Identification and Analysis of Key Influencing Factors of Technical Security Risks in Personal Cloud Storage Services - Postprint

Authors: Huiping Cheng, Peng Qi

Date: 2023-07-26T00:00:00+00:00

Abstract

[Purpose/Significance] In recent years, technical security issues in personal cloud storage services have occurred frequently, severely affecting the continuous usage rate of personal cloud storage service users. Identifying and analyzing the key influencing factors of technical security risks in using cloud storage services is of important practical significance for personal cloud storage service providers to offer secure cloud storage services and improve user stickiness. [Method/Process] Based on literature review, expert interviews, cloud computing security reports (Gartner), and cloud computing security architectures and standards (ENISA, CSA, FedRAMP, MTCS), an indicator system for influencing factors of technical security risks in personal cloud storage services is constructed. Through expert questionnaire surveys, the direct influence matrix among various influencing factors in the technical security risk assessment system for personal cloud storage services is obtained. The Fuzzy-DEMATEL method is employed to analyze the causal relationships and importance degrees of technical security risk influencing factors in personal cloud storage services, revealing the key influencing factors. [Results/Conclusion] The key influencing factors of technical security risks in personal cloud storage services include: access control, service/account hijacking, software security risks, virtualization vulnerabilities, and data transmission security. Finally, based on the empirical research conclusions, feasible technical recommendations are provided for personal cloud storage service providers to build secure cloud storage services. This study enriches the theoretical research outcomes on security risks in personal cloud storage services and provides practical reference for personal cloud storage service providers to ensure user data security.

Full Text

Identification and Analysis of Key Influencing Factors on Technical Security Risk of Personal Cloud Storage Services

Cheng Huiping[1],[2], **Peng Qi**[1] [1] School of Economics and Management, Hubei University of Technology, Wuhan 430068 [2] School of Public Management, Northwest University, Xi' an 710127

Abstract

In recent years, technical security problems in personal cloud storage services have become increasingly common, severely hindering users' continuous usage of these services. Identifying and analyzing the key influencing factors of technical security risk in cloud storage services holds significant practical importance for providers to offer secure cloud storage services and enhance user engagement. Based on literature surveys, expert interviews, cloud computing security reports (Gartner), and cloud computing security architectures and standards (ENISA, CSA, FedRAMP, MTCs), this study constructs a technical security risk factor indicator system for personal cloud storage services. Through expert questionnaire surveys, we obtained the direct influence matrix among factors in the technical security risk assessment system. Using the Fuzzy-DEMATEL method, we analyzed the causal relationships and importance levels of these risk factors, revealing the key influencing factors of technical security risk in personal cloud storage services. The critical factors include: access control, service/account hijacking, software security risk, virtualization vulnerability, and data transmission security. Finally, based on empirical findings, we provide feasible technical recommendations for building secure cloud storage services. This research enriches theoretical studies on personal cloud storage security risks and offers practical references for providers to safeguard user data security.

1. Introduction

The rapid development of the Internet, social media, and mobile devices has brought great convenience to people' s social lives while causing exponential growth in personal information data, creating urgent demand for efficient data storage. Personal cloud storage services have become an effective solution to this problem. With advantages such as high efficiency, convenience, and low cost, personal cloud storage has attracted increasing attention from Internet users. Individuals can purchase storage services on demand, which saves storage resources compared to traditional storage methods and reduces constraints arising from limited personal storage and computing resources.

However, personal cloud storage integrates multiple technologies including Service-Oriented Architecture (SOA), Web 2.0, and virtualization. During its development, security risks arising from immature technologies have directly affected the normal operation of personal cloud storage systems, significantly

damaging provider reputations. In recent years, data leakage incidents caused by technical vulnerabilities have become common. We have compiled numerous recent cloud service security incidents abroad (see Table 1).

According to a 2016 research report on China' s personal cloud storage industry released by iMedia Consulting, China's personal cloud storage user scale dropped sharply to 396 million users in 2016, with only 7.3% continuously using cloud drives. The primary reason for this phenomenon is users' distrust of providers' security assurance and risk control capabilities. With frequent cloud computing security risk incidents and low switching costs for online application-based personal cloud storage users, insufficient continuous usage has created dilemmas for personal cloud storage service development. How to promote continuous user usage while ensuring technical security is fundamental to sustainable market development. Therefore, technical security represents a critical issue requiring urgent resolution in personal cloud storage service practice.

This study aims to achieve two objectives: (1) identify security risk factors of personal cloud storage services from a technical security perspective and construct a technical security risk assessment indicator system; and (2) reveal causal relationships among factors in the complex system of personal cloud storage technical security risks and determine the key influencing factors.

2. Literature Review

Existing cloud computing security research primarily comprises two components:

(1) Cloud Computing Security Risk Factor Composition and Assessment Research. Cloud computing security has attracted extensive academic attention, with literature focusing on three aspects: First, cloud computing security risk composition studies. ENISA [3] proposed 35 risk factors from four perspectives: policy and organizational risks, technical risks, legal risks, and unspecified cloud risks. D. Zissis et al. [4] identified 28 threats and 18 security requirements across application, virtualization, and physical layers. A. Singh et al. [5] constructed a cloud computing security indicator system covering eight dimensions: data storage and computing security, virtualization security, Internet and service-related security, network security, access control, software security, trust management, and compliance and law.

Second, theoretical extraction of primary cloud computing security risk factors. As early as 2008, Gartner' s [6] research report "Assessing the Security Risks of Cloud Computing" proposed seven major cloud computing risks. The Cloud Security Alliance (CSA) [7] listed the "Treacherous Twelve" cloud security threats for 2016. N. Khan et al. [8] and G. Ramachandra et al. [9] proposed 12 threats and vulnerabilities, many aligning with CSA' s 2016 threats, including service/account hijacking, shared technology risks, insecure APIs, malicious insiders, data leakage, and denial-of-service attacks. These studies primarily involve simple qualitative discussions of cloud computing security risk factors.

Third, cloud computing security risk assessment methods. A. Shameli-Sendi et al. [10] proposed a cloud computing security risk assessment framework and conducted empirical research using an industrial automotive company. J. Liu et al. [11] developed a risk assessment method based on fuzzy entropy weight. G. T. R. Lin et al. [12] constructed a hierarchical model of critical success factors for information security management in cloud computing and applied fuzzy analytic hierarchy process for empirical analysis. F. Lin et al. [13] proposed a cloud computing system risk assessment method based on cloud focus theory, validating its feasibility through simulation experiments.

(2) Cloud Computing Security Standards and Control System Research. Cloud computing security has attracted high attention from governments and standards organizations, yielding numerous security standards, control systems, and guidelines. The ISO/IEC 27017 international cloud assurance standard provides development direction for secure cloud storage for cloud service providers, serving as a benchmark document for protection controls and proposing relevant control patterns to address cloud security threats and risks [14-15]. The Federal Risk and Authorization Management Program (FedRAMP) aims to provide standardized approaches for federal agencies to regulate and authorize cloud computing services, focusing more on cloud computing security maintenance compared to ISO/IEC [16]. The Singapore Multi-Tier Cloud Security (MTCS) standard (SS584) clarifies security requirements for cloud service providers to meet different users' needs for privacy data and critical business security, primarily focusing on cloud service availability [17]. CSA' s "Security Guidance for Critical Areas of Focus in Cloud Computing" proposes 13 key security domains for cloud computing, providing references for risk identification [18]. ENISA's "Guide to Monitoring Security Service Levels in Cloud Contracts" offers guidance for compliant operations from a Service Level Agreement (SLA) perspective [19].

In summary, existing cloud computing security research primarily involves theoretical discussion, with empirical analysis requiring strengthening. Research specifically addressing personal cloud storage security risk influencing factors is scarce, particularly lacking quantitative studies from a technical security dimension that reveal interrelationships among factors. This study identifies technical security risk factors affecting personal cloud storage services, analyzes their interrelationships and relative importance, and identifies critical technical security risk factors to provide theoretical foundations for stakeholders in personal cloud storage service security risk management decision-making.

3. Technical Security Risk Indicators for Personal Cloud Storage Services

Personal cloud storage is an emerging online storage system encompassing distributed storage and efficient sharing characteristics of cloud computing. Therefore, technical security risks in personal cloud storage services include both traditional information technology security risks and cloud-specific technical security

risks arising from distributed storage and sharing technologies [6, 20]. Through literature surveys, expert interviews, cloud computing security reports (Gartner), and cloud computing security architectures and standards (ENISA, CSA, FedRAMP, MTCs), we constructed a technical security risk influencing factor indicator system for personal cloud storage services (see Table 2). From an integrated perspective of traditional and cloud-specific technical security risks, we built the indicator system (see Figure 1 [Figure 1: see original paper]).

3.1 Traditional Technical Security Risks

(1) Access Control primarily includes user authentication and authorization. Authentication, also called identity verification, confirms user identity information accessing personal cloud storage systems. Personal cloud storage systems face massive user groups, each with unique identity information, requiring robust authentication technology. Additionally, since users often register on different platforms with identical credentials, providers must offer stronger authentication. Authorization refers to granting or denying permissions to users or applications. Malicious authorized users or applications can access prohibited resources and perform illegal data manipulation. Particularly noteworthy is limiting internal personnel permissions, as malicious insiders may violate professional ethics and illegally access user data, causing privacy leakage.

(2) Service/Account Hijacking occurs when attackers steal authorized user login credentials to illegally access critical cloud areas, eavesdrop on user activities, conduct improper data transactions, manipulate data, and prevent normal user login. This can be achieved through fraud, phishing, and software vulnerabilities.

(3) Resource Exhaustion refers to uncontrolled resource consumption exceeding planned usage. Cloud storage resource allocation involves calculation risks, including inaccurate resource usage models, fairness issues in public resource allocation algorithms, and insufficient resource allocation, leading to service interruption and reputation damage. This risk may also result from denial-of-service attacks.

(4) Data Integrity Risk concerns data integrity stored in the cloud, including data loss/leakage and data tampering/destruction. Data loss/leakage involves illegal deletion, alteration, and theft without backup, primarily caused by immature authentication, authorization, and disaster recovery technologies. Data tampering/destruction involves attackers modifying user data or destroying data structures. Both result in data integrity loss, causing users to lose confidence in providers.

(5) Encryption and Key Management includes data encryption technology and key management technology. Immature encryption technology may allow attackers to directly decrypt data, causing leakage. Additionally, encryption technology vulnerabilities may destroy data structures, causing data invalidation or damage. Loss or damage of encryption keys used for encryption,

authentication, or digital signatures may lead to data loss or denial-of-service.

(6) Network Security Risk primarily includes network bandwidth and malicious code/software injection. Network bandwidth directly affects cloud service performance; only high-speed, stable networks can support numerous concurrent users without interruption or delay. Many cloud data security crises originate from network attacks. Although providers have implemented network monitoring and prevention measures, current technology remains imperfect and cannot monitor all possible network attacks.

(7) Hardware Security Risk refers to risks from storage hardware device damage. Due to imperfect equipment monitoring and protection technologies, data loss or leakage may occur when hardware suffers from natural disasters or human destruction.

(8) Data Backup and Recovery refers to providers' ability to timely backup user data and quickly restore it when needed, reducing data loss or unavailability risks from equipment failure.

(9) Server Engine Vulnerability refers to potential vulnerabilities in server engine code that are susceptible to attacks or unexpected failures. Illegal users attacking the server engine can bypass virtual isolation between users to obtain other users' data access permissions for improper data operations.

(10) Software Security Risk includes software update/upgrade risks, insecure interfaces and APIs, and software vulnerabilities. Mobile terminal systems face updates and upgrades, each potentially introducing various problems. User interaction with cloud platforms depends on software interfaces or APIs provided by personal cloud storage service providers. Once these interfaces develop vulnerabilities exploited by attackers, cloud services may fail to function properly. Software vulnerabilities provide opportunities for attackers to easily bypass system protections.

3.2 Cloud-Specific Technical Security Risks

(1) Virtualization Vulnerability. Virtualization technology is core to cloud computing, enabling on-demand storage. However, it introduces new technical security risks—virtualization vulnerabilities. These include virtual machine image management vulnerabilities, virtual machine monitor vulnerabilities, virtual machine cloning vulnerabilities, inter-virtual machine vulnerabilities, denial-of-service attacks, and data isolation. Cloud dynamics allow users to create new virtual machine images or use previously created ones, potentially enabling malicious users to create images containing malware or find attack points in image code. Malicious virtual machine images may improperly observe user activities or data, causing information leakage. The complexity and multi-access nature of virtual machine monitor internal structures may introduce numerous virus-carrying media attacks. Virtual machine monitor transparency may cause Rootkit attacks, allowing malicious users to control monitors and spy on other

virtual machines to steal user data. Virtual machine cloning, the process of moving virtual machines to other servers, may leak images containing user private keys and other privacy information to other virtual machines during simultaneous copying. While virtual machine replicability facilitates rapid personal cloud storage development, associated risks cannot be ignored. Inter-virtual machine vulnerabilities refer to mutual attacks among virtual machines in a cluster, including cross-virtual machine attacks, virtual machine hopping attacks (attackers stealing access permissions of other virtual machines on the same monitor), replay attacks, and side-channel attacks. Denial-of-service attacks involve attackers controlling a single virtual machine to exhaust all resources, causing other virtual machines to malfunction due to resource scarcity and denying normal user service requests. The multi-tenant model of personal cloud storage makes data isolation measures between different users particularly important. Although virtual machines are logically independent, they actually share the same resource pool, potentially causing inter-virtual machine attacks and data leakage.

(2) Data Migration technology is crucial for long-term stable operation of personal cloud storage systems. Due to distributed storage characteristics, data migration between different SaaS platforms may cause data loss due to incompatible import/export formats. Additionally, service interruption or hacker attacks during migration may cause data loss or leakage.

(3) Data Transmission Security. Due to distributed systems and shared technology characteristics, cloud storage data transmission technology has more transmission channels than traditional storage technology, introducing more uncontrollable risks. Data transmission may involve sniffing, spoofing, man-in-the-middle attacks, and side-channel attacks.

(4) Data Deletion. Incomplete data deletion may cause user data leakage. Cloud data may be backed up and stored in multiple locations. When users send deletion instructions, providers may not thoroughly delete all backup data or may violate professional ethics by not executing deletion operations and instead trading user data, causing data leakage.

4. Fuzzy-DEMATEL Method

The Decision-Making Trial and Evaluation Laboratory (DEMATEL) method analyzes mutual influence degrees among factors in complex systems. Based on graph theory, it constructs visual causal diagrams of system factors to better understand element relationships and obtain efficient solutions [32]. Due to uncertainty in real-world problems, experts often use fuzzy semantic expressions like "important" or "relatively important" when scoring. To reduce DEMATEL' s subjectivity and fuzziness, we integrated fuzzy theory with DEMATEL for computational analysis. The Fuzzy-DEMATEL calculation steps are as follows:

Step 1: Determine the set of influencing factors $F = \{F_1, F_2, \ldots, F_n\}$ for the research problem, design an expert evaluation semantic scale, and divide the

influence strength between factors into five levels (see Table 3).

Step 2: Invite experts to score the influence degree between factors based on understanding the semantic scale, obtaining an original direct influence matrix A. Matrix A is a non-negative matrix with zeros on the main diagonal, where a_{ij} represents the influence degree of element F_i on element F_j.

Step 3: Fuzzify the original direct influence matrix A using triangular fuzzy numbers, and defuzzify using the Converting Fuzzy data into Crisp Scores (CFCS) method developed by S. Opricovic [33] to obtain the clear direct influence matrix Z.

Using the membership function formula for triangular fuzzy numbers (see formula (1)), calculate appropriate triangular fuzzy numbers $N = (l, m, r)$, where l represents the conservative value of influence strength, m represents the possible value, and r represents the optimistic value, yielding the semantic conversion table (see Table 3).

$$\mu_N(x) = \begin{cases} 0, & x < l \\ \frac{x-l}{m-l}, & l \le x < m \\ \frac{r-x}{r-m}, & m \le x \le r \\ 0, & x > r \end{cases} \tag{1}$$

Let $a_{ij}^k = (l_{ij}^k, m_{ij}^k, r_{ij}^k)$ represent the triangular fuzzy number corresponding to the influence degree of factor i on factor j assessed by the k-th expert, where $k = 1, 2, \ldots, K$. The specific calculation process of the CFCS method is shown in formulas (2)-(10).

Normalize the triangular fuzzy numbers:

$$l_{ij}^{k'} = \frac{l_{ij}^k - \min l_{ij}^k}{\Delta_{\max}} \tag{2}$$

$$m_{ij}^{k'} = \frac{m_{ij}^k - \min l_{ij}^k}{\Delta_{\max}} \tag{3}$$

$$r_{ij}^{k'} = \frac{r_{ij}^k - \min l_{ij}^k}{\Delta_{\max}} \tag{4}$$

where $\Delta_{\max} = \max r_{ij}^k - \min l_{ij}^k$ for $1 \le k \le K$.

Calculate left standard value (x_{ls}) and right standard value (x_{rs}):

$$x_{ls} = \frac{m_{ij}^{k'}}{1 + m_{ij}^{k'} - l_{ij}^{k'}} \tag{5}$$

$$x_{rs} = \frac{r_{ij}^{k'}}{1 + r_{ij}^{k'} - m_{ij}^{k'}} \tag{6}$$

Calculate total clear value:

$$x_{ij}^{k} = \frac{x_{ls}(1 - x_{ls}) + x_{rs}x_{rs}}{1 - x_{ls} + x_{rs}} \tag{7}$$

Calculate average clear value:

$$z_{ij} = \frac{x_{ij}^{1} + x_{ij}^{2} + \cdots + x_{ij}^{K}}{K} \tag{8}$$

Step 4: Normalize matrix Z to obtain the direct influence matrix H (see formulas (9) and (10)), where q is the normalization factor:

$$q = \frac{1}{\max_{1 \le i \le n} \sum_{j=1}^{n} z_{ij}} \tag{9}$$

$$H = q \cdot Z \tag{10}$$

Step 5: Calculate the total influence matrix T, where t_{ij} represents the indirect influence relationship between factors i and j (see formula (11)), where I is the identity matrix:

$$T = H(I - H)^{-1} \tag{11}$$

Step 6: Calculate the row sum (D) and column sum (R) of each factor in matrix T. D represents the influence degree, indicating the total direct and indirect influence of a factor on other factors in the personal cloud storage service technical security risk system. R represents the influenced degree, indicating the total direct and indirect influence a factor receives from other factors. $D + R$ represents the centrality, indicating the importance of a factor in the system. $D - R$ represents the cause degree, dividing factors into cause groups (factors that influence others more than being influenced, actively affecting other factors) and effect groups (factors that are influenced by others more than they influence others, passively affected). The specific calculation process is shown in formulas (12) and (13):

$$D = \sum_{j=1}^{n} t_{ij} \tag{12}$$

$$R = \sum_{i=1}^{n} t_{ij} \tag{13}$$

In all formulas above, $i, j = 1, 2, \ldots, n$.

5. Key Influencing Factor Identification and Analysis

Regarding expert interview sample size, G. Guest et al. [34] noted that 12 interview subjects can be considered a sufficient sample in interview research. In personal cloud storage service research, K. Ghaffari et al. [35] selected 12 users for semi-structured interviews to reveal usage phenomena in developing countries. Drawing on this experience, our survey subjects included: 11 project leaders and core members of National Natural Science Foundation and National Social Science Foundation projects in cloud computing security, 3 authors who have published cloud computing security risk assessment research, and 2 senior personal cloud storage service users with over 3 years of experience, totaling 16 experts or users. All participants had computer science backgrounds, including 3 with senior professional titles, 4 with associate senior titles, 12 with doctoral degrees, and 4 with master' s degrees.

We conducted in-depth interviews and questionnaire surveys with selected experts on personal cloud storage service technical security risks. Three core members of our research group conducted thorough discussions and statistical analysis of the collected questionnaires. Following the Fuzzy-DEMATEL model calculation steps, we obtained the total influence matrix T (see Table 4), centrality $D + R$, and cause degree $D - R$ indicators (see Table 5). Based on Table 5 data, we plotted the causal diagram (see Figure 2 [Figure 2: see original paper]).

5.1 Inter-factor Relationships

Personal cloud storage service technical security risk influencing factors inherit traditional IT security risks while exhibiting cloud-specific security characteristics. The numerous risk elements involved are interrelated and interact with each other, forming a complex mechanism with varying intensities and scopes that collectively constitute a complex system of personal cloud storage security risk factors.

Based on the positive or negative cause degree values, factors can be divided into cause groups and effect groups. As shown in Table 5 and Figure 2, F_3 (resource exhaustion), F_6 (network security risk), F_7 (hardware security risk), F_9 (server engine vulnerability), F_{11} (virtualization vulnerability), and F_{14} (data deletion) belong to the cause group. Virtualization vulnerability (F_{11}) has the largest D value among all factors, with relatively low R ranking 10th, showing strong activeness—indicating that virtualization vulnerability strongly influences

other factors but is less influenced itself. For example, hackers controlling virtual machine monitors through virtualization vulnerability attacks can steal user identity information from virtual machines on the same host, leading to service/account hijacking, resource exhaustion, user privacy data leakage, and other security risks [13]. Network security risk (F_6) shows similar characteristics to F_{11}, with high D ranking and low R ranking, demonstrating strong activeness.

Resource exhaustion (F_3), hardware security risk (F_7), server engine vulnerability (F_9), and data deletion (F_{14}) have relatively low D and R scores among all factors, indicating these four factors are relatively isolated from other factors.

Factors with cause degree less than 0 belong to the effect group. Table 5 shows that F_1 (access control), F_2 (service/account hijacking), F_4 (data integrity risk), F_5 (encryption and key management), F_8 (data backup and recovery), F_{10} (software security risk), F_{12} (data migration), and F_{13} (data transmission security) are effect group factors. As shown in Figure 2, effect group factors generally have $D + R$ values above average, indicating these influencing factors are particularly important. Effect group factors most directly impact personal cloud storage service technical security risk and are more susceptible to cause group factors. Among them, data transmission security (F_{13}) has the largest influenced degree, but its D score is also high (ranking 2nd), indicating F_{13} has strong connections with other factors. F_{13} is most easily influenced by other factors while also strongly influencing others. Although its passivity exceeds its activeness, it overall remains an effect group factor. Data transmission involves multiple risks that may cause user data leakage.

Data integrity risk (F_4), encryption and key management (F_5), and software security risk (F_{10}) have R and D rankings at 3rd/13th, 4th/7th, and 2nd/6th positions respectively, showing strong passivity. Access control (F_1) and service/account hijacking (F_2) have negative $D - R$ scores, but their D rankings exceed their R rankings—caused by cloud computing environment complexity, with cause degree values only slightly below 0, overall showing some passivity. All personal cloud storage users have unique login identity information; if leaked, this can easily cause data integrity risks, encryption key loss, illegal data operations, and other issues. Hackers illegally obtaining administrator identity information can control personal cloud storage systems, causing denial-of-service attacks, service/account hijacking, and other problems. Data backup and recovery (F_8) and data migration (F_{12}) have relatively low D and R values, indicating F_8 and F_{12} are relatively isolated from other factors in the personal cloud storage service technical security risk influencing factor system.

5.2 Key Influencing Factor Identification

We identified key influencing factors by combining D, R, and $D + R$ indicators. First, virtualization vulnerability (F_{11}) has the largest influence degree among 14 factors and can strongly influence changes in the other 13 factors, thus identified

as a key influencing factor. Second, although data transmission security (F_{13}) is an effect group factor, its D and R levels are both high, with $D + R$ ranking first, indicating this factor' s importance in the system and close connections with other factors. Evidently, personal cloud service providers should consider this a key factor in both long-term and short-term implementations to ensure data transmission security and prevent illegal intrusion.

Third, software security risk (F_{10}) has negative cause degree but relatively high D level (ranking 6th), indicating certain influence on other factors. Its high $D + R$ level (ranking 2nd) further validates F_{10} as a key factor. Fourth, access control (F_1) and service/account hijacking (F_2) have $D - R$ scores of -0.077 and -0.066 (slightly below 0), indicating F_1 and F_2 are less influenced by other factors while exerting certain influence on other personal cloud storage technical security risk factors. Meanwhile, both factors have high D, R, and $D + R$ scores, confirming them as key factors. This conclusion further supports ENISA' s mention that malicious insiders may cause damages affecting data or IP confidentiality, integrity, and availability [3].

Resource exhaustion (F_3), hardware security risk (F_7), server engine vulnerability (F_9), data deletion (F_{14}), data backup and recovery (F_8), and data migration (F_{12}) have relatively low D, R, and $D + R$ scores, indicating F_3, F_7, F_9, F_{14}, F_8, and F_{12} are relatively isolated from other factors and less important in the system. Therefore, these are non-key influencing factors. Data integrity risk (F_4) and encryption and key management (F_5) show strong passivity with average $D + R$ values. While short-term measures may improve personal cloud storage security, their susceptibility to other factors means they may not yield good long-term results, making them unsuitable as key factors.

Comprehensive analysis reveals that our findings align with 7 of the 10 technical risks in CSA' s "Treacherous Twelve" cloud security threats: identity/credential and access management deficiencies, insecure interfaces and APIs, system vulnerabilities, account hijacking, malicious insiders, shared technology issues, and denial-of-service [7].

6. Conclusions and Implications

6.1 Conclusions

Factors influencing personal cloud storage service technical security risk are complex, with cross-interactions among factors, yet different factors have varying influence mechanisms and degrees. Existing literature rarely examines interrelationships among personal cloud storage service technical security risk factors. Based on literature surveys, expert interviews, cloud computing security reports (Gartner), and cloud computing security architectures and standards (ENISA, CSA, FedRAMP, MTCs), we proposed 14 factors affecting personal cloud storage service technical security risk. Using the Fuzzy-DEMATEL method, we obtained influence degree, influenced degree, centrality, and cause degree indicators for each factor. Based on cause degree scores, we identified resource

exhaustion (F_3), network security risk (F_6), hardware security risk (F_7), server engine vulnerability (F_9), virtualization vulnerability (F_{11}), and data deletion (F_{14}) as cause group factors. Access control (F_1), service/account hijacking (F_2), data integrity risk (F_4), encryption and key management (F_5), data backup and recovery (F_8), software security risk (F_{10}), data migration (F_{12}), and data transmission security (F_{13}) are effect group factors. Comprehensive indicator analysis identified five key influencing factors: virtualization vulnerability (F_{11}), data transmission security (F_{13}), software security risk (F_{10}), access control (F_1), and service/account hijacking (F_2).

6.2 Research Significance

Theoretical significance: Compared with existing research, this study constructed a complete technical security risk assessment indicator system for personal cloud storage services from both traditional and cloud-specific technical security perspectives, including 14 evaluation indicators. It revealed causal relationships and relative importance among factors in the personal cloud storage service technical security risk influencing factor system, analyzing key technical security risk factors. The conclusions basically align with technical threats in CSA' s "Treacherous Twelve" cloud security threats, further enriching theoretical research on personal cloud storage service security risks. Additionally, our results provide theoretical references for personal cloud storage service stakeholders to evaluate and verify cloud storage technical security risks during actual development. The constructed indicator system can also provide theoretical references for security risk assessment in other cloud computing domains.

Practical significance: Based on our findings, personal cloud storage service providers can reduce technical security risks and improve continuous usage growth rates from the following aspects: (1) Further improve virtualization technology by reducing disk quantities in personal cloud storage systems to lower operational costs and resource consumption. Virtualization technology improvements can also extend existing storage equipment lifespan to reduce procurement costs and service costs for consumers. (2) Strengthen network monitoring technology. As an emerging cloud computing-based storage technology, personal cloud storage inevitably faces data transmission risks. Providers should adopt enhanced network intrusion detection technology to ensure transmission channel security. Strengthening network monitoring prevents hackers from injecting malicious code/network malware, ensuring data transmission channel security. Additionally, providers should enhance cooperation with third-party network service providers to offer users stable and sufficient bandwidth resources. (3) Verify interfaces corresponding to different endpoint types and adopt Secure Sockets Layer (SSL) for protection; continuously improve cloud storage software, identify and fix software vulnerabilities, and continuously repair software logs and patches to ensure service interruption or data incompatibility issues do not occur after software updates and upgrades. (4) Improve user identity authentication and authorization technologies to effectively control risks of ille-

gal users stealing authorized user identities to improperly manipulate user data, and reduce service hijacking security incidents.

6.3 Innovation and Limitations

This study' s main innovation lies in constructing a scientific and complete indicator system for evaluating personal cloud storage service technical security risk and revealing key factors and their causal relationships in the risk factor system. Research limitations include: this study used a small sample survey. Future research could expand expert sample size and scope, such as surveying personal cloud storage service industry practitioners, to test conclusion robustness. This study only identified and analyzed key influencing factors of personal cloud storage service security risk from a technical security perspective. The next step will discuss personal cloud storage service security risk from management, policy, and legal dimensions to achieve a trinity assessment goal, enrich cloud computing security theoretical research, and provide more comprehensive practical recommendations for sustainable personal cloud storage service development.

References

[1] Hashizume K, Rosado D G, Fernández-Medina E, et al. An analysis of security issues for cloud computing[J]. Journal of internet services & applications, 2013, 4(1): 1-13.

[2] iMedia Consulting. 2016 China personal cloud drive industry research report[EB/OL]. [2018-07-05]. http://www.iimedia.cn/45865.html.

[3] ENISA. Cloud computing benefits, risks and recommendations for information security: cloud computing security risk assessment[EB/OL]. [2018-07-17]. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

[4] Zissis D, Lekkas D. Addressing cloud computing security issues[J]. Future generation computer systems, 2012, 28(3): 583-592.

[5] Singh A, Chatterjee K. Cloud security issues and challenges: a survey[J]. Journal of network & computer applications, 2017, 79(2): 88-115.

[6] Gartner Group. Assessing the security risks of cloud computing[EB/OL]. [2018-07-17]. https://www.gartner.com/doc/3535553/assessing-security-risks-cloud.

[7] CSA. 'The treacherous twelve' cloud computing top threats in 2016[EB/OL]. [2018-07-05]. https://www.prnewswire.com/news-releases/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016-300227806.html.

[8] Khan N, Al-Yasiri A. Identifying cloud security threats to strengthen cloud computing adoption framework[J]. Procedia computer science, 2016, 94: 485-490.

[9] Ramachandra G, Iftikhar M, Khan F A. A comprehensive survey on security in cloud computing[J]. Procedia computer science, 2017, 110: 465-472.

[10] Shameli-Sendi A, Cheriet M. Cloud computing: a risk assessment model[C]//IEEE International Conference on Cloud Engineering. Washington: IEEE, 2014: 147-152.

[11] Liu J, Guo Z. Research on cloud security risk assessment based on fuzzy entropy weight model[J]. Electronics, electronics, and computer science, 2016, 139: 390-395.

[12] Lin G T R, Lin C C, Chou C J, et al. Fuzzy modeling for information security management issues in cloud computing[J]. International journal of fuzzy systems, 2014, 16(4): 529-540.

[13] Lin F, Zeng W, Yang L, et al. Cloud computing system risk estimation and service selection approach based on cloud focus theory[J]. Neural computing and applications, 2017, 28(1): 1863-1876.

[14] ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services[EB/OL]. [2018-07-17]. https://www.iso.org/standard/43757.html.

[15] BSI Group. ISO/IEC 27017, Extending ISO/IEC 27001 into the Cloud[EB/OL]. [2018-07-17]. https://www.bsigroup.com/LocalFiles/EN-AU/_{Brochures}/ISO%2027017%20Whitepaper-JULY2016.pdf.

[16] FedRAMP. Security assessment framework[EB/OL]. [2018-07-17]. https://www.fedramp.gov/assets/resources/documents/FedRAMP_{{{Security}}}*{{Assessment}}*{Framewo

[17] Singapore MTCS. SS584(2016), Specification for multi-tiered cloud computing security[EB/OL]. [2018-07-17]. https://www.singaporestandardseshop.sg/Product/Product.aspx?id=88be0cea4-4a59-801d-9fcedbba88f.

[18] CSA. Security guidance for critical areas of focus in cloud computing V2.1[EB/OL]. [2018-07-17]. https://www.rationalsurvivability.com/blog/2009/12/cloud-security-alliance-v2-1-security-guidance-for-critical-areas-of-focus-in-cloud-computing-available/.

[19] ENISA. A guide to monitoring of security levels in cloud contracts[EB/OL]. [2018-07-17]. https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts.

[20] Shahzad F. State-of-the-art survey on cloud computing security challenges, approaches and solutions[J]. Procedia computer science, 2014, 37: 357-362.

[21] Shirvani M H, Rahmani A M, Sahafi A. An iterative mathematical decision model for cloud migration: a cost and security risk approach[J]. Software practice & experience, 2018, 48(6): 449-485.

[22] Mackay M, Baker T, Al-Yasiri A. Security-oriented cloud computing platform for critical infrastructures[J]. Computer law & security review, 2012, 28(6):

679-686.

[23] Kang W M, Dong-Lee J, Jeong Y S, et al. VCC-SSF: service-oriented security framework for vehicular cloud computing[J]. Sustainability, 2015, 7(2): 2028-2044.

[24] Walterbusch M, Fietz A, Teuteberg F. Missing cloud security awareness: investigating risk exposure in shadow IT[J]. International journal of information management, 2017, 30(4): 644-652.

[25] Jiang R, Yang M, Ma Z, et al. Cloud computing security risk measurement, assessment and management[M]. Beijing: Science Press, 2016.

[26] Coppolino L, D' Antonio S, Mazzeo G, et al. Cloud security: emerging threats and current solutions[J]. Computers & electrical engineering, 2017, 59: 126-140.

[27] Choi M, Lee C. Information security management as a bridge in cloud systems from private to public organizations[J]. Sustainability, 2015, 7(9): 12032-12051.

[28] Singh S, Jeong Y S, Park J H. A survey on cloud computing security: issues, threats, and solutions[J]. Journal of network & computer applications, 2016, 75(9): 200-222.

[29] Ruan S, Weng J, Mao H, et al. Cloud security risk assessment measurement model[J]. Journal of Shandong University: Natural Science Edition, 2018, 53(3): 71-76.

[30] Rong C, Nguyen S T, Jaatun M G. Beyond lightning: a survey on security challenges in cloud computing[J]. Computers & electrical engineering, 2013, 39(1): 47-54.

[31] Brender N, Markov I. Risk perception and risk management in cloud computing: results from a case study of Swiss companies[J]. International journal of information management, 2013, 33(5): 726-733.

[32] Lin R J. Using fuzzy dematel to evaluate the green supply chain management practice[J]. Journal of cleaner production, 2013, 40(7): 32-39.

[33] Opricovic S, Tzeng G H. Defuzzification within a multi-criteria decision model[J]. Uncertain fuzzy, 2003, 11(5): 635-652.

[34] Guest G, Bunce A, Johnson L. How many interviews are enough?: an experiment with data saturation and variability[J]. Field methods, 2006, 18(18): 59-82.

[35] Ghaffari K, Lagzian M. Exploring users' experiences of using personal cloud storage services: a phenomenological study[J]. Behaviour & information technology, 2018, 37(3): 295-312.

Author Contributions: Cheng Huiping: Proposed the research topic and core ideas, revised the paper; Peng Qi: Wrote and revised the initial draft.