electronics

Review

Transportation of Service Enhancement Based on Virtualization Cloud Desktop

Fan Li [1], Tengda Guo [2], Xiaohui Li [3,*], Junfeng Wang [1], Yunni Xia [4] and Yong Ma [5]

[1] College of Computer Science, Sichuan University, Chengdu 610065, China
[2] College of Software Engineering, Sichuan University, Chengdu 610065, China
[3] School of Cyber Science and Engineering, Sichuan University, Chengdu 610065, China
[4] School of Computer, Chongqing University, Chongqing 400030, China
[5] School of Computer Information Engineering, Jiangxi Normal University, Nanchang 330022, China
* Correspondence: lixiaohui@scu.edu.cn

Abstract: Cloud desktop represents an outstanding product in the domain of cloud computing, which refers to the desktop cloud, desktop virtualization and virtual desktop. Cloud desktop explores the virtualization technology to concentrate computing resources, which delivers traditional computer desktops (operating system interfaces) or applications deployed in the pooled computing resources to polymorphic terminals through the Internet. As a distinctive product of cloud computing, cloud desktop has been a hot topic since its inception. Today, the virtualized resource pool of cloud computing achieves the elastic and dynamic expansion of resources, which brings the desktop system from an independent personal computer to a centralized physical server. Consequently, the great improvement in basic network conditions makes it possible to transmit high-quality desktops over the network. There are two key factors for cloud desktops, one of which is the virtualization technology on the server side and the other one, which is the transmission protocol of cloud desktops. The cloud desktop transmission protocol mainly completes the transmission of graphics, images and audio from the server to the user terminal. The transmission of input information from the user terminal, called DaaS (Desktop-as-a-Service), includes the input information of peripherals such as a mouse, keyboard, printer and so on. The efficiency of the transmission protocol determines the basic delivery capability of the cloud desktop, while the bearer protocol and graphics and image processing methods in the transmission protocol determine the interactive experience of the cloud desktop. Different protocols have their characteristics and applicable space. This paper spies on application and transport layer communication protocols to meet DaaS communication requirements. This paper describes the internal mechanism of various transport protocols applicable to a cloud desktop from the principle level and points out the pros and cons and the current application environment. It can be seen that these methods solve the transmission efficiency of burst traffic, improve user experience and reduce bandwidth consumption, which are the development direction of transmission protocols.

Keywords: cloud desktop; virtualization; transport protocol; quality of experience

check for updates

Citation: Li, F.; Guo, T.; Li, X.; Wang, J.; Xia, Y.; Ma, Y. Transportation of Service Enhancement Based on Virtualization Cloud Desktop. *Electronics* **2023**, *12*, 1572. https://doi.org/10.3390/electronics12071572

Academic Editor: Cheng-Chi Lee

Received: 2 March 2023
Revised: 21 March 2023
Accepted: 23 March 2023
Published: 27 March 2023

1. Introduction

Cloud computing is a mature and widely used technology on the current Internet. People have come into contact with cloud computing invisibly. For example, people such as company personnel department staff can use cloud computing at home for cloud office work. Desktop as a service (DaaS), software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) are the four services provided by cloud computing [1]. Recently, general service providers have combined these three services to provide users with much higher work efficiency.

The global cloud computing market maintained steady growth in 2021, growing to USD 90.89 billion from USD 64.29 billion in 2020, according to Gartner data [2]. Among global cloud platforms, the share of Amazon web services (AWS) fell slightly compared with last year, reaching 38.92%. Microsoft and Alibaba Cloud ranked second and third, respectively, while their market shares have expanded. Among the top six global cloud vendors, there are three Chinese cloud vendors, with Alibaba Cloud, Huawei Cloud and Tencent Cloud ranking third, fifth and sixth, respectively.

From a regional perspective, the growth rate of the cloud computing IaaS market in Asia Pacific (APAC) is much higher than the global average [3]. In 2021, it achieved a scale of 33.16 billion US dollars, up 47.92% year on year. Among them, markets such as Malaysia, Indonesia and Thailand are leading the growth rate in the Asia-Pacific region. Gartner data shows that the Alibaba Cloud has long been at the forefront of the Asia-Pacific market share and reached 25.53% in 2021. In addition, Amazon AWS, Microsoft, Huawei and Tencent rank second to fourth in that order.

DaaS [4] represents a cloud-based hosting service that allows subscribers to deploy virtual desktops to subscribers employees. These kinds of desktops can be effortlessly deployed anyplace and near any client. Therefore, this enables workers to access applications and businesses when required. Desktops are centrally administered and have no use for any in-house infrastructure to host. When hosted in the central cloud, DaaS is analogous to the virtual desktop infrastructure rather than an on-premises data center. DaaS provides a steady virtual desktop environment to improve collaboration among enterprise users. DaaS has obvious advantages, the first one of which is to improve security. Data security is critical to any company, and to be sure, several companies want to enforce strict desktop management policies for employees who have full control and manage and access employees' data over the network. DaaS providers typically do not keep data on local computers, thus eliminating the possibility of data breaches or unauthorized access. Secondly, DaaS can be accessed from any device that can connect to the Internet, regardless of device software or operating system. Business users can securely access their cloud desktops from any device. Thirdly, DaaS effectively reduces and minimizes operating costs. The cost of maintaining and installing the hardware required to run each virtual desktop ranges from capital to operating expenses. Most DaaS providers provide access to cloud desktops on request to consolidate a set of memory, computing and storage resources to meet user needs. Fourthly, it enhances business continuity. In situations where the physical presence of current employees or staff is challenging, the need for a simple, secure and convenient approach to business continuity has increased. Overall, DaaS is one such convenient method to enhance business continuity, improve the overall agility of an enterprise and respond to rapidly changing business environments. Since the data are on a cloud desktop, they provide the added advantage of simplifying disaster recovery.

The virtual network computing (VNC) protocol is a bridge between the terminal device and the private cloud. When users use the private cloud desktop environment for office work, they use the VNC protocol to transmit messages such as images, mice and keyboards [5,6]. VNC enables users to remotely operate cloud resources. The image transmission of VNC adopts the remote frame buffer (RFB) protocol. The RFB protocol works on the frame buffer level and does not depend on any operating system and terminal equipment [7]. It is for this reason that VNC can be cross-platform, but VNC's lack of support for audio and video streaming has become its weakness. It has little effect on people who only use VNC for office work. However, with the continuous development of multimedia, people are not satisfied with exploiting a private cloud for office work, and the shortcomings of VNC have gradually attracted people's attention.

In the private cloud desktop environment, it needs to be a set of protocols that can connect to the cloud desktop environment. VNC, remote desktop protocol (RDP) [8], simple protocol for independent computing environment (SPICE) [9] and other remote desktop connection protocols are remote desktop connection protocols widely used in cloud computing. VNC has the advantage of being cross-platform, using the VNC protocol in the private cloud desktop environment enables office staff to use Apple computers or mobile phones for office work. For Internet companies, VNC can be used for server-side operation and maintenance management. This protocol is a lightweight protocol, which is easy to install and does not require special configuration, and there are many versions of VNC protocols on its network, such as Real VNC, Tight VNC and Ultra VNC versions [10], some of which are open-source code. It is because of these advantages that this protocol is favored by people.

However, with the continuous advancement of science and technology, computer hardware and software have been greatly improved. Office workers are not satisfied with exploiting VNC to edit documents and make PPTs but hope that they can be used for entertainment during their rest time, such as listening to music, watching movies, etc. The shortcomings of VNC, that is, VNC's lack of support for audio and video [11], are also clearly exposed. These shortcomings also make VNC gradually lose its market competitiveness, so the optimization and improvement of VNC protocol in audio and video are also imminent.

The improvement of audio and video transmission technology is mainly reflected in the realization of the compression algorithm of audio and video data and the synchronization of audio and video. For the compression algorithm of video data, there is H.264, joint photographic experts group (JPEG) and JPEG2000 and other video compression algorithms [12]. In recent years, H.265 algorithms have also quietly emerged. These algorithms have a high data compression ratio, which greatly reduces the amount of video data transmission. There are also many audio compression algorithms, such as Opus, and adaptive cruise control (ACC), which are all excellent audio compression algorithms.

In this paper, both application and transport layer communication protocols are investigated to fulfill the DaaS communication requirements. To this end, this article first outlines the traditional cloud desktop transfer protocol and then briefly introduces the performance factors that affect the desktop transfer protocol. Then, this paper investigates possible potential protocol candidates, the main features of each version of the protocol, and summarizes the performance issues of each protocol. In addition, this article also researches business-oriented metrics, such as data latency, bandwidth and video playback quality, to evaluate performance in document editing, audio and video streaming and web browsing.

2. Related Work

For audio and video synchronization, many scholars in academia have conducted in-depth research [13], and many kinds of audio and video synchronization strategies have been produced to improve user experience and achieve audio and video synchronization. For example, in the time axis synchronization method proposed by Jansen [14], the SPICE protocol uses a synchronous timestamp solution to solve the problem of audio and video synchronization. The timestamp synchronization technology is divided into relative timestamp and absolute timestamps, which is the absolute timestamp of the whole network used. For some streaming media, people adopt a synchronization scheme based on real-time transport protocol (RTP) in pursuit of real-time video so as to achieve the effect of audio and video synchronization.

The performance of an efficient desktop transmission protocol can be measured from resource occupation (CPU, network bandwidth), desktop fluency (whether it is stuck in use), frame loss rate (whether part of the picture is lost), picture quality (picture clarity and color reproduction), peripheral support (compatibility, recognition speed, read and write speed) and other aspects to test and evaluate. Currently, epidemic remote desktop connection protocols include Microsoft's RDP protocol [15], Red Hat's SPICE protocol [16] and VNC protocol, which have their own advantages and disadvantages in audio and video transmission.

Desktop cloud has been widely used in various fields in recent years because of its advantages of providing users with the desktop, application, and data delivery services in one-stop and ensuring user experience. Schematic diagram of the smallest cloud computing system is shown as Figure 1. To use virtual desktops or applications in the cloud data center, users must rely on the remote desktop protocol to interact with remote virtual machines through network transmission. The remote desktop protocol is one of the key technologies that determine the user experience in the desktop cloud. At present, the mainstream protocols mainly include Microsoft's RDP protocol, Citrix's inter-center agreement (ICA) protocol [17], VMware's PC over IP (PCoIP) protocol [18], the open-source SPICE protocol and the VNC protocol.

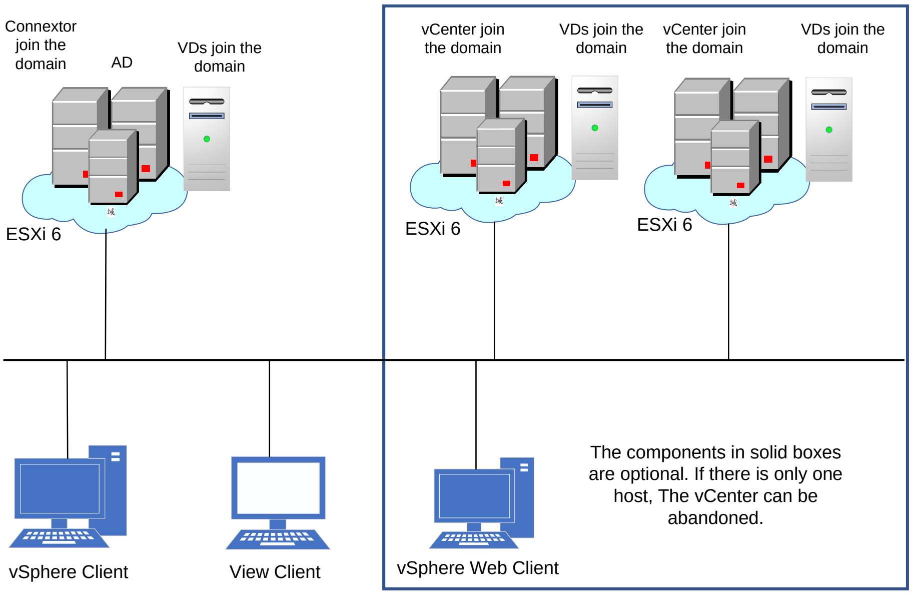

Figure 1. Schematic diagram of the smallest cloud computing system.

The RDP protocol was first developed by Citrix and has been continuously optimized and improved since it was purchased by Microsoft. The RDP protocol has supported graphic processing unit (GPU) acceleration since version 7.1, which has improved the user's visual experience qualitatively. The RDP protocol has also achieved good results in device redirection and audio and video. RDP 8.0 protocol relies on the underlying transmission control protocol (TCP) and user datagram protocol (UDP) and no longer supports only TCP like the previous version. Consequently, the transmission provides maximum performance in the case of network loss and can be changed based on network conditions between the two protocols. It can be used for conversion; that is, data retransmission is avoided by using the forward error connection technology, which greatly improves the transmission performance. In terms of video transmission, the RDP protocol can use two schemes, which are image-based rendering and video-based encoding [19]. Before transmission, the performance of the client will be judged to decide which video transmission scheme to use. The image transmission based on the video coding scheme will segment the image, entropy encodes the image and transmit its video image to the client. It has its own audio transmission channel in audio transmission and adds the audio redirection function, which streams audio from the remote session host to the client. However, its code is not open-source and not cross-platform, making it difficult to use in the enterprise.

The ICA protocol is developed by the Citrix company. It is more complete than the RDP protocol in terms of function and performance. ICA can control the bandwidth and is independent of the operating system that supports it well. The ICA protocol uses some data compression, data encryption and connection optimization technologies so that the user's connection only occupies a small amount of bandwidth, which efficiently reduces the amount of data transmission and greatly improves the overall performance. The security design controls the authorization of centralized access through policy-based control and establishes a secure access network. At the same time, it strengthens the authentication of user identity and conducts corresponding audit monitoring to improve its security. In terms of peripheral device redirection, ICA uses a bus-driven device redirection method, so it can be used normally in most user environments.

The PCoIP protocol was originally developed by Teradici to improve the responsiveness of desktop images and the quality of virtual desktops displayed. After 2008, it was jointly developed by Teradici and VMware. Unlike traditional desktop display protocols, which are designed to deliver applications, the PCoIP protocol was built from the ground up for desktop delivery. Highly optimized with adaptive technology to ensure the best user experience regardless of where the user is located on the local area network (LAN) or wide area network (WAN).

Different from many other protocols, the transport layer of the PCoIP protocol is based on the UDP protocol. This can maximize the use of bandwidth, making it smooth during video playback. Its transmission efficiency will be faster than the RDP protocol. The PCoIP protocol flexibility supports multiple platforms, such as Windows, Linux, Mac, Android, iOS, Chrome and the web. The latest version is released with VMware Horizon 6.0, which has low bandwidth usage and good image quality.

The SPICE protocol is a remote desktop connection protocol proposed by Redhat and is open-source. The protocol has the characteristics of high reliability and dynamic adaptation. The remote desktop effect realized on the client side based on the SPICE protocol can achieve the same experience as a real computer desktop. This protocol is mainly used for accessing virtualized desktops shown in Figure 2, through which users can directly access virtual machine desktops. The SPICE protocol, based on a multi-layer structure design, provides users with a large number of multimedia interfaces. Its core design realizes intelligent access to virtual machine server hardware resources and terminal device resources. The protocol will decide whether to render the access result on the server or the terminal device through dynamic judgment. The dynamic determination method can cope with a variety of network environments, so even in a poor network environment, it can still present a good desktop display effect. The SPICE protocol is one of the few open-source protocols that can be compared with commercial protocols.

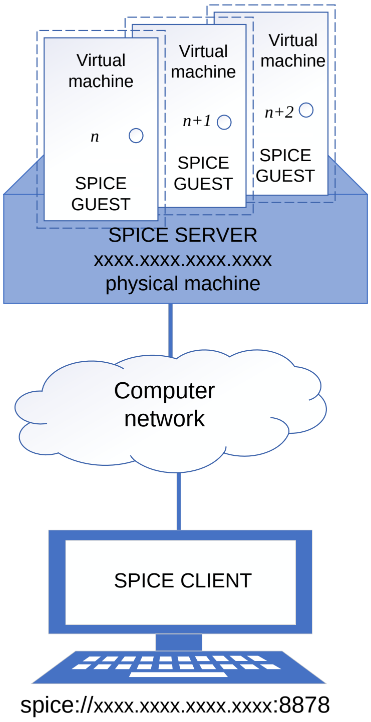

Figure 2. SPICE communication protocol.

The general process of the SPICE protocol in audio and video transmission is that when the SPICE server detects that there is video playback, motion joint photographic experts group (MJPEG) [20] is used to compress the video data. The audio and video data are stamped with a system timestamp and sent to the SPICE client. When the client receives the audio and video data sent by the SPICE server, it decodes and plays synchronously. The video of the SPICE protocol is encoded and transmitted by MJPEG, but its compression rate is low, and there are repetitions. In the case of compression, in terms of audio transmission, SPICE has a custom audio channel. However, it is directly transmitted without encoding and compression in audio transmission. Lan Yuqing [21] et al. improved the SPICE protocol and changed the MJPEG encoding to JPEG2000 [22], which is used for encoding and transmission. The JPEG2000 algorithm is an improvement of the JPEG algorithm. It can handle the conversion between ordinary images and videos well and has a good video streaming effect. Because the SPICE protocol also has the disadvantage that the video freezes under low bandwidth, and compressing the video on the server will consume more CPU resources [23]. The media player and media agent modules are added to SPICE to overcome the disadvantages of SPICE and reduce CPU consumption by adapting it to low-bandwidth networks.

Compared with the above four protocols, the overall design idea of the VNC protocol is simpler because it uses pixel data as the display encoding primitive for desktop images, unlike low-level graphics commands that require the cooperation of the operating system to display. This feature of the desktop makes it not limited by the operating system; that is, the VNC protocol has good cross-platform performance. The initial application scenario of VNC was to provide interaction for thin terminal systems. Later, with the development of cloud computing, it was applied to the cloud platform as a remote desktop protocol. Because of this, the VNC protocol is not essentially generated by the desktop cloud, so when the VNC protocol is used in the cloud platform, many features are not suitable for the cloud platform in terms of function and performance. For example, in the desktop cloud scenario, the user needs to play audio, or because of the particularity of the office environment, the local USB device needs to be redirected to the virtual machine desktop. However, these functions are not supported by VNC, which greatly limits the user's usage scenarios. Although the VNC protocol supports image transmission, it does not have many optimization mechanisms for application scenarios where the frame rate changes rapidly. Therefore, in the application scenario where the frame rate changes rapidly, such as playing a video, the picture will be seriously stuck and dropped, and the user's sense of use is extremely poor.

The VNC protocol is a cross-platform remote interaction protocol. Although it supports both lazy update and server-side active push strategy in image transmission, its default main method is the lazy update strategy. In the beginning, there was no development of VNC. Considering the use of VNC to transmit video streams, the RFB protocol used does not support video streams [24]. Compared with protocols such as RDP and SPICE, VNC does not support audio, which is also a major disadvantage. When optimizing video transmission, on the other hand, there are already some good solutions abroad, such as adding a message accelerator on the VNC server to speed up the transmission of images, but the image encoding has not been improved, and there will be update requests and request responses on the transmission channel. Therefore, for VNC audio and video transmission, it is necessary to select an audio and video encoding method suitable for network transmission, achieving its synchronization effect while transmitting and finally making users have a good viewing experience. After scholars and experts have proposed many audio and video transfer schemes, they need to have a transfer standard to regulate so as to meet the judgment of whether audio and video are synchronized in different scenarios. Therefore, the standardization organization has formulated the quality of service (QoS) standard to specify the audio and video synchronization range [25,26].

3. Performance Factors Affecting Desktop Transport Protocols

There are many transport schemes where QoS standards are required. We call it audio and video synchronization under this scheme. This section will emphasize the factors that affect the performance of desktop transport protocols.

3.1. Graphical Data Processing Method

At present, there are two main ways to process graphics data:

- Based on bitmap data transmission, the graphics data are rendered on the server side and then compressed and transmitted. However, the disadvantage is that under high resolution, the edges of the text and pictures will have jagged edges, such as Sangfor's service rating application protocol (SRAP) protocol.
- Vector-based data transmission splits multiple formats of the client and then transmits it to the client for rendering. The feature is that it is clear whether it is enlarged or reduced. The vector data transmission mode occupies a lower bandwidth than that of the bitmap.

3.2. Transport Layer Protocol

There are two main types of transport methods:

- The TCP protocol is mainly used to transmit data with high-security requirements, such as printer data, user operation data, etc., but it is slower than UDP transmission;
- The UDP protocol is used for some data transmissions that do not require high completeness. Although fast, it will drop frames. For example, when watching a video, several frames may be skipped in the middle. For example, the frame loss phenomenon of NComputing's user experience platform (UXP) protocol is more serious.

3.3. Compression and Caching Technology

Lossy compression and lossless compression are the two main methods for solving this problem, which is shown in Figure 3. According to the literal, it is also well understood that lossy compression means that the transmitted data are damaged, while lossless compression means that the data are complete and undamaged. The most intuitive difference between the two is the transmission of image data (as shown in the figure below). There are two compression techniques:

- The image after lossless compression is still clear, while the image after lossy compression is blurred. Lossy compression can only ensure clear images unless it is used in conjunction with client-side rendering.
- For lossless compression, if the amount of data transmission is large, it will also appear unsmooth. For example, the RDP protocol belongs to lossless compression, but the fluency is not good. Microsoft's later launch of RemoteFX technology accelerated the image transfer, which was this time smooth, but still has some losses. Therefore, there must be a trade-off between the two. A high-quality compression algorithm needs to balance the two, which can not only ensure clear image quality but also effectively reduce the amount of data transmission, thereby reducing the bandwidth requirements.

3.4. Peripheral Support Technology

In fact, each protocol provides technology for virtual multi-channel support. Simply put, in order to guarantee the normal operation of peripheral devices, the desktop transmission protocol must establish a path for each device to ensure its normal and orderly passage. Caching technology saves frequently used display elements, such as fonts and graphics, and obtains them directly if needed without sending repeated requests to the server so as to provide efficient desktop transmission performance.

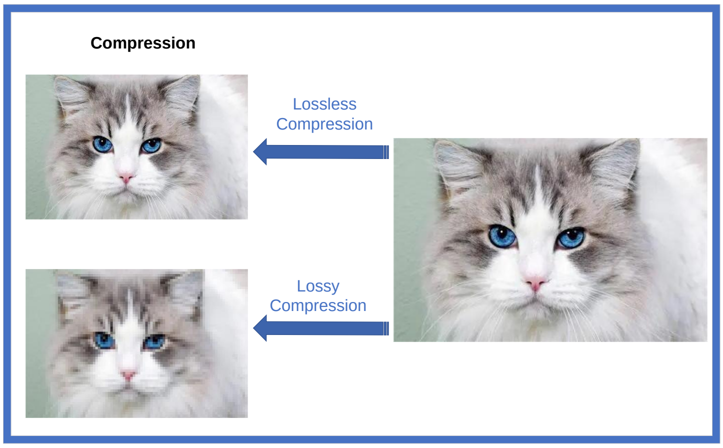

Figure 3. Cloud virtual desktop image compression technology.

4. Efficient Desktop Transport Protocol

The desktop transmission protocol is an important part of the cloud desktop solution. It directly specifies the data transmission method between the cloud host and the cloud terminal. It is a set of rules for orderly and efficient data transmission between the cloud host and the cloud terminal. People often say "is the desktop speed fast" and "the number of users with them" to ask whether the desktop transmission protocol is efficient or not.

4.1. Different Perspectives for Improving Virtual Cloud Desktop Delivery

An efficient desktop transmission protocol is to achieve faster data transmission and higher resource utilization with a better algorithm so as to deliver a cloud desktop solution with a smooth, short response time, clear picture and sound and high user density. Therefore, the desktop transfer protocol is the technical core of the cloud desktop.

4.1.1. For the Host

Other conditions being equal, the better the host configuration, the higher the user density. However, the host itself is not a product that cloud desktop manufacturers must provide; on account friends can buy it by themselves. It is just because the deployment process of some domestic cloud desktop solutions is more complicated and requires manufacturering professionals to complete. Therefore, for the convenience of customers or other commercial factors, manufacturers simply install and configure their own cloud desktop software on the cloud host and then bundle and sell them to customers, which is what we call a "one-stop" intimate service.

4.1.2. For the Network

The stability directly affects the stability of the cloud desktop. Generally speaking, the data of the host and the cloud terminal rely on the internal LAN transmission. As for the external network, it depends on your own needs and can be purchased from a telecom operator.

4.1.3. For Desktop Transfer Protocol

The desktop transmission protocol refers to a set of special data transmission rules, which can make the data transmission between the cloud host and the cloud terminal orderly and efficient so as to achieve a "rich and smooth" user experience. In brief, it is a set of rules for playing football. Each player (each data) has its own path, and players must cooperate well to pass the ball and score goals quickly.

It directly determines the cloud desktop performance and is a key factor. When we look at the performance of cloud desktops, the first thing to look at is this. There are two main transport layer protocols:

- The TCP protocol is mainly used to transmit data with high security requirements, such as printer data, user operation data, etc., but it is slower than UDP transmission;
- The UDP protocol is used for data transmission that does not require high completeness. Although fast, it will drop frames. For example, when watching a video, several frames may be skipped in the middle. For example, the frame loss phenomenon of NComputing's UXP protocol is more serious.

The data transmitted between the cloud host and the cloud terminal includes video, audio, image, keyboard and mouse inputs and other peripheral inputs. The performance of the efficient desktop transmission protocol can be measured from resource occupation, desktop fluency, frame loss rate, drawing, peripherals support and other aspects to test and evaluate. It should be noted that the desktop transfer protocol applied to virtual desktop infrastructure (VDI) and shared cloud desktops are different. When other conditions are the same, exploiting the same desktop transmission protocol in a shared cloud desktop, the transmission speed will be faster than that of a VDI. After all, the stadium is different (because the virtual cloud desktop VDI has more virtual layers), the distance is long and the passing time will naturally be longer.

In fact, with the same desktop transmission protocol, cloud desktops with different architectures have different effects on the resource utilization of the host. The host resource utilization of shared cloud desktops is higher than that of VDI, which is shown in Figure 4, because of the principle difference between the two cloud desktops. The shared cloud desktop can directly utilize the host's hardware resources, while the virtual cloud desktop calls the host's hardware resources through the intermediate virtual layer. In virtual cloud desktops, the first-class bare metal version of the virtual software has higher resource utilization than the second-class virtual software based on the installation of virtual software on the system.

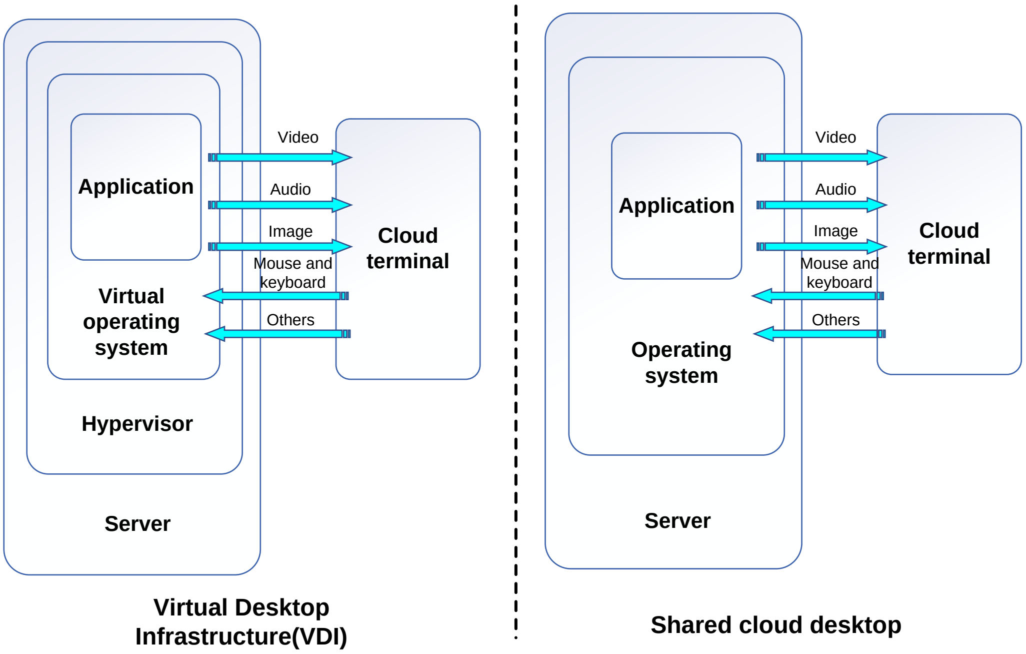

Figure 4. Desktop transport protocol architecture.

Cloud desktop transmission protocols are mostly low-overhead, fast and instant communication protocols. Cloud desktop protocols are mainly oriented to applications, including file editing, audio and video streaming and web surfing. Such protocol methods or strategies can also be applied to satellite communication links, sensor communication links such as drones, intelligent transportation communication links, Internet of Things, mobile applications and small networked devices, such as smart homes, smart medical care, etc. The metrics that the cloud desktop protocol focuses on are data latency, bandwidth and video playback quality. The quality of video playback includes two layers of meaning. One is to estimate the output based on the traffic in the network, and the other is to evaluate the user-perceived QoE of real experience.

4.2. Algorithms for DaaS Transfer

Most cloud desktop communication optimization protocols are improved by the transmission mechanism, mainly for low-cost, low-bandwidth instant messaging. The message queuing telemetry transport (MQTT) protocol [27] is also based on the TCP/IP protocol stack, which mainly uses the publish/subscribe message mode, which is a message publishing mode that realizes one-to-many communication through lightweight code. The protocol is not only lightweight but also simple, highly open and easy to implement, which has extensive applications. There are three participating identities for MQTT protocol communication, namely publisher, broker and subscriber. When messages are transmitted by this protocol, they have an associated QoS and topic. In general, the device under the cloud is equivalent to the client. The client uses the MQTT program or device, which can publish application messages to other correlative subscribers. Clients subscribe to request to receive related application messages, and clients unsubscribe to remove the request to accept app messages. Clients can also disconnect from the server. The server adopts network connections from subscribers, accepts business messages published by subscribers, processes subscription and unsubscribe requests from subscribers and relays application messages to eligible subscribed subscribers. The server is not the endpoint of the data, it is just a transit point for the data. Subscriptions contain a topic filter and the utmost QoS level. Subscriptions are matched with a single session, which can contain multi-subscription. Each subscription to a session has a specific topic filter.

The levels of MQTT message quality are segmented into three aspects, with level 0 being handed out at most once. The delivery of the data packets is integrated and dependent on the underlying TCP/IP network. There is no response and retransmission defined in this policy, and the data packets will either be turned over at the server only once. The packet by Level 1 policy is distributed at least once. The server's message reception is confirmed by the PUBACK segment. If the communication link or the sending device is exceptional, or the confirmation data packet is not received within the prescriptive time, the sender will resend the data packet with the DUP bit set in the message header. Level 2 is only dispatched once, which is the top level of data packet delivery; packet loss and duplication are unacceptable, and there is connatural overhead in exploiting this quality of service level.

For the RDP protocol, previous studies have not conducted research on public virtual scenarios and traffic models. In [17], the traffic model and QoE measurement of virtual hosts in the public cloud are studied, especially the evaluation of traffic data experienced a delay, occupied bandwidth and video traffic quality. It focuses on comparing multiple transport remote desktop protocol solutions in different WAN environments, evaluates the user-perceived experience quality for image quality, interactivity and gives mean opinion score (MOS) values. The research results show that burst data flow is still an important problem facing the cloud desktop transmission protocol and has issues that need to be addressed.

In [28], it was evaluated by studying the application of PCoIP (PC-over-IP) protocol in WAN scenarios. In 2008, VMware announced the joint development of PCoIP with Teradid to improve its own VDI solution, VMware View. PCoIP is closely integrated with hardware, data encoding and decoding and graphics processing can be performed through specialized hardware, allowing the CPU to have the energy to do other things, and there are monitors that integrate PCoIP display chips. PCoIP is based on the UDP protocol, and UDP transmission is unreliable, but UDP does not have the complex checksum data recovery of the TCP three-way handshake, and the transmission speed is fast, which is suitable for multimedia transmission. The native PCoIP protocol does not have the redirection capability of peripherals, such as serial and parallel ports, but some TC manufacturers make up for the lack of this function through additional port redirection plug-ins.

In [29], the performance of the RDP protocol is explored for different applications, and experiments are carried out with its user application experience, such as playback quality and delay. In [17], the author also conducted an analogical QoE study, mainly aimed at the ICA protocol. Although all of the papers provide MOS assessments, especially for RDP, VNC, ICA, and PCoIP are compared.

In [30,31], video quality is assessed in terms of transmitted data size, and the findings of cloud QoE are carried out for disparate cloud-based services, including cloud storage with lower latency and interactivity requirements, system services, multimedia on-demand services, communication and teleconferencing services and cloud desktop interaction services. The achievement of these studies provides a basis for developing prospective cloud services with QoE requirements and for determining the scale of the underlying network supply infrastructure, Especially with respect to mobile access technology. In the literature [32], the user's QoE is also evaluated by detecting the task time completed by the user's application level, such as the time taken by the user to complete text input, mouse operation and click refresh. The scheme comparison is carried out, and in the paper [33], the same author does compare the RDP with the ICA protocol. Studies have shown that these common cloud desktop protocols each have their own areas of adaptation, but most of the research is not based on real scene environments, and most of the research work is based on some simulation verification platforms, such as NetEm [34], and other simulation environment tools with certain random packet loss and link delay.

In research [35], a new network transport protocol is built based on AWS. It supplies an extraordinarily reliable, extendable and low-budget infrastructure platform in the cloud environment, supporting more than one million enterprises, governments, startups and organizations in hundreds of countries around the world. This protocol is a scalable and reliable data transmission protocol. It utilizes the large-scale network paths of the public cloud and takes into account the problems of unbalanced load and differential link delay of the protocol, realizing multi-tenancy in an elastic network with scalability and on-demand capacity. The problem of transmission cost-effectiveness is to avoid the problem of data overload on a certain path by sending a large amount of data to multiple network paths as much as possible, but it may cause the problem of out-of-sequence data packets. SRD responds to network congestion as quickly as possible by customizing the Nitro network interface card (NIC) to avoid frequent pulling of data traffic.

For transmission throughput, packet loss rate (PLR), inter-protocol fairness, intra-protocol fairness and high-speed file transfer, research [36] controls data congestion by judging network conditions. The protocol mainly uses round-trip time (RTT) to determine the bottleneck queue size, known as delay-based adaptive congestion control (DACC), by considering the presence of background flows. This kind of strategy explores the network state immediately and modulates the transfer delivery rate appropriately. Theoretical experiments prove that the advantages of DACC are better in multiple QoS indicators, and the identification of congestion is more prepared.

In research [36], the authors propose a new cross-layer-based cwnd initialized method for DACC. This method provides the best incipient value of the congestion window based on the available bandwidth. It can quickly adapt to network conditions so as to reduce packet loss and retransmission. DACC incorporates a queuing delay variation-based scheme that properly takes into account the impact of data flow and all other background flows on congestion. DACC incorporates a scheme based on the variation of queuing delay, which properly takes into account the impact of data flow and all other background flows when a traffic jam happened.

Current real-time video systems usually consist of two portions: the transport protocol and the video codec. The transport protocol is responsible for delivering the compressed video to the subscriber, processing acknowledgment and congestion indication. After that, the mean data rate on the network route is assessed and feeds the estimated data rate back to the codec module. The codec chooses the encoding parameters, e.g., frame rate and quality settings, after which it produces a compressed video stream with a medial bit rate close to the predicted network's natural capacity. Ultimately, the complete transmission of the video can be guaranteed without stuttering or the dropped frames phenomenon. In research [37], Salsify combines the packet-by-packet congestion control of the transport protocol and the frame-by-frame rate control of the video codec. Salsify is a dedicated architecture for network video transfer with instantaneity that tightly integrates a video codec and a network transport protocol. The method responds seasonably to changing network conditions without causing packet loss and queuing delays. It avoids causing network buffer overflows or queuing delays by matching network varying capacity and video transfer rates. Salsify's video codec explores optional encodings for each video frame at various quality degrees to match the compressed length to the instantaneous capacity of the network. When the network can accommodate a video frame, the corresponding video frame is sent. Salsify achieves lower video latency and higher video quality over variable network paths compared to FaceTime, Hangouts, Skype and WebRTC.

In [38], two problems with existing PCCs working over WAN are addressed. First, wide-area traffic has different RTTs, which can cause real-time data corruption problems caused by imperfect scheduling. Second, there is an RTT delay in credit-triggered data transmission, which reduces network performance. This paper studies FLASHPASS, a transmission method with high throughput and low loss through ACC on shallow-buffer WAN, which can effectively solve the above two problems. First, the problem of the imperfect height of data packets is avoided by performing data transmission timing calibration. Efficient credit allocation is then carried out through selective discarding mechanisms and over-provisioning. The evaluation shows that FLASHPASS effectively reduces the overall process completion time of TCPCubic and ExpressPass, and achieves a better QoS experience for users.

In the multi-path data transmission research literature [39], in order to cope with the dynamic workload, application-aware performance should be maintained. New protocol designs must be able to reconfigure routing and inter-Pod topology. The key to Gemini is the optimal integration of topology and routing, exploiting robust estimates of upcoming traffic from multiple historical traffic matrices as input. Gemini is a system designed to achieve these targets on commodity hardware while infrequently reconfiguring the network, making these modular designs applicable enough to deploy very shortly. Gemini reduces data bursts by sending these bursts of data traffic to multiple paths, thereby reducing data packet loss. The research uses a variety of data schemes for testing, such as dividing the data into low-volatility data, high-volatility data, etc. For low-volatility data, the protocol finds the topology and routing scheme with the least cost as quickly as possible. For highly fluctuating data, the protocol uses a tuned multi-traffic matrix and hedging to avoid frequent topology reconfiguration and only slightly increases the data route length. For this reason, Gemini can sustain existing traffic loads over a multi-path topology, combined with powerful decision-making algorithms to determine when to reconfigure and whether to use hedging, ultimately significantly reducing the cost of existing structures.

In addition [40], the multi-path transmission control protocol (MPTCP) coupled congestion control algorithm concentrates on combining multiple available links to increase the bandwidth, MPTCP is designed to adhere to the following two principles, first, application compatibility with applications as long as those that can run in the TCP environment can be run in the MPTCP environment without any modification. Second, network compatibility, MPTCP is compatible with other protocols. It also avoids using MP-TCP more aggressively than regular TCP streams on each link. This gives rise to very traditional action when network paths do not share congested links. Targeting network paths with different characteristics (i.e., available bandwidth, PLR and latency) increases the likelihood of network congestion, resulting in higher reordering, buffer congestion and unnecessary retransmission overhead. The currently implemented MP-TCP scheduler suffers from low channel utilization due to its traditional congestion window (cwnd) adaptation scheme. Therefore, this protocol hurts application-level throughput performance. To address these issues, the study proposes an adaptive data scheduling strategy (ADSS) [41], which dynamically adjusts the enhancement of cwnd according to the RTT changes of the paths. To adjust the transmission rate of each route according to the estimated RTT variation, an adaptive fast retransmission strategy is also designed and implemented. Research shows that compared with the MP-TCP scheduler, A-DSP can effectively reduce data transmission time, and the scheme can still guarantee the throughput of data transmission under different link packet loss rates, bandwidth and delay, effectively improving the efficient data transmission under multi-path.

For short remote procedure calls (RPCs), it provides a tail latency of <50 µs and a cloud environment architecture with a packet loss rate close to zero. Swift [42] achieves terminal-to-terminal latency by exploiting additive increase multiplicative decrease (AIMD) control and pacing under extreme congestion. The Swift protocol utilizes very-low base latency as a solution to respond quickly to network and end-host dynamics. The scheme is a centralized or in-network credit-based/explicit feedback scheme. In a large number of high-speed transmission protocols, the delay has always been the best measure of network congestion. Swift further decomposes the end-to-end RTT to separate the structure from the host problem. Forward fabric delay is the summation of the serialization, propagation and queuing delays of packets on the switch between the source and destination. It also includes NIC serialization latency and better control of network congestion by separating fabric and host delays. Swift realizes the continuous low tail completion time of short remote procedure calls and provides high throughput for long remote procedure calls.

Higher link speeds also mean congestion is more likely to occur. The current solution is usually to use some reactive protocols similar to TCP, DCTCP and TIMELY. These protocols only react after congestion occurs. Reactive protocols have many problems, including excessively long switch queues, severe packet loss due to in-cast problems and very slow convergence. These problems get worse at higher link speeds. In [43], a congestion control scheme based on proactive congestion control (PCC) is proposed. Compared with reactive congestion control, it has a queue length close to 0, 0 packet loss and faster convergence speed. Unlike reactive solutions, proactive solutions proactively schedule network transfers based on the availability of network resources. The three receiver drivers shown here are typical active congestion control protocols, which allocate link resources by sending credits from the receiver. Aelous adopts the minimum rate control, all streams will be sent at wire speed within the first RTT, and these packets sent at wire speed are called unscheduled packets. The packets after the first RTT will adjust the sending rate through credit, and call them schedule packets, the planned packets. The purpose of this is to maximize the use of spare bandwidth. The problem that the first RTT of PCC cannot be used is solved by selective packet loss, the priority queue (that is FIFO) is not used, and the excellent performance of PCC is also retained.

Many Internet applications require high bandwidth but are not time-sensitive and can also be effectively utilized in cloud desktop data transmission. This prompts the congestion control "scavenger" to voluntarily give in to higher-priority applications. Low extra delay background transport (LEDBAT) has the following three goals: First, it can fill the bandwidth and get the utmost out of the network when there is no other flow on the neck of a bottle link. The second is to ensure a low queuing delay when there is no other data flow; due to the increase in the window of the CUBIC flow, when the queuing delay is introduced, it tries not to increase the queuing delay. The third is when there is high priority competition for bandwidth, LEDBAT actively sells the bandwidth and reduces the window. However, the existing scavenger protocol LEDBAT often fails to budge suffers from performance flaws and requires a separate codebase from other transport protocols. In research [44], it was proposed that PCC Proteus could act as an efficient scavenger or master protocol. The goals of the Proteus and LEDBAT protocols are the same; both are to utilize the remaining bandwidth in the link. However, in order to achieve higher link utilization, delay skew is used as a competing signal, as well as noise tolerance techniques in dynamic environments. The protocol has more possible business capabilities and can switch between multiple data transmission modes, which should indicate that the Proteus protocol can significantly improve page load times and DASH video delivery capabilities, and its hybrid mode significantly reduces bandwidth constraints, such as rebuffering in restricted environments.

4.3. Privacy Preserving for DaaS Transfer

The precondition for fully utilizing and mining the excellent performance of cloud desktops is a trustworthy cloud data environment, including cloud data storage security and cloud data transmission security. Data integrity and privacy are key issues in cloud computing, and data are stored in different geographical locations, so consideration is given. Therefore, data integrity and privacy protection clauses are the most prominent factors that users worry about in the cloud computing environment. This section will mainly discuss the security of cloud data and use this as support for cloud desktops.

As the world digitizes, the pressure on data storage continues to grow, and massive storage of data has driven the development of cloud storage. However, this increases possible risks, such as unauthorized access, data disclosure, sensitive information disclosure and privacy disclosure. Refs. [45,46] propose a general cloud storage security framework and analyze the challenges it faces. It discusses antileakage and data integrity, which points out the difficulties in solving new issues such as privacy protection and machine learning in cloud storage. Moreover, advanced encryption standard (AES) ciphers can be used for data security. The delay calculation of data encryption increases the delay time of encrypted data. An encryption method for cloud data storage is proposed [47]. Users and cloud service providers, respectively, use elliptic curve integrated encryption schemes (ECIES) and AES for encryption to achieve storage integrity, confidentiality and efficient computing. CryptoGA [48], based on the genetic algorithm (GA), is proposed to solve the integrity and privacy issues of cloud data transmission. Ref. [49] discusses the implementation of cloud data security from another perspective. Data are divided into ordinary data and sensitive data, and more sensitive data are further divided into two parts. Each part is encrypted and distributed across multiple clouds, while ordinary data are uploaded in encrypted form to a single cloud, which is more efficient and faster than popular encryption methods.

On the other hand, on the basis of ensuring the security of cloud storage, the security of cloud transmission is also of great value for discussion. Ref. [50] explains cloud cryptography. Several mechanisms are used in cloud cryptography to add a high level of security to protect data from infiltration, hacking or being compromised by malware. This can also play a certain role in cloud data transmission. Based on the above discussion on data security and privacy, with the further development of the research, cloud security will be further guaranteed, and the use value of cloud desktops will be further improved.

5. Conclusions

Desktop virtualization has flourished and has been widely deployed over the past several years. In order to be content with the transmission requirements of timeliness and reliability of screen updatse in a desktop virtualization environment, a QoE-based perceptual transmission scheme is urgently needed. This paper first introduces the related concepts and architecture of the desktop cloud, then introduces the related concepts of the remote desktop protocol, reviews the optimization applied to data delivery in the desktop virtualization system and briefly introduces the transmission scheme carried out for delay-sensitive data and communicates the methods for visual perception QoE measurement. After research, the solutions to several current mainstream protocols are compared and analyzed. The video encoding and compression algorithms involved in the image transmission in the remote desktop protocol are compared and analyzed. Finally, the remote desktop protocol and high-speed transfer protocol are reviewed. We study application layer protocols designed or adapted for DaaS solutions, focusing on their possible implementation in IoT, cloud computing and data center-based systems.

Users only need to focus on business, have operating systems and applications to use, install appropriate desktop system templates, install application software for terminal devices that access cloud desktops, prepare images, publish to users and upgrade and maintain images. Cloud desktop service providers provide back-end service reading and writing hardware and provide corresponding cloud desktop transmission protocol support services and system management to ensure users' QoE experience in the process of exploiting cloud desktops. High desktop transmission protocol is important to achieve faster data transmission and higher resource utilization with better algorithms so as to improve the user experience, that is, smooth delivery, short response time, clear picture and sound and high user density. The desktop transfer protocol is the technical core of cloud desktop manufacturers.

Author Contributions: All members of our team have different contributions to the research work. More specifically, F.L., T.G. and X.L. drafted the manuscript, and performed validation. J.W., Y.X. and Y.M. supervised and revised the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: The National Key Research and Development Program under Grant 2022YFB3305203; the National Natural Science Foundation of China under Grant U2133208 and Grant 62101368; the Basic Research Program of China under Grant 2021-JCJQ-ZQ-082; the Sichuan Youth Science and Technology Innovation Team under Grant 2022JDTD0014; the Sichuan Province Science and Technology Support Program under Grant 2022YFG0168; the Science and Technology Program of Guizhou Province under Grant Qianke Support [2022] General 076; the Sichuan University Postdoctoral Research and Development Fund under Grant 2022SCU12115.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable to this article as no new data were created.

Acknowledgments: This work was supported in part by the National Key Research and Development Program under Grant 2022YFB3305203; in part by the National Natural Science Foundation of China under Grant U2133208 and Grant 62101368; and in part by the Basic Research Program of China under Grant 2021-JCJQ-ZQ-082; and in part by the Sichuan Youth Science and Technology Innovation Team under Grant 2022JDTD0014; and in part by the Sichuan Province Science and Technology Support Program under Grant 2022YFG0168; and in part by the Science and Technology Program of Guizhou Province under Grant Qianke Support [2022] General 076; and in part by the Sichuan University Postdoctoral Research and Development Fund under Grant 2022SCU12115.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AWS	Amazon Web Services
ACC	Adaptive Cruise Control
ICA	Inter-Center Agreement
PCoIP	PC over IP
VNC	Virtual Network Computing
RFB	Remote Frame Buffer
SPICE	Simple Protocol for Independent Computing Environment
IoT	Internet of Things
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
DaaS	Desktop as a service
RTP	Real-time Transport Protocol
RDP	Remote Display Protocol

GPU	Graphic Processing Unit
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
LAN	Local Area Network
WAN	Wide Area Network
MJPEG	Motion Joint Photographic Experts Group
USB	Universal Serial Bus
DTN	Delay Tolerant Networks
SRAP	Service Rating Application Protocol
UXP	User Experience Platform
VDI	Virtual Desktop Infrastructure
MQTT	Message Queuing Telemetry Transport
PSNR	Peak Signal to Noise Ratio
MOS	Mean Opinion Score
QoS	Quality of Service
QoE	Quality Of Experience
RD	Remote Desktop
NICs	Network Interface Cards
HPC	High Performance Computing
ML	Machine Learning
EC2	Elastic Compute Cloud
SRD	Software Defined Radio
RTT	Round Trip Time
DACC	Delay-Based Adaptive Congestion Control
PLR	Packet Loss Ratio
ACC	Active Congestion Control
MPTCP	Multi-path Transmission Control Protocol
ADSS	Adaptive Data Scheduling Strategy
AIMD	Additive Increase Multiplicative Decrease
RPCs	Remote Procedure Calls
SPF	Scheduled Packet First
LEDBAT	Low Extra Delay Background Transport
NDP	Neighbor Discovery Protocols
FCT	Flow Completion Time
ITS	Intelligent Transportation System
HTTP	HyperText Transfer Protocol
CoAP	Constrained Application Protocol
REST	Resource Representational State Transfer

References

1. Mohammed, C.M.; Zeebaree, S.R. Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review. *Int. J. Sci. Bus.* **2021**, *5*, 17–30.
2. Bello, S.A.; Oyedele, L.O.; Akinade, O.O.; Bilal, M.; Delgado, J.M.D.; Akanbi, L.A.; Ajayi, A.O.; Owolabi, H.A. Cloud computing in construction industry: Use cases, benefits and challenges. *Autom. Constr.* **2021**, *122*, 103441. [CrossRef]
3. Tsai, W.L. Constructing assessment indicators for enterprises employing cloud IaaS. *Asia Pac. Manag. Rev.* **2021**, *26*, 23–29. [CrossRef]
4. Zheng, H.; Wang, J.; Zhang, J.; Li, R. IRTS: An Intelligent and Reliable Transmission Scheme for Screen Updates Delivery in DaaS. *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* **2021**, *17*, 1–24. [CrossRef]
5. Benomar, Z.; Longo, F.; Merlino, G.; Puliafito, A. Cloud-based enabling mechanisms for container deployment and migration at the network edge. *ACM Trans. Internet Technol. (TOIT)* **2020**, *20*, 1–28. [CrossRef]
6. Trevizan, R.D.; Obert, J.; De Angelis, V.; Nguyen, T.A.; Rao, V.S.; Chalamala, B.R. Cyberphysical Security of Grid Battery Energy Storage Systems. *IEEE Access* **2022**, *10*, 59675–59722. [CrossRef]
7. Wang, H.; Dai, H.; Qiu, M.; Liu, M. Optimization of Remote Desktop with CNN-based Image Compression Model. In Proceedings of the Knowledge Science, Engineering and Management: 14th International Conference KSEM 2021, Tokyo, Japan, 14–16 August 2021; Springer: Cham, Switzerland, 2021; pp. 692–703.
8. Bai, T.; Bian, H.; Abou Daya, A.; Salahuddin, M.A.; Limam, N.; Boutaba, R. A machine learning approach for rdp-based lateral movement detection. In Proceedings of the 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrueck, Germany, 14–17 October 2019; pp. 242–245.

9. Hou, W.; Wang, J. Video region detection algorithm for virtual desktop protocol. *J. Comput. Appl.* **2018**, *38*, 1463.
10. Bitton, R.; Shabtai, A. A machine learning-based intrusion detection system for securing remote desktop connections to electronic flight bag servers. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 1164–1181. [CrossRef]
11. Garcia, M.; Quiroga, J.; Ortin, F. An infrastructure to deliver synchronous remote programming labs. *IEEE Trans. Learn. Technol.* **2021**, *14*, 161–172. [CrossRef]
12. Xiao, W.; Wan, N.; Hong, A.; Chen, X. A Fast JPEG Image Compression Algorithm Based on DCT. In Proceedings of the 2020 IEEE International Conference on Smart Cloud (SmartCloud), Washington, DC, USA, 6–8 November 2020; pp. 106–110.
13. Kanellopoulos, D. Inter-destination Multimedia Synchronization: A Contemporary Survey. *Infocommun. J.* **2019**, *XI*, 10–21. [CrossRef]
14. Jansen, J.; Cesar, P.; Bulterman, D.C.; Stevens, T.; Kegel, I.; Issing, J. Enabling composition-based video-conferencing for the home. *IEEE Trans. Multimed.* **2011**, *13*, 869–881. [CrossRef]
15. Kraev, Y.; Firsov, G.; Kakov, D. Authentication via RDP Using Electronic Identifiers. In Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), Moscow, Russia, 26–29 January 2021; pp. 2361–2365.
16. Qin, D. A compression and transmission method for surveillance video data using SPICE protocol and DWT in cloud desktop environment. *J. Ambient. Intell. Humaniz. Comput.* **2019**, 1–9. [CrossRef]
17. Magana, E.; Sesma, I.; Morato, D.; Izal, M. Remote access protocols for Desktop-as-a-Service solutions. *PLoS ONE* **2019**, *14*, e0207512. [CrossRef]
18. Pocarovsky, S.; Orgon, M. Comparison of application dynamics in two types of CLOUD solutions. In Proceedings of the 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, 5–7 October 2020; pp. 154–158.
19. Garcia, D.C.; Dorea, C.; Ferreira, R.U.; Freitas, D.R.; de Queiroz, R.L.; Higa, R.; Ismael Seidel Testoni, V. Differential Transform for Video-Based Plenoptic Point Cloud Coding. *IEEE Trans. Image Process.* **2022**, *31*, 1994–2003. [CrossRef] [PubMed]
20. Venkatesan, R.; Pandiaraj, A.; Selvakumar, M. A Recurrent Neural Network for Image Deblocking Detection and Quality Enhancement. In Proceedings of the 2023 5th International Conference on Smart Systems and Inventive Technology, Tirunelveli, India, 23–25 January 2023; pp. 1–8.
21. Lan, Y.; Xu, H. Research on technology of desktop virtualization based on SPICE protocol and its improvement solutions. *Front. Comput. Sci.* **2014**, *8*, 885–892. [CrossRef]
22. Li, W.; Wang, B.; Yu, J.; Zhu, C.; Xiao, S.; Sheng, J. The optimization of Transparent-Desktop service mechanism based on SPICE. *Concurr. Comput. Pract. Exp.* **2016**, *28*, 4543–4556. [CrossRef]
23. Cesar, P.; Bulterman, D.C.; Kernchen, R.; Hesselman, C.; Boussard, M.; Spedalieri, A.; Gao, B. Multimodal Adaptation and Enriched Interaction of Multimedia Content for Mobile Users. In *Taiwanese-French Conference on Information Technology*; INRIA: Taipei, Taiwan, 2008; pp. 230–239.
24. Richardson, T.; Wood, K.R. *The RFB Protocol*; ORL: Cambridge, UK, 1998.
25. Marri, S.R.; Reddy, P.C. A Survey on Streaming Adaptation Techniques for QoS and QoE in Real-Time Video Streaming. In *Smart Computing Techniques and Applications*; Springer: Singapore, 2021; pp. 455–465.
26. Pokhrel, S.R.; Qu, Y.; Gao, L. QoS-aware personalized privacy with multipath TCP for industrial IoT: Analysis and design. *IEEE Internet Things J.* **2020**, *7*, 4849–4861. [CrossRef]
27. Shinde, S.A.; Nimkar, P.A.; Singh, S.P.; Salpe, V.D.; Jadhav, Y.R. MQTT-message queuing telemetry transport protocol. *Int. J. Res.* **2016**, *3*, 240–244.
28. Metzler, J. *Virtualization: Benefits, Challenges, and Solutions*; Riverbed Technology: San Francisco, CA, USA, 2011; pp. 1–24.
29. Huse, S.M.; Mark Welch, D.B.; Voorhis, A.; Shipunova, A.; Morrison, H.G.; Eren, A.M.; Sogin, M.L. VAMPS: A website for visualization and analysis of microbial population structures. *BMC Bioinform.* **2014**, *15*, 41. [CrossRef] [PubMed]
30. Casas, P.; Schatz, R. Quality of experience in cloud services: Survey and measurements. *Comput. Netw.* **2014**, *68*, 149–165. [CrossRef]
31. Kim, M.; Cui, Y.; Han, S.; Lee, H. Towards efficient design and implementation of a hadoop-based distributed video transcoding system in cloud computing environment. *Int. J. Multimed. Ubiquitous Eng.* **2013**, *8*, 213–224.
32. Schlosser, D.; Staehle, B.; Binzenhöfer, A.; Boder, B. Improving the QoE of citrix thin client users. In Proceedings of the 2010 IEEE International Conference on Communications, Cape Town, South Africa, 23–27 May 2010; pp. 1–6.
33. Jarschel, M.; Schlosser, D.; Scheuring, S.; Hoßfeld, T. An evaluation of QoE in cloud gaming based on subjective tests. In Proceedings of the 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Seoul, Republic of Korea, 30 June–2 July 2011; pp. 330–335.
34. Zheng, H.; Liu, D.; Wang, J.; Liang, J. A QoE-perceived screen updates transmission scheme in desktop virtualization environment. *Multimed. Tools Appl.* **2019**, *78*, 16755–16781. [CrossRef]
35. Shalev, L.; Ayoub, H.; Bshara, N.; Sabbag, E. A cloud-optimized transport protocol for elastic and scalable hpc. *IEEE Micro* **2020**, *40*, 67–73. [CrossRef]
36. Verma, L.P.; Sharma, V.K.; Kumar, M.; Kanellopoulos, D. A novel Delay-based Adaptive Congestion Control TCP variant. *Comput. Electr. Eng.* **2022**, *101*, 108076. [CrossRef]

37. Fouladi, S.; Emmons, J.; Orbay, E.; Wu, C.; Wahby, R.S.; Winstein, K. Salsify: Low-Latency Network Video through Tighter Integration between a Video Codec and a Transport Protocol. In Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18), Renton, WA, USA, 9–11 April 2018; pp. 267–282.
38. Zeng, G.; Qiu, J.; Yuan, Y.; Liu, H.; Chen, K. FlashPass: Proactive congestion control for shallow-buffered WAN. In Proceedings of the 2021 IEEE 29th International Conference on Network Protocols (ICNP), Dallas, TX, USA, 1–5 November 2021; pp. 1–12.
39. Zhang, M.; Zhang, J.; Wang, R.; Govindan, R.; Mogul, J.C.; Vahdat, A. Gemini: Practical reconfigurable datacenter networks with topology and traffic engineering. *arXiv* **2021**, arXiv:2110.08374.
40. Tomar, P.; Kumar, G.; Verma, L.P.; Sharma, V.K.; Kanellopoulos, D.; Rawat, S.S.; Alotaibi, Y. CMT-SCTP and MPTCP Multipath Transport Protocols: A Comprehensive Review. *Electronics* **2022**, *11*, 2384. [CrossRef]
41. Verma, L.P.; Sharma, V.K.; Kumar, M.; Mahanti, A. An adaptive multi-path data transfer approach for MP-TCP. *Wirel. Netw.* **2022**, *28*, 2185–2212. [CrossRef]
42. Kumar, G.; Dukkipati, N.; Jang, K.; Wassel, H.M.G.; Wu, X.; Montazeri, B.; Wang, Y.; Springborn, K.; Alfeld, C.; Ryan, M.; et al. Swift: Delay is simple and effective for congestion control in the datacenter. In Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication, Virtual, 10–14 August 2020; pp. 514–528.
43. Hu, S.; Bai, W.; Zeng, G.; Wang, Z.; Qiao, B.; Chen, K.; Tan, K.; Wang, Y. Aeolus: A building block for proactive transport in datacenters. In Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication, Virtual, 10–14 August 2020; pp. 422–434.
44. Meng, T.; Schiff, N.R.; Godfrey, P.B.; Schapira, M. PCC proteus: Scavenger transport and beyond. In Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication, Virtual, 10–14 August 2020; pp. 615–631.
45. Yang, P.; Xiong, N.; Ren, J. Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access* **2020**, *8*, 131723–131740. [CrossRef]
46. Lee, B.H.; Dewi, E.K.; Wajdi, M.F. Data security in cloud computing using AES under HEROKU cloud. In Proceedings of the 2018 27th Wireless and Optical Communication Conference (WOCC), Hualien, Taiwan, 30 April–1 May 2018; pp. 1–5.
47. Tyagi, M.; Manoria, M.; Mishra, B. A Framework for Data Storage Security with Efficient Computing in Cloud. In *International Conference on Advanced Computing Networking and Informatics: ICANI-2018*; Springer: Singapore, 2019. [CrossRef]
48. Tahir, M.; Sardaraz, M.; Mehmood, Z.; Muhammad, S. CryptoGA: A cryptosystem based on genetic algorithm for cloud data security. *Clust. Comput.* **2021**, *24*, 739–752. [CrossRef]
49. Shahid, F.; Ashraf, H.; Ghani, A.; Ghayyur, S.A.K.; Shamshirband, S.; Salwana, E. PSDS–Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud. *IEEE Access* **2020**, *8*, 118285–118298. [CrossRef]
50. Dubey, H.; Kumar, S.; Chhabra, A. Cyber Security Model to Secure Data Transmission using Cloud Cryptography. *Cyber Secur. Insights Mag.* **2022**, *2*, 9–12.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.