International Journal of Computer Science and Information Technology
ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 4, Number 1, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v4n1.12
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Data Security Issues in Intelligent Cloud Computing Systems

Shiqi Hao *

Jinling High School Hexi Campus, Nanjing, Jiangsu, 210019, China
*Corresponding Author: haoshiqi0618@icloud.com

ABSTRACT

This project takes the intelligent cloud computing system as the main research object. It mainly uses the literature analysis method to explore the data security problems in the intelligent cloud computing system. By investigating the development background of intelligent cloud computing, the author summarizes the definition of cloud computing and the characteristics of cloud computing. The author also makes a specific analysis of the advantages of cloud computing, and concludes that cloud computing is possible through safe and reliable data, low demand for clients, shared cloud data and unlimited possibilities. These four points are the main reasons major enterprises choose cloud computing to replace traditional computing resources. In the topic, the author studied the data security problems in cloud computing from three aspects: the problems exposed in the development process of cloud computing, the effective measures to protect data security in cloud computing and predicting the future development trend of improving data security. The authors believe that future research should focus on a balance between network security issues in cloud computing and building a secure and reliable data system.

KEYWORDS

Cloud computing systems; Data security

1. INTRODUCTION

With the development of network technology and computer technology, the researchers found that the development prospect of computers is currently in a bottleneck period. The development of network technology enhances the connection of the world so that computing resources can be shared worldwide. The research has found that the market has always had a very strong demand for computing resources, and the emergence of cloud computing has solved the market demand. Cloud computing is one of the emerging technologies in the field of computing in recent years. The characteristics of cloud computing, such as large-scale scalability, ubiquitous distribution and sociality, provide a lot of convenience for the market. To make cloud computing more meet the market demand, cloud computing needs to be improved. However, the development of cloud computing was found to it exposed some problems, such as no unified cloud computing standards, data security and charging model, and the lack of laws, and all these factors have an impact on the development of cloud computing. Among them, data security is a challenging problem.

The research goal of this paper is to study the impact of data security factors on the development of cloud computing, put forward the solution to the data security problems, and finally explore the future development direction of data security in the cloud computing scenario. The author also believes that the three main aspects of data security are: confidentiality, integrity and availability. Strengthening data security from these three aspects can greatly improve the security of cloud computing. The importance and originality of this topic: The technical innovation of this topic is to summarize and

analyze the impact of data security on the development of cloud computing. From three main aspects: confidentiality, integrity and availability, we should consider how to improve data security, and then use statistical analysis methods to analyze the feasibility. Finally, through these schemes to improve the data security, we can predict the future development trend of the data security improvement.

2. LITERATURE REVIEW

2.1. Define Cloud Computing

The authors find that there are many definitions of cloud computing, and there is no unified definition. Wang, Z. (2014) And others believe that cloud computing is an Internet-based service, while mobile cloud computing is the availability of cloud computing services in the mobile environment. While Makwe, A. (2024) and so on, the cloud is based on the virtual mode to provide users with high-quality services. In addition, the cloud can also provide users with computing resources and service access to customers according to their needs. Faiza Qazi (2024) believes that cloud computing belongs to distributed computing, which provides hosting services for users based on the Internet. Karamany, T.S. (2024) et al., cloud computing is based on the virtualization principle of operation, which is used for multiple customers based on a large machine, and believes that they all have their proprietary resources. After summarizing some representative definitions, Teng Ping (2012) will finally define cloud computing as the release of applications through Internet service-based services, and realize the relevant system software and hardware involved in these services. Brzozowska-Rup, K. (2024) According to the definition given by the National Institute of Standards and Technology, we concluded that cloud computing is a model, which can realize the shared pool of ubiquitous, convenient and on-demand network access to configurable computing resources.

2.2. Characteristics of Cloud Computing

First, cloud computing is a new technology based on the analysis of big data. Galego, N.M.C. (2023) It is believed that big data is characterized by large quantity, fast speed, large type, scalability, flexibility and cost effect. Big data organizes large and complex data sets generated from various sources. Cloud computing can counter computing that analyzes large amounts of data by improving scalability and low-cost solutions. Whereas Karamany, T.S. (2024), believe that cloud computing has revolutionized the way people manage and use computing resources. It provides better computing methods such as scalability, flexibility and cost-effectiveness, which are also the characteristics of cloud computing. In addition, cloud computing also provides cost-saving opportunities for small and medium-sized enterprises to avoid buying expensive hardware resources, which also reflects the relatively low price of cloud computing. Because cloud computing has the significant advantages of managing resources and business continuity in unlimited storage in the cheapest way, cloud computing is popular in the IT industry. Teng Ping (2012) found that the characteristics of cloud computing include safe and reliable data, low client demand, easy sharing of data and unlimited possibilities. In addition, she concluded that the development of the ICT business platform and IDC centre in recent years both need the support of cloud computing technology and establishment and development based on the cloud computing model, which is also the reason why cloud computing has been a hot topic in recent years. Brzozowska-Rup, K. (2024) also mentioned that since cloud computing can flexibly and scalably provide infrastructure and computing capabilities, reduce costs, provide professional services and manage on demand, it can still update software without the need to install or maintain software. Cloud computing has a special position in services because of these advantages. As an innovative information technology, it can share and use external software resources, and cloud solutions are provided by subscription instead of purchase and maintenance. As a result, individuals, businesses, and public institutions have all decided to migrate to computers.

3. SAFETY PROBLEM ANALYSIS OF CLOUD COMPUTING

Data security issues are very important to the development of cloud computing. Cloud computing is developed based on big data, and data sharing is the most common form, which usually refers to the unified management and storage of all data in a resource pool. According to the market demand, cloud computing is directly or indirectly used in many businesses. For enterprise companies, computing data is very important, and for enterprise customers, data loss or leakage can have very serious consequences. If the data security problem in the cloud computing platform cannot be solved, it will not effectively isolate and protect the data of each enterprise, and then the enterprises will not choose to use the cloud computing platform to store their data, which will also limit the widespread use of cloud computing technology. Therefore, in the process of improving the cloud computing platform, we need to pay attention to ensure the security and integrity of enterprise data, and determine the access scheme of data storage. G. Visalaxi (2023) has proposed that various security vulnerabilities in cloud computing systems will affect any network and computing in open networks and distributed environments. This type of client-server architecture and internal communication processing has been important because of the risk assessment of different cloud system layers and components. Security issues occur during handling important data, transactions and public communications, including internal and external attacks, such as attacks on users, hardware quality, etc., which put the entire cloud computing system at risk.

Cloud security refers to the security measures that protect the data, applications, and infrastructure stored in the cloud. Since the vast majority of enterprises are currently using cloud computing in some form, cloud security is necessary in this case. B. Ranganatha Rao (2023) and others mentioned that, to protect all security, cloud security must handle connections to all, applications, and data. Public cloud security is used to ensure that customers always have access to applications and data, which also helps service providers address any potential security issues promptly. Shivaramakrishna, D. (2023), believe that advanced security mechanisms are the basis for the rapid spread of cloud computing and that security mechanisms can be used to protect sensitive data stored in remote servers. But the shift also poses a host of security issues, especially in protecting private information stored on cloud servers. Cloud solutions show unparalleled advantages of scalability, accessibility, and availability over traditional local data storage. The cloud computing system stores its data in remote data centres that run under a decentralized architecture introduced by cloud computing. However, security vulnerabilities can often occur in environments where data is moved, processed, and stored across networks, with important issues such as data leakage, unauthorized access, and internal threats. In addition, as cloud resources are shared, concerns are raised about the isolation and division of data between users. The authors believe that maintaining data confidentiality is the core principle of secure cloud data storage. The authors believe that the best way to address this problem is to conduct regular integrity checks and audits to promptly detect any unauthorized changes.

4. EFFECTIVE MEASURES TO PROTECT THE DATA SECURITY IN CLOUD COMPUTING

4.1. Data Security System

Cloud data security systems can determine the basic security of a product because the system is built based on careful experiment and evaluation strategies. Ensuring the quality of cloud computing data security products is conducive to the improvement of cloud computing and information safety. Establishing a physical security system is an effective measure to maintain data security, and the system can never be accessed through cloud services. To protect users' data security, service providers must provide the necessary security settings for personal network clouds from a distance. The author studies the security problem of cloud computing and finds that the lightweight data security system can be applied to maintain the data security problem of cloud computing platforms. The core factor

of encryption technology is a common key encryption way that utilizes secret data to encrypt the initial report and transmits the key with the encoded data to the destination. The danger associated with symmetric encryption is the private-key transmission over the network. The authors find that the threat of symmetric encryption can be resolved through a secure approach, passed to different clients, and distributing data securely by encrypted information, sender and recipient, before making concessions to the key while trying to make it appropriately longer. However, the purpose of this study is to create and establish a strategy to achieve security by using lightweight keys acting as a tool to mediate users and operations. The survey found that encryption still provides high protection for the data. Considering the performance and security issues, they remain incredibly difficult even if it is in the verifiable case.

To address the various inefficiencies of existing server solutions, it is now necessary to create a unique cloud data security model. Cybersecurity capabilities can be studied by providing tutorial exercises and cryptography research, as well as group security innovations. Based on a massive decomposed simple encryption system, there is an inevitable trade-off between the safety of ciphertext and its encryption. The result of allowing consumers to audit cloud storage with extremely lightweight connectivity and computing costs is a rapid localization of information errors while ensuring solid cloud capacity, which is also identifiable evidence of entry into the prank server. Sometimes, outsourcing is the only way to protect data privacy and combat random visit within the cloud.

4.2. Blockchain IAS Protocol

The most important goal of the blockchain IAS model is to achieve a digital signature. This usually requires five basic components, the specific function of the hash, the dual group key, and each confidential communication instance value. The study is mainly divided into three parts: digital identity administration, visit control of information sharing and blockchain-based validation agreement.

4.2.1. Digital Identity Administration

Digital Identity administration is the course of establishing and administering a special digital identity for an individual or entity in a safe and interoperable mode. At the current, digital identity administration has attracted much attention because of its scattered and safe storage of user identity data. Studies have found that users' identity data, for example names, ages, and social numbers, could all be stored in their separate accounts in a scattered mode. This account also has a number identifier, which is called a cloud identity. They are controlled by a blockchain network that uses licensed and smart contract-based identity managers. Blockchain can store private keys to these identity managers and be used for certification to visit information or services provided by tissues or service providers that build duty with the platform.

4.2.2. The Digital Identity Administration Treaty

The main application of blockchain technology on cloud computing platforms is the digital administration treaty, which is projected to administer identity and ascribes to a scattered manner. The treaty is mainly divided into two stages. The first stage includes the intelligent contract, which fills a post a limiting surface. In addition, the administration of identity and attribute management are its main functions. In the next place, the intelligent treaty pays attention to digital addresses, which also include cabinet keys and governmental keys or signatures. Among them, duty plays an important role in exchanging properties between different instances in the system to guarantees actuality. Digital identity administration mainly involves four aspects, namely, forefront identity manager, attribute patent manager, information centre and cloud users. By using this treaty, mandatory access control lists can be executive and precise rights are available to consumers. The validation process proceeds with each calculation during the visit, which makes it extremely challenging for an attacker to visit the digital accordance. In conclusion, the utility of blockchain method in the identity governance Treaty provides an effective solution to enhancing the security and privacy of cloud computing.

4.2.3. Blockchain-based data sharing and access control

The authors view a blockchain-based visit control institution as a theory that facilitates safe visit to cloud computing platforms by accomplishing a scattered and constant general account of employ command strategies. At the same time, it can ensure that only licenses can access cloud resources by using a licensed blockchain network with an access control list. Currently, access control systems work by keeping employ command strategies in a blockchain technology, which is subsequently performed by smart agreements. These strategies provide precise access to each consumer or group of consumers. After utilizing a digital identity administration treaty, which invests blockchain theory to produce and process numerical accordance. In an access control institution, each visit request to a cloud computing platform parents the confirmation course of a smart treaty-based visit possess institution, which makes sure that merely franchised consumers with suitable rights can visit the information on the cloud computing platform. The utility of blockchain theory is to spread out access control systems, be tamper-proof and tough illegal variations, thus intensifying the safety and privacy of the cloud computing circumstance. In addition, research has found that both identity management and access control management processes are based on a blockchain using smart contracts. And each data provider runs its access control manager contract. Each identity token is displayed in a format and stored in Lgdr.

5. CONCLUSION

The author explores the reasons why the market chooses cloud computing compared with the traditional computing methods from the aspects of the development background of cloud computing, the definition of cloud computing, the characteristics of cloud computing and the analysis of the advantages of cloud computing. The author found that compared with traditional computing systems, intelligent cloud computing systems are more flexible, and cloud services have certain benefits for both enterprises and individuals. After the analysis of the advantages of cloud computing, the author found that the security and reliability of data, the low demand for clients, the shared data and the infinite possibility have become the biggest reasons for people to choose it.

In addition, the author also puts forward suggestions for the future development of cloud computing from the problems exposed in the development process of cloud computing, the effective measures to protect data security in cloud computing and predicting the future development trend of improving data security. First, the author analyzes the problems exposed in the development process of cloud computing, mainly analyzing the current shortcomings of cloud computing from the standardization, security and business model issues. The analysis found that the current problems are data security, cloud platform service charging model inconsistency and inconsistent cloud computing standards. This topic mainly analyzes the problem of data security and puts forward some effective measures to protect data security in cloud computing, such as the establishment of a data security system and blockchain IAS protocol. The author believes that cloud computing can be better used in the market in the future after improving security. Data security issues can be solved or improved after some measures. Future research will focus on finding a balance between network security issues in cloud computing and establishing a secure and reliable data system.

REFERENCES

[1] Admass, W.S., Munaye, Y.Y., & Diro, A.A. (2023). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031. https://doi.org/10.1016/j.csa.2023.100031

[2] Almudarra, F., & Qureshi, B. (2014). Issues in Adopting Agile Development Principles for Mobile Cloud Computing Applications. Procedia Computer Science, 52, 1133-1140. https://doi.org/10.1016/j.procs.2015.05.131

[3] Belal, M.M., & Sundaram, D.M. (2022). A comprehensive review on intelligent security defences in the cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends.Journal of King Saud University - Computer and Information Sciences, 34(10), 9102-9131. https://doi.org/10.1016/j.jksuci.2022.08.035

[4] Brzozowska-Rup, K., Nowakowska, M., & Zdradzisz, M. (2024). Cloud computing in the Polish public administration: Current state and development prospects.Technological Forecasting and Social Change, 205, 123500. https://doi.org/10.1016/j.techfore.2024.123500

[5] Ferrer, A.J., Pérez, D.G., & González, R.S. (2015). Multi-cloud Platform-as-a-service Model, Functionalities and Approaches. Procedia Computer Science, 97, 63-72. https://doi.org/10.1016/j.procs.2016.08.281

[6] Galego, N.M.C., Martinho, D.S., & Duarte, N.M. (2023). Cloud computing for big data analytics How cloud computing can handle processing large amounts of data and improve real-time data analytics.Procedia Computer Science, 237, 297-304. https://doi.org/10.1016/j.procs.2024.05.108

[7] He Ming, Zheng Xiang, Lai Hai-Guang & Jiang Feng. (2010). Development and application of cloud computing technology. Telecommunication Science (05), 42-46.

[8] Hosny, K.M., Awad, A.I., Said, W., Elmezain, M., Mohamed, E.R., & Khashaba, M.M. (2024). Enhanced whale optimization algorithm for dependent tasks offloading problem in multi-edge cloud computing. Alexandria Engineering Journal, 97, 302-318. https://doi.org/10.1016/j.aej.2024.04.038

[9] Karamany, T.S., & Yakoub, A. (2024). A hybrid approach to secure and compress data streams in a cloud computing environment. Journal of King Saud University - Computer and Information Sciences, 36(3), 101999. https://doi.org/10.1016/j.jksuci.2024.101999

[10] Kumar, P.R., Raj, P.H., & Jelciana, P. (2017). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science, 125, 691-697. https://doi.org/10.1016/j.procs.2017.12.089

[11] Makwe, A., Kanungo, P., Kautish, S., Madhu, G., Almazyad, A.S., Xiong, G., & Mohamed, A.W. (2024). Cloud service prioritization using a Multi-Criteria Decision-Making technique in a cloud computing environment. Ain Shams Engineering Journal, 15(7), 102785. https://doi.org/10.1016/j.asej.2024.102785

[12] Manogaran, G., Thota, C., & Kumar, M.V. (2015). MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing. Procedia Computer Science, 87, 128-133. https://doi.org/10.1016/j.procs.2016.05.138

[13] Mohammed, S., Nanthini, S., Bala Krishna, N., Srinivas, I.V., Rajagopal, M., & Ashok Kumar, M. (2023). A new lightweight data security system for data security in cloud computing.Measurement: Sensors, 29, 100856. https://doi.org/10.1016/j.measen.2023.100856

[14] Musarat, M.A., Alaloul, W.S., Khan, M.H.F., Ayub, S., & Guy, C.P.L. (2024). Evaluating cloud computing in construction projects to avoid project delay. Journal of Open Innovation: Technology, Market, and Complexity, 10(2), 100296. https://doi.org/10.1016/j.joitmc.2024.100296

[15] Prasad, S.N., & Rekha, C. (2023). Blockchain-based IAS protocol to enhance security and privacy in cloud computing. Measurement: Sensors, 28, 100813. https://doi.org/10.1016/j.measen.2023.100813

[16] Qazi, F., Kwak, D., Khan, F.G., Ali, F., & Khan, S.U. (2024). Service Level Agreement in cloud computing: Taxonomy, prospects, and challenges.Internet of Things, 25, 101126. https://doi.org/10.1016/j.iot.2024.101126

[17] Ranganatha Rao, B., & Sujatha, B. (2023). A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security.Measurement: Sensors, 29, 100870. https://doi.org/10.1016/j.measen.2023.100870

[18] Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control.Alexandria Engineering Journal, 84, 275-284. https://doi.org/10.1016/j.aej.2023.10.054

[19] Singh, A.P., & Pasupuleti, S.K. (2015). Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing.Procedia Computer Science, 93, 751-759. https://doi.org/10.1016/j.procs.2016.07.286

[20] Teng P. (2012). Development analysis of cloud computing technology and its application. Information Network Security (11), 89-91.

[21] Visalaxi, G., & Muthukumaravel, A. (2023). IoT monitoring membrane computing based on quantum inspiration to enhance security in the cloud network. Measurement: Sensors, 27, 100755. https://doi.org/10.1016/j.measen.2023.100755

[22] Wang, Z., Sun, G., & Chen, D. (2014). A new definition of homomorphic signature for identity management in mobile cloud computing.Journal of Computer and System Sciences, 80(3), 546-553. https://doi.org/10.1016/j.jcss.2013.06.010

[23] Yu, Y., Miyaji, A., Au, M.H., & Susilo, W. (2017). Cloud computing security and privacy: Standards and regulations. Computer Standards & Interfaces, 54, 1-2. https://doi.org/10.1016/j.csi.2017.03.005