set to only provide one or more services, while other services are handed over to other servers, so here There is collaboration and cooperation between several servers to provide services and information to several clients[23].

A server is a computer system found on a computer network to provide a service to users referred to as clients. Behind its use, the server has carried out many processes to fulfill requests from clients, therefore often The server is experiencing problems due to the server not having the resources capable of meeting these needs. This causes the server service to shut down suddenly because the kernel decided to disable server services that require large resources[24].

III. METHOD

This research uses a structured methodology to design and implement a network security system on virtualization using Proxmox VE. The initial stage begins with a literature study to understand the basic concepts of network security, virtualization, and the Proxmox VE platform. After that, planning is carried out, including setting objectives, defining scope, and creating an implementation schedule, as well as identifying the necessary hardware and software.

In the system development stage, the first step is to install VirtualBox on the host computer and add the necessary extensions. Next, a new virtual machine is created in VirtualBox with the appropriate configuration, and Proxmox is installed on that virtual machine. After installation, virtual network configuration is performed in Proxmox, followed by downloading and installing network security tools such as OPNsense or pfSense.

Implementation and testing involved activating nested virtualization in Proxmox and configuring network security tools to enable firewalls, VPNs, IDS/IPS, and IAM. Testing is conducted to ensure that security policies function correctly and network vulnerabilities are identified and analyzed. The system is also monitored for security logs and alerts to detect threats or issues.

The final stage is the documentation and reporting of research results. Each step in the design and implementation process is documented, and the final report is compiled, covering background, problem formulation, research objectives, methodology, discussion, implementation testing, and conclusions. This methodology is expected to produce an optimal network security system in a virtualized environment using Proxmox VE while also providing practical experience for students in implementing and identifying network security vulnerabilities.

IV. RESULT AND DISCUSSION

Here are the detailed steps to virtualize network security on Proxmox running in VirtualBox:

A. Install VirtualBox

- Download and install VirtualBox on your host computer from https://www.virtualbox.org/ .
- Make sure to install the "VirtualBox Extension Pack" to enable nested virtualization features.

B. Create a Virtual Machine for Proxmox

- Open VirtualBox and click "New" to create a new virtual machine.
- Select "Linux" as the Operating System Type and choose "Debian (64-bit)" as the Version.
- Allocate an appropriate amount of RAM (recommended minimum is 4GB).
- Create a new virtual hard disk or use an existing virtual hard disk.

C. Install Proxmox on the Virtual Machine

- Once the virtual machine is created, select it and click "Settings".
- Click the "System" tab and check the "Enable Nested VT-x/AMD-V" option.
- Click the "Storage" tab and select the Proxmox installation ISO file as the optical drive.
- Start the virtual machine and follow the Proxmox installation instructions.

D. Enable Nested Virtualization in Proxmox

- After Proxmox is installed, log into the Proxmox web interface.
- Go to the "Node" tab and select "Kernel Setup".
- Check the "Host Nested Virtualization" box.

E. Configure Virtual Network in Proxmox

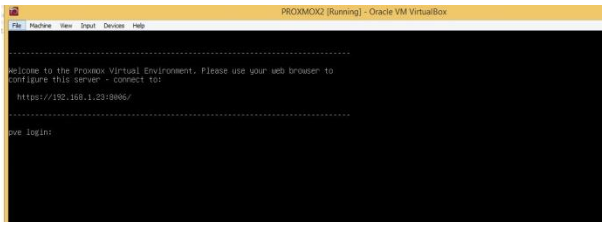
- In Proxmox, go to the "Network" tab and create a new virtual network (eg, vmbr0).
- Configure the virtual network as needed (bridge mode or NAT).

F. Install Network Security Tools

- Download the desired network security tools (eg, OPNsense or pfSense).
- In Proxmox, create a new virtual machine and import the security tools.
- Configure the resources (RAM, CPU) and network settings for the network security tools.

G. Configure Network Security Tools

- Access the web interface of the network security tools (eg, https://192.168.XX).
- Configure firewall, VPN, IDS/IPS functions, etc., according to your network security policies.
- Set up rules and policies to protect your virtual network.

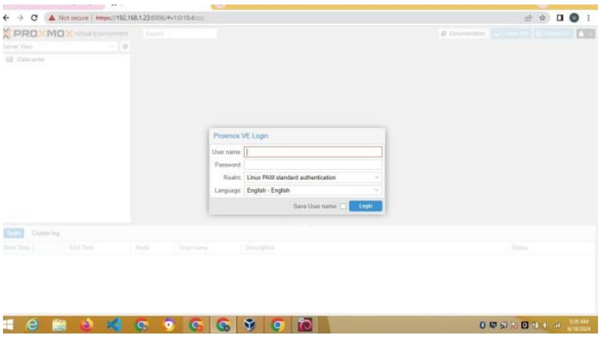

PROXMOX2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
------------------------------------------------------------------------------

Welcome to the Proxmox Virtual Environment. Please use your web browser to
configure this server - connect to:

  https://192.168.1.23:8006/

------------------------------------------------------------------------------

pve login:
```

Figure 1Running Proxmox in VirtuaBox

H. Test and Monitor Network Security

- Conduct tests to ensure that network security policies are functioning as expected.
- Monitor logs and alerts from the network security tools to identify threats or issues.



Proxmox VE Login

User name:

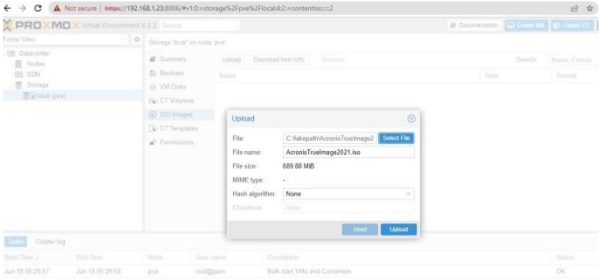
Password:

Realm: Linux PAM standard authentication

Language: English - English

Save User name: □ Login

Figure 2Access Proxmox Web Interface



Upload

File: C:\fakepath\AcronisTrueImage2 Select File

File name: AcronisTrueImage2021.iso

File size: 689.88 MiB

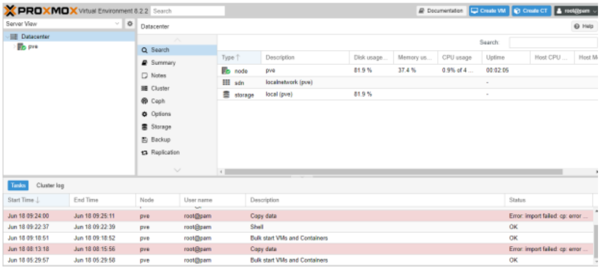
MIME type: -

Hash algorithm: None

Checksum: none

Abort Upload

Figure 3. ISO File Upload Interface



Type ↑	Description	Disk usage...	Memory us...	CPU usage	Uptime	Host CPU ...	Host M
node	pve	81.9 %	37.4 %	0.9% of 4 ...	00:02:05		
sdn	localnetwork (pve)				-		
storage	local (pve)	81.9 %			-		

Start Time ↓	End Time	Node	User name	Description	Status
Jun 18 09:24:00	Jun 18 09:25:11	pve	root@pam	Copy data	Error: import failed: cp: error ...
Jun 18 09:22:37	Jun 18 09:22:39	pve	root@pam	Shell	OK
Jun 18 09:18:51	Jun 18 09:18:52	pve	root@pam	Bulk start VMs and Containers	OK
Jun 18 08:13:18	Jun 18 08:15:56	pve	root@pam	Copy data	Error: import failed: cp: error ...
Jun 18 05:29:57	Jun 18 05:29:58	pve	root@pam	Bulk start VMs and Containers	OK

Figure 4. Upload Process Completion

However, this process was not successful because the ISO file upload can only be completed successfully if done outside of VirtualBox.

I. Important Notes:

- Ensure that virtualization is enabled in both VirtualBox and Proxmox so that the network security virtual machines can run correctly.
- Configure the virtual network properly to allow the network security virtual machines to communicate with the outside network and effectively protect network traffic.
- Allocate sufficient resources (RAM, CPU, storage) to both Proxmox and the network security virtual machines to ensure performance is not compromised.
- Follow the documentation guidelines from the network security equipment vendors for appropriate configuration according to your needs.

By following these steps, you can virtualize network security on Proxmox running in VirtualBox. However, keep in mind that performance may not be as good as running Proxmox natively on physical hardware.

V. Conclusion

The conclusion of the report "Design and Implementation of Network Security Systems in Virtualized Networks" states that the use of virtualization technology through Proxmox VE running in VirtualBox is capable of optimizing the hardware resources available in the software laboratory of the Bacharuddin Jusuf Habibie Institute of Technology (ITH). By implementing security mechanisms such as firewalls, encryption, IDS/IPS, VPN, and IAM, the virtualized network can be operated securely and efficiently. Proxmox VE has proven to be an effective open-source virtualization platform, despite some drawbacks such as a steep learning curve and limited vendor support. The structured implementation steps, from installing VirtualBox to testing and monitoring network security, ensure that the network security system in the virtualized network functions optimally. Identifying and addressing security vulnerabilities using appropriate network security tools ensures protection against potential threats. Moreover, this research provides valuable practical experience for students in implementing and identifying network security vulnerabilities, preparing them to face real-world challenges. This study successfully achieves its objectives of designing and implementing an optimal network security system in a virtualized environment using Proxmox VE.

References

[1] H. Li, “Simulation of education digital network security and anomaly detection based on neural networks,” *Comput. Electr. Eng.*, vol. 112, p. 108992, Dec. 2023,

doi: 10.1016/j.compeleceng.2023.108992.

[2] M. Wang, “Optimization of Network Security in University Laboratories Based on Anomaly Intrusion Detection in Public Cloud Networks,” *Comput. Electr. Eng.*, vol. 111, p. 108968, Nov. 2023, doi: 10.1016/j.compeleceng.2023.108968.

[3] J. Braun and F. Derbel, “Wireless sensor network for fire detection with network coding to improve security and reliability,” *Meas. Sensors*, p. 101404, Dec. 2024, doi: 10.1016/j.measen.2024.101404.

[4] A. Ali *et al.*, “An optimized multilayer perceptron-based network intrusion detection using Gray Wolf Optimization,” *Comput. Electr. Eng.*, vol. 120, p. 109838, Dec. 2024, doi: 10.1016/j.compeleceng.2024.109838.

[5] M. Rajkumar, J. Karthika, and S. S. Abinayaa, “Multi-View Consistent Generative Adversarial Network for Enhancing Intrusion Detection with Prevention Systems in Mobile Ad Hoc Networks Against Security Attacks,” *Comput. Secur.*, p. 104242, Nov. 2024, doi: 10.1016/j.cose.2024.104242.

[6] F. Dong *et al.*, “Floor failure behavior and water disaster prevention system of ultra-wide opposite pulling working face mining on confined aquifer,” *Eng. Fail. Anal.*, vol. 165, p. 108736, Nov. 2024, doi: 10.1016/j.engfailanal.2024.108736.

[7] M. J. Pasha, K. P. Rao, A. MallaReddy, and V. Bande, “LRDADF: An AI enabled framework for detecting low-rate DDoS attacks in cloud computing environments,” *Meas. Sensors*, vol. 28, p. 100828, Aug. 2023, doi: 10.1016/j.measen.2023.100828.

[8] S. A. A. Mohamed and S. Kurnaz, “Classified VPN Network Traffic Flow Using Time Related to Artificial Neural Network,” *Comput. Mater. Contin.*, vol. 80, no. 1, pp. 819–841, 2024, doi: 10.32604/cmc.2024.050474.

[9] X. He and Q. Zhang, “Cloud Computing Based Digital Media Content Distribution Technology,” *Procedia Comput. Sci.*, vol. 247, pp. 461–468, 2024, doi: 10.1016/j.procs.2024.10.055.

[10] J. Lu and X. S. Zhou, “Virtual track networks: A hierarchical modeling framework and open-source tools for simplified and efficient connected and automated mobility (CAM) system design based on general modeling network specification (GMNS),” *Transp. Res. Part C Emerg. Technol.*, vol. 153, p. 104223, Aug. 2023, doi: 10.1016/j.trc.2023.104223.

[11] Y. Mansouri and M. A. Babar, “A review of edge computing: Features and resource virtualization,” *J. Parallel Distrib. Comput.*, vol. 150, pp. 155–183, Apr. 2021, doi: 10.1016/j.jpdc.2020.12.015.

[12] E. Ali, Susandri, and Rahmaddeni, “Optimizing Server Resource by Using Virtualization Technology,” *Procedia Comput. Sci.*, vol. 59, pp. 320–325, 2015, doi: 10.1016/j.procs.2015.07.572.

[13] A. Aldribi, I. Traoré, B. Moa, and O. Nwamuo, “Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking,” *Comput. Secur.*, vol. 88, p. 101646, Jan. 2020, doi: 10.1016/j.cose.2019.101646.

[14] R. Zhang and Z. Hu, “Access control method of network security authentication information based on fuzzy reasoning algorithm,” *Measurement*, vol. 185, p. 110103, Nov. 2021, doi: 10.1016/j.measurement.2021.110103.

[15] Q. Liu and T. Zhang, “Deep learning technology of computer network security detection based on artificial intelligence,” *Comput. Electr. Eng.*, vol. 110, p. 108813, Sep. 2023, doi: 10.1016/j.compeleceng.2023.108813.

[16] E. Andrade, J. Granjal, J. P. Vilela, and C. Arantes, “A Security Gateway for power distribution systems in open networks,” *Comput. Secur.*, vol. 111, p. 102492, Dec. 2021, doi: 10.1016/j.cose.2021.102492.

[17] A. A and L. NG, “Analysis and Detection of Weeds Using Artificial Neural Networks,” *ITEJ (Information Technol. Eng. Journals)*, vol. 7, no. 2, pp. 123–131, Dec. 2022, doi: 10.24235/itej.v7i2.107.

[18] E. Chisari, J. Cho, M. Wouthuyzen-Bakker, and J. Parvizi, “Periprosthetic Joint Infection and the Trojan Horse Theory: Examining the Role of Gut Dysbiosis and Epithelial Integrity,” *J. Arthroplasty*, vol. 37, no. 7, pp. 1369–1374, Jul. 2022, doi: 10.1016/j.arth.2022.03.030.

[19] F. N. Laukotka and D. Krause, “Virtual Representations of Physical Assets – a literature study about Digital Twins from the perspective of application in aviation’s retrofit,” *Procedia CIRP*, vol. 119, pp. 926–931, 2023, doi: 10.1016/j.procir.2023.03.136.

[20] M. Revilla-León, A. Zandinejad, M. K. Nair, A. B. Barmak, A. J. Feilzer, and M. Özcan, “Accuracy of a patient 3-dimensional virtual representation obtained from the superimposition of facial and intraoral scans guided by extraoral and intraoral scan body systems,” *J. Prosthet. Dent.*, vol. 128, no. 5, pp. 984–993, Nov. 2022, doi: 10.1016/j.prosdent.2021.02.023.

[21] B. Dordevic, V. Timcenko, N. Kraljevic, and N. Jovicic, “Performance comparison of KVM and Proxmox Type-1 Hypervisors,” in *2022 30th Telecommunications Forum (TELFOR)*, IEEE, Nov. 2022, pp. 1–4. doi: 10.1109/TELFOR56187.2022.9983666.

[22] V. Oleksiuk and O. Oleksiuk, “The practice of developing the academic cloud using the Proxmox VE platform,” *Educ. Technol. Q.*, vol. 2021, no. 4, pp. 605–616, Dec. 2021, doi: 10.55056/etq.36.

[23] A. Anees, M. Field, and L. Holloway, “A neural network-based vertical federated learning framework with server integration,” *Eng. Appl. Artif. Intell.*, vol. 138, p. 109276, Dec. 2024, doi: 10.1016/j.engappai.2024.109276.

[24] A. Sharma and N. Marchang, “A review on client-server attacks and defenses in federated learning,” *Comput. Secur.*, vol. 140, p. 103801, May 2024, doi: 10.1016/j.cose.2024.103801.