World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Security and privacy protection in the distributed cloud: a hyper-converged architecture-based solution

Hongtao Liu *

Hangzhou MacroSAN Technologies Co., Ltd. Vice President, 310052 Hangzhou, Zhejiang, China.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(01), 425–435

Publication history: Received on 12 August 2024; revised on 19 September 2024; accepted on 21 September 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.1.0440

Abstract

With the emergence of cloud computing technology, distributed cloud is one of many options in which enterprises and organizations can acquire computing resources and services. However, data security and user privacy protection in the distributed cloud environment will have many problems, for example, data leaks, unauthorized access, and cross-domain resource sharing. Thus, this paper seeks to analyze a security and privacy protection solution using hyper-converged architecture to enhance security for distributed cloud environments. Based on the analysis of the characteristics of current security technologies and hyper-converged architectures, this paper has designed a new security architecture framework, which includes encryption technology, access control, and data isolation. The proposed scheme is evaluated in the distributed cloud environment and the experimental results demonstrate high security enhancement as well as high performance and availability. Besides, the features of the implementation details, the advantages and limitations of the scheme, and further research ideas are also provided in this paper. Altogether, the research of this study offers new angled approaches/technical assistance to security and privacy preservation in a distributed cloud setting.

Keywords: Distributed Cloud; Hyper-Converged Architecture; Privacy Protection; Comprehensive Security Framework; And Performance Optimization**.**

1. Introduction

In the ever-evolving technology world of computing technologies, the distributed cloud has become an important model for delivering resources and computing services to enterprises or organizations. Distributed cloud computing is akin to conventional cloud systems but it part processes requested information and stores it in other geographic regions closer to the consumers to minimize delay and improve service [1]. This is in line with the current advancements in Edge Computation as well as the Internet of Things, and IoT applications where data has to be processed at the source to meet certain performances. Of course, as these clouds are distributed by nature, numerous security and privacy hazards cannot simply be solved with traditional cloud security safeguards.

Another issue that becomes significant in distributed cloud environments is the security concern especially when working with distributed and multi-tenant architecture [3]. While using a distributed cloud, data tends to move across several boundaries and becomes exposed to threats like data interception, unauthorized access, cross-vendor issues, etc. However, the multi-tenancy aspect adds to the complexities of rendering data isolation and this often makes it hard to avoid interoperability between tenants that are on the same physical infrastructure [4]. Owing to the growing popularity of distributed cloud services for organizations, top-notch security features, and privacy shield provisions are of utmost necessity to protect data as well as the users' confidence.

* Corresponding author: Hongtao Liu.

As a result, the implementation of enhanced security approaches for distributed cloud scenarios has been accompanied by a search for different technologies, such as hyper-converged infrastructure (HCI). This study defines HCI as a unified computing, storage, networking, and virtualization infrastructure that serves to consolidate resources and systems, thus making them easier to manage. Through software-defined convergence of IT resources, HCI presents an enhanced scalability capability, flexibility, and agility, which are paramount characteristics when it comes to the management of the dispersed topological nature inherent in distributed cloud implementations [6]. Further, the characteristics of HCI that embrace security functions including data encryption, access control, and real-time monitoring are advantageous in strengthening the security of distributed cloud assets [7].

Though there is a shift towards the integration of HCI in distributed cloud environments, the existing literature on using HCI for integrated security and privacy is scarce. Previous publications are limited to studying isolated aspects of security, including the cryptographic algorithms used or the access control models that are implemented, but the holistic perspective of security that comprises distributed clouds is not discussed [8]. A call has been made to combine these technologies into a system such that they will form part of a coherent security model that will take advantage of the features eased by HCI to propose security solutions that are reliable, elastic, and malleable for distributed cloud environments [9].

This study seeks to fill these gaps by designing a security and privacy protection framework for hyper-converged architecture for distributed cloud environments. Therefore, the integration of selected measures involving advanced encryption, access control procedures, and data isolation measures and their implementation in a hyper-converged environment offers advanced protection against uncontaminated threats in distributed cloud environments. The acquisition of all these technologies increases the security and privacy of data and also reduces management and overhead costs when implemented in a distributed cloud environment, making it suitable for enterprises.

Some of the issues that are likely to be faced when implementing distributed cloud security include the following;

There are many security and privacy issues in distributed cloud environments, mostly because of the decentralized nature of the cloud and the issues involved in handling data across the different domains. Most conventional security processes like firewalls, outer shell protection, and rudimentary encryption are often not sufficient for the distributed environment in which data is continually transferred and processed through many nodes [3]. Also, the very nature of multi-tenancy in distributed clouds creates daunting questions related to data segregation and malicious access. Lack of proper separation of data between tenants poses risks of data leakage, whereby information belonging to one tenant might be accessed by another tenant and this is detrimental to the privacy and regulation laws.

To meet these issues, researchers have discussed various strategies; for instance, attribute-based access control (ABAC) and role-based access control (RBAC) to offer fine-grained access control than the previous conventional models [10]. They include ABAC which enables decision-making on the permissible access in terms of roles, type of resources, and the environment thus providing a solution to the security in the distributed cloud [11]. However, compared to conventional access control, all these mechanisms might be even more effective but need secure connection with encryption technologies and data isolation solutions to provide a perfect security solution.

1.1. Seriously considering Hyper-Converged Architecture to Boost Security

Hyper-converged infrastructure (HCI) has emerged as one of the disruptive solutions that can help mitigate many of the security issues characteristic of distributed clouds. Originally, justification for HCI can be seen in the characteristics of software-defined environments which enable the single security framework integrated with other infrastructures of the cloud [12]. For example, by enhancing the virtual storage layers and software-defined networking, HCI provides flexibility in resource allocation and compartmentalization of the resources to improve data protection and minimize the probabilities and instances of breaches [13]. In addition, the application of centralized management throughout HCI makes it manageable to monitor and specifically enforce security measures regardless of the differentiations of the cloud infrastructures across the distributed organization setting.

The proposed security framework incorporates the strengths of HCI to adopt a layered approach for security that entails, data encryption, access control, and data isolation as well as monitoring. The framework also insists on data encryption techniques like AES-256, which means data is secured during both transit and when at rest which significantly reduces the risks of data vulnerability in the course of transmission from one node in the cloud system to another [14]. In addition, RBAC is also incorporated in the hyper-converged configuration that enables control of data access through the setting of roles and responsibilities of users [15].

The framework also uses some of the most advanced data isolation mechanisms including virtualization where data belonging to different tenants is isolated. This makes the system secure from any intruder and keeps the details of each tenant in its own virtual area which enhances the security level. Furthermore, the presence of a security audit module helps in identifying and responding to security violations and behavioral patterns as they occur, while a knowledge management facility assists in sharing knowledge with peers besides offering up-and-running coverage for the security system.

2. Literature review

2.1. Existing security measures and technologies for the distributed cloud

As a new form of cloud computing, distributed cloud has attracted much attention for its security. Traditional cloud computing security measures mainly include identity authentication, access control, data encryption, firewall, and other technical means. However, due to the highly decentralized nature of the distributed cloud environment, traditional security measures are often difficult to fully meet its needs. At present, researchers have proposed a variety of security measures for distributed cloud environments, such as identity authentication and access control, in distributed cloud environments, because data and services across multiple physical locations, traditional boundary-based access control strategies are no longer applicable. Many mechanisms, such as attribute-based access control (ABAC) and role-based access control (RBAC), have been proposed to meet more complex access control requirements[4]. To protect the security of data during transmission and storage, researchers have developed various encryption algorithms and protocols, such as AES, RSA, etc., and combined them with the characteristics of distributed cloud optimization, to improve the speed and efficiency of encryption and decryption. Virtualization technology is one of the core technologies of distributed cloud, but in the virtualization environment, problems such as VM escape attacks and data leakage between VMS are becoming increasingly prominent. Therefore, strengthening the security protection of the virtualization layer has become one of the focuses of research. To improve the security of identity authentication, multi-factor authentication technology is widely used in distributed cloud environments. It combines various authentication modes such as passwords, biometrics, and hardware tokens to enhance the security of the system [5]

2.2. Research status of hyperfusion architecture

Hyperconverged architecture is a technology that integrates computing, storage, and network functions on the same platform to achieve unified resource management and scheduling in a software-defined manner. Hyperconverged architecture not only helps in the management of data centers but also increases the efficiency of the available resources and increases the flexibility and reliability of the system. In the past few years, with the development of the distributed cloud concept, the hyper-converged architecture has also been implemented in the distributed cloud to construct more effective and reliable cloud service systems. Specifically, the application of hyper-converged architecture in the distributed cloud is mainly reflected in the following aspects: Resource management. The hyper-converged architecture has the ability for centralized management of the resource pool and can dynamically allocate and balance the resources in the distributed cloud environment which in turn leads to efficient utilization of the resources.

The hyper-converged architecture in the distributed cloud also implements the concepts of fault recovery and fault tolerance [5]. The hyper-converged architecture has inherent redundancy and failover options that enable it to recover from the failure of distributed nodes and provide high availability of the system. Another key characteristic of hyper-convergence architecture in the distributed cloud is Security management. The hyper-convergence architecture is designed to offer security protection modules to cover the entire scenario for security protection such as firewall, IDS/IPS, and antivirus, which ensure the security of the distributed cloud environment.

3. Review of key technologies for security and privacy protection

To meet the security and privacy protection challenges in the distributed cloud environment, researchers have explored a series of key technologies, including but not limited to the following four aspects: First, data encryption and privacy protection technology: by encrypting sensitive data, prevent unauthorized access; Meanwhile, differential privacy and homomorphic encryption are adopted to protect user privacy. Second, access control and permission management, through fine-grained access control policies to ensure that only authorized users can access the corresponding resources[6]. Third, audit and monitoring, establish a perfect log recording and monitoring system, real-time monitoring system status, timely discovery, and response to security incidents. Fourth, safety protocols and standards, follow international and industry standards, such as ISO/IEC 27001, NIST CSF, etc., and develop strict safety management specifications to ensure system compliance [10]

3.1. The inadequacies of current solutions

Although there have been many research results on distributed cloud security and privacy protection, there are still some shortcomings. Inconsistent cross-domain security coordination: In the distributed cloud environment, security policies of different regions may differ. Therefore, how to achieve cross-domain security coordination is a major challenge. The balance between performance and security is different: security measures often introduce additional overhead, and how to achieve a high level of security without compromising system performance still needs further research. The effectiveness of privacy protection is not perfect: although there are a variety of privacy protection technologies, how to ensure the effectiveness of technology and user acceptance in practical applications still needs to be explored.

Sun stresses the key issues & concerns relating to security and privacy for cloud computing scenarios. This research is relevant as cloud computing has emerged as one of the standard types of solutions in IT environments, and the growing usage of cloud-based services causes essential questions related to the security of data, violation of privacy, and loss of information. It examines such issues as operational, technical, and other risks about data privacy, protection, and accessibility as well as the dynamic and distributed nature of the multi-tenancy of cloud systems. It also features the need to invent more complex patterns in cryptography and methodologies of access control. The results reveal that although security is proactively implemented, there are still areas where the total protective shield is not in place hence posing a threat to user trust and possibly discouraging the use of cloud services. Thus, Sun suggests improving security structures through the use of AI in threat identification, increasing the stringency of the set regulation, and developing successful cooperation between cloud service suppliers and consumers to address emerging threats effectively. All these steps are important if cloud systems have to guard against future threats and be more resistant [16].

Asaad and Zeebaree's work aims at solving the research problem of improving security and privacy in distributed cloud settings which has become a challenge due to the evolving nature of the environment. This work is therefore important because it provides an extensive analysis of the related protocols and mechanisms intended for the security of the information in distributed cloud systems popular with the continuously enlarging cloud computing environment. The study has revealed the following about existing security strengths and weaknesses of traditional security models including encryption, identification, authentication, and intrusion detection/ prevention solutions Many current applications and solutions are found to be rudimentary and insufficient against modern sophisticated cyber threats. According to the results of the protocols, it is observed that though most have strong security measures integrated into them, they lack provisions for expansion, fluidity, and options for more security risks. These sources suggest the following as key strategies for adapting to new threats: The first approach is the use of multi-layered security where the authors propose the use of new encryption techniques combined with a zero-trust architectural approach and machine learning based on anomaly detection. Such strategies are crucial for the strengthening of security and privacy characteristics in distributed cloud settings making them credible and reliable to the user [17].

To address the research problem, Ometov et al. focus on security in cloud, edge, and fog computing, which are the foundational components of today's distributed systems and present significant security risks. The contribution of the study is in a comprehensive assessment of security risks associated with these computing paradigms that are critical to meeting the emerging need for decentralized and low-latency applications. The study shows some of the risks as data loss, unauthorized access, and insecure transfer of data show the need to improve security. The outcomes showed that different methods like encryption, access control, and others are implemented, but they do not have sufficient adaptability and speed in comparison with the actual demands of edge and fog computing. From the study, technical suggestions include establishing a single consolidated security paradigm that is inclusive of all three configurations with the utilization of artificial intelligence threat identification mechanisms, proper application of blockchain for increased data reliability, and better encryption mechanisms. These recommendations are essential for developing sustainability in security arrangements in cloud, edge, and fog computing [18].

Haque et al. investigate the research issue of finding a secure and distributed solution for privacy-preserving healthcare systems which is very important due to the growing issues regarding patient data confidentiality in developing healthcare systems where technology is playing a great role. The study is important as it contributes to developing a new means of protection of health information as patient data is crucial to maintaining patients' trust and is subject to strict privacy regulations. The major discoveries show that centralized models, which have been implemented in numerous facilities across the world, rarely provide sufficient protection of patient data as they have numerous points of weakness related to the storage and transmission of data. Below are the proposed architecture and their respective features in data security, integrity, and availability: These findings confirm that the enhancement of the method provides a tangible boost to the privacy of the information alongside retaining the functional efficiency of the healthcare data processing and availability. The authors also advise a further fine-tuning of the architecture to enhance the result

and the suggestion of the use of machine learning approaches for threat detection, as a means to identify possible security threats in advance, thus, guaranteeing an adequate level of privacy protection in the sphere of healthcare [19].

3.2. Theoretical basis

To build a security and privacy protection scheme based on hyper-converged architecture, it is necessary to clarify the relevant theoretical basis, including the basic principle of hyperconverged architecture and the relevant theories of security and privacy protection.

3.3. The fundamentals of hyperconverged architecture

Hyper-Converged Infrastructure (HCI) is a solution that integrates computing, storage, networking, and virtualization resources on a unified platform. The core idea is to integrate traditionally separate hardware components into a single system in a software-defined manner for more efficient resource management, greater flexibility, and faster deployment. Here are a few key components of the hyper-converged architecture and how it works: With the help of virtualization the HCI platform provides the physical server resources in the form of Virtual Machines, which can be utilized on an as-and-when basis. The virtualization layer is the foundation of the model as it offers the resource pooling ability to adjust the number of resources necessary for the workload. In HCI, storage is also virtualized to create a single storage pool of storage resources. This storage pool can span across multiple physical storage devices and enhance data access and throughput by the use of replication and striping. Moreover, the storage layer often has the features like data protection, in the form of snapshots, clones, and deduplicate to enhance the data protection and overall efficiency. Network function is also an important part of HCI through which network resources are virtualized using the SDN technology. SDN enables administrators to be able to control the entire network from one central point, this makes it easier to set up and solve problems in the network. The hyper-converged architecture provides a unified management interface through which administrators can comprehensively monitor and manage the computing, storage, and network resources of the entire system. The unified management platform simplifies the IT operation and maintenance work and improves the maintainability and expansibility of the system [10]

3.4. Theory of security and privacy protection

In a distributed cloud environment, security and privacy protection are two closely related concepts, which together form the basis for protecting user data and business processes from infringement. The security model is a framework used to describe and analyze the security of computer systems. Common security models include the Bell-LaPadula model, Biba model, etc. These models define different levels of security policies to help system designers understand and implement access control mechanisms. Access control is the core mechanism to protect information systems from unauthorized access. There are three main types of access control: Autonomous access control (DAC), Mandatory Access Control (MAC), and role-based access control (RBAC). Of these, RBAC is the most commonly used because it automatically grants appropriate permissions based on the user's role, reducing the administrative burden. In a distributed cloud environment, encryption is a key tool for securing data and preventing unauthorized access by converting raw data into an unreadable form. Encryption algorithms are divided into symmetric encryption (such as AES), which uses the same key for encryption and decryption, and asymmetric encryption (such as RSA), which uses a pair of public and private keys. Privacy protection, as an important technology, aims to protect personal information from abuse. Common privacy protection technologies include differential privacy and homomorphic encryption. Differential privacy obsesses individual data by adding random noise, while homomorphic encryption allows operations to be performed on encrypted data without decryption. In addition to technical considerations, it is also necessary to comply with relevant laws and regulations, such as GDPR (European Union General Data Protection Regulation), CCPA (California Consumer Privacy Act), etc. These regulations require companies to take appropriate technical and organizational measures to protect personal data.

4. Methodology

To systematically study and design security and privacy protection schemes based on hyper-converged architecture, this section will elaborate on the methodology adopted in the research, including research methods and design, data collection and analysis tools, and a description of the experimental environment.

4.1. Research method and design

This work proposes a security and privacy protection solution based on hyper-converged architecture to address security challenges in the distributed cloud environment and ensure proper protection of users' data privacy. Specific goals include: The following are proposing to design a holistic security and privacy protection model that includes data encryption, access control, and data segregation, among others, to avail comprehensive security. Assessment of the

framework in the actual distributed cloud environment and experimental validation of the scheme under load conditions. Explore the scalability and compatibility of the framework **: It is necessary to achieve that the solution can be applied for various scenarios and effectively meet the requirements of different scale distributed cloud environments. To verify the validity of the study, the following hypotheses were proposed: To verify the validity of the study, the following hypotheses were proposed:

Hypothesis 1: Through the integration features of hyperconverged architecture, the security and privacy protection level of distributed cloud environments can be significantly improved.

Hypothesis 2: The security and privacy protection scheme based on hyperconverged architecture can ensure data security while maintaining good system performance.

Hypothesis 3: The designed solution has good scalability and can adapt to distributed cloud deployment of different scales.

This study follows the following steps: According to the characteristics of the distributed cloud environment, the main security threats and privacy protection needs are identified. Based on the results of the requirement analysis, a security and privacy protection scheme based on hyperconverged architecture is designed. Set up the experimental environment and design the experimental scheme to verify the effectiveness of the scheme. The experimental data are collected and statistically analyzed to evaluate the performance and effect of the program. Based on the data analysis results, the advantages and disadvantages of the scheme are discussed, and suggestions for improvement are put forward.

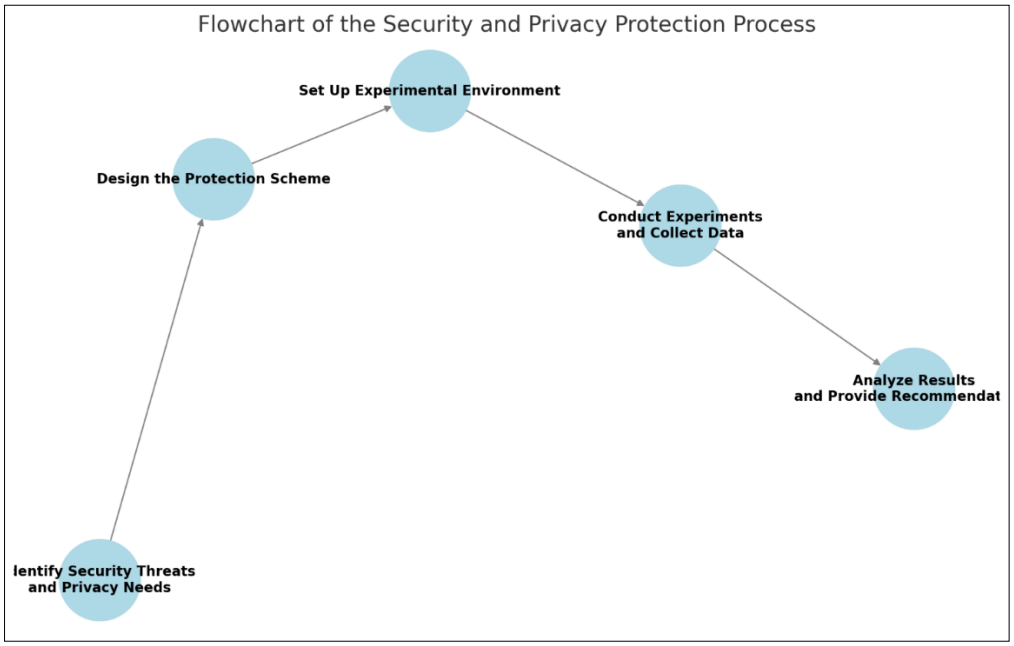

Figure 1 Security and Privacy Protection Process

4.2. Data collection and analysis tools

To ensure scientific and rigorous research, the following tools are used in this study to collect and analyze data: Log tools are used to record log information during system operation, including system performance indicators and security event records. This enables the monitoring of the normal status and the unknown state of the system. The simulators that are used to test system performance under different loads are JMeter and LoadRunner. With these tools, the managing of response-ability and stability of the scheme during high concurrent requests is assessable. Nessus and OpenVAS are security scanning tools that are used to scan the systems periodically to find out the vulnerabilities and security loopholes. These tools are useful in the detection of some of the security threats that may exist so that the system can be well secured. Some of the software that is used in the analysis of experimental data include Python's Pandas library, the R language, and others. By using these tools, the data collected can be processed and statistically analyzed to the maximum level. Charts and diagrams are made with the help of libraries like Matplotlib and Tableau for the visual representation of the results. These tools also help in the making results of data analysis more comprehensible and interpretable.

Table 1 Security Tools and Their Functions

Tool	Purpose	Examples
Log Tools	Monitor performance and security events	Custom Log Monitor
Performance Testing	Simulate system under load	JMeter, LoadRunner
Security Scanning	Identify vulnerabilities	Nessus, OpenVAS
Data Analysis	Process and analyze data	Pandas, R

This table summarizes the various tools employed in the study, highlighting their roles and specific examples used, thereby providing a clear overview of the data collection and analysis methodologies adopted in this research.

4.3. Description of experimental environment

To verify the effectiveness of the security and privacy protection scheme based on hyper-converged architecture, the following experimental environment was established in this study: The physical infrastructure which is distributed cloud nodes, several powerful servers were utilized in this work, and each server had Intel Xeon processors, 64GB RAM, and SSD storage. This configuration guarantees high efficiency and stability during the experiment as compared to the previous one. Operating system: It is also important to have Linux installed on each node so that all nodes will be similar. The experiment uses the Linux operating system which has good stability and security to ensure sound support for the experiment. Hyper-converged software-defined solution based on similar solutions like Nutanix and SimpliVity is used to create a single pool of computing, storage and network. Such platforms have an integrated management console that helps in managing resources and scheduling them. Those that include enhanced encryption schemes including AES and RSA, access control features including RBAC, data segregation techniques, and others. It is these components that enhance data security and privacy. Generate test data and generate data with different types of data such as text, images, video, and other forms and come up with data sets that will mimic real life scenarios. With these data sets it is possible to assess the effectiveness of the scheme on various types of data. It is also possible to use the Metasploit tool to mimic most of the common network attacks and analyze the system's ability to respond to them. These tools facilitate a demonstration of how the scheme performs and how it can defend against real-life invasions.

5. Security and privacy protection solution based on hyper-converged architecture

5.1. Architecture Design

To achieve efficient and secure and private protection in a distributed cloud system, this work present a comprehensive solution based on hyper-converged architecture. The solution is meant to contain all the aspects of security by incorporating various security technologies and measures as well as privacy. Add data encryption module: To protect the data, the advanced encryption standard (AES-256) is used in the encryption of the data to make sure that the data is not accessed by an unauthorized person in the course of transfer and storage. The encryption of the data will be done before the data is introduced to the distributed cloud and the decryption will be done after the data has left the distributed cloud in order to protect the data. Set up access control modules: Enforce RBAC in order to limit users to work with only the data and resources that they are supposed to work with by defining roles and permissions for these roles. Further, the fine-grained access control policies are used to control the access rights in more detail. Add data isolation module: In the hyper-converged architecture, data is logically isolated through virtualization technology. The data of each tenant is placed in an independent virtual storage space to prevent data leakage or misuse. Added security audit module: Records all access behaviors and operation logs, which facilitates follow-up and audit. The security audit module is also capable of automatically detecting unusual activity and issuing alerts when potential security threats are identified.

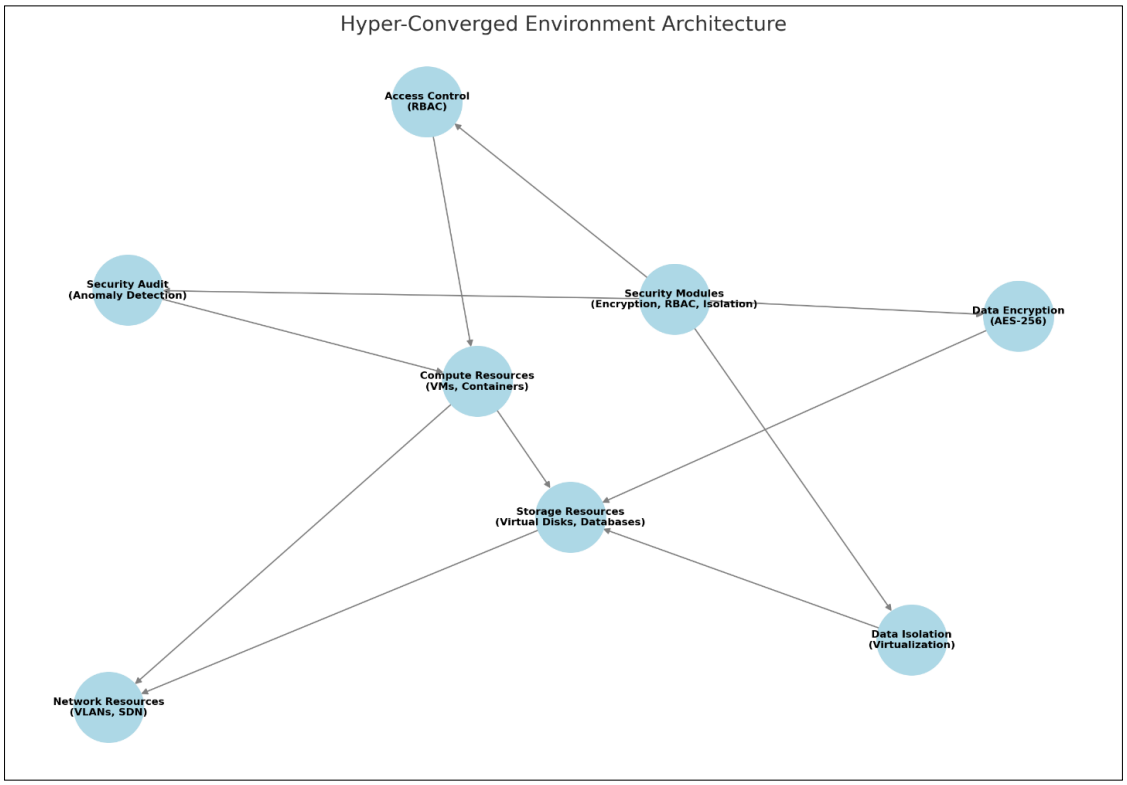

Figure 2 Hyper-coverage Environment Architecture

When processing and analyzing user data, differential privacy technology is used to mask individual data by adding random noise, to protect user privacy. Allowing operations to be performed on encrypted data without decryption ensures that data remains encrypted during processing, further enhancing privacy protection. For the information that does not need to retain the user's identity, anonymous processing technology is adopted to remove or replace the data elements that can identify the user's identity. Considering the characteristics of the distributed cloud, the security modules and privacy protection mechanisms are designed to be distributed and deployed to accommodate different geographic areas and resource pools. Each module can be deployed and managed independently, but can also be combined and extended as needed. Through the integration of automatic operation and maintenance tools, automatic updates and configuration of security modules can be achieved, reducing manual intervention and improving system reliability and efficiency.

5.2. Technical implementation details

In this scheme, AES-256 is chosen as the main encryption algorithm. Advanced Encryption Standard (AES) is a symmetric encryption algorithm with high security. The 256-bit key length was chosen to provide a higher level of security. In addition, for some specific application scenarios, asymmetric encryption algorithms such as RSA will be used to ensure the secure exchange of keys. The access control mechanism adopts role-based access control (RBAC) and implements fine-grained access control by defining roles, permissions, and responsibilities. Each user is assigned one or more roles, and each role corresponds to a set of permissions. When a user attempts to access a resource, the system checks whether the user's role has the corresponding permissions to determine whether to allow access. Data isolation policies include physical isolation and logical isolation. In physical isolation, the data of different tenants is stored on different physical storage devices. In logical isolation, the data of different tenants is divided into different logical storage Spaces on the same physical storage device through virtualization technology. In addition, data redundancy and backup strategies are employed to ensure that data is not lost due to a single point of failure.

5.3. Implementation case

A large manufacturing company plans to move its critical business systems to a distributed cloud environment to improve business continuity and flexibility. However, companies have encountered data security and privacy concerns in the decision-making process. Because businesses store a lot of sensitive data, including customer information, production data, and financial records, any data breach can lead to serious consequences. As a result, companies have

been very cautious during the migration process and have been looking for a solution that can both keep data secure and protect user privacy.

In response to this situation, enterprises decide to adopt the security and privacy protection scheme based on the hyperconverged architecture proposed in this study. The AES-256 encryption algorithm is used to encrypt the key data of the enterprise. Before the data enters the distributed cloud, all sensitive data is encrypted using dedicated encryption tools and decrypted when the data leaves the distributed cloud environment. In this way, even if the data is intercepted during transmission, the attacker will not be able to interpret the data content. According to the organization structure and business process of the enterprise, a role-based access control (RBAC) mechanism is designed. Different roles are defined for each department and position, and corresponding authority is given. For example, employees in the finance department can only access financial data related to their responsibilities, but not data from other departments. Virtualization technology is used to achieve logical data isolation. Each department's data is allocated to different virtual storage Spaces, which are independent of each other to prevent cross-access to data. The security audit module is deployed to record the access behavior of all users to the system. The module is capable of automatically detecting abnormal activity and issuing alerts when potential security threats are detected. In addition, audit records can be used to investigate subsequent security incidents.

After the above solution is implemented, key services of the enterprise are successfully migrated to the distributed cloud environment, and the expected results are achieved: After the AES-256 encryption algorithm is adopted, data is effectively protected during transmission and storage, and data content is difficult to be interpreted even if a data breach occurs. The RBAC mechanism and data logical isolation policy ensure that user data is not abused. The privacy of user data is effectively protected. The security audit module helps enterprises detect several unauthorized access attempts at an early stage and take corresponding countermeasures in time to prevent potential security threats from evolving into actual security incidents. The design of the solution fully considers the requirements of relevant laws and regulations to ensure compliance with the distributed cloud environment.

6. Discussion

After the completion of the design and experimental verification of the security and privacy protection scheme based on hyperconverged architecture, this part will conduct an in-depth analysis of the advantages and limitations of the scheme, compare it with other existing technologies, and discuss future research direction.

6.1. The advantages and limitations of the scheme

The solution takes full advantage of the hyper-converged architecture and integrates compute, storage, network, and security functions on a single platform, greatly simplifying system management operation and maintenance. Through modular design, the solution can be flexibly adapted to different application scenarios, whether it is a small enterprise or a large organization, you can find your deployment. The solution integrates multiple security technologies and privacy protection mechanisms, such as data encryption, access control, and data isolation, to effectively prevent multiple security threats and ensure data security and privacy. Through the application of virtualization technology and automatic operation and maintenance tools, the solution can provide high system performance and meet high concurrency requirements in the distributed cloud environment without ensuring security. The solution has good scalability, can be smoothly expanded with the growth of services, and supports the dynamic changes of the distributed cloud environment.

Since the hyper-converged architecture itself requires some hardware and software support, the initial deployment cost is relatively high, which may constitute a certain threshold for some small businesses with limited budgets. Although the solution is designed with automated operation and maintenance tools, for the first contact with the hyperconverged architecture of the enterprise, still needs certain technical reserves and learning costs. Business scenarios in different industries may vary greatly, and the solution may require further customization to meet specific business requirements. Some security components and technologies may rely on third-party vendors, which can lead to dependency issues for technical support and updates.

6.2. Comparative analysis with prior art

Traditional cloud computing security solutions usually consist of multiple independent security products, such as firewalls and intrusion detection systems, but solutions based on hyperconverged architecture integrate these functions to provide a more concise management interface. In the traditional solution, security policies may need to be adjusted frequently to meet rapidly changing service requirements. However, the hyper-converged architecture supports flexible resource allocation and can respond to service changes more quickly. While traditional solutions can also provide basic

security, solutions based on hyper-converged architectures perform better when it comes to data isolation, encryption, and so on, especially in large-scale distributed deployments. The encryption technology in the scheme is not only limited to data encryption but also includes key management, encryption and decryption algorithm selection, etc. It provides a complete solution. Compared with traditional access control mechanisms, role-based access control (RBAC) provides more granular permission management and is more suitable for multi-tenant scenarios in distributed cloud environments. Data isolation by virtualization technology can use resources more efficiently and reduce maintenance costs than physical isolation.

Table 2 Comparison of Hyper-converged Architecture vs. Traditional Cloud Security

Feature	Hyper-converged Architecture	Traditional Cloud Security
Integration Level	High (Integrated Management)	Low (Separate Components)
Data Isolation	Virtualization	Physical/Basic Logical
Scalability	High	Moderate
Ease of Management	Simplified	Complex
Performance Under Load	Optimized	Variable

This table is very useful for comparing the hyper-converged architecture and the traditional cloud security solutions, and highlighting the feature, integration, scalability, and performance benefits of hyper-converged systems. This is illustrated by explaining how the proposed solution engulfs increased manageability and improved security due to integrated components thus making it more flexible to complex cloud environments.

6.3. Future research direction

Although the security and privacy protection scheme based on hyper-converged architecture has achieved certain results in the current stage, there are still many directions worth further exploration: to further improve the automation level of the scheme, the use of machine learning and artificial intelligence technology to achieve adaptive adjustment and intelligent protection of security policies. How to make the solution better adapt to the needs of different industries and application scenarios, and improve its compatibility, so that IT can seamlessly connect to the existing IT ecosystem. Global data protection regulations need to be improved

7. Conclusion

This paper aims to explore a security and privacy protection scheme based on hyperconverged architecture to solve data security and user privacy protection problems in a distributed cloud environment. The background and significance of the research are clarified by summarizing the current status and technology development of distributed cloud security. On this basis, we design a set of comprehensive security and privacy protection framework, which includes data encryption, access control, data isolation, and other key modules, and expound its implementation details and technical points in detail. Through experimental verification, we prove the effectiveness and feasibility of this scheme in a distributed cloud environment. The experimental results show that the security and privacy protection scheme based on hyperconverged architecture can not only significantly improve the security of the system, but also maintain good performance under the premise of ensuring data security. In addition, the scalability and flexibility of the scheme have been fully demonstrated, which can adapt to the requirements of distributed cloud deployment in different scales and scenarios. The scheme proposed in this study has important practical significance, mainly reflected in the following aspects: Firstly, by integrating multiple security technologies and privacy protection mechanisms, the solution effectively improves the security level of the distributed cloud environment and can resist various types of security threats. Secondly, based on ensuring security, the solution realizes performance optimization through the application of virtualization technology and automated operation and maintenance tools and meets the high concurrency requirements in the distributed cloud environment. Moreover, through the integration characteristics of the hyper-converged architecture, the scheme simplifies the management operation and maintenance of the system and reduces the operating cost of the enterprise. Finally, the scheme has good scalability and flexibility, can adapt to different scales of distributed cloud deployment requirements, and has a wide range of applicability. Although the research in this paper has made some achievements, there are still many fields worthy of further discussion. In short, the security and privacy protection solution based on hyper-converged architecture provides an effective solution for a distributed cloud environment and helps to promote the healthy development of cloud computing technology. It is hoped that the

research in this paper can provide useful reference and inspiration for researchers and practitioners in related fields, and jointly promote the progress and innovation of distributed cloud technology.

References

[1] Xia, Z., Xiong, N. N., Vasilakos, A. V., & Sun, X. (2017). EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing. *Information Sciences*, *387*, 195-204.

[2] Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), 11.

[3] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

[4] Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International journal of information security*, *13*, 113-170.

[5] Shen, Z., Hu, H., Zhao, M., Lai, M., & Zaib, K. (2023). The dynamic interplay of phonology and semantics in media and communication: An interdisciplinary exploration. *European Journal of Applied Linguistics Studies*, *6*(2).

[6] Shen, Z., Xu, Q., Wang, M., & Xue, Y. (2022). Construction of college English teaching effect evaluation model based on big data analysis. In *Proceedings of the 2nd International Conference on New Media Development and Modernized Education*.

[7] Rittinghouse, J. W., & Ransome, J. F. (2017). *Cloud computing: implementation, management, and security*. CRC press.

[8] Shen, Z., & Zhao, M. (2024). An Analysis and Comparison of the Differences in the Realization of Interpersonal Functions in Different Political Keynote Speeches. *International Journal of Linguistics*, *16*(2), 42-60.

[9] Shen, Z., Xu, Q., Wang, M., & Xue, Y. (2022). Construction of college English teaching effect evaluation model based on big data analysis. In *Proceedings of the 2nd International Conference on New Media Development and Modernized Education*.

[10] Bester, Ron, and M. Arif Khan. "Next Generation Cloud Computing: Security, Privacy and Trust Issues from the System View." 2021 18th International Joint Conference on Computer Science and Software Engineering (JCSSE). IEEE, 2021.

[11] Shen, Z., Zhao, M., & Lai, M. (2023). Analysis Of Politeness Based On Naturally Occurring And Authentic Conversations. *Journal of Language and Linguistic Studies*, *19*(3).

[12] Gupta, Karan, et al. "From Hyper Converged Infrastructure to Hybrid Cloud Infrastructure." 12th USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage 20). 2020.

[13] Wen, Hao. Improving Application Performance in the Emerging Hyper-converged Infrastructure. Diss. University of Minnesota, 2019.

[14] Magsi, Zeeshan, et al. "Conceptual framework transformation of converged infrastructure (CI) into hyper-converged technology for virtualization of server infrastructure." 2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS). IEEE, 2020.

[15] Shetty, Abhishek Jayakar, and K. C. Ganashree. "Comprehensive review of datacenter architecture evolution." (2020).

[16] Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*, 102642.

[17] Asaad, R. R., & Zeebaree, S. R. (2024). Enhancing Security and Privacy in Distributed Cloud Environments: A Review of Protocols and Mechanisms. *Academic Journal of Nawroz University*, *13*(1), 476-488.

[18] Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A survey of security in cloud, edge, and fog computing. *Sensors*, *22*(3), 927.

[19] Haque, R. U., Hasan, A. T., Daria, A., Rasool, A., Chen, H., Jiang, Q., & Zhang, Y. (2023). A novel secure and distributed architecture for privacy-preserving healthcare system. *Journal of Network and Computer Applications*, *217*, 103696.