Proceedings of the 6th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/64/20241372

The intelligent prediction and assessment of financial information risk in the cloud computing model

Yufu Wang[1,*,†], Mingwei Zhu[2,†], Jiaqiang Yuan[3], Guanghui Wang[4], Hong Zhou[5]

[1]Computer Science & Engineering, Santa Clara University, Santa Clara, CA, USA
[2]Computer Information System, Colorado state university, Fort Collins, CO, USA
[3]Information Studies, Trine University, phoenix, AZ
[4]Computer Science, Independent Contributor, Shanghai, CN
[5]Computer Technology, Peking University, Beijing, CN

*Corresponding author: stephenwyf1@gmail.com
[†]Yufu Wang and Mingwei Zhu contributed equally to this work and should be considered as co-first authors.

Abstract. cloud computing (cloud computing) is a kind of distributed computing, referring to the network "cloud" will be a huge data calculation and processing program into countless small programs, and then, through the system composed of multiple servers to process and analyze these small programs to get the results and return to the user. This report explores the intersection of cloud computing and financial information processing, identifying risks and challenges faced by financial institutions in adopting cloud technology. It discusses the need for intelligent solutions to enhance data processing efficiency and accuracy while addressing security and privacy concerns. Drawing on regulatory frameworks, the report proposes policy recommendations to mitigate concentration risks associated with cloud computing in the financial industry. By combining intelligent forecasting and evaluation technologies with cloud computing models, the study aims to provide effective solutions for financial data processing and management, facilitating the industry's transition towards digital transformation.

Keywords: Cloud Computing, Financial Information Processing, Intelligent Technologies, Data Security, Regulatory Frameworks.

1. Introduction

Applying the cloud computing model to financial information processing has become a major trend in today's financial industry. Cloud services have become an important part of the global financial industry's information technology toolbox. Against the background of the application of cloud technology in the financial industry, this report highlights the potential risks of financial institutions' use of third-party technology service providers, draws on the regulatory frameworks of different jurisdictions, and proposes policy recommendations to enhance information gathering and sharing, strengthen cross-border coordination and solutions, and ensure that regulatory tools are fit for purpose. To mitigate the potential concentration risks posed by cloud computing applications in the financial industry. Traditional data processing methods have found it difficult to meet the growing data needs and processing requirements of the financial industry. Especially in the aspect of financial data entry and

DOI: 10.54254/2755-2721/64/20241372

analysis, the traditional OCR[1] model has many limitations, which cannot meet the requirements of high efficiency and high accuracy of data processing by financial institutions. In addition, data security, privacy and other issues in the cloud computing environment also bring new challenges to financial information processing. This study aims to solve the risks and challenges of financial information in the cloud computing environment by using intelligent forecasting and evaluation technology combined with the cloud computing model. Through such research, more effective data processing and management solutions can be provided to the financial industry, and the entire industry can be promoted towards intelligent and digital transformation.

2. Related work

2.1. Cloud computing model

Cloud computing is a model that makes it easy to access a common set of configurable computing resources (such as networks, servers, storage devices, applications, and services) over a network. There are four main types of cloud computing: private cloud, public cloud, hybrid cloud and multi-cloud. Tthere are three main cloud computing service models: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), these three are the current mainstream cloud computing service models, the future, with the development of technology, cloud computing will develop into the fourth model: S2S (service to service). This is the International Institute of Electrical and Electronics Engineers [2](IEEE Fellew), the American Computer Society outstanding scientist Mr Zhang Liangjie put forward. For cloud computing, there are three main services provided: Infrastructure-as-a-service (IaaS), which provides hardware resources similar to the traditional model of CPU, storage, and I/O; Platform as a Service (PaaS), which provides an environment for software to run, similar to the operating system and programming framework under the traditional programming model; Software as a Service (SaaS) provides application software functionality, similar to the traditional model of application software. In the cloud computing model, users no longer buy or buy some hardware, system software or application software to become the owner of these resources, but purchase the use time of resources, and consume according to the billing model of the use time. It can be seen that cloud computing takes all resources as services and consumes them in a pay-as-you-go manner, which is the characteristic of the host era. [3]In the host era, all users are charged based on the CPU time and storage capacity consumed when they connect to the host through the display terminal and network cable. The difference is that in host mode, the computation takes place on a single host; In cloud computing, computing takes place in a cluster of servers or in a data center.

2.2. The application of cloud computing in the financial field

1. Banking. Cloud computing is mainly used in IT operations management and open underlying platforms. The application of cloud computing technology to build an open cloud platform can build a comprehensive financial service ecosystem with the help of API, providing "financial + non-financial" services such as life payment, information inquiry, online shopping, and the combination of financial services and life scenarios enhances the value of financial accounts.

2. Securities fund field. Cloud computing is mainly used in client market query and peak trading volume allocation. Through the business system as a whole in the cloud, under the deployment mode of database sub-database and sub-table, the parallel computing equivalent to thousands of clearing systems and real-time trading systems can be realized[6].

3. Insurance. Cloud computing is mainly used in personalized pricing and product online sales. Customized cloud software can quickly analyze real-time customer data, provide personalized pricing, and provide specialized insurance services to targeted customers through social media.

2.3. Features of cloud computing environment

1) High degree of resource integration. Compared with the local computing environment, the resource utilization level obtained by a single user in the cloud computing platform may not be superior due to

DOI: 10.54254/2755-2721/64/20241372

the network speed and other reasons, but the utilization rate of some idle resources has been greatly improved, thus maximizing the utilization rate of limited overall resources and greatly improving the resource utilization rate of the whole society. 2) Strong impact resistance. [6]The cloud platform adopts the distributed data storage mode, which not only provides the basis for data recovery, but also makes various network attacks become confused, and plays an important role in improving the security and anti-impact capability of the system. 3) High scalability. The cloud platform adopts a modular design. At present, the mainstream cloud computing platform integrates hardware and software devices and middleware software with different functions at each layer according to SP architecture. A large number of middleware software and devices provide a common interface to the platform, allowing users to add extended devices for this layer. 4) Low use cost. Due to the adoption of distributed data storage, cloud computing mode greatly saves hardware equipment acquisition costs, so that users can use the remaining idle funds to order according to their own planning and needs, and improve the utilization rate of funds.

3. Methodology

3.1. Experimental background

By analyzing the online migration of financial business and the extensive penetration of Internet business model, this paper finds that business transaction scale and business peak per second show geometric growth. In this context, cloud native is gradually recognized and favored by business teams as an important tool for enterprise cloud. However, with the increasing prominence of financial information security risks, financial institutions urgently need to combine cloud-native technology with security measures to ensure the safety and reliability of financial information. Cloud native not only can achieve cost reduction and efficiency, improve system resource utilization, but also has many advantages such as simple use, high availability, and strong expansion. It also has intelligent load, elastic scaling, log monitoring, [7]DevOps and other functions, can achieve multi-application on-demand selection and intelligent release, so as to cope with sudden business traffic, quickly achieve expansion and contraction capacity, greatly improve development efficiency, reduce operation and maintenance costs. However, with the continuous evolution of financial information security threats, financial institutions must strengthen the security control of cloud-native environments, including data encryption, access control, identity authentication and other security measures to ensure that financial data is not leaked or tampered with. In this process, financial institutions need to pay attention to information security governance, establish a sound security management system, including the formulation of security policies, strengthening security training, implementation of security audits and other measures to ensure that financial information in the cloud native environment is safe and controllable[8].

3.2. Introduction to cloud native storage

In the container cloud environment, the demand for intelligent prediction of financial information security is also very important. Because financial institutions can utilize a variety of storage methods to protect important financial data. For example, through the internal storage methods such as EmptyDir, HostPath[9], and Local PV, financial institutions can store and share temporary data. At the same time, combined with external CSI, NAS, and SAN storage methods, they can achieve secure storage and management of persistent data. On this basis, financial institutions can use intelligent prediction technology to make more accurate and effective prediction and evaluation of financial information security. By continuously optimizing and improving intelligent prediction models, financial institutions can improve their ability to identify and respond to security threats and ensure the security and stability of financial information. Therefore, the combination of storage in the container cloud environment and intelligent prediction technology can provide financial institutions with a more comprehensive and effective information security solution.

DOI: 10.54254/2755-2721/64/20241372

3.3. Container cloud nonpersistent storage requirements

In the cloud native container cloud environment, the demand for intelligent prediction of financial information security is also critical. In this environment, there are usually some non-persistent storage of sensitive services, these services need to use the container application's image warehouse, running container instances, and generated logs and other data. Scenarios for storage needs of financial institutions in the container cloud include, but are not limited to:

Table 1. Cloud-Native Persistent Storage Requirements

Requirement	Description
Persistent Demand	Essential for production system business logs and foundational for business analysis, requires permanent storage.
Pod Drift	After Pod migration, state data migration is achieved by mounting the same storage on another node.
Shared Storage	Distributed sharing requirements for business files, images, and other data.
Scalability	Flexible scalability requirements for storage, as well as flexible expansion and migration capabilities for container nodes.
Performance	Directly related to the concurrency support capability of business systems, especially for application files such as images and documents.
Security & High Availability	Requires intranet storage to ensure dual-center architecture.

To meet the above storage requirements, financial institutions can select a proper non-persistent storage model based on specific service scenarios and performance requirements. Generally speaking, local storage and block storage can be used for scenarios with high IO and low latency. Local storage can be achieved by building hostpaths or using centralized block storage for higher IOPS and bandwidth. For local hard disks, you are advised to configure RAID to improve the reliability of the overall service system and reduce the impact of single point of failure.

Table 2. Technologies Distribution in Various Categories

Category	Technologies	Percentage
Database	Cassandra, MariaDB, MongoDB, MySQL, Neo4j, PostgreSQL, Redis, etcd	64.38%
Content Management	Drupal, CKAN, MediaWIKI, DNN, Joomla	10.96%
Continuous Integration	Jenkins, GitLab, Maven, Puppet	42.47%
Big Data	Hadoop, Hypertable, Mesos, Presto, Solr, Spark, Storm	12.33%
Analysis & Search	Grafana, ElasticSearch, Prometheus, Kibana, Logstash	10.96%
Web Services	NGINX, WordPress, Apache HTTP Server, Tomcat, httpd	45.21%
Infrastructure	RabbitMQ, Memcached, Kafka, ZooKeeper, Node.js, NATS, WildFly	9.59%
Development Tools	LAMP	16.44%
AI	MxNet, PyTorch, TensorFlow Notebook, TensorFlow ResNet	5.48%
Others		8.22%

In the cloud native container cloud environment, financial information security intelligent prediction needs to fully consider the selection and performance requirements of storage schemes to ensure the safe storage of financial data and the effective realization of intelligent prediction. [10]By properly configuring and optimizing the storage system, financial institutions can improve their ability to identify and respond to security threats, thus ensuring the security and stability of financial information.

3.4. Cloud native information storage

Cloud-native storage should be combined with tenant rights mechanisms. Because cloud native is an application-centered software development method, it provides practitioners with an efficient, scalable and replicable way to maximize the ability of the cloud and play the value of the cloud. Securities

DOI: 10.54254/2755-2721/64/20241372

companies also need to continuously improve their software research and development capabilities. We can build an [11]IT delivery model that is as agile and flexible as an Internet company, with rapid trial and error and rapid innovation.

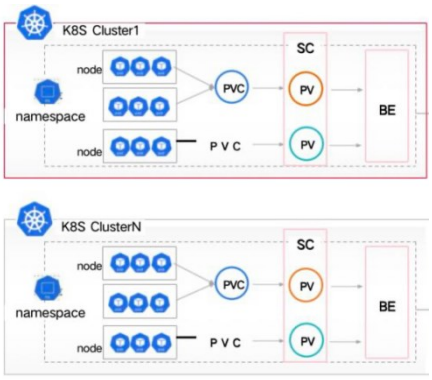

Figure 1. Cloud-native storage isolation

Microservices and containers in a cloud-native architecture can scale and scale independently to accommodate changes in traffic. In addition, the cloud native architecture also supports a variety of programming languages and frameworks, can flexibly choose their own technology stack, its high scalability and agility, shape the cloud native application cluster in the high availability, according to the characteristics of the business, if the business read and write request requirements are not high, can be adopted to achieve "by drift instead of cutting", POD drift instead of master/slave switching, single copy instead of multiple copies. And usability does not degrade; If services have high requirements on database read/write performance, connection number, and concurrency, you can use the primary/secondary cluster mode to implement read/write separation, personalized data initialization design, and strong data consistency.

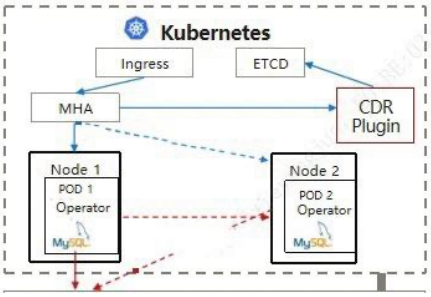

Figure 2. The cloud native database is highly available

In conclusion, the methodology outlined here presents a robust framework for addressing the evolving landscape of financial information security within cloud-native environments. By leveraging a combination of cloud-native storage solutions and intelligent prediction technologies, financial institutions can effectively mitigate security risks while optimizing data management and operational efficiency.

4. Conclusion

Cloud-native agile deployment and delivery, increased reliability and fault tolerance, increased scalability and flexibility, and increased security. This kind of future-proof architecture pattern can help enterprises build efficient, reliable, flexible and secure application ecosystems. From the perspective of application architecture, cloud native can easily support microservice architecture to realize application modernization and more flexible response to changes and elastic expansion. In terms of software

DOI: 10.54254/2755-2721/64/20241372

lifecycle management, cloud-native technology can help implement DevOps and other best practices into applicable standardized tools and frameworks, greatly improve development efficiency, accelerate iteration, help developers and enterprises more easily move to the cloud and cloud, and enable applications to dynamically migrate in their own data centers and clouds. By combining cloud computing with financial markets, we can enable more efficient and accurate processing of financial information and effectively address security and privacy challenges. First, the application of intelligent forecasting and evaluation technology will greatly improve the ability of financial institutions to process and manage data, so as to better grasp business opportunities and risks. Secondly, through the adoption of the cloud computing model, financial institutions can quickly obtain and release computing resources, which greatly improves the flexibility and response speed of the business. At the same time, the resource integration, strong anti-attack capability and high scalability in the cloud computing environment also provide strong support for the security protection of financial information. However, with the growing demand for financial information processing, we are also faced with challenges such as data security and privacy protection. Therefore, financial institutions need to strengthen the control and protection of data security in the cloud computing environment, and take a series of effective security measures to ensure the security and stability of financial information. Through continuous technological innovation and cooperation, the financial industry will be able to better cope with future challenges, achieve the goal of digital transformation, and inject new vitality and momentum into the development of the financial market.

References

[1] B. Rajkumar, Market-oriented Cloud Computing: Vision, Hype, and Reality of DeliveringComputing as the 5th Utility, Proc. Of the 9th lEEE/ACM International Symposium on ClusterComputing and the Grid, Washington, DC, May 2009, pp.75-80S.

[2] Amit, K. Saurabh, D. Jaideep and V. Vasudeva, Towards Analyzing Data Security Risks inCloud Computing Environments, Communications in Computer and Information Science, vol.54, pp.255-265, June 2010

[3] Top threats to cloud computing [R/OL]. Cloud Securit.Alliance,2016[2017-08 307.bttps://dloudsecurityallianoeorg/document/top threats-to-cloud-computing-2016/

[4] The notorious nine cloud computing top threats in 2013[R/OL]. Cloud Security Allianee,USA, 2013[2017-08 https://cloudsecurityalliance. org/download/the notoriousnine cloud computing-top threats in-2013/

[5] Cloud controls matrix v3.0.1R/0L]. Cloud Security Alliance,2013[2017-08-30]. https://cloud security alliance.org/download/cloud-controls-mnatrix-v3-0-1/NIST 800-144 Guidelines on Security and Privacy in PublicCloud Computing[S]. National Institute of Standards and Technology,2011.

[6] Che, C., Lin, Q., Zhao, X., Huang, J., & Yu, L. (2023, September). Enhancing Multimodal Understanding with CLIP-Based Image-to-Text Transformation. In Proceedings of the 2023 6th International Conference on Big Data Technologies (pp. 414-418).

[7] Xu, Z., Gong, Y., Zhou, Y., Bao, Q., & Qian, W. (2024). Enhancing Kubernetes Automated Scheduling with Deep Learning and Reinforcement Techniques for Large-Scale Cloud Computing Optimization. arXiv preprint arXiv:2403.07905.

[8] Gong, Y., Huang, J., Liu, B., Xu, J., Wu, B., & Zhang, Y. (2024). Dynamic Resource Allocation for Virtual Machine Migration Optimization using Machine Learning. arXiv preprint arXiv:2403.13619.

[9] Zhang, Y., Liu, B., Gong, Y., Huang, J., Xu, J., & Wan, W. (2024). Application of Machine Learning Optimization in Cloud Computing Resource Scheduling and Management. arXiv preprint arXiv:2402.17216.Wang, Yong, et al. "Construction and application of artificial intelligence crowdsourcing map based on multi-track GPS data." arXiv preprint arXiv:2402.15796 (2024).

DOI: 10.54254/2755-2721/64/20241372

[10] Song, B., Xu, Y., & Wu, Y. (2024). ViTCN: Vision Transformer Contrastive Network For Reasoning. arXiv preprint arXiv:2403.09962.
[11] NIST 800-53 Security and Privacy Control for Federal Information Systems and Organizations [S]. NationalInstitute of Standards and Technology, 2010.
[12] Security guidance for critical areas of focus incloucomputing v3.0[R/L]. Cloud Security Alliance,2011[2017-08-30].