Fuzzy Systems and Data Mining VI
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA200733

Construction of Cloud ERP Security Evaluation Index System Based on Text Mining

Ying GAO [a], Qin SU [a,1], Yue FANG [a]and Pinyan LAI [a]
[a] *School of Management, Xi'an Jiaotong University, Xi'an, China*

Abstract. The aim of this study is to investigate and discuss the potential security issues arising from the deployment of the Cloud Enterprise Resource Planning system, and to propose a perfect and standard set of security evaluation index system for Cloud ERP security issues. Considering the issues which may be inherent in the conventional Enterprise Resource Planning systems and new ones brought by Cloud Computing, Cloud Platform, Cloud ERP, we use text mining technology to mine the related standard files in this paper. Since the standard literature is based on the comprehensive results of technology, science and practice, its characteristics of standardization, objectivity and validity also ensure the effectiveness and applicability of indicators. By using NLP methods, we construct a Cloud ERP security evaluation index system consisting of five parts: evaluation method security, information access security, data security, management security and others. The entropy method is used to assign weights for the Cloud ERP security evaluation index system, which is more scientific and rational and the method moderates the lack of objectivity caused by traditional evaluation methods which over-relies on evaluators. By analyzing cases of Cloud ERP collected in various application reports and research papers, we improve our system and find that compared to other evaluation systems, our system can evaluate the security of Cloud ERP more comprehensively.

Keywords. Cloud ERP, security evaluation index, text mining

1. Introduction

With the development of Internet technology and digital information technology, as well as the higher requirements for data processing speed, cloud computing has come into. According to a survey in 2011, 43% of IT executives said they would use cloud services to replace current systems. Global Industry Analysts, a research firm, estimates the global market for cloud computing services is on the verge of reaching \$127 billion[1].

Cloud ERP introduces cloud computing to ERP software and makes it possible for enterprises to run ERP software on the cloud computing platform of suppliers, which further promotes the development of enterprises. With this technology, companies can safely provide services on a global scale, regardless of geographic location. This may address some of the risks and challenges of ERP, for example, it eliminates implementation

[1] Corresponding Author: No. 28, Xianning West Road, Xi'an, Shaanxi Province 710049, China. E-mail address: qinsu@mail.xjtu.edu.cn (Q. Su).

time and cost, reduces hardware investment and maintenance, and enhances security[2]. However, cloud computing also has security issues, including governance, data management, architecture, application, and assurance[3]. It will bring huge losses, if the cloud ERP system encounters problems such as confidentiality of important business data, loss of personal information, malicious attacks, etc.Therefore, it is very important to ensure the information security of ERP system. The current literature on cloud ERP only puts forward security as a problem, but does not clearly point out what the security problems of cloud ERP are. Due to the limited resources for cloud ERP security issues, this article analyzes the security standard literatures relating to traditional ERP system, cloud computing and cloud platform, uses text mining methods to extract the evaluation indicators from text databases, screens and improves the indicators through qualitative and quantitative analysis, and finally builds and tests the cloud ERP security standard evaluation indicator system.

On the theoretical level, this research adopts text mining based on cloud ERP security standard documents. On the one hand, it puts forward the important role of security standards in enterprise practice. On the other hand, the text mining method provides a certain objective basis for the establishment of cloud ERP evaluation system. On the practical level, the cloud ERP security evaluation system proposed in this study provides a certain sense of reference value for the security management practices of enterprises (ERP users) and suppliers. Through this evaluation system, enterprises can measure the cloud ERP security level more efficiently and conveniently, and put forward relevant measures and suggestions based on the specific evaluation results to improve the security management level of the cloud ERP system.

2. Related literature

Traditional ERP systems have limited capabilities in terms of multi-user access, performance and resource availability. The complex structure behind ERP has caused security problems and maintenance difficulties[4], so the traditional ERP has always focused on internal controls to limit user's behavior and privileges[5]. For example, faulty or incomplete access enforcement conditions can cause information resource access security problems[6].

Cyber security incidents or threats on China's cloud platforms have further intensified in the first half of 2019 compared to 2018, according to the Internet Security Situation in China in the first half of 2019[7]. At the same time, CNCERT also pointed out in the report that cloud service providers and cloud users should work together to improve the defense capability of cloud platform network security.

Data security and trust problems of users's lack of relying on the cloud to provide IT infrastructure are the priorities of cloud computing security research. For example, Feng[8] proposed cloud computing security standards and an assessment system with data security and privacy protection as the main target, security objectives verification and security service level evaluation as the core. Xu[9] classified the security framework of cloud computing platform based on data confidentiality, integrity, non-repudiation, availability and reliability.

3. Construction of cloud ERP security evaluation index system

3.1. Text sources

Standard literature has both the function of general scientific and technological literature and the legal effect to ensure that the products or services developed by different subjects can have the same quality. Therefore, in order to ensure the effectiveness and applicability of the indicators, a total of 39 standard literatures are adopted in this study, including national standards, industry/local standards and international standards. The standard literatures are all from the official website of ISO and the Open Standards Website of China. See appendix for details.

3.2. Text preprocessing

Since the original file format is an image-type PDF, the file format needs to be converted firstly to facilitate text analysis. 39 PDF standard literatures in picture format are extracted by Python. And then the API interface of picture and text recognition in Baidu intelligent cloud platform is used to extract all the words in each picture. Finally a TXT format text file of each standard literautre is obtained.

In order to better identify the keywords of the whole text, we extract all the headings of the text, including the first level headings and sub-headings of other levels.

3.3. Natural language processing

3.3.1. Chinese word segmentation

The precise mode of PythonâĂŹs jieba library[10] is used to segment the text, at the same time, some special words are imported to the custom dictionary and refer to it when we are doing the word segmentation. In this paper, both the standard full-text text and the standard title text are divided. The standard full-text refers to a text file summarizing the content of all standard literatures, while the standard title text refers to a text file summarizing the title part of all standard literatures.

3.3.2. Word frequency statistics

The word frequency of each word after word segmentation is counted, and the word with higher word frequency is found as our keyword, because the higher frequency a word appears in the text, the better it can reflect the central content of the text. At the same time, we also need to remove some stop words. Finally, the top 30 words of standard full-text and standard title frequency are selected respectively, as shown in table 1.

3.3.3. Keyword filtering

After counting the top 30 words in the frequency of standard full-text text and standard title text respectively,taking its 23 common words as our text keywords.

TF-IDF is a commonly used weighting technique for text mining and information retrieval, which is used to evaluate the importance of words to one of the documents in the file base. In order to filter out the keywords with a high degree of differentiation, this study calculates the IDF value of all keywords, and sorts them from small to large.

Table 1. Word frequency statistics

Word frequency of title (30)				Word frequency of text (30)			
evaluation	925	control	78	security	4320	platform	1244
requirement	858	access control	69	requirement	3448	user	1211
method	704	technology	68	certificate	2510	strategy	1166
security	525	information assurance	67	service	2090	visit	1112
management	231	identify	67	data	1884	property	1111
certificate	151	user	64	cloud service	1814	personnel	1083
data	140	protection	64	information	1767	document	1070
information	132	environment	64	system	1740	audit	1044
service	117	visit	62	evaluation	1589	function	1043
audit	115	platform	61	management	1486	extension	1043
extension	112	strategy	61	cloud-computing	1474	public key	1007
cloud service	111	test	59	client	1450	resource	997
resource	104	client	56	check	1432	method	979
cloud-computing	101	function	55	cloud service providers	1406	business	949
property	96	system	53	component	1375	technology	923

The results are shown in Table 2. Words with IDF value less than 0.05 are selected as the final keywords. Finally, a total of 15 keywords are selected, namely security, management, information, user, technology, requirement, data, system, access, evaluation, service, function, audit, method and cloud computing.

Table 2. IDF value of keywords

IDF value					
security	0	access	0.011899	strategy	0.07684
management	0	evaluation	0.024134	paltform	0.09108
information	0	service	0.024134	cloud service	0.105804
user	0	function	0.024134	customer	0.18799
technology	0	audit	0.036723	extension	0.18799
requirement	0.011899	method	0.049688	property	0.422074
data	0.011899	cloud computing	0.049688	certificate	0.526809
system	0.011899	resource	0.063052		

3.4. Indicators extraction

3.4.1. Clustering analysis

In order to further analyze and classify keywords, keywords need to be quantified. In this paper, TF value is taken as the quantized data of keywords, and TF value of each keyword in each standard is calculated and normalized. Then, the quantified data are imported into SPSS, and the Pearson correlation is used as the measurement standard of the interval for systematic clustering analysis of the data.

At the distance of 20, 15 keywords can be divided into five groups. In view of the common characteristics of each group of keywords, the common characteristics of each group are summarized to form the first-level index of the cloud ERP security evaluation index system. The first group is the security of evaluation method; the second group is information security; the third group is data security; the fourth group is management security and the fifth group is other security.

3.4.2. *Analysis of paragraph contribution*

After the construction of the first-level index, this paper adopts the method of piecewise review of the text, gives priority to the extraction of the second-level index and the third-level index from the important, valuable and highly relevant paragraphs, so as to improve the accuracy of the index extraction.

Firstly, each standard literature is divided into paragraphs according to its first-level title to form several paragraphs-ending documents. Then the contribution of keywords is calculated for each paragraph. Each paragraph has 15 contribution values. The calculation method of contribution degree is keyword word frequency multiplied by keyword position weight. When a keyword appears in a first-level title, other levels or the text, a position weight of 10,5,1 is assigned respectively.

According to the previous literatures [11,12,13], we find that for convenience of users' practical construction, usually they are willing to have different levels for management concern. So we construct an evaluation system consisting of 5 first-level indexes, 21 second-level indexes and 105 third-level indexes.

4. Index weight

Due to the limitation of subjective weighting method and objective condition limitation, entropy value method is used to assign weights to each index in this study. We extract the keywords of the third-level index included in n=21 second-level index from m=39 standard literatures. Matrix is obtained by text mining.

(1)Standardize the data: $x'_{ij} = \frac{x_{ij}-\min\{x_{1j},\dots,x_{nj}\}}{\max\{x_{1j},\dots,x_{nj}\}-\min\{x_{1j},\dots,x_{nj}\}}$

(2)Quantify the indicators in the same degree, the proportion of the i_{th} sample value of the j_{th} index in this index:
$\mathbf{p}_{ij} = \frac{x_{ij}}{\sum_{i=1}^{n} x_{ij}}, i = 1,\dots,\mathrm{n} \quad \mathrm{j} = 1,\dots,\mathrm{m}$

(3) The entropy value of the j_{th} index:
$e_j = -k\sum_{i=1}^{n} p_{ij} \ln(p_{ij}), j = 1,\dots,\mathrm{m} \quad k = \frac{1}{\ln(n)} > 1$

(4)The coefficient of difference of the j_{th} index: $d_j = 1 - e_j, \quad j = 1,\dots,m$

(5)The weight of each index: $\mathrm{w}_j = \frac{d_j}{\sum_{j=1}^{m} d_j}, \quad \mathrm{j} = 1,\dots,\mathrm{m}$

5. The empirical analysis

5.1. *Data collection*

In this paper, security-related contents in various cloud ERP software application reports and research papers on cloud ERP are collected at home and aboard. In order to improve the accuracy of data extraction and reduce the deviation caused by subjective factors, the Delphi method[14] is adopted to consult the selected expert group members for investigation and 68 pieces of security data are finally summarized.

Through the case data segmentation and word frequency statistics, as shown in Table 3, we find that data, management, access, personnel security and other words are more important. This is also consistent with our index system.

Table 3. word frequency statistics

data	43	information	10	record	7	document	6
user	27	application	10	management	7	staff	6
system	21	service	10	backups	7	specific	6
access	21	authorization	9	client	6	event	5
security	14	organization	8	business	6	segregation	5
ERP	12	organization	8	storage	6	sensitivity	5
permission	10	log	8	law	6	supplier	5

5.2. Case evaluation

According to the cloud ERP security evaluation index system proposed in this paper and the weight of each index obtained by entropy method, the security evaluation score of this case is calculated as 46.7. In order to verify the effectiveness of the security evaluation index system, we adopt another cloud computing security evaluation model[13] for appraisement. This model is based on the evaluation requirements of information security level protection in China. And the security evaluation score of this case is 44.6.

The calculation shows that the evaluation model proposed in this paper has completed the quantification of the security level of the cloud ERP security example, and the evaluation result is consistent with the comprehensive conclusion obtained through the evaluation of the other schemes, what proves the feasibility and effectiveness of the evaluation system to a large extent.

5.3. Perfection of the system

Through case evaluation and comparison with cloud computing security evaluation model[13], we further improve the index system accordingly, and finally obtain a quantifiable cloud ERP security three-level evaluation index system, as shown in Table 4.

6. Conclusion

In this paper, based on the method of text mining, we have realized the representativeness and objectivity of index extraction, and obtained the specific and applicable cloud ERP security evaluation index. On the one hand, it affirms the significance and value of the standard literature, on the other hand, it provides relevant supporting basis for the extraction of evaluation index.

Compared with the traditional ERP security evaluation system[5,6,15,16],the characteristics of multi-tenancy and scalable of cloud ERP determine that the cloud ERP

Table 4. Cloud ERP security evaluation index system

First-level index	Second-level index	Third-level index
A1. Evaluation method security (0.2055)	B1. Evaluation method (0.1062)	whether the evaluation method is objective and impartial
		whether the evaluation method is reusable
		whether the evaluation method is flexible
		Whether the evaluation method has little impact on it operation
	B2. Evaluation results (0.066)	Whether the evaluation method includes interview, examination, etc
		Whether the evaluation results are reproducible
		whether the evaluation results are supported by evidence
	B3. Evaluation organization 0.0333	whether the evaluation organization has a high level of confidentiality
A2. Information access security (0.1043)	B4. Resource access control (0.0365)	Whether the information flow control strategy is established
		Whether to have a remote access policy
		Whether there is an identification strategy
		Whether to use technical measures to restrict the address range of the access terminal
	B5. Resource access authorization (0.0387)	Whether access to information resources conforms to the minimum authorization principle
		Whether access to information resources conforms to the separation of duties principle
		Whether there is an authentication authorization verification mechanism
	B6. Information security incidentsn (0.0291)	Whether all userâĂŹs information can be protected
		Whether to provide corresponding strength security protection for different types of information
		Whether it can respond to information security incidents quickly, effectively and orderly
		Whether there is a documented procedure consistent with information security incident response
		Whether there is a document that provides users with the relevant information security events
		Whether it can monitor and warn information security events in real time
A3. Data security (0.3294)	B7. Data transmission (0.0405)	Whether to take effective measures to guarantee the confidentiality of data transmission process
		Whether to take effective measures to ensure the integrity of the data transmission process
		Whether it can detect the data transmission process is damaging and take recovery measures
		Whether effective measures can be taken to prevent electromagnetic leakage of data transmission medium
		Whether the reliability of transmission network can be guaranteed
	B8. Data storage (0.0314)	Whether effective measures are taken to safeguard the confidentiality of data stored procedures
		Whether effective measures are taken to ensure the integrity of data stored procedures
		Whether to provide an effective virtual machine image file loading protection mechanism
		Whether data with different security levels is stored in different Spaces
		Whether an effective method of disk protection or data fragmentation storage is provided
		Whether to take effective measures to ensure the environmental security of data storage equipment and media
	B9. Data usage (0.06)	Whether data usage is authorized and validated
		Whether the use of sensitive data is audited and an audit log is formed
	B10. Data backup and recovery (0.0434)	Whether to provide data backup and restore function
		Whether automatic and manual backup of data is supported
		Whether to support local and remote backup of data
		Whether there is a disaster recovery policy
		Whether there is a disaster backup and recovery center
	B11. Data isolation (0.0444)	Whether to take effective measures to isolate data from different users
		Whether to take effective measures to isolate different business application data
		Whether to take effective measures to isolate different levels of security data
		Whether to partition different data security domains
	B12. Data migration(0.0472)	Whether it can ensure that data migration does not affect business continuity
		Whether to establish a data migration plan
		Whether to establish a risk control strategy for data migration
		Whether to use a distributed migration strategy
		Whether to monitor the data migration
		Whether there are effective measures to guarantee the confidentiality of the data migration process
		Whether there are effective measures in place to ensure the integrity of the data migration process
		Whether there are measures for data backup and recovery during data migration
	B13. Data disposal (0.0625)	Whether it can clear all legacy data and data copies
		Whether to take effective measures to prohibit the recovery of destroyed data
		Whether data destruction generates appropriate logging
		Whether is it possible to ensure that all data is completely cleared before the storage space is reallocated
		Whether the storage device or media should be cleaned up before being discarded
A4. Management security (0.182)	B14. Security management policy (0.0582)	Whether there is the daily management procedure
		Whether there is a comprehensive information security management system
		Whether to check and revise the safety management system regularly
		Whether the security management system is issued in a formal and effective manner
		Whether to establish safety management system for all kinds of management contents in safety management activities
	B15. Personnel management (0.0518)	Whether to establish a functional department of information security management
		Whether to set up a leading group to manage information security work
		Whether the responsibilities of each department and position of the safety management organization are clearly defined
		Whether to conduct regular safety review and skill assessment for personnel
		Whether to provide safety awareness education and relevant training to personnel regularly
		Whether the safety education and training are documented
	B16. System management (0.0276)	Whether there is a clear system boundary and security protection level
		Whether to select basic security measures according to the security protection level of the system
		Whether there is a master plan for information security construction
		Whether it can grade the system regularly
		Whether the rating is evaluated in time when the system changes
		Whether to maintain the system according to the operation manual
	B17. Operations management (0.0444)	Whether to establish the asset safety management system
		Whether to establish media safety management system
		Whether to establish supporting facilities, software and hardware maintenance management system
		Whether each device has a detailed operation log
		Whether to establish network security management system
		Whether the network system is regularly scanned for vulnerabilities
		Whether to exercise the emergency plan on a regular basis
		Whether to assess the potential risk to the machine room
		Whether to implement strict access control to the machine room
		Whether to maintain and manage the machine room facilities regularly
		Whether it can provide enough space and capacity to meet the needs of facility expansion
		Whether it can reasonably divide the physical area of the computer room and arrange the information system components
		Whether the data use and system management meet the requirements of local laws and regulations

A5. Others (0.1788)	B18. Network security (0.0402)	Whether to draw the network topology diagram that is consistent with the current operation
		Whether the business processing capacity of key network equipment is guaranteed to have redundant space
		Whether there are different subnets, segments, or security groups
		Whether to deploy access control devices at network or segment boundaries
		Whether to limit the maximum number of network traffic and network connections
		Whether the network boundary can be realized inspection
	B19. Host security (0.0463)	Whether each group of hosts has implemented the security protection system
		Whether to monitor important servers
		Whether to install anti-malicious code software
		Whether the security audit can cover every operating system user and database user
		Whether the operating system can follow minimum installation principles
	B20. Application security (0.051)	Whether it can severely restrict user access to the application
		Whether the permissions for applications to call each other are strictly limited
		Whether the audit scope covers significant events in the user's application
	B21. Virtualized security (0.0413)	Whether isolation between virtual machines is supported
		Whether it has the ability to identify and deal with malicious attacks on the virtual machine
		Whether to provide a virtual network structure map that matches the current health
		Whether virtual network critical logs are monitored and audited
		Whether to monitor the virtual machine's running state, resource occupancy and other information
		Whether it has the ability to spot vulnerabilities in the virtualization platform

evaluation system constructed in this paper pays more attention to user authentication and access control security in the cloud environment, such as data isolation, data backup and data recovery. Compared with the cloud computing security evaluation index system[13,17], the cloud ERP system designed in this paper focuses on physical security, namely the security of the storage media data center, such as the security of the computer room, on the basis of virtual security.

In short, this cloud ERP security evaluation index system not only provides theoretical reference for cloud ERP security evaluation and directions for strengthening cloud ERP security, but also provides method reference for the practical application of text mining technology in the evaluation.

In further research, we will modify the index system, so that the evaluation system can be adjusted continuously as the cloud ERP software structure and application changes, and enhance the automation function of the evaluation proces.

7. Acknowledgement

The work was funded by the National Key R &D Program of China (No. 2019YFB1704103).

References

[1] Trend Micro. Despite security concerns, businesses moving to the cloud(Op/Ed). https://blog.trendmicro.com/despite-security-concerns-businesses-moving-to-the-cloud/. November 30,2011.

[2] Torbacki, Witold. SaaS–direction of technology development in ERP/MRP systems. Archives of Materials Science and Engineering.2008(32).

[3] II John, Alhamdani Wasim. Who can you trust in the cloud? A review of security issues within cloud computing. Proceedings of the 2011 Information Security Curriculum Development Conference.2011(9).

[4] Brehm Nico, Gómez Jorge. Secure Web service-based resource sharing in ERP Networks. Journal of Information Privacy and Security.2005(1):29-48.

[5] Shen Shen. ERP Security Status and Solutions [J]. Network Security Technology and Application.2005(05):16-17.

[6] Elisabeth J Umble, Ronald R Haft, M.Michael Umble,Enterprise resource planning: Implementation procedures and critical success factors.European Journal of Operational Research.2003(146):241-257.

[7] National Internet Emergency Response Center. China's Internet Network Security Situation in the First Half of 2019.August 13, 2019.

[8] Feng Dengguo, Zhang Min, Zhang Yan, Xu Zhen. Research on cloud computing security [J].Journal of software.2011(22):71-83.

[9] Xu Xiaoping. The Application of trusted Computing Technology in Cloud Computing Security [J]. Computer Nerd.2016(01):26-27.

[10] https://pypi.org/project/jieba.

[11] Yang Aimin, Gao Fang, Bian Minhua, Yang Shulei. Cloud computing security evaluation and countermeasure based on AHP-fuzzy comprehensive evaluation[J]. Journal on Communications.2016,(37):104-110.

[12] Zheng Jinghua, Li Kun, Zhao Yonggang. Research on cloud system security evaluation index [J]. Shandong Industrial Technology.2015(09):188-189.

[13] Jiang Zhengwei, Zhao Wenrui, Liu Yu, Liu Baoxu. Cloud computing security assessment model based on hierarchical protection [J]. Computer science.2013(40):151-156.

[14] https://en.wikipedia.org/wiki/Delphi-method.

[15] Cheng Naiwei. Study on Safety Risk Assessment Methods of ERP Systems [A]. Proceedings of 2010(Shenyang) International Colloquium on Safety Science and Technology[C].Northeastern University: Center for Safety Engineering, Northeastern University,2010(4):50-53.

[16] Zheng Ziqiu, Zhang Weidong, Liu Ning, Fu Qiuxuan, Yin Xingkang, He Hongmei. Application of Information Security Technology in enterprise ERP system [J]. Science and Technology Innovation and Application.2019(18):174-176.

[17] Sengupta Shubhashis, Kaulgud Vikrant,Sharma Vibhu Saujanya. Cloud Computing Security–Trends and Research Directions. Proceedings - 2011 IEEE World Congress on Services, SERVICES 2011(20):524-531.

Appendix

	Standard number	Standard name
1	ISO/IEC 19086-4:2019	Cloud computing-Service level agreement (SLA) framework-Part 4: Components of security and of protection of PII
2	ISO/IEC 27009:2016	Information technology-Security techniques-Sector-specific application of ISO/IEC 27001-Requirements
3	ISO/IEC 27017:2015	Information technology-Security techniques-Code of practice for information security controls based on ISO/IEC 27002 for cloud services
4	ISO/IEC 27018:2019	Information technology-Security techniques-Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
5	ISO/IEC 27036-4:2016	Information technology-Security techniques-Information security for supplier relationships-Part 4: Guidelines for security of cloud services
6	ISO/IEC TR 23186:2018	Information technology-Cloud computing-Framework of trust for processing of multi-sourced data
7	ISO/IEC 9594-8:2017	Information technology-Open Systems Interconnection-The Directory-Part 8: Public-key and attribute certificate frameworks
8	ISO 22381:2018	Security and resilience-Authenticity, integrity and trust for products and documents-Guidelines for establishing interoperability among object identification systems to deter counterfeiting and illicit trade
9	GA/T 1345-2017	Information security technology-Security technical requirements for cloud computing network intrusion prevention system
10	GA/T 1346-2-17	Information security technology-Security technical requirements forcloud operating system
11	GA/T 1347-2017	Information security technology-Security technical requirements for cloud storage system
12	GA/T 1348-2017	Information security technology-Security technical requirements for desktop cloud system
13	GA/T 1390.2-2017	Information security technology-General requirements for classified protection of cyber security-Part 2: Special security requirements for cloud computing
14	GA/T 1527-2018	Information security technology-Security technical requirements for cloud computing security comprehensive defense products
15	GB/T 31167-2014	Information security technology-Security guide of cloud computing services
16	GB/T 31168-2014	Information security technology-Security capability requirements of cloud computing services
17	GB/T 34080.1-2017	Security specifications of electronic government common platform based on cloud computing-Part 1: General requirements
18	GB/T 34080.2-2017	Security specification of electronic government common platform based on cloud computing-Part 2: Information resources security
19	GB/T 34942-2017	Information security technology-The assessment method for security capability of cloud computing service
20	GB/T 34982-2017	Cloud computing data center basic requirement
21	GB/T 35279-2017	Information security technology-Security reference architecture of cloud computing
22	GB/T 35301-2017	Information technology-Cloud computing-Platform as Service(PaaSïijL'reference architecture
23	GB/T 36326-2018	Information technology-Cloud computing-General operational requirements of cloud service
24	GB/T 37739-2019	Information technology-Cloud computing-Platform as a service deployment requirments
25	GB/T 37740-2019	Information technology-Cloud computing-Guide for application and data migration between cloud platforms
26	GB/T 37950-2019	Information security technology-Security technical requirements for desktop cloud
27	GB/T 37956-2019	Information security technology-Technology requirement for website security cloud protection platform
28	GB/T 37972-2019	Information security technology-Operation supervision framework of cloud computing service
29	GB/T 38249-2019	Information security technology-Security guide of cloud computing services for government website
30	GB/T 26327-2010	Implementation guide for enterprise informationization system integration
31	DB13/T 3000-2019	Information security technology-E-government cloud security protection technology and management norms
32	DB37/T 3304-2018	Information security technology-Cloud computing operation and maintenance security management specifications
33	DB44/T 1342-2014	Information security technology-Cloud computing operation and maintenance security management specifications
34	JR/T 0167-2018	Information security technology-Cloud computing operation and maintenance security management specifications
35	SJ/T11293âĂŤ2003	Technical specifications for enterprise informatization-Part 1: Enterprise resource Planning system (ERP) specifications
36	YDB 156-2015	Security baseline requirement of cloud computing
37	YD/T 3148-2016	Security framework for cloud computing
38	YD/T 3157-2016	Security protection requirements for public cloud service
39	YD/T 3158-2016	Security protection test requirements for public cloud service