Hindawi
Scientific Programming
Volume 2022, Article ID 4767725, 9 pages
https://doi.org/10.1155/2022/4767725

Research Article

Application of Cloud Computing Technology in Computer Secure Storage

Fenglian Cao,[1] **Lihong Zhang**,[1] **Darshana A. Naik**,[2] **José Luis Arias Gonzáles**,[3] **Neha Verma**,[4] **Amit Jain**,[5] **Rituraj Jain**,[6] **and Ashutosh Sharma**[7]

[1]*Laiwu Vocational and Technical College, Jinan, Shandong 271100, China*
[2]*Ramaiah Institute of Technology, Bangalore, India*
[3]*Pontificia Universidad Católica del Peru, San Miguel, Peru*
[4]*Department of Information Technology, Vivekananda Institute of Professional Studies, GGSIPU, Delhi, India*
[5]*Sir Padampat Singhania University, Udaipur, Rajasthan, India*
[6]*Department of Electrical and Computer Engineering, Wollega University, Nekemte, Ethiopia*
[7]*Department of Informatics, University of Petroleum and Energy Studies, Dehradun, India*

Correspondence should be addressed to Fenglian Cao; caofenglian7@163.com and Rituraj Jain; jainrituraj@wollegauniversity.edu.et

Received 17 July 2022; Revised 27 August 2022; Accepted 30 August 2022; Published 16 September 2022

Academic Editor: Punit Gupta

To investigate the use of cloud computing technologies in safe computer storage, firstly, it is proposed to complete the central control function by building a cloud computing data center, collect multiple platforms and network safety technologies, and then connect computers in unlike sites to confirm computer information security. Then, based on the implementation advantages of cloud computing technique in computer network safe storage, specific applications are analyzed. Finally, a cloud computing secure modeling and analysis idea based on multiqueue and multiserver is proposed. The proposed cloud security approach ensures that both data and applications are easily accessible to authorized users. One always has a consistent way to access your cloud data and applications, allowing you to address any potential security issues as soon as they arise. It has greatly improved computer security storage convenience while also greatly improving computer network storage security. After verification, with the cloud computing technology platform to carry out relevant businesses at any time, the operation effectiveness has been meaningfully enhanced by 80%. At the same time, it promotes the construction of information sharing and gives full performance to the benefits of hardware, accelerates the process of resource integration, and provides information support for the formulation of enterprise strategic plans. Combined with the actual situation, the current study discusses the development and application direction of cloud computing, so as to add new impetus to the economic growth of enterprises.

1. Introduction

In the context of big data, the factors affecting data security are gradually increasing, so security protection is particularly important. Among many security protection methods, cloud computing technology has become the first choice of many users. Currently, information storage mainly includes computer hard disk storage and mobile device storage [1]. Data encryption, hashing, tokenization, and access control are all data security solutions that protect data across all platforms and apps. Encryption is the process of masking or hiding data by changing the format so that it can no longer be interpreted or understood unless decrypted. As a result, the data remain but are scrambled or hidden. Tokenization is a process in which you try not to own the data, similar to how credit card merchants store the information instead of encrypting it and giving it a key; imagine it as a safe deposit box. Hashing is a mathematical equation or algorithm that is used to process information. Organizations all over the world are investing heavily in information technology (IT) cyber security skills to protect their critical assets [2, 3].

Whether such a company has to protect its brand, intellectual capital, and customer information or it needs continue providing controls for critical infrastructure, incident identification, and resolution include three basic components: people, processes, and technology [4, 5]. Both methods are read on a fixed disk. Although the mobile device can replicate on various hardware devices, it is very easy to cause data loss or virus infection. Cloud computing is a sort of asset hypervisors that is relatively new (Figure 1). It maximizes the use of physical assets by dynamically expanding services. It fully combines a variety of new technologies to achieve distributed processing of big data, improves processing efficiency, and is applied in many fields. It has the characteristics of low cost, wide range, and various functions. Integrating hot backup redundancy, network storage, and other technologies, it is divided into multiple services on the existing physical resources and then provided to multiple users [6]. Cloud data security is implemented when technology solutions, policies, and procedures are put in place to protect cloud-based systems, implementations, and the data and user access that go with them. One area of data security that entities struggle within cloud technology is who is responsible for security. Your company is in charge of the infrastructure and on-premises data centres. However, because you are utilising a vendor's cloud services, the distinction among both roles may appear hazy. Business cloud backup works through copying and storing your server's files on another server in a different specific address. A company can back up some or all server files, depending on its needs. Cloud security, also known as cloud computing environments, is a set of rules, controls, processes, and tools that help to ensure the safety of cloud-based systems, data, and infrastructure [7, 8]. These security measures are in place to protect cloud data, aid compliance with regulatory requirements, protect customers, privacy, and provide authentication mechanisms for specific users and devices. From login to traffic filtering, cloud security may be tailored to fit the specific needs of the organization [9, 10]. There is no longer a need to invest in hardware, software, on-site data center infrastructure, including server racks, round-the-clock power generation for power and cooling, and IT professionals to oversee the infrastructure, with cloud computing. One of the benefits of cloud computing services is the flexibility of elastic scaling. In cloud-speak, this means providing an adequate number of IT resources. Cloud computing makes data storage easy and affordable. It is because data can be mirrored at backup system sites on the cloud provider's network. Moreover, big data security is critical for all safeguards and tools used to protect analytics and data processes from intrusions, theft, and other fraudulent behavior that could be harmful or negatively impact them. Like other types of cyber-security, the big data variant is concerned with attacks that originate from either the online or the offline spheres. Cloud computing technology uses virtual methods to store data. Users upload data to cloud storage space, and they can view and download data at any location and time as long as they log in to their account. A collection of innovative technologies for distributed big data processing that enhances process efficiency and is used in a range of sectors. The mobile device may be replicated on a variety of hardware. To store data, cloud computing technology employs virtual ways. Virtualization, which introduces a new real correlation between hardware and software, is one of the main components of cloud computing technology that enables full utilization of cloud computing capabilities. Furthermore, virtualization is now a standard feature of enterprise IT architectural history and a critical factor in cloud computing economics. However, in the real network environment, network security issues have always been difficult to eliminate, so it is essential to reinforce the secure storing of computer network data under cloud computing technology [11]. A network can be large and complex at times, and it is likely to rely on a large number of linked endpoints. While this is advantageous to your company's operations and makes your workflow more controllable, it also creates a security concern [12, 13]. The issue is that, without the free movement of people within your network, if a hostile actor gains access, they may roam around and cause havoc, often without your knowledge. These network security issues put your company at danger of data leak [14, 15]. The platform for secure storage is shown in Figure 1. When a computer's software and hardware fail, the cloud computing system's restoration technology will safely retrieve the computer's vital files.

2. Literature Review

Liu et al. believe that the biggest hidden danger of computer information storage security is hacker intrusion and virus intrusion. The reasons leading to the above security risks include the following: data are not properly encrypted, key management is lax, and identity authentication technology [16]. In order to strengthen the security of computer data storage, Sun and He propose cloud computing technology to focus on solving the above problems. [17]. Manel et al. believe that users can use the network to use distributed computing, load balancing, and other technologies to share and retrieve resources [18]. Rezvani et al. believe that there are two ways to store traditional computer data information. The first is to store the information in the computer directly in an external storage device, such as a tablet computer, a USB flash drive, and other external mobile devices [19]. Cardoso et al. believe that although these two storage methods are relatively simple and commonly used, this storage method has great disadvantages. First, it is not safe, and some private information and data are not easy to hide. Second, it is easy to lose user data if unexpected events such as the loss of USB flash disk or computer damage occur [20]. Therefore, Lv et al. allow users to save information and data in the cloud storage virtual space without any hardware equipment, and the security is particularly high. The most important thing is to realize information and data sharing, which takes prodigious expediency to the transmission and storage of data and information [21]. Figure 2 illustrates this Alibaba Cloud Computing. Cai et al. trust that, in the process of network safety storage, the identity authentication technology can accurately authenticate the user's identity through the corresponding data, which greatly improves the information security of network storage [22]. Xing et al. believe that cloud computing-based user identity authentication technology is a key technology [23]. Currently, Cai et al. have proposed three commonly used verification methods for their technology. The first is to enter the

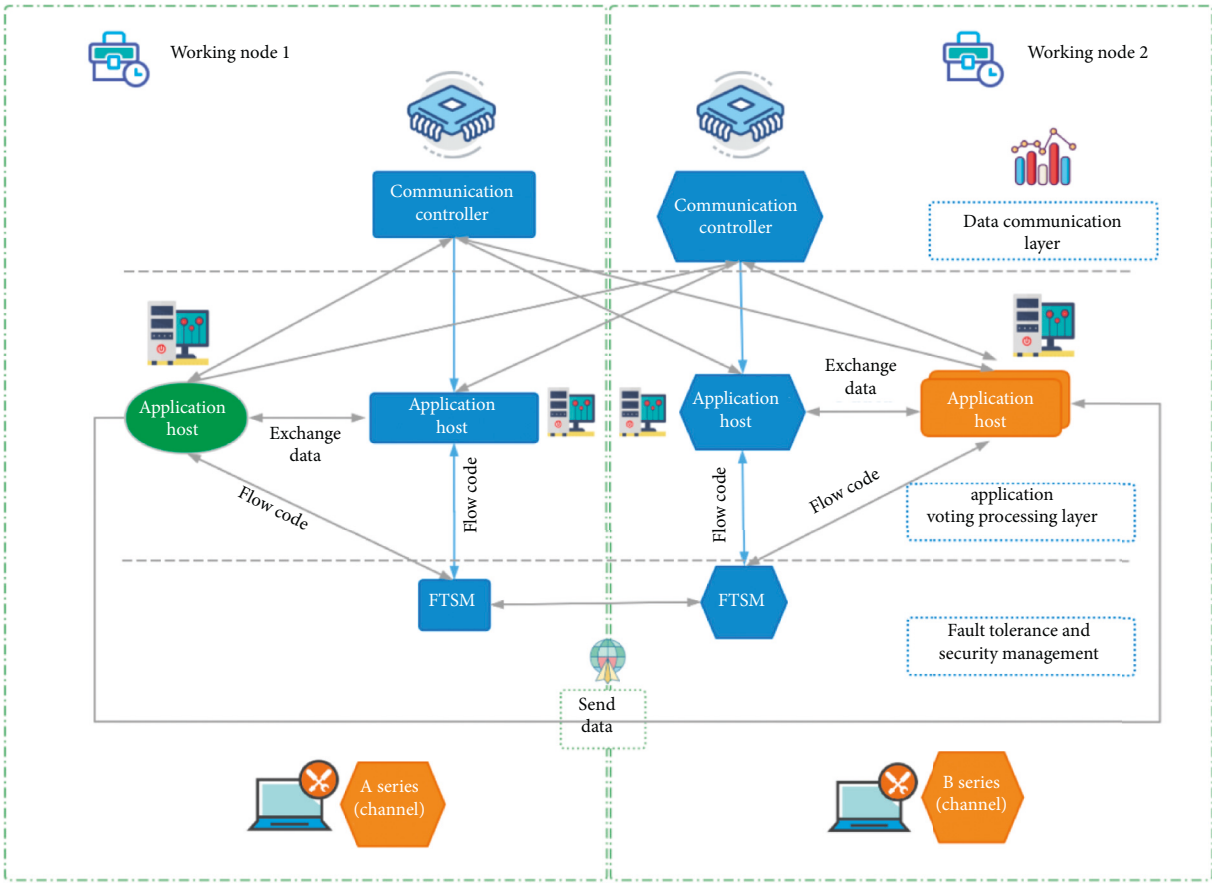

Figure 1: Secure computer platform based on cloud computing.

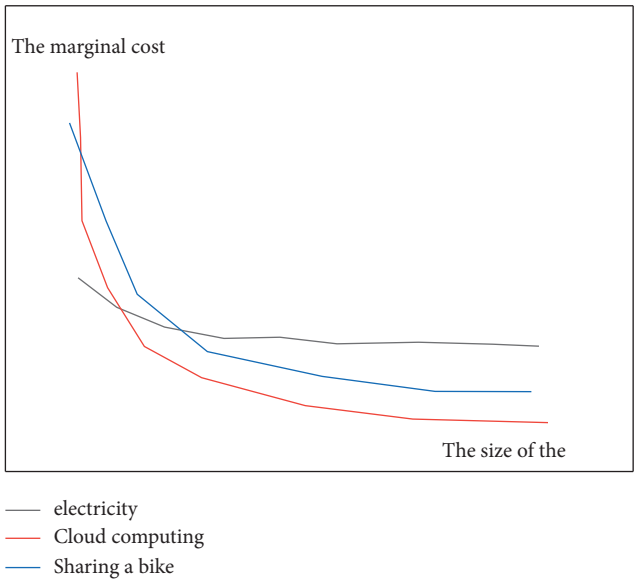

Figure 2: Alibaba leads cloud computing.

relevant password: this method requires the user to enter the accurate user name, and the corresponding password according to system prompts to complete user identification. The second is the smart IC card authentication method. Data are not adequately encrypted, key management is loose, and verification technologies and other factors all contribute to the aforesaid security threats. The first option is to save the data directly to an external storage device, such as a tablet computer or a USB flash drive, on the computer. Second, unforeseen circumstances such as the loss of a USB flash disc or computer damage make it possible to lose user data. The most crucial issue is to actualize data and information sharing, which requires tremendous speed in data transmission and storage. The user needs to prepare the IC card before verification and then complete the identity authentication, which has strong stability and security. The third is PKI identity authentication. This authentication method mainly uses the public key as a verification facility. The public key is encrypted and decrypted through the matching key. Then, under the system mechanism of key recovery, backup, and update, the secure storage of the network is ensured.

3. Cloud Computing Security

3.1. Cloud Computing Service Model. There are several security risks to consider when deciding whether one should switch to cloud computing. When organizations move large amounts of sensitive data to a cloud environment that is connected to the Internet, they expose themselves to more cyber threats. Malware attacks are a common threat to securely access security, and evidence suggests that, as cloud

usage increases, security breaches become more likely for nearly 90% of businesses. Data leakage is becoming a growing concern for businesses, with more than 60% citing it as their top cloud security concern. The advancement of technologies such as network connectivity, dispersed computing, and application computing gives strong assistance for cloud computing deployment. People will have access to virtual servers rapidly and with minimum maintenance and interface expenses [24]. On-demand self-service, broad network access, efficient resource sharing, high elastic computing, and measurement payment support are all five functional aspects of cloud computing. The organization intends of cloud technology may be separated into Software as a Service (SaaS), Platform as a Service (PaaS), and infrastructure as a service (IaaS) depending on the various kinds of providers supplied by cloud computing (IaaS). As part of the software as a service (SaaS) distribution model, a cloud provider hosts applications and makes them available to users online. In this model, an independent software vendor (ISV) may contract with a third-party cloud provider to host the application. The server canister renting service supplied by Microsoft and IBM might be considered a new industry model [25], and it is known as a hardware as a solution (HaaS). Figure 3 illustrates this. Higher-level cloud vendors can easily develop customer services on their own, or they can acquire information services from lower-level cloud services [26].

In fact, with the continuous upward movement of the service mode level, the service functions and conditions to be met show an increasing enclosure association.

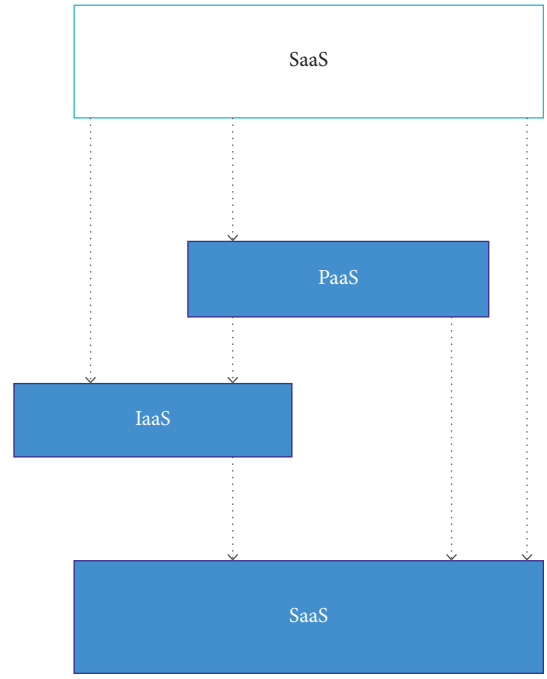

Figure 3: Cloud computing service delivery mode.

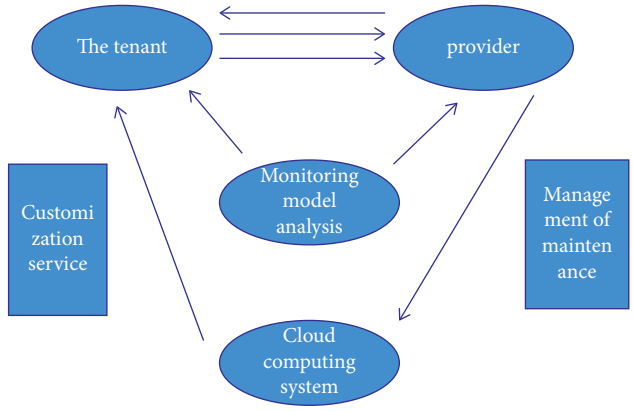

Figure 4: Cloud computing security service framework.

3.2. Cloud Computing Service Framework. This section will describe a cloud computing security service architecture based on model analysis, in light of the security problems that cloud computing presents. Cloud computing systems [27] are operated by providers, who then distribute the resulting products they supply over the Internet. As shown in Figure 4, users access and utilise the cloud computing system according to the authority granted by the service supplier. Several cloud computing providers, such as Salesforce, now offer monitoring and presentation modules that may show users the system's operational activity in real time. To enable cloud computing really a fluid, visible, and controlled system, we think a model analysis module must be included to the integrated service [28].

3.3. Application Technology of Cloud Computing in Computer Network Secure Storage

3.3.1. Data Backup Technology. As part of a cloud backup service, data and applications on the Internet which allows are backed up and stored on a remote server. Businesses choose to back up to the cloud to keep files and data accessible in the situation of a system failure, outage, or natural disaster. Business cloud storage works by copying and storing your server's files on another server in a various physical location. A company can back up some or all server files, depending on its needs. The computer system is composed of software and hardware. Once hardware is damaged, the loss to the computer is irreversible, causing the data to be unreadable or unrecoverable. The cloud computing technology has backup and security audit technology. Among them, backup technology refers to backing up computer hardware data [29]. When software and hardware of the computer fail, the recovery equipment in the cloud computing system will safely recover the important files of the computer system. When the system information is leaked, the host cluster will automatically transfer the main files in the computer to the recovery system and help the host process the data information.

3.3.2. Encrypted Storage Data. Encrypted storage of data denotes the usage of encryption technology to provide

protection for the security of network data. Through encryption technology, the encryption level of the files in the computer can be improved [30]. A person or entity attempting to gain unauthorised access to encrypted data sees it as scrambled or unintelligible ciphertext, also known as encrypted data. Data encryption is used to prevent malicious or careless individuals from accessing sensitive data. Because it makes it difficult in using intercepted data, encryption is a critical component of a cyber security architecture. The core files need to be checked for identity and can only be accessed by authorized users. This greatly improves the security of computer file storage. Commonly used encryption technologies include passwords technology and encryption algorithm.

3.3.3. Identity Authentication Technology. Identity authentication technology is a fairly basic security technology in network security protection, and it has a certain protective effect on the security of cloud computing technology operation [31].

3.3.4. System Vulnerability Protection. System vulnerability protection is another key application of cloud computing technology in computer network storage security. At present, many network attacks take advantage of system vulnerabilities, so system vulnerabilities must be well protected.

Cloud computing includes backup and security auditing capabilities. When a computer's software and hardware fail, the cloud computing system's restoration technology will safely retrieve the computer's vital files. The encryption level of computer files can be enhanced using encryption technologies. Password technology, encryption algorithms, and other encryption technologies are commonly employed.

4. Model Evaluation of Cloud Computing Security

The essential technique for achieving manageable, controlled, and quantifiable cloud computing security is the cloud computing security model. This section discusses the cloud computing security indicator system, the formal description of indicators, security models, and analysis methods and proposes a cloud computing security modeling method based on the multiqueue multiserver model [32, 33].

4.1. Measurable Index System. Research on cloud computing security should not be based solely on outdated security. The service system is necessary to deliberate all features of service excellence. Facts have shown that including security in credibility for research is helpful not only to clarify the relationship between security and other attributes of the system but also to formulate a more balanced security strategy [34]. Therefore, the following will first introduce the system's measurable index system from the perspective of credibility and then further discuss the new features of security in the cloud computing environment and the relationship with other credible attributes. The above attribute relationship diagram is shown in Figure 5.

The security of the system is an important part of credibility, and there is an antagonistic and unified relationship with other attributes of credibility. This phenomenon is more prominent in the cloud computing atmosphere [35, 36]. Because the traditional system is relatively closed and independent, the owner of the system is the user of the system, and the security signs that the system provider and system user care about are basically the same. Facts demonstrate that adding security in research credentials not only helps to understand the link between security and other system features but also helps to design a better balanced security plan. The system's security is a crucial aspect of reliability, and it has an oppositional and unified connection with other authenticity traits. For example, increased scalability might constitute a major security risk. Although isolation improves security, it also affects system efficiency.

4.2. Formal Description Method of Security Indicators. Currently, the cloud computing system includes real-time monitoring services, allowing system utility workers to get real-time information on the system's state. To make it easier for system maintenance staff to improve the system security strategy, the formal definition of suitable security indicators must meet the measurement requirements of average and real-time values, as well as cover diverse perspectives, granularities, and numerous dimensions.

Taking availability as an example, availability is defined as the ratio of time that the system can run safely within a specific time. It is a quantitative description of the process of system security state change [37], which clearly describes the possibility that the system can still operate safely in the case of its own defects or external attacks. Assuming that SA is the collection of the system's security state, the system's transient availability, that is, the possibility that the structure is in a security state instantaneously is

$$A_I(t) = P\{X(t) \in S_A\}. \tag{1}$$

The steady-state accessibility of the system, that is, the chance that the system is in a secure condition in a steady position, is much more significant for the system:

$$A_S = \lim_{t \longrightarrow \infty} \frac{\int_0^t A_I(u)\mathrm{d}u}{t}. \tag{2}$$

It may also be calculated by calculating the state's steady-state probability vector in the state diagram, whereπ_i is the system's steady-state possibility of being from the time and steady-state accessibility is represented as follows:

$$A_S = \sum_{t \in S_A} \pi_i. \tag{3}$$

For the formal description of other security -related indicators, they are summarized in Table 1.

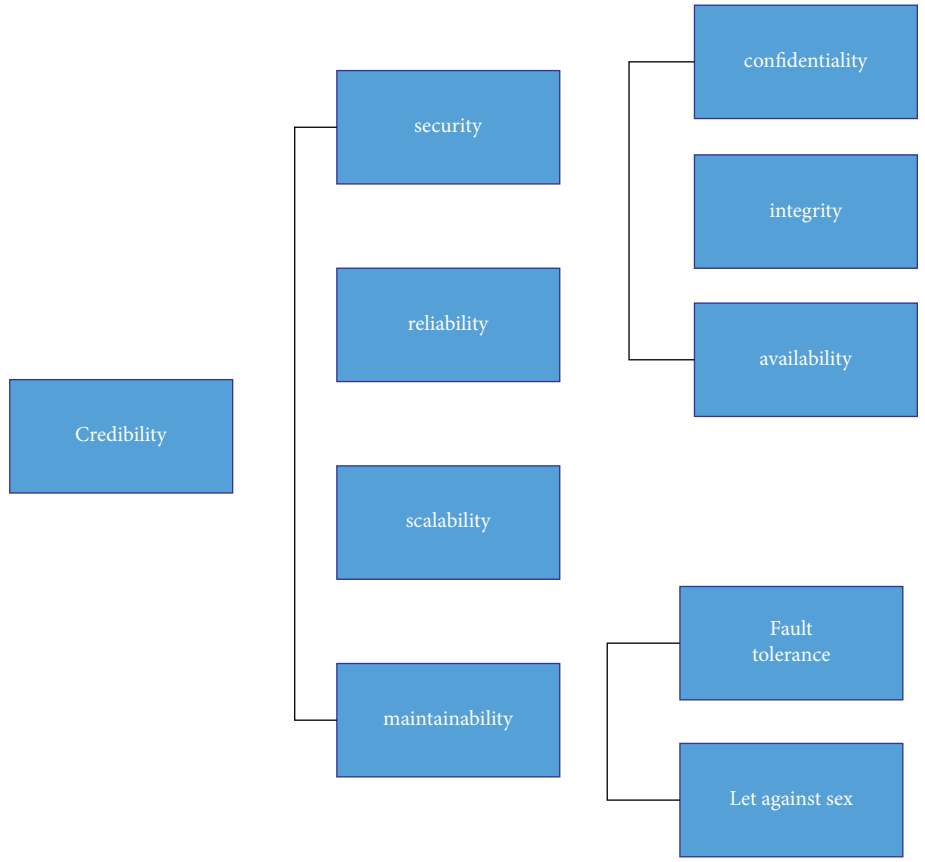

Figure 5: Schematic diagram of the relationship between the credible index systems.

Table 1: Formal description of system perspective indicators.

Mechanism	Classification	Scope of application		
		The identity authentication	Data and information	Application platform
Test	Web-based testing	√	√	√
Certification	Application center certification		√	√
Isolation	Network isolation	√	√	√
Monitoring	Software to monitor	√		
Restore	The overall recovery	√	√	√

4.3. Security Model and Analysis. The scale of cloud computing systems is growing rapidly. Due to the influence of factors such as analysis efficiency and analysis costs, the method of system security analysis through deployment and testing is increasingly unable to encounter the requirements of current cloud computing growth. At the same time, analysis methods based on mathematical models have gained more and more attention and become an important method for analyzing system characteristics. Many effective analysis models have also appeared. After nearly 40 years of development analysis models are divided into qualitative analysis models and quantitative analysis models according to the different analysis results. While the development of quantifiable analysis models is relatively sheath because of its fundamental position in strategy selection and SLA formulation, research in this area has become a hot spot in the field of model analysis. The reliability block diagram method, fault tree analysis method, model detection analysis method, attack tree analysis method, and graph-based analysis techniques, among others, are widely accepted cumulative model types of analysis. The approach of system security assessment via implementation and testing is progressively able to fully meet the needs of contemporary cloud computing expansion due to the effect of variables such as analysis effectiveness and analysis expenses. Because of its critical role in strategy selection, the creation of quantified analytical models is relatively crucial. Model detector, for example, can automatically create attack tree branches and attack graphs. Figure 6 shows a simple attack tree architecture. The entire framework of the data security is

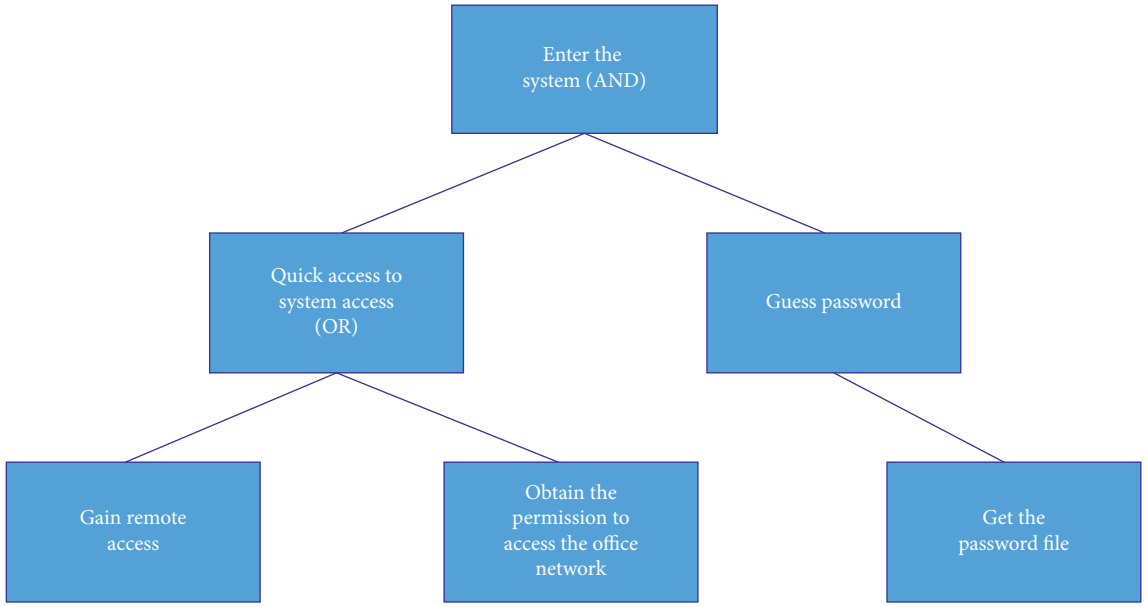

Figure 6: Simple attack tree model of unix system.

demonstrated in Figure 6. It is a set of various steps. Through the model, computer secure storage is achieved and thus allows full performance to the benefits of hardware.

5. Discussion

Cloud computing technology has surpassed other security protection strategies in the eyes of many users. Currently, mobile device storage and computer hard disc storage make up the majority of information storage. Data security solutions that safeguard data across all platforms and apps include data encryption, hashing, tokenization, and access control. Implementing technology solutions, policies, and procedures to safeguard cloud-based systems, implementations, and the data and user access, they contain constitutes cloud data security. The suggested approach to cloud security makes sure that authorised users can easily access both data and applications. Your cloud data and applications will always be accessible in the same way, giving you the flexibility to address any potential security issues as soon as they appear. Both the ease of computer security storage and the security of computer network storage have significantly improved. After verification, the operation effectiveness has been significantly increased by 80% when using the cloud computing technology platform to conduct pertinent business at any time. At the same time, it encourages the development of information sharing and fully utilises the advantages of hardware.

6. Conclusion

Computer technology has become an indispensable aspect of people's life in the information era, work, and social development. However, computer and network not only bring convenience and quickness to people but also bring some risks to information security. Once the security of computer network storage cannot be effectively guaranteed, and problems such as information loss and leakage will not only affect the security of users' personal information but also have negative social impacts. Cloud computing technology has brought great convenience to network security storage, which greatly guarantees the security of computer network storage. To increase network drive security in the new phase, it is vital to constantly upgrade and investigate the development and use of cloud computing technology in network security storage. Overall, cloud computing offers a significant application benefit in network security storage, ensuring the security, consistency, and dependability of computer network storage. In the future, regarding the application of cloud computing technology, the integration with other technologies should also be strengthened to provide a full range of security protection for the secure storage of computer networks and eliminate hidden dangers of information and data storage as much as possible.

Data Availability

The data can be obtained from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] W. Li, B. Jiang, and W. Zhao, "Obstetric imaging diagnostic platform based on cloud computing technology under the background of smart medical big data and deep learning," *IEEE Access*, vol. 8, pp. 78265–78278, 2020.

[2] T. Limbasiya, M. Soni, and S. K. Mishra, "Advanced formal authentication protocol using smart cards for network

applicants," *Computers & Electrical Engineering*, vol. 66, pp. 50–63, 2018.

[3] S. S. Priscila, A. Sharma, S. Vanithamani et al., "Risk-based access control mechanism for internet of vehicles using artificial intelligence," *Security and Communication Networks*, vol. 2022, Article ID 3379843, 13 pages, 2022.

[4] V. Jagota, M. Luthra, J. Bhola, A. Sharma, and M. Shabaz, "A secure energy-aware game theory (SEGaT) mechanism for coordination in WSANs," *International Journal of Swarm Intelligence Research*, vol. 13, no. 2, pp. 1–16, 2022.

[5] P. K. Sarangi and B. K. Nayak, "Stock market behavior prediction using pattern matching approach," *International Journal of Engineering and Computer Science (IJECS)*, vol. 3, pp. 2319–7242, 2014.

[6] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application," *IEEE Access*, vol. 8, pp. 101079–101092, 2020.

[7] R. Nair, S. Gupta, M. Soni, P. Kumar Shukla, and G. Dhiman, "An approach to minimize the energy consumption during blockchain transaction," *Materials Today Proceedings*, 2020.

[8] J. Bhola and S. Soni, "Information theory-based defense mechanism against DDOS attacks for WSAN," in *Advances in VLSI, Communication, and Signal Processing*, pp. 667–678, Springer, Singapore, 2021.

[9] S. Sanober, I. Alam, S. Pande et al., "An enhanced secure deep learning algorithm for fraud detection in wireless communication," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–14, 2021.

[10] D. Y. Jiang, H. Zhang, H. Kumar et al., "Automatic control model of power information system Access based on artificial intelligence technology," *Mathematical Problems in Engineering*, vol. 2022, Article ID 5677634, 6 pages, 2022.

[11] Z. Ning, F. Xia, X. Kong, and Z. Chen, "Social-oriented resource management in cloud-based mobile networks," *IEEE Cloud Computing*, vol. 3, no. 4, pp. 24–31, 2016.

[12] G. S. Sriram, "Security challenges of big data computing," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 1, pp. 1164–1171, 2022.

[13] S. Kaur, G. Kaur, and M. Shabaz, "A secure two-factor Authentication framework in cloud computing," *Security and Communication Networks*, vol. 2022, Article ID 7540891, 9 pages, 2022.

[14] B. Prasanalakshmi, K. Murugan, K. Srinivasan, S. Shridevi, S. Shamsudheen, and Y.-C. Hu, "Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography," *The Journal of Supercomputing*, vol. 78, no. 1, pp. 361–378, 2022.

[15] G. S. Sriram, "Green cloud computing: an approach towards sustainability," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 1, pp. 1263–1268, 2022.

[16] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing," *Future Generation Computer Systems*, vol. 78, no. 3, pp. 1020–1026, 2018.

[17] H. Sun, R. He, Y. Zhang, R. Wang, W. H. Ip, and K. L. Yung, "Etpm: a trusted cloud platform enclave tpm scheme based on intel sgx technology," *Sensors*, vol. 18, no. 11, p. 3807, 2018.

[18] M. Oussalah, A. Amirat, M. R. Laouar, and M. Gherari, "Mcsim: a mobile cloud simulation toolkit based on cloudsim," *International Journal of Computer Applications in Technology*, vol. 57, no. 1, p. 72, 2018.

[19] M. Rezvani, M. K. Akbari, and B. Javadi, "Resource allocation in cloud computing environments based on integer linear programming," *The Computer Journal*, vol. 58, no. 2, pp. 300–314, 2015.

[20] A. Cardoso, F. Moreira, and D. F. Escudero, "Information technology infrastructure library and the migration to cloud computing," *Universal Access in the Information Society*, vol. 17, no. 3, pp. 503–515, 2017.

[21] Z. Lv, Z. Tan, Q. Wang, and Y. Yang, "Cloud computing management platform of human resource based on mobile communication technology," *Wireless Personal Communications*, vol. 102, no. 2, pp. 1293–1306, 2018.

[22] M. Y. K. Chua, F. R. Yu, and S. Bu, "Dynamic operations of cloud radio access networks (c-ran) for mobile cloud computing systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1536–1548, 2016.

[23] L. Xing, L. Yun, and H. H. Chen, "Wireless resource scheduling based on backoff for multi-user multi-service mobile cloud computing," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 11, p. 1, 2016.

[24] L. Cai, Y. Tian, Z. Liu, Q. Cheng, J. Xu, and Y. Ning, "Application of cloud computing to simulation of a heavy-duty machine tool," *International Journal of Advanced Manufacturing Technology*, vol. 84, no. 1-4, pp. 291–303, 2016.

[25] S. Jeong, O. Simeone, and J. Kang, "Mobile edge computing via a uav-mounted cloudlet: optimization of bit allocation and path planning," *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 2049–2063, 2018.

[26] S. Baek, "System integration for predictive process adjustment and cloud computing-based real-time condition monitoring of vibration sensor signals in automated storage and retrieval systems," *International Journal of Advanced Manufacturing Technology*, vol. 113, no. 3-4, pp. 955–966, 2021.

[27] A. Almogren, "An automated and intelligent Parkinson disease monitoring system using wearable computing and cloud technology," *Cluster Computing*, vol. 22, no. S1, pp. 2309–2316, 2019.

[28] S. Wu, M. Wang, and Y. Zou, "Bidirectional cognitive computing method supported by cloud technology," *Cognitive Systems Research*, vol. 52, pp. 615–621, 2018.

[29] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Distributed resource allocation and computation offloading in fog and cloud networks with non-orthogonal multiple access," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12137–12151, 2018.

[30] X. Yang, X. Huang, and J. K. Liu, "Efficient handover authentication with user anonymity and untraceability for mobile cloud computing," *Future Generation Computer Systems*, vol. 62, pp. 190–195, 2016.

[31] X. Li, J. Song, and B. Huang, "A scientific workflow management system architecture and its scheduling based on cloud service platform for manufacturing big data analytics," *International Journal of Advanced Manufacturing Technology*, vol. 84, no. 1-4, pp. 119–131, 2016.

[32] D. S. Linthicum, "Connecting fog and cloud computing," *IEEE Cloud Computing*, vol. 4, no. 2, pp. 18–20, 2017.

[33] X. Wen and X. Zhou, "Servitization of manufacturing industries based on cloud-based business model and the down-to-earth implementary path," *International Journal of Advanced Manufacturing Technology*, vol. 87, no. 5-8, pp. 1491–1508, 2016.

[34] N. Ghosh, D. Chatterjee, S. K. Ghosh, and S. K. Das, "Securing loosely-coupled collaboration in cloud environment through dynamic detection and removal of access conflicts," *IEEE Transactions on Cloud Computing*, vol. 4, no. 3, pp. 349–362, 2016.

[35] S. Namasudra and P. Roy, "Time saving protocol for data accessing in cloud computing," *IET Communications*, vol. 11, no. 10, pp. 1558–1565, 2017.

[36] J. Zhang, L. Zhang, H. Huang, Z. L. Jiang, and X. Wang, "Key based data analytics across data centers considering bi-level resource provision in cloud computing," *Future Generation Computer Systems*, vol. 62, pp. 40–50, 2016.

[37] C. Li, J. Bai, and Y. Luo, "Efficient resource scaling based on load fluctuation in edge-cloud computing environment," *The Journal of Supercomputing*, vol. 76, no. 9, pp. 6994–7025, 2020.