Security Concerns in Cloud Computing for Knowledge Management Systems

Thanyatida Gunadham[1] and Pramote Kuacharoen[2]

[1]Martin de Tours School of Management and Economics, Assumption University of Thailand, Bangkok, Thailand
thanyatidagnd@msme.au.edu
[2]School of Applied Statistics, National Institute of Development Administration, Bangkok, Thailand
pramote@as.nida.ac.th

Abstract. This study discusses major security issues and concerns related to cloud computing environment in regard to knowledge management system processes such as knowledge creation, refining, storing, sharing, and utilization. This study uses the exploratory approach to address major security concerns and whether they need consideration for each knowledge management process. The result of this study reveals main cloud computing security concerns such as data security and confidentiality issues, access controls, data loss or leakage prevention, cyber-attacks, availability and reliability issues, and browser security and analyzes these security concerns from knowledge management systems' point of view. Also, solutions and recommendations for security concerns are discussed to provide guidance for the organization initiating cloud-based knowledge management systems.

Keywords: security, cloud computing, knowledge management system

1. Introduction

Nowadays businesses and organizations are taking cloud computing adoption into consideration because of high cost saving, high speed internet availability, and high performance of web browser. People believe that these benefits would be able to support and improve organizational processes. Knowledge Management Systems (KMS) like other systems would benefits from cloud computing as well; therefore, many organizations attempting to utilize cloud computing to support KMS are now overwhelmed with a number of issues related to cloud computing especially security issues. This paper discusses the leading security issues related to a cloud environment and specifies the most critical cloud computing security issues which must be considered when implementing KMS by considering knowledge management processes such as knowledge creation, refining, storing, sharing, and utilization. In addition, some solutions and recommendations against these security concerns are introduced to assist the enterprises aiming to implement cloud-based KMS.

2. Literature Review

2.1 Cloud Computing Models

Cloud computing refers to the use of hardware and software resources to provide them to users either on the Internet or an organization's internal network [1]. Cloud computing is scalable and flexible as it simply enables capacity increase or supplementary capabilities addition without the need for high cost investments such as new infrastructure, new personnel training, or more software service licenses.

Normally, cloud services have three delivery models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Each service model has different objectives and targets different customers. SaaS is similar to application service provider (ASP) where the customer uses an application from the cloud providers via the Internet [2]. However, the customer does not control the operating system, hardware, or network infrastructure which supports the application. For PaaS, the customer uses a hosting environment for their applications and controls the applications running in the environment. In some cases, the customer has some control over the hosting environment but does not control the operating system, hardware, or network infrastructure supporting the application. Therefore, the platform is usually regarded as an application framework. IaaS provides computing resources such as processing power, storage, networking components or middleware for the customer. The operating system, storage, deployed applications and perhaps networking components can be controlled by the customer. However, the customer does not control the cloud infrastructure underneath them.

There are four types of cloud computing deployment models, namely, public cloud, private cloud, community cloud, and hybrid cloud. Public cloud refers to model of cloud whose infrastructure is hosted at vendor's premises, available on the Internet, and accessible via web browser [3]. The capital expenses are reduced due to cost distribution and sharing among individuals and businesses. On the other hand, private cloud is the model whose infrastructure is setup for a specific organization and within an organization's internal datacenter. Two types of private clouds are on-premise private clouds and externally hosted private clouds. Externally hosted private clouds are generally cheaper than on-premise private clouds because cloud infrastructure is hosted by a professional third party. A company with strict control over a unique product or service typically uses the private cloud. A private cloud existed within a shared or public cloud is known as a Virtual Private Cloud (VPC) which only allows connection over a virtual private network such as IPsec. Community cloud occurs when the organizations with similar interests and requirements share the cloud infrastructure which can be managed internally and hosted within the organization or by a third party and hosted externally. A community cloud has medium costs due to costs sharing among fewer users than a public cloud. Lastly, a combination of two or more clouds (public, private, or community) called hybrid cloud, benefits individuals and organizations from multiple deployment models. Both on-premises resources and off-site (remote) server based cloud infrastructure are required for Hybrid Cloud architecture. Having lack of security and certainty of in-house applications, Hybrid clouds are still flexible and scalable. For example, the organization can host critical applications with highly sensitive information on private clouds and less security concerned applications with less sensitive data on public clouds [4]. As a result of these advantages, hybrid cloud is becoming popular among modern businesses that have various requirements.

2.2 Security Concerns in Cloud Computing

Several concerns for organizations considering to adopt cloud computing is security, performance, and availability. Among these concerns, security issues seem to be main cloud computing concern [5]. Due to the considerable resources of cloud providers, many experts believe that security in a cloud environment is more robust than one in an in-house environment. However, hybrid cloud solutions offered by many cloud providers today allow the clients to have some control over the security of their data. Security and privacy issues also depend on the sector of the business; for example, the integrity and privacy of customers' data is critical for the banking sector so a cloud service such as IaaS appears to be unsecure and incompatible with the security requirements. According to Alqahtani and Sant [6], the level of challenges and threats of cloud computing security is classified into trust, access, Internet, software, computation, and virtualization. Computation and access level are the majority of the identified challenges which account for approximately 51%. The identified challenges regarding the computation issues are: sanitization, malware, cryptography, and storage. The customers have concern about the concept of outsourcing data storage because of the customers' desire to know their data location, procedure in storing data, and data access control. For the access level, the issues of authentication and physical access are a concern. The user ID and password are normally used to authenticate the user's identity by cloud service providers. Several password techniques exist but the most common one is a simple text password which cannot achieve the required level of authentication.

Data security and confidentiality issues are also a primary security concern in cloud computing because data could be exposed to unauthorized persons. This case often occurs when the data owner is inside the organization and the data provider is outside. Cryptographic protection mechanisms such as encryption or hashing are used to protect data. It is also argued that a lack of control over the physical infrastructure, especially relating to who controls and monitors the data center in the cloud, is the main security and privacy issue in cloud computing [2]. Data security lifecycle relates to problems such as who can create, access, and modify data, where the data is stored, how the back-up is done, or how the data is transferred, etc [3]. This lifecycle in a cloud environment is much more complex and lead to higher security risks because it is difficult for the cloud customer to effectively check that the data is handled properly. Therefore, more careful management is necessary. Strategies such as data encryption, particular public key infrastructure, data distribution, standardization of APIs, etc. are recommended as security measures to counter those risks and thus create a trusted and secure environment.

Access control is the most important security concern in cloud computing apart from confidentiality issues. This issue is mostly concerned especially when a public cloud hosts applications and data since multiple individuals or businesses are supported by a cloud [1]. In a shared hosted cloud, if an application has been breached, it could cause the breach of other applications using the same pool of resources as well. Another concern is while the data in the shared pool of resources can be leaked to unauthorized parties that have access to the same infrastructural components. Therefore, cloud customers need to verify that the cloud provider has the ability to dispose data securely to prevent data loss or leakage.

Moreover, a cloud environment is vulnerable to cyber-attacks such as malicious insiders, XML signature element wrapping, and cloud malware injection attack. A person motivated to create a bad impact on the organization’s mission and take action that compromises information confidentiality, integrity, and availability is known as a malicious insider [3]. The confidentiality, integrity and availability of data and services with impact on the internal activities, customer’s trust, and organization’s reputation could be compromised by the malicious activities of an insider. It is particularly high-risk of malicious insider occurrence in cloud computing environment because cloud architectures require certain roles such as cloud administrators, cloud auditors, and cloud security personnel. However, it is still wise to invest company’s long-term employees with higher trust although trusted employees can make mistakes or commit fraud.

XML signature element wrapping is a well-known web service attack while an attacker manipulates a SOAP message by copying the target element and inserting any value and moving the original element to other positions on the SOAP message [7]. The malicious message created from this attack will be finally processed by the Web services. For example, an attacker might intercept the SOAP message from e-mail web service application and alters the receiver’s e-mail address to that of the attacker, the web service will then forward the e-mail to the attacker. Normally, WS-Security uses XML signature to protect an element’s name, attributes and value from unauthorized parties but not the positions in the document. The possible countermeasure is to use a combination of WS-Security with XML signature to sign particular element and digital certificated such as X.509 issued by trusted Certificate Authorities (CAs). Also, a list of elements used in the system should be created and maintained at the web server side in order to reject unexpected messages from clients.

Another attack attempting to inject a malicious service, application, or even virtual machine into the cloud system is regarded as cloud malware injection attack [7]. An attacker creates his own malicious application, service or virtual machine instance; add it to the cloud system; and tricks the cloud system to treat the malicious application as a valid instance. Once normal users request the malicious service instance, the malice is executed successfully. Apart from this, a virus or trojan program may be uploaded to the cloud system by an attacker and once treated as a valid service; the virus program is automatically executed. The infected cloud system can damage the hardware of the cloud system and may affect the other cloud instances that run on the same hardware. Virus programs can also be used to attack other users on the cloud system as the cloud system can send the virus to any client via the Internet. Once the virus executes on the client’s machine, the client’s computer becomes infected. To control this attack, the cloud system need to perform a service instance integrity check for incoming requests by comparing the hash value of the original service instance image with that of all new service instance images. Consequently, if an attacker attempts to trick the cloud system and inject a malicious instance into the cloud system, the attacker needs to create a valid hash value comparison.

Furthermore, availability and reliability issues are discussed. In general, the cloud system provides dynamically scalable resources which benefit in the term of variability in usage. Cloud system automatically scale up by starting up new service instances when receiving more requests from the clients. This characteristic can be highly vulnerable for flooding attack such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks which the attacker makes a multitude of requests to a certain service. A DoS attack to a cloud system is realized as extra requests so the cloud system will attempt to provide more computational resources and finally consume all of the resources. Thus, the system is unable to provide services for normal requests from users. However, some people argue that DoS and DDoS attacks cannot cause substantial damage in the cloud due to the distribution of the processing load [1]. To reduce the attack surface, the centralization of cloud services may be introduced but this may cause a single point of failure. Referring to the example of Gmail disruption in April 2012 while Gmail services were unavailable for almost one hour, the company admitted that the disruption affected 10% of their customers which is equal to approximately 35 million users [3]. Due to the effect of this kind of outage on large numbers of customers, IT decision makers might assess the possibility of using desktop functionality instead of the functionality offered by the cloud. Also, cloud providers have set high standards in terms of reliability which are actually difficult to achieve in an internal environment. Some high level quality services set by the leading cloud providers may come at higher costs for the clients and occasionally the decision makers would decide to pay for the cheaper services. In addition, uncertainty of service availability and reliability, specifically unexpected system downtime and disruption, can increase project and business risks hence preventing companies from adopting cloud computing.

Another important aspect is browser security as web browser is a common method the client uses to connect to the cloud systems. Nowadays, browsers rely heavily upon SSL/TLS process and are unable to apply WS-Security concept including XML Signature and XML Encryption to the authentication process [7]. A web browser when requesting a service from the web service in a cloud system cannot use XML Signature to sign the client's credentials for client authentication and XML Encryption to encrypt the SOAP message for data protection from unauthorized parties. Instead, the web browser uses SSL/TLS to encrypt the credential and use SSL/TLS 4-way handshake process for client authentication. SSL/TLS has the limitation in its capacities in an authentication for cloud computing because SSL/TLS only supports point-to-point communications. Having a middle tier between the client and the cloud server such as a proxy server or firewall, with SSL/TLS the data need to be decrypted on the intermediary host. An attacker can sniff packages on that host, retrieve the credentials, and use them to access the cloud system as a valid user. Besides, in July 2009 Marlinspike used the technique called "null prefix attack" to break SSL/TLS by performing undetected man-in-the-middle attacks against SSL/TLS implementation. With this technique, attackers are able to request services from cloud systems without a valid authentication. The possible countermeasure is that the vendors apply WS-Security concept with their web browsers. WS-Security works at message level so web browsers are able to use XML Encryption to provide end-to-end encryption in SOAP messages without decryption at intermediary hosts. The attackers therefore cannot sniff and obtain plain text of SOAP messages at the intermediary hosts. This is why WS-Security is more suitable than SSL/TLS.

2.3 Knowledge Management Systems

A knowledge management system is defined as information systems designed specifically to facilitate the classification, collection, integration, and distribution of organizational knowledge [8]. With KMS, the organizations are able to respond more timely to changing market conditions and improve decision making and productivity. To maximize the value of the knowledge assets within organizations, KMS is utilized to support the integrated knowledge management process. Using Web 2.0 technologies, KMS primarily focuses on knowledge collection in a centralized repository and knowledge integration and collaboration within communities of practice [9]. Regarding KMS deployment, several managers concerning technological issues such as technical infrastructure and the security of data on the Internet. According to the survey by Singh [8] regarding technologies being used in KMS development, 90% of the organizations use browser tools to display and distribute knowledge in organizations on the Internet. Electronic mail and search/retrieval tools are the other two most common tools. In general, KMS requires a variety of technological tools in database and database management, communication and messaging, and browsing and retrieval. With the emergence of cloud computing, organizations are considering to use cloud services to support various applications including KMS. The availability and immediacy of cloud based KM application empowers users to expand their IT environment. The cloud service providers control KM content applications such as knowledge creating, refining, storing, using, and sharing and make them available to users upon requests [10]. None of these mentioned literatures ever discussed cloud computing security concerns in terms of knowledge management processes before. Therefore, this paper discusses security concerns from KMS's point of view by considering KMS processes including knowledge creation, refining, storing, sharing, and utilization. Also, certain related solutions and recommendations are presented to provide guidance for businesses that need to adopt cloud services to support KMS.

3. Discussion

3.1 Security Concerns for Knowledge Management Systems

The model of cloud-based KM application surrounded by security concerns is illustrated in Figure1 and the analysis of cloud computing security concerns in each of knowledge management process including knowledge creation, refining, storing, sharing, and utilization is specified in Table 1.

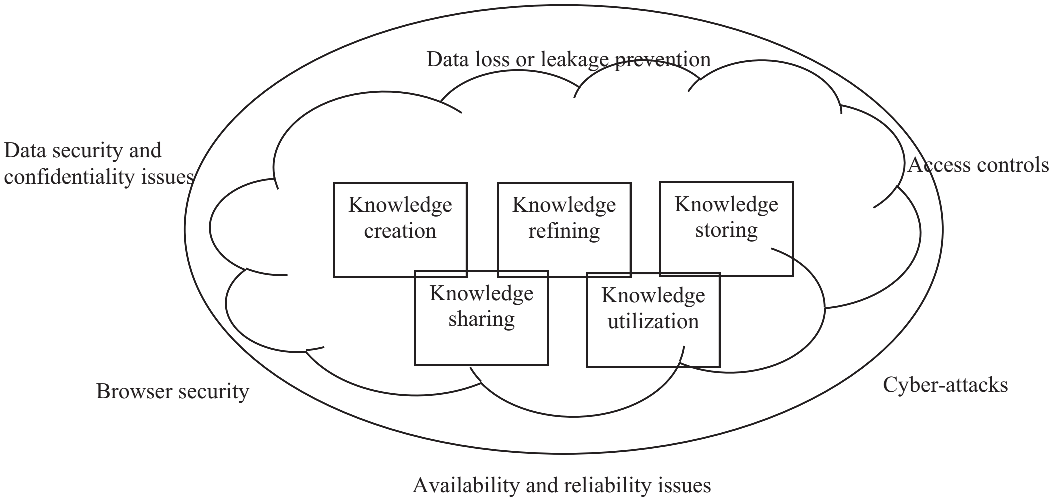

Figure 1: Cloud-based KM Application Surrounded by Security Concerns

From Table 1, data security and confidentiality issues (No.1) are related to all KM processes. Confidentiality in data transmission is highly required in knowledge creation, refining, sharing, and utilization. At the same time, a need to be concerned about the confidentiality of data stored in the database can better support knowledge storing process. Concerns regarding Access Controls (No.2) are a must in all KM processes because in each process the organization should be able to control who has access and authority to perform particular activities to knowledge assets of the organization. Data loss or leakage prevention (No.3) appears to be an issue that needs to be concerned only in knowledge storing process where the organization attempts to preserve knowledge for future use as much as possible. Next, during all KM processes the organization needs to take cyber-attacks (No.4) into consideration since many different types of cyber-attacks could happen at any point either when the users interact with knowledge repository or when knowledge resides within the repository. Another issue, availability and reliability (No.5), is an extreme concern in all KM processes as well. The system must be available and reliable whenever the users need to use it. For example, if the users often cannot retrieve, share, or use existing knowledge, it would cause a bad impression and the users may hesitate to use the system. Moreover, a DoS or DDoS attack can damage any server supporting all these KM processes. Lastly, browser security (No.6) is also another aspect that needs to be considered in nearly all KM processes because the browser is the common tool users use to interact with the system. Since users need to perform all activities through the browser, an unsafe browser can harm users' computers and also frustrate the users. In summary, almost all of different types of security concerns play an important role for all knowledge management processes. Therefore, data security and confidentiality issues, access controls, cyber-attacks, and availability and reliability issues are equally the most critical security concerns for successful cloud-based KMS. The second most critical security concern would be browser security issue which contributes to four KM processes. Even though, data loss or leakage prevention issue which only relates to knowledge storing process still cannot be ignored due to the importance of knowledge repository concerning the secrecy of organizational knowledge.

Table 1: Cloud Computing Security Concerns in Knowledge Management Process

No.	Cloud Computing Security Concerns	Knowledge Management Process				
		Knowledge Creation	**Knowledge Refining**	**Knowledge Storing**	**Knowledge Sharing**	**Knowledge Utilization**
1	Data Security and Confidentiality Issues	/	/	/	/	/
2	Access Controls	/	/	/	/	/
3	Data Loss or Leakage Prevention			/		
4	Cyber-Attacks	/	/	/	/	/
5	Availability and Reliability Issues	/	/	/	/	/
6	Browser Security	/	/		/	/

3.2 Solutions and Recommendations

First of all, the details of how cloud vendors would manage security and legal issues, asset control, data transfer and deletion, business continuity, backups and security policies need to be specified clearly in the service level agreements (SLA). The businesses whenever use cloud vendors' services should apply the ISO/IEC 27002 framework consisting of the three broad categories: organizational infrastructure, technical infrastructure and information protection which need to be specified in the SLA [11]. The organizational infrastructure concerns information system governance procedures, the enterprises' assets, and security policies. The enterprises need to ensure that the vendors provide appropriate level of security to protect their assets and offer proper information system governance procedures and security policies including standards and the guidelines. Technical infrastructure includes access control where vendor must enforce access control policies to protect networks from unauthorized activities and provide secure remote access to data. Systems development and maintenance, communications and operations management, physical and environmental security, and incident management are also parts of technical infrastructure that vendors must have appropriate security controls and procedures written in the SLA. Additionally, information protection concerns human resources security, business continuity management, compliance, and risk management. Vendors need to follow policies and procedures in hiring, provide training to users, and perform risk analysis and risk evaluation. The enterprises must have business continuity plans and independent plans for backups or migration to other cloud providers in case disasters occur.

Technical measures used to improve data security are the protection of data-at-rest on the server, the encryption of data during transfer, and client-side data encryption. Client-side data encryption will not be discussed because it is not attractive to most businesses and not recommended because of several reasons. For example, sharing encrypted data would mean passing down the private symmetric key, which may result in other security problems. Also, if users lose their private key or forget their password, the access cannot be restored by the administrator so this could lead to complete data loss. For server-side encryption, businesses can use third party software or features provided by the OS, such as "BitLocker" or the built-in encryption mechanism of the NTFS file system [12]. Both techniques offer the protection when the attackers access hardware directly or unauthorized users enter the system at OS level. For server-side encryption on the application level, an optional ownCloud extension should be used. The activation of this feature has no functional limitations but only file contents are encrypted, while file names remain readable. However, businesses need to be aware that some information such as a search index may not be encrypted as it still contains plaintext contents.

Another solution is to implement techniques mentioned in [13] which use data masking and data encryption. However, the masking and encryption operations are performed at the organization's server instead of at the client machine or at the cloud server. KM data are stored in a cloud database in a masked or encrypted form providing data confidentiality and privacy while allowing data to be queried.

The protection of data during transfer is also essential because cloud storage service is also accessible via public networks like the Internet which data may be intercepted during transfer. Businesses should use Hypertext Transfer Protocol Secure (HTTPS), which uses Secure Socket Layer (SSL) or Transport Layer Security (TLS) for authentication and encryption of communication. For security reasons, it is recommended to use TLS in version 1.1 or 1.2 in combination with modern browsers while TLS 1.0 and SSL 3.0 should only be applied for compatibility reasons. HTTPS can ensure that the counterpart is in fact the party it is supposed to be and that no one can easily read sensitive data. Furthermore, the prioritization of the system's preferred cipher suites is still recommended. Cipher suites, a standardized set of cryptographic algorithms, comprise algorithms in key exchange, digital signature, hashing functions, and data encryption. Cipher suites are used for different purposes during the communication by SSL/TLS. In general, it is widely advisable to use key exchange protocols based on Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) algorithms, specifically ECDHE preferred concerning performance. Cipher suites based on the fast RSA procedure for key exchange are recommended regarding compatibility. Either RSA or the Elliptic Curve Digital Signature Algorithm (ECDSA) can be adopted in regard to the signature algorithm. The newer SHA-2 algorithms should be applied instead of SHA-1 for hash functions because SHA-1 can no longer provide sufficient protection.

Fine-grained access control (FAC) policies should be enforced in the cloud environment. A FAC protocol which uses additive homomorphic encryption scheme along with proxy re-encryption properties [14] is recommended. This encryption function is secure as a given set of cipher texts and corresponding public key prevent an adversary to retrieve any additional information regarding the plaintext. Moreover, a protocol like Secure Data Sharing (SDS) should be used along this direction. SDS allows the data owner to provide fine-grained access control to users over data outsourced in the cloud service. The data owner can authorize other users to securely access the data at any time. SDS protocol is created using additive homomorphic with proxy re-encryption properties. SDS framework allows secure query processing (SQP) over the encrypted data while the SQP should reveal the query output to the authorized user only. Nothing should be revealed to the cloud or to other adversaries during this process. However, it may incur heavy cost on the end-user as even a few records of data are filtered; the cloud always sends total number of authorized records for decryption. For the organizations which tend to have the dynamic collaboration environment, Secure Dynamic Cloud-based Data sharing (SDCD) is recommended [15]. Once users are added to SDCD, no further interaction with the data owner is required. SDCD effectively enable users to share data entities although the data owner is unavailable. More importantly, SDCD does not re-encrypt data when uploading to the cloud instead users can use the master public key directly. This reduces complexity and improves performance in the cloud during data upload. Nevertheless, in this design permissions to read and write cannot be differentiated and an authorized user either has no restricted access or no access at all.

Federated Identity Management (FIM) System should be used to manage identities by permitting an identity subject to establish links between his/her identities and to be used for a various service across organizational borders [16]. Identity federation refers to establishing a logical link between identities and the federation is a group of organizations establishing trust among them for secure business cooperation. One of the examples of federated identity is the process to repeat user authentication or simply called single sign-on. Single sign-on causes the damage in information leakage if a user identity is compromised. Another issue is FIM systems nowadays still lack of dynamic federation and agile mechanism. Therefore, FIM systems should be properly implemented, monitored, and improved further to mitigate those security risks.

One of the other common solutions is the use of firewall to reduce the attack surface of virtualized servers in cloud computing environments. A bi-directional firewall should be deployed on individual virtual machines to provide centralized management of server firewall policy and should include predefined templates for common enterprise server types [1]. The firewall should enable features such as virtual machine isolation, fine-grained filtering, coverage of all IP-based protocols, coverage of all frame types, prevention of denial of service attacks, ability to design policies per network interface, and location awareness to enable tightened policy. Intrusion detection/prevention system should also be deployed on virtual machines to protect vulnerabilities in operating system and enterprise applications against known and zero-day attacks. Integrity monitoring software should be applied at the virtual machine level to detect malicious and unexpected changes on operating system and application files which potentially compromise cloud computing resources. Finally, log inspection software should be applied at the virtual machine level to collect and analyze operating system and application logs related to security events. These events can be sent to a stand-alone security system or to a centralized logging server for correlation, reporting, and archiving for the maximum benefit.

Security solutions that should be used with each KM process are summarized in Table 2.

Table 2: Security solutions for Knowledge Management Process

No.	Security solutions	Knowledge Management Process				
		Knowledge Creation	**Knowledge Refining**	**Knowledge Storing**	**Knowledge Sharing**	**Knowledge Utilization**
1	ISO/IEC 27002 framework	/	/	/	/	/
2	Data Masking			/		
3	Data Encryption	/	/	/	/	/
4	HTTPS	/	/		/	/
5	FAC Policies	/	/	/	/	/
6	SDS Protocol				/	/
7	Federated Identity Management	/	/	/	/	/
8	Other Common Solutions*	/	/	/	/	/

*Other common solutions include Firewall, Intrusion detection/prevention system, Integrity monitoring software, and Log inspection software.

4. Conclusion

Security issues discussed in this paper are the primary security concerns regarding the adoption of cloud computing for knowledge management systems. By examining the contribution of these issues to each knowledge management process, the most critical issues are data security and confidentiality issues, access controls, cyber-attacks, and availability and reliability issues. The next important issue is browser security. Other issues which however cannot be ignored are data loss and leakage prevention issues. Moreover, major solutions and recommendations are provided in this paper. Several aspects of security issues regarding cloud computing technology exist and more and more issues will be discovered in the future due to technology development. The organization which desire to use cloud computing should realize this matter and continue to maintain up-to-date list of security concerns and countermeasures for the benefit of the organization.

References

1 Lokhande, T.S., Shelke, R.R.: A Review Paper on Cloud Computing Security. IJARCS. 4, 70-73 (2013)

2 Lin, A., Chen, N.C.: Cloud computing as an innovation: Percepetion, attitude, and adoption. IJIM. 32, 533–540 (2012)

3 Ogigau-Neamtiu, F.: Cloud Computing Security Issues. JoDRM. 3, 141-148 (2012)

4 Kumar, A.: World of Cloud Computing & Security. IJ-CLOSER. 1, 53-58 (2012)

5 Sultan, N.: Knowledge management in the age of cloud computing and Web 2.0: Experiencing the power of disruptive innovations. IJIM. 33, 160-165 (2013)

6 Alqahtani, H.S., Sant, P.: Cloud Computing Security Challenges and Threats: A Systematic Map. IJAET. 8, 457-465 (2015)

7 Jamil, D., Zaki, H.: Security Issues in Cloud Computing and Countermeasures. IJEST. 3, 2672-2676 (2011)

8 Singh, J.: Practicing Knowledge Management System. IJIBM. 5, 209-230 (2013)

9 Sampson, D.G., Zervas, P.: Learning object repositories as knowledge management systems. KM&EL. 5, 117–136 (2013)

10 Liao, C.N., Chiha, I.L., Fua, Y.K.: Cloud computing: A conceptual framework for knowledge management system. HSM. 30, 137–143 (2011)

11 Srinivasan, M.: Building a secure enterprise model for cloud computing environment. AIMSJ. 15, 127-133 (2012)

12 Gastermann, B., Stopper, M., Kossik, A., Katalinic, B.: Secure Implementation of an On-Premises Cloud Storage Service for Small and Medium-Sized Enterprises. In: 25th DAAAM International Symposium on Intelligent Manufacturing and Automation. vol. 100, pp. 574-583. Procedia Engineering, Vienna (2015)

13 Kuacharoen, P.: Combination of Data Masking and Data Encryption for Cloud Database, Applied Mechanics and Materials: Computers and Information Processing Technologies I. International Conference on Computers and Information Processing Technologies. vol. 571-572, pp. 617-620. Trans Tech Publications (2014)

14 Samanthula, B.K., Elmehdwi, Y., Howser, G., Madria, S.: A secure data sharing and query processing framework via federation of cloud computing. IS. 48, 196-212 (2015)

15 Piechotta, C., Olsen, M.G., Jensen, A.E., Coleman, J.W., Larsen, P.G.: A secure dynamic collaboration environment in a cloud context. FGCS. 55, 165-175 (2016)

16 Khalil, I.M., Khreishah, A., Azeem, M.: Cloud Computing Security: A Survey. Computers. 3, 1-35 (2014)